

The 2021 Perch MSP Threat Report



PERCH

a  ConnectWise solution

An intro from the CISO

If MSPs were in a boxing match against threat actors, I'd say we've just begun the third round. We're battered, bruised, and trying to keep our feet against a towering and intimidating adversary. The first round was messy, and we found ourselves on the ropes more than once. But we withstood the storm. While we faltered, we dodged the knockout blow as one MSP after another suffered from Buffalo Jumps (a new tactic for ransomware distributors to ransom a service provider and many of their customers at once).

But the second round was ours. We fought back, we held our ground, and we showed why we have the resiliency to be in the fight. While I wouldn't say our adversary is yet fearful or is close to throwing in the towel, I believe we're renewed in our morale with a clear pathway toward victory. MSPs have woken up to the fact that they are in a cyber fight for their lives.

If we pause to think about what the past three years have held for MSPs, it seems as if we've been in an evolution of security moving at light speed. 2018 proved what we all feared: threat actors might finally discover how lucrative an MSP target could be. 2019 was the dark storm. MSPs were relentlessly attacked, and a great many fell. In the Perch 2020 MSP Threat Report, which we wrote in late 2019, all of the predictions we provided came true. Are we security soothsayers? Cyber prophets? Well, no. But also, maybe yes.

We predicted the beginning of data exfiltration as an attachment to ransomware. And it happened. We said ransoms would continue to settle in the six figures for MSPs. We said the cloud would finally get a security makeover. That clearly happened, though no one could predict COVID-19 was the primary driver on that one.

And speaking of COVID-19, as an immigrant to the glass-half-full optimist mindset that we CISOs sorely lack, I believe the pandemic has been a net positive for our industry in ways we could never imagine. Many MSPs have used the pandemic to bring up security conversations they were begging to have with their clients. Cyber budgets actually increased. And our cyber resilience became a net positive and source of strength.

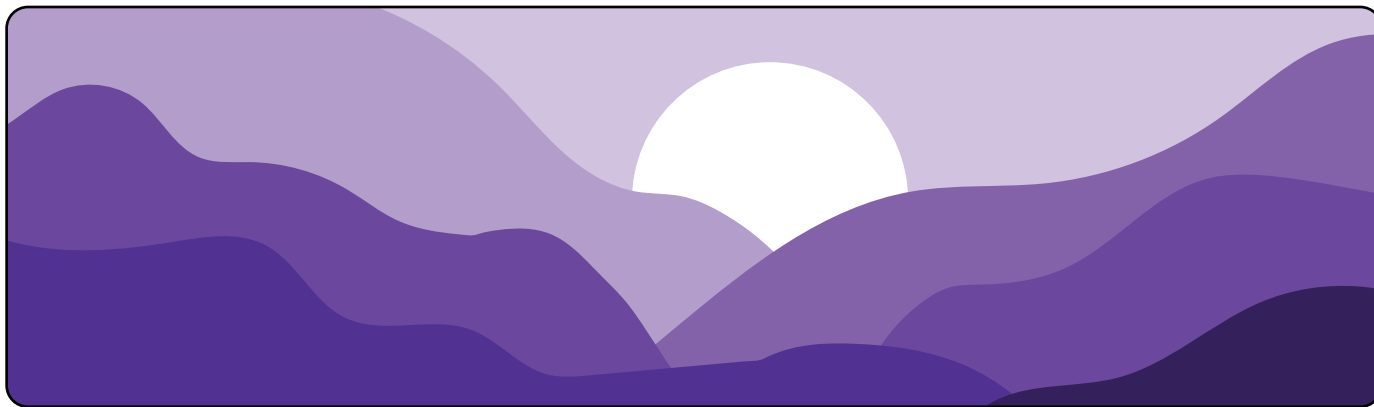
And that is why we won the second round in our bout against an ever-present and dangerous adversary. But that brings us back to the third round. The bell has just rung. What do our futures hold? What new tactics will our adversary try? How will outside influences like cyber insurance, impending regulation, and client tolerance for cybersecurity impact us? Time will tell.

The third round has begun. And it's time to roll with the punches and stand our ground yet again.



Wes Spencer

CISO, Perch Security



Wake up

Why is the world on fire with security incidents? Here's one clear reason: the security industry is focused on securing the largest enterprises, even though 99.7% of companies have fewer than 500 employees.

Perch was created to enable service providers to secure SMBs with the same defenses the most well-resourced and largest enterprises enjoy. We're turning on the fire hose by informing service providers about security risks and enabling them with the high-functioning capabilities they need.

In 2020, we published the security industry's first and only threat report for Managed Service Providers (MSPs). We realized the need for an MSP-focused threat report for a few reasons:

- **MSP are valuable targets: they're the gateway to the networks and hosts of the organizations they manage.**
- **Hackers have realized the value of MSPs and their herds of customers. Why hack one business when you can go after many in one fell swoop?**
- **Attackers understand MSP tools. They know how to exploit the vulnerabilities and legitimate uses of the tools MSPs depend on.**

Our predictions from the 2020 MSP Threat Report came true with uncanny accuracy. Everything we said would happen actually happened, and that's something we find pretty depressing.

So, what did we see?

- **Continued buffalo jumps**
- **Ransomware data exfiltration**
- **Ransomware moved to the cloud**

We prepared you for 2020, and we're back with a fresh report for 2021. This report, the 2021 Perch MSP Threat Report, includes an analysis of major MSP-related security events and trends from 2020 and our top predictions for 2021 with contributions from MSPs, partners, and security experts.

The MSP Threat Report is just one way Perch helps secure communities and put out the raging fire. We're focused on bringing world-class threat detection and real-time threat sharing to MSPs to solve small- and medium-sized businesses' security challenges.

The burden of responsibility makes it dangerous to go alone. Take Perch with you.

Let's get this party started!

Table of contents

An intro from the CISO	2	What to look out for	13	Predictions from the CISO	19
Wake up	3	MSP Tool Exploits	13	Sources	21
		Password Reuse / Weak Passwords / Password Spraying	14		
		Monitoring Remote Workers	15		
MSPs are valuable targets	5	Survey results	16		
Built for use	6	Threat landscape	17		
Cat herding	6				
Resource constraints	6	REvil (aka Pinchy Spider) - Sodinokibi	17		
		??? - Mespinoza aka Pysa	17		
Timeline	7	Wizard Spider - Ryuk/Conti	17		
		ENRAGED DUCK	17		
Q1 & Q2	7	Dharma	18		
Q3 & Q4	8	Dark Halo (UNC2452)	18		
		FIN6 TA2101 Twisted Spider - Maze	18		
MSPs are waking up	9				
The 3 MSP personas	9				
Recommendations for the herd	11				
Thoughts from Jason Slagle	12				

MSPs are valuable targets

In last year's report, we warned that MSPs would be targets due to their collective value.

Why are they so valuable?

When they're attacked, we call this a Buffalo Jump - essentially, it's a supply chain attack that leverages scale.

MSPs hold the keys to dozens - if not hundreds - of organizations, each with even more employees to boot. Hackers already know the software MSPs use to manage their clients well, making

them the perfect distribution method that's just ripe for the taking.

We profiled a successful MSP with 100 employees, \$10,000,000 in annual revenue, and 53 fully managed organizations with an average of 600 employees each.

In total, the MSP is managing approximately 32,000 users.

In economics, we measure how much revenue the average person contributes to the economy as the Gross Domestic Product (GDP). For the United States, the GDP per

capita is \$65,000.

Now, let's have the MSP in the example above represent an enterprise organization that employs 32,000 people that, on average, generate \$65,000 in value for the United States.

Collectively, that's about \$2,000,000,000 (yeah, that's 2 billion) in value. How does this compare to other companies with similar user counts to secure?

Company	Managed Users	Estimated Revenue
VMware	20,000	9 Billion
3M	36,000	32 Billion
Cisco	37,000	51 Billion

Large enterprises might be Big Game, but MSPs are valuable because they control the Big Herd.

Even though MSPs and very large enterprises face many of the same challenges, it's often more difficult for the MSP to secure their herd for several reasons:

- **Enterprise-grade security solutions are rarely built for use for MSPs**
- **MSPs represent a large number of companies, each with its own appetite for risk**
- **MSPs are heavily targeted but have fewer resources to deal with the problem**

Let's take a deeper look at those.



Built for use

The security industry has historically been focused on securing enterprise companies while ignoring small and medium-sized businesses (SMBs).

According to the most recent Census Bureau's Statistics of U.S. Businesses, 84.9% of C corporations have less than twenty employees, 96.4% have less than 100, and 99.0% have less than 500. Because security controls aren't built for use by MSPs, it makes the job harder.

MSPs need software that performs differently because they are managing multiple organizations. MSPs need tools that are multi-tenant that integrate with the existing software ecosystem. That isn't something typically available in many enterprise-focused tools.



Cat herding

MSPs have a diverse set of client organizations to support. Each managed company has its own priorities, compliance requirements, and risk tolerance. Educating clients about security and convincing them to pay for more security can lead to some challenging conversations (if you haven't had the security Birds and Bees talk with your clients yet, you should).

Additionally, some clients will have existing security controls that MSPs have to support or manage. The diversity of products that aren't built for use by MSPs make the overall job harder.

With dozens of clients, it can be like herding cats to keep everyone safe.



Resource constraints

Some MSPs don't know they are valuable targets, but others have realized this. Either way, MSPs have limited security resources compared to similarly-sized enterprises. Additionally, the organizations that MSPs manage are typically small and medium businesses with their own resource constraints.

These resource constraints make targeting SMBs all the more valuable for hackers, and MSPs are the shiny gateway to a whole bunch of them.

Timeline

Q1

Jan. Sodinokibi



Colorado-based Complete Technology Solutions was hit, disrupting operations for more than 100 dentistry practices.⁴

Jan. Sodinokibi



A server run by LogicalNet was compromised by hackers, resulting in a Buffalo Jump that impacted its clients - including Albany International Airport, who ultimately paid a ransom to regain access to its computers.⁵

Jan. Selling Access



Cyber-criminals were found selling access to sensitive databases and email access to various corporate environments as well as access to point-of-sale terminals.⁶

Jan. Vulnerability



A vulnerability found in ConnectWise Control would allow cyber-criminals the ability to hijack an MSP's systems as well as client machines.⁷

Jan. Sodinokibi



An MSP out of California, Synoptek, fell victim to a Buffalo Jump that impacted its clients. The company reportedly paid a ransom to restore operations.⁸

Jan. Vulnerability



A zero-day vulnerability in SolarWinds N-central would allow an unauthenticated user to register agents and dump customer configurations that contained active directory credentials.⁹

Feb. Insider Threat



A team of security professionals from Huntress, Datto, and ConnectWise helped federal agents track down a systems engineer at an MSP attempting to sell access to their employer.¹⁰

Q2

Apr. Maze



Cognizant, a large IT services provider, publically announced on April 18 that they were the victim of a Maze ransomware attack.¹¹

Apr. Maze



Dakota Carrier Network (DCN), a group of 14 independent broadband companies, was hit by Maze, who published some administrative data on the internet.¹²

June Maze



Collabera was infiltrated by hackers who stole employee personal information and infected systems with ransomware. They were able to successfully restore access from backup files.¹³

June Enraged Duck



ConnectWise disclosed a vulnerability in ConnectWise Automate that could allow a remote authenticated user to exploit a specific Automate API and execute commands and/or modifications within an individual Automate instance.¹⁴

June Maze



Conduent, an IT service provider with clients in healthcare and banking, fell victim to a Maze ransomware attack that impacted its European operations.¹⁵



= Buffalo Jump



= Selling Access



= Vulnerability



= Failed Attack



= Ransomware



= Warning

Timeline

Q3

July Unknown



Managed services provider Pivot Technology Solutions fell victim to a ransomware attack that resulted in some stolen sensitive data, but no encrypted systems.¹⁶

July Nefilim



Orange Business Services suffered a ransomware attack, with the Nefilim hackers gaining access to data from 20 customers.¹⁷

July Unknown



Xchanging, a subsidiary of DXC Technology and an MSP for the insurance industry, announced that they were victims of a ransomware attack that impacted clients.¹⁸

July Warning



In a security alert, Secret Service officials said their investigations team (GIOC -- Global Investigations Operations Center) has been seeing an increase in incidents where hackers breach MSP solutions and use them as a springboard into the networks of their clients.¹⁹

Q4

Oct. Ryuk/Conti



Sopra Steria, a French IT services company, had its data stolen and database locked during a Ryuk ransomware attack. After identifying the attack, the company implemented security measures to contain it.²⁰

Nov. Sodinokibi



Managed web hosting provider [Managed.com](#) was forced to take their entire system down during a Sodinokibi/REvil ransomware attack.²¹

Nov. APT29 aka Cozy Bear



SolarWinds announced that their SolarWinds Orion business software was trojaned with malware referred to as SunBurst, impacting thousands of organizations around the world.²²



= Buffalo Jump



= Selling Access



= Vulnerability



= Failed Attack



= Ransomware



= Warning

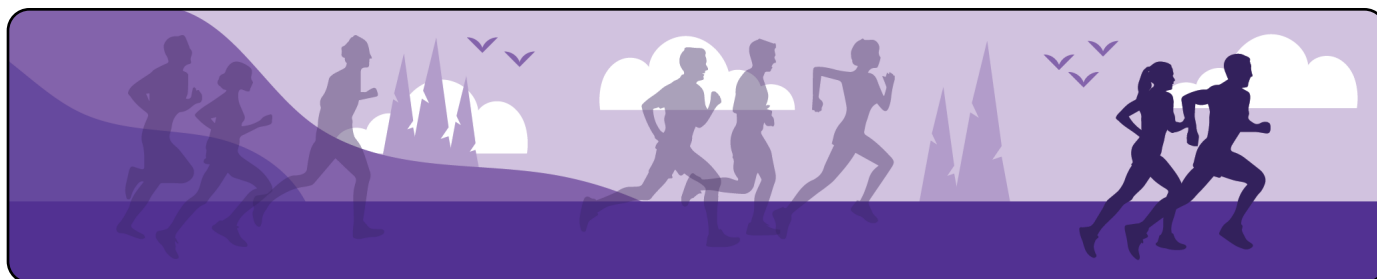
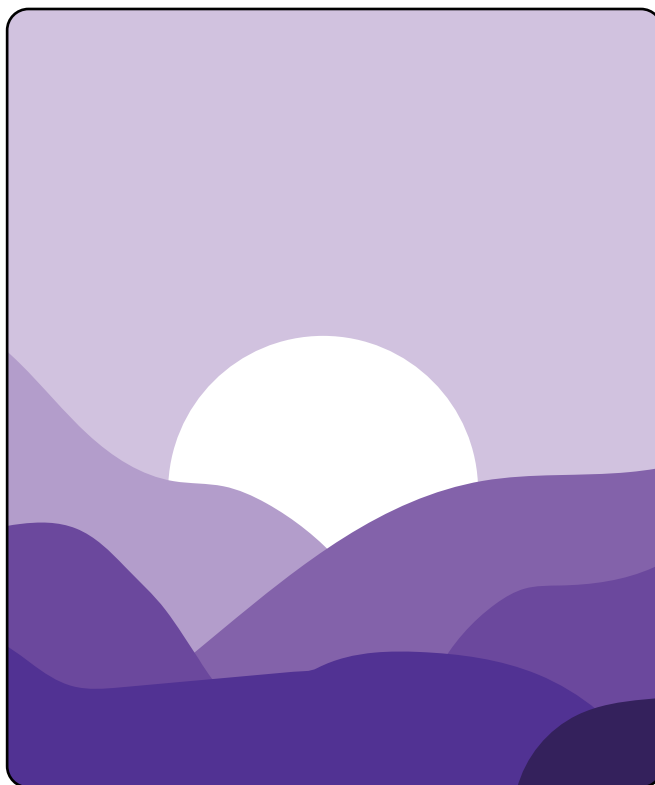
MSPs are waking up

While buffalo jumping MSPs was a new concept for the last report, MSPs have started to wake up to their ever-growing risk.

The 3 MSP personas

As part of this year's annual report, we sent out a survey to MSPs asking about their security journey. When looking at their confidence in their security posture and their ability to handle threats, we saw three distinct personas emerge from the herd.

Here's some of what they say.



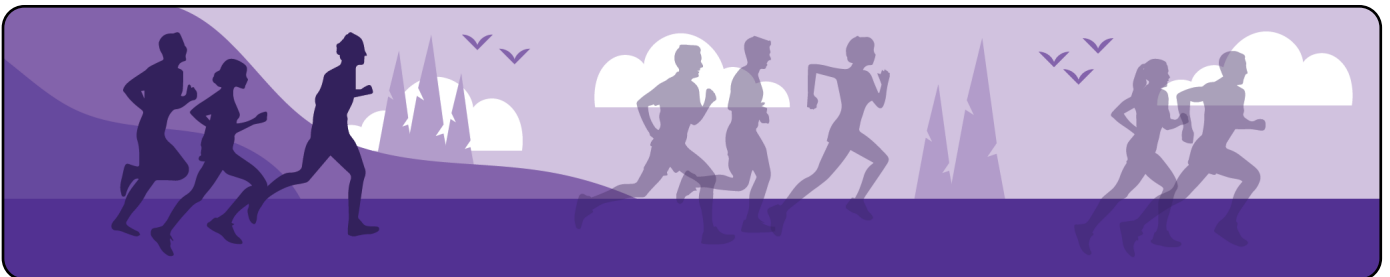
Front Runners

- “We’ve had a strong focus on security. We put a lot of energy into staying on top of things. Cautious and wary. It will never end.”
- “We are probably in the top 10% of MSPs with security, but there is always room to improve. We are ready to help our clients respond to security incidents, but we are always looking at new ways to protect us and our clients. We regularly verify that our tools, processes, and policies are the best we can do. We have a good grasp of the threat landscape, enough to know we need to constantly evaluate, change, upgrade and move with the landscape to be safe.”
- “We support other MSPs and help SMBs that do not have the minimum security resources to have good cybersecurity hygiene. We are constantly learning too. We are always looking to improve our internal security.”
- “[Jump] in with two feet. Utmost importance!”



Trying To Keep Up

- “It keeps me up at night! We know we’re a valuable target, and it’s not easy. We realize there is a problem.”
- “We’re early in the process, but we have a plan for our security practice, products, services. but we’re not there yet.”
- “We are adopting a security-first approach, but we don’t have the skills and bandwidth to address the threat landscape. We have started dedicating resources and staff to security. We are still very reactive.”
- “We are better than in the past, but we continually find gaps and ways to improve.”
- “We haven’t gone through a real-world test, but our exercises have gone OK.”
- “We are constantly challenged and changing internal processes to address the threats we see.”
- “The threats out there are ever-evolving and concerning.”
- “Admit you have a problem.”



Lagging Behind

- “Ignorance is bliss, but we’re concerned because it’s a crazy world.”
- “We’re having trouble educating leadership about our blind spots and making changes to keep our customers secure. We’re understaffed and underskilled in security, and there is an insufficient budget for security. We’re uncomfortable with the threat landscape. It’s a big unknown for us.”
- “Clients aren’t adopting the security they need. They only care about security after an incident. That makes it hard to be proactive and competitive. Security is expensive, and the solutions are very fragmented. It’s hard to know the best way forward.”
- “It’s a challenge to stay on top of the threats and educate our clients about the seriousness of the issues.”

Why are MSPs challenged by being a target?

“Time, money, and maybe the lack of at least one person in the organization willing to learn and push the agenda.”

- Jesse Connor

Chief Business Development Officer, Simplefusion

“MSPs run on a model of economies of scale and keeping margins down via automations and tools. A lot of the security things presently don’t have enough tooling here to allow those economies of scale to hold up. This results in struggles for the MSPs.”

- Jason Slagle

VP of Technology, CNWR, Inc.

Recommendations for the herd

As a community, we have the responsibility to help everyone along their cybersecurity journey. If not, attackers will keep pursuing those lagging behind.

- **Valuable Target** - Recognizing you’re a valuable target is step one. After that, you need to jump in with both feet.
- **Community** - Without staff and training, threats will keep you up at night. You can lean on trusted partners and peers to better understand threats.
- **Growth** - Security can grow your bottom line – it doesn’t have to be a drain on your business.
- **Educating Customers** - Educating customers on the value of security can be challenging. The front runners in secure MSPs are being more assertive with customers and bundling security into all packages.
- **Educating Leadership** - An organization can’t change without top-down support. Leadership needs to realize the organization is a valuable target and the risks from current gaps.
- **Budget** - Educating leadership on the gaps and risks is necessary to get an increased security budget. Perform a self-assessment to show gaps.
- **Staffing** - Tools aren’t enough. You must reserve human capacity to operate and interact with security solutions. If you have the resources to hire and train dedicated security resources, great. If you need help with security, look for managed security services.
- **Tool sprawl** - Try to find security controls that can work well together and with your current ticketing systems.

We asked Jason Slagle, VP of Technology at CNWR, Inc., his thoughts on what 2021 brings for MSPs.

Are MSPs prepared for these trends in 2021?

“The MSPs that aren’t taking security seriously will find themselves getting attacked and essentially forced out of business.”

What can they do to fortify in 2021?

“Security is an onion. Also, be on the lookout for things that can complement your stack.”

Should MSPs mandate and bundle security into their plans or offer security a la carte?

“For sure, there should be a base level you can’t give on. We’re bundling almost everything in almost every case now. I believe that is the way forward. Otherwise, customers will drop things to save a buck then blame you for not forcing their hand when they get burned.”

What should they be bundling into basic packages?

“Network-level defense that’s more than just a firewall. SOC/SIEM is nice and quickly becoming a must-have. Other XDR/MDR/EDR tools layered add a good amount of extra protection for not a lot of overhead or cost.”

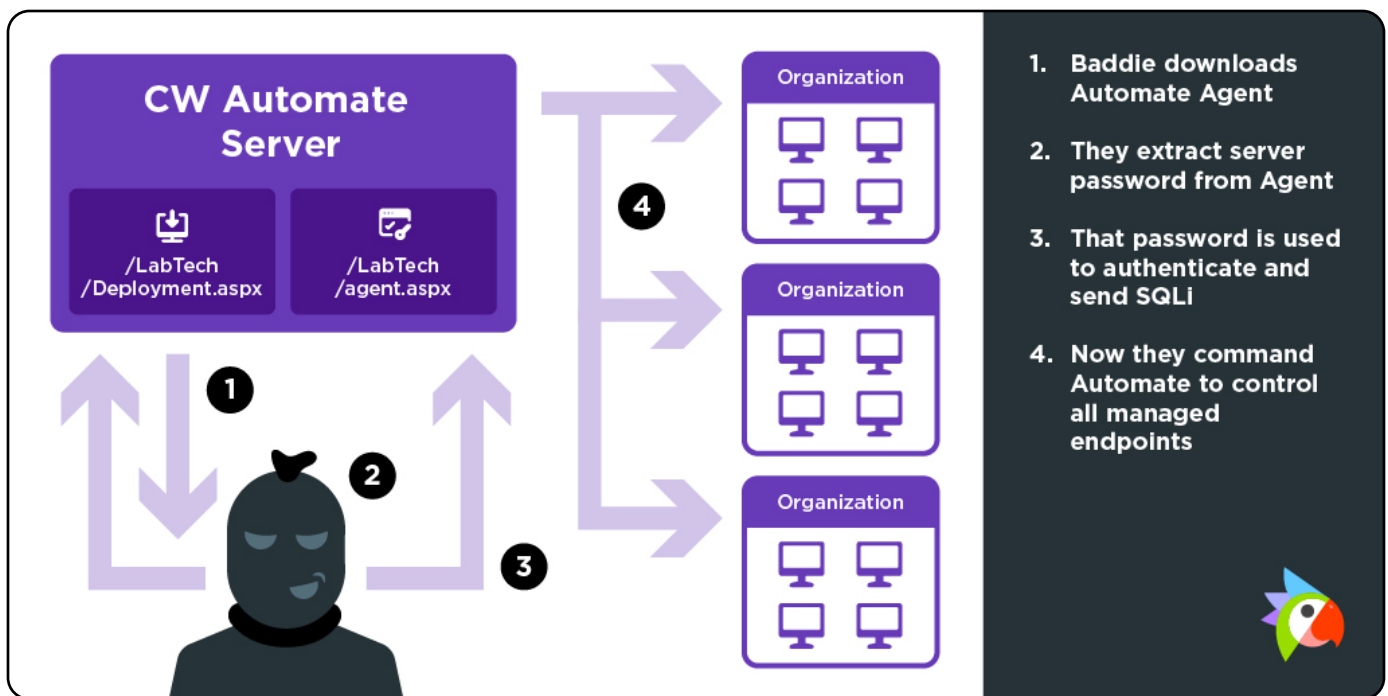
What to look out for

MSP Tool Exploits

ConnectWise Automate

For 2020, we warned about application exploits targeting the software MSPs use. We also warned it would be used in Buffalo Jumps by herd-hunting hackers.

On June 10th, 2020, a command execution vulnerability in ConnectWise Automate was disclosed by ConnectWise. The vulnerability was discovered by Syswarden.³



Perch was the first security company on the scene to discover multiple campaigns targeting MSPs before and after the vulnerability was disclosed.

Perch observed three active campaigns: one actor from Russia, one actor leveraging Private Internet Access (VPN), and a small amount of scanning activity using AWS infrastructure indicating a third.

When attackers were successful, they leveraged their ConnectWise Automate control to perform Buffalo Jumps.

Because of the active campaign and no CVE to track the vulnerability details, Perch sought CVE registration for the vulnerability, but gave attribution to Syswarden.

SolarWinds N-central

ConnectWise Automate wasn't alone last year. On January 21, 2020, Packet Storm released information on a zero-day vulnerability in SolarWinds N-central, another RMM tool used by MSPs.

The vulnerability would allow unauthenticated users to perform privileged tasks such as register new agents or dump configuration information, including cleartext Active Directory credentials.⁹

What security threat trends are you worried about for 2021?

"A lot of trust is placed in the software vendors MSPs use. The problem is there is no way for us to know what software development looks like at these vendors we trust. Simply throwing software into the mix without understanding it, auditing it, learning it, and picking it apart can just end up with you introducing more vulnerabilities...It happens to both small and large firms.

Some of this has become apparent with the recent SolarWinds issue, but I do not think people realize how vast this problem can be."

- Jesse Connor
Chief Business Development
Officer, Simplefusion

Password Reuse / Weak Passwords / Password Spraying

Over and over again, passwords are the weak link. We do like to blame interns with poor passwords, but ultimately the failure is in the systems. Training for users is important, especially around password reuse. But we should be able to architect more secure systems.

Implement multi-factor authentication where possible. Or, consider using security keys. Where possible, do not use passwords. SSH should always be with a password-protected key. Use Single-Sign-On where possible.

Where you must use passwords, create processes to audit systems for weak passwords and commonly used passwords.

"Tackle the simple things like MFA, passwords, and training."

- Jesse Connor
Chief Business Development
Officer, Simplefusion

Monitoring Remote Workers

We can't talk about MSP security threats in 2020 without mentioning the elephant in the room: COVID-19.

Last year, MSPs moved at lightspeed to support businesses moving from traditional working arrangements to just about everyone working from the comfort of their own home.

Even though remote work was seen as a temporary solution to a (hopefully) temporary problem, we believe that it's here to stay.

Businesses quickly found out that their employees still work effectively and maintain productivity, even when not in the office. No industry that can work from home has seen a decrease in productivity. Some industries have even seen increased productivity. Additionally, many businesses cut office expenses and realized savings.^{1, 2}

Workers benefit from shorter commute times, are moving to cheaper housing markets, and now can work in pajamas from the waist down.

That isn't to say that there aren't drawbacks to work-from-home for both employees and businesses, but a large portion of both are inclined to continue the new status quo.

And so, work from home is likely here to stay. What does that mean for MSPs and cybersecurity?

Remember those temporary changes you made to support the move? They're no longer temporary. Make sure they're secure.



Another thing to think about is that some security solutions lost visibility and effectiveness during the work-from-home pivot. If you haven't already, you should evaluate each security solution in use to understand how users working from home impact its operation.

- **Review the effectiveness of your security controls in terms of where employees work for your MSP and for your customers**
- **Identify controls that are no longer effective**
- **Determine an alternate deployment architecture or control to cover the risk**

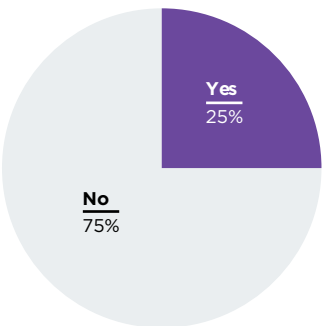
Because of this shift, legacy security controls that effectively cover many employees at a physical location are getting deprioritized. We recommend security solutions that operate as software and report to the cloud to help secure employees at home. That way, users have the best threat detection regardless of where they take corporate assets.

Survey results

As part of the MSP Threat Report, we surveyed MSPs to collect direct feedback for use in the report. All numbers are from the last twelve months. We've focused on some of the most interesting tidbits to share with you.

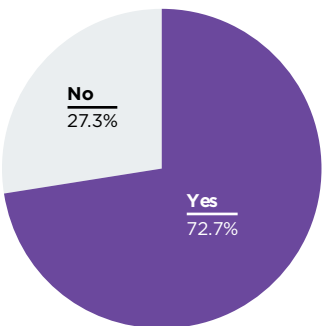
In a bit of good news, only 25% of MSPs who suffered a security incident reported that it was related to ransomware.

If your MSP experienced a security incident, was it related to ransomware?



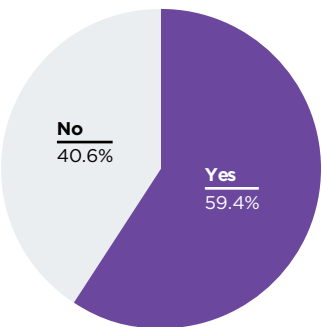
However, nearly 73% of MSPs reported that at least one client had a security incident.

Have any of your clients had a security incident in the last 12 months?



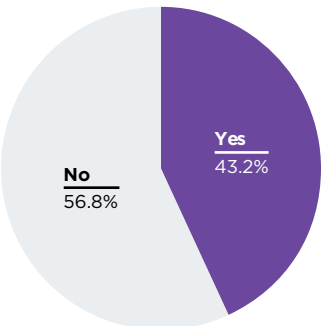
We found that nearly 60% of MSP client incidents were related to ransomware. Ransomware actors are targeting SMBs because they are perceived as easy targets.

Did the client incident involve ransomware?



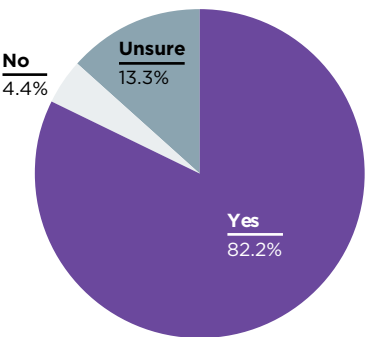
We're always on the lookout for potential buffalo jumps. We collected these survey results before FireEye announced the SolarWinds breach - we imagine this number would be higher now.

Have any of your service providers reported a security incident to you in the last 12 months?



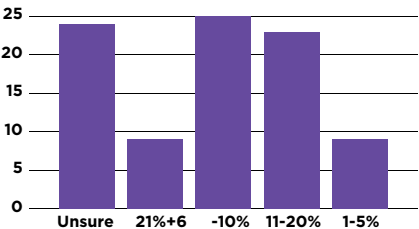
In a sign that many MSPs are closing the gaps in security, over 82% of MSPs surveyed indicated that the portion of their budget reserved for cybersecurity increased in 2020.

Did the percentage of your security budget increase from 2019?



And this year, MSPs are gearing up for even more security spending, with 75% of respondents indicating that their spending would increase on average 12.1%.

What percentage will your security budget increase in 2021?



Threat landscape



REvil (aka Pinchy Spider) - Sodinokibi

- First observed in January 2018, GandCrab ransomware quickly established a RaaS operation with a dedicated set of affiliates. PINCHY SPIDER joined the growing trend of big game hunting
- GandCrab claimed to retire, but released Sodinokibi
- Sodinokibi has shifted to buffalo jumping and now threatens to leak data
- PINCHY SPIDER sells access to Sodin with a 60-40 split in profits (60 percent to the customer), as is common among eCrime actors, but PINCHY SPIDER is also willing to negotiate up to a 70-30 split for “sophisticated” customers



Wizard Spider - Ryuk/Conti

- Ryuk ransomware was originally attributed to North Korea because of similarities to Hermes ransomware, however it was later attributed to WIZARD SPIDER
- WIZARD SPIDER is the Russia-based operator of the TrickBot banking malware, previously focusing on wire fraud. With Ryuk, they leverage TrickBot to ransom the organization for big game hunting
- Ryuk is now retired, but has been replaced by Conti Ransomware. With Conti, WIZARD SPIDER now leaks exfiltrated data to hold as part of the ransom. Additionally, Conti has been seen in numerous ransomware incidents involving MSPs



??? - Mespinsa aka Pysa

- Pysa is a ransomware that encrypts files using asymmetric encryption, adding .pysa as a file extension
- According to Dissecting Malware, the extension “pysa” is probably derived from the Zanzibari Coin with the same name



ENRAGED DUCK

- ENRAGED DUCK was first spotted by Perch Security after the disclosure of a ConnectWise Automate vulnerability
- They use Private Internet Access (a VPN) to scan for targets
- They’re familiar with the tools MSPs love to use the most: their RMMs



Dharma

- According to MalwareBytes, the Dharma Ransomware family is installed manually by attackers hacking into computers over Remote Desktop Protocol Services (RDP)
- The attackers will scan the internet for computers running RDP, usually on TCP port 3389, and then attempt to brute force the password for the computer
- Once they gain access to the computer, they'll install the ransomware and let it encrypt the computer. If the attackers are able to encrypt other computers on the network, they'll attempt to do so as well



Dark Halo (UNC2452)

- Reporting around activity related to the SolarWinds supply chain injection has grown quickly since initial disclosure on 13 December 2020
- A significant amount of press reporting has focused on the identification of the actor(s) involved, victim organizations, possible campaign timeline, and potential impact
- The US Government and cyber community have also provided detailed information on how the campaign was likely conducted and some of the malware used. MITRE's ATT&CK team — with the assistance of contributors — has been mapping techniques used by the actor group, referred to as UNC2452/Dark Halo by FireEye and Volexity respectively, as well as SUNBURST and TEARDROP malware



FIN6 TA2101 Twisted Spider - Maze

- First observed in May 2019, the group gained notoriety in November 2019 with their brazen attitude toward victims and their willingness to speak with security researchers as they began using big game hunting, with a 2020 move to buffalo jumping
- Proofpoint researchers detected campaigns from a threat actor, tracked as TA2101, targeting organizations with malicious emails to install backdoor malware. The actor impersonated a trustworthy and familiar organization with lookalike domains, verbiage, and stolen branding in the emails
- The actor chose Cobalt Strike, a commercially licensed software tool that is generally used for penetration testing and emulates the type of backdoor framework used by Metasploit, a similar penetration testing tool
- The group is capable of moving laterally and exfiltrating data for extortion. It is likely that Twisted Spider targets victims opportunistically and does not focus on specific sectors
- According to CrowdStrike, they likely operate not only the now shutdown Maze, but also Egregor. Egregor is the ransomware to watch out for in 2021²³

Predictions from the CISO

Last year, we made some predictions. We consulted the CISO's crystal ball. Or was it his Magic 8-Ball? Either way, it ended up a foreboding and unfortunate prediction of the future. Even more so when you consider we wrote our predictions way back in 2019. So let's see what's in store for 2021.



1. The era of regulation has come

Enough is enough. That's what I hear from the insurance carriers anyway. We've seen many carriers choose to close out policies with breached MSPs. Some are even not renewing policies for MSPs across the board. Buffalo Jumps and their subsequent damages have caused insurance carriers to realize they may have bitten off far more than they can chew with regards to MSPs' cyber policies. We predict that cyber insurance carriers will continue to demand better cybersecurity maturity for any MSP wishing to obtain coverage. For a similar history lesson, take a peek at the genesis of PCI-DSS.

Additionally, we're beginning to see the attention of state governments drawing their eye to the MSP. Louisiana's state government now requires MSPs that manage IT for the state's public bodies to register with the date. Other states will follow suit. We may additionally see the federal government follow in similar movements, though it is too early to say exactly which agency might make a move and when.

Regardless, opportunity is here for MSPs. Whether driven by the government or insurance carriers, we predict that new regulations or compliance minimums are on the way. MSPs still have a voice in this discussion. That voice needs to be used quickly before others outside our industry dictate the future for us.

2. Attackers will exploit your lack of visibility or understanding across multiple programs

The cloud is the future. It's here to stay. Threat actors are keenly aware of our reliance upon the cloud while also banking on the fact that it's a source of poor visibility for us. That's a scary combination. Criminals will continue to focus on cloud-based attacks, leveraging credential theft, exploiting misconfigurations, and leveraging API-based attack vectors to sink their dirty hands into our precious data in the cloud.

And what might be the result of that? Ransomware doesn't always have to be encryption. Recall our prediction from last year that data exfiltration and subsequent ransom demands over that data would become the norm. And it did. That's because the data itself is as valuable as anything for you and your clients. We predict that cloud-based attacks will result in data-hostage scenarios where criminals will demand a ransom to not leak that data. That's pretty scary.

Predictions from the CISO

3. Cyber extortion will vastly increase costs of a breach and time to recover

In an interview with my friend and colleague Chris Loehr from Solis Security, a new prediction came to mind that I wanted to share. In last year's report, we predicted that cyber extortion will become the norm.

Loehr confirmed this, saying: "Not only has that become true, but it's going to create all sorts of new challenges that many MSPs are unprepared for. In the olden days, a ransomware incident was as simple as paying or not paying a ransom and moving into recovery. But not today."

Loehr is correct, as usual (but please don't tell him I said that). Today, things are completely different with cyber extortion. State and federal privacy laws will compound the complexity in several ways. First, digital forensics costs will skyrocket in a ransomware breach due to privacy laws demanding additional research. The questions of when the attack first occurred, how much data was obtained, how it was obtained, and more must all be answered. Every one of those questions requires answers from skilled, credentialed digital forensics experts.

Loehr indicated that cyber breach costs will continue to rise due the increased requirements of digital forensic investigations. "And not only that," Loehr said, "the time to recovery is going to take much longer as well. I don't think many MSPs are prepared for the increased time it takes to fully recover from a breach as well." Once again, I believe Loehr is correct.



Sources

1. <https://www.shrm.org/hr-today/news/hr-news/pages/study-productivity-shift-remote-work-covid-coronavirus.aspx>
2. <https://www.oecd.org/coronavirus/policy-responses/productivity-gains-from-teleworking-in-the-post-covid-19-era-a5d52e99/>
3. <https://syswarden.com/blog/connectwise-automate-vulnerability-send-trending-sqli>
4. <https://krebsonsecurity.com/tag/complete-technology-solutions-ransomware/>
5. <https://dailygazette.com/2020/01/10/albany-airport-pays-hackers-ransom-regains-data-from-computers/>
6. <https://www.sentinelone.com/blog/evil-markets-selling-access-to-breached-msps-to-low-level-criminals-2/>
7. <https://blog.huntresslabs.com/validating-the-bishop-fox-findings-in-connectwise-control-9155eec36a34>
8. <https://www.jmaddington.com/2020/01/another-it-provider-hacked/>
9. <https://blog.huntresslabs.com/validating-the-solarwinds-n-central-dumpster-diver-vulnerability-5e3a045982e5>
10. <https://www.crn.com/news/security/-i-m-selling-access-to-an-msp-how-three-vendors-teamed-to-foil-hacking-plot>
11. <https://www.crn.com.au/news/cognizant-breach-10-things-to-know-about-maze-ransomware-attacks-546951>
12. <https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/maze-hits-dcn/>
13. <https://www.theregister.com/2020/07/14/collabera-ransomware/>
14. <https://www.securitynewspaper.com/2020/06/22/partners-of-connectwise-cybersecurity-firm-were-infected-by-ransomware-viruses-due-to-company-software/>
15. <https://www.cyberscoop.com/conduent-maze-ransomware/>
16. <https://www.bleepingcomputer.com/news/security/canadian-msp-discloses-data-breach-failed-ransomware-attack/>
17. <https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/orange-business-services-report/>
18. <https://www.bleepingcomputer.com/news/security/ransomware-attack-on-insurance-msp-xchanging-affects-clients/>
19. <https://www.zdnet.com/article/us-secret-service-reports-an-increase-in-hacked-managed-service-providers-msps/>
20. <https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/ryuk-ransomware-attack-could-cost-french-it-services-firm-nearly-60m/>
21. <https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/>
22. <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
23. <https://adversary.crowdstrike.com/adversary/twisted-spider/>