Executive Summary

2022 MSP Threat Report

CONNECTWISE

Cyberattacks have become more focused on MSPs for at least two reasons: First, attacks on mid-size businesses attract less government attention, and second, attacking MSPs creates the lucrative potential to ransom several of their clients at once. Considering these developments, MSPs need business-specific information to proactively protect their business and customers.

This report was created by the ConnectWise Cyber Research Unit (CRU) team. They hunt threats, identify new vulnerabilities, and perform research, ultimately sharing their results with the entire IT community. The most recent developments are documented below, covering significant cyberthreat events in 2021, continuing trends, predictions about the future of cybersecurity, and action items for MSPs.

MSP-Focused Hacks of 2021 Timeline

The threat landscape for MSPs drastically changed in 2021. Worldwide law enforcement drove a significant increase in taking down various cybercrime groups responsible for high-profile attacks (e.g., Colonial Pipeline) and recovering money. This led to a shift in priorities for attackers. Some groups disappeared, but others regrouped and changed their focus to more vicious attacks on mid-sized businesses. Key observations from the timeline of attacks and government actions in 2021 include:

- Government agencies worldwide increase their efforts to take down major cybercrime groups, showing that everyone must do their part to protect the industry, from individuals to global law enforcement.
- The average ransom increases, with some companies receiving demands for up to $50 million.
- The US government steps up its role in cybersecurity, including announcing sanctions, declaring cyberattacks an act of terrorism, and forming a new ransomware task force.
- Large enterprises—Colonial Pipeline and JBS Foods—are forced to shut down partially or fully after suffering ransomware attacks, resulting in substantial monetary losses and other issues.
- Large enterprises partner with the US federal government to create the Joint Cyber Defense Collaborative to combat ransomware.
- REvil disappears then reappears with new victims posted; the group shares that its spokesperson “disappeared without a trace.”
- Late-year predictions say over 700 million ransom attacks will happen by the end of 2021.

  At least two large players acknowledge the shift of bad actors targeting MSPs and other IT solution providers (ITPS) specifically.

Take a closer look at significant cyberthreat events in 2021, continuing trends, predictions about the future of cybersecurity, and action items for MSPs.

[Read the full report]

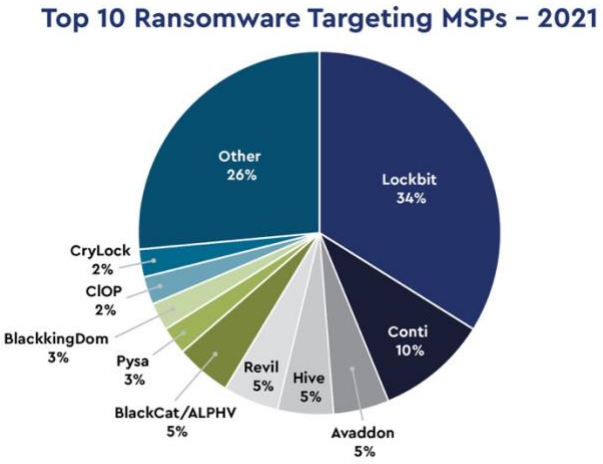
Executive Summary

2022 MSP Threat Report

CONNECTWISE

2021 Top Threat Actor Profiles

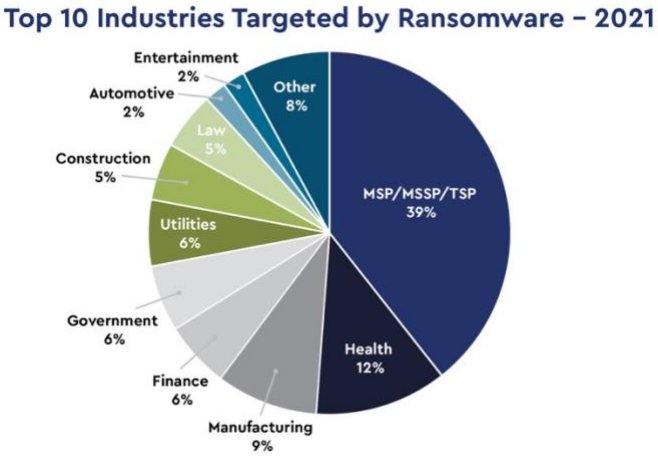
Several ransomware groups now see MSPs are prime targets. The CRU gathered information on the top five ransomware groups that are targeting MSPs and their clients. They mapped each group's tactics, techniques, and procedures (TTPs) to the **MITRE ATT&CK® framework**, a data-driven knowledge base currently used by threat actors. It is a handy tool that provides a common language to describe how threat actors operate. MITRE has also defined common mitigation techniques that defenders can use and mapped these mitigations to each ATT&CK technique and sub-technique. The maps appear in the full report.



Notable Findings

The data suggests that MSPs are in the spotlight more than ever. Throughout 2021, the CRU collected data for 500 cybersecurity incidents from ConnectWise MSP partners and their clients. Of those 500 incidents, 40% were related to ransomware, 25% were directly related to Exchange vulnerabilities, and 10% were coin miners with some overlap. Most incidents occurred in Q1 and Q3.

There was a significant increase in ransomware incidents targeting MSPs in the second half of 2021, with 72% of all ransomware incidents directly targeting MSPs occurring in the second half of 2021. For the purposes of this report, we recorded the mass ransomware attacks that happened during the July 2 Kaseya incident as a single incident. This attack targeted at least 40 MSPs and over 1500 of those MSPs' clients, putting MSPs in the spotlight for threat actors, researchers, and government officials alike.



Executive Summary

2022 MSP Threat Report

CONNECTWISE

2022 Predictions from the CRU

As ransomware continues to escalate in severity, cost, and volume, the pressure will continue to mount. Ransomware attacks in Q3 2021 surpassed those of Q1 and Q2 combined, and we expect that trend to continue. Government efforts to find and prosecute cybercriminals will continue, but the changes won't be swift. So, we predict that more critical infrastructure will be targeted in 2022 until the political climate reaches a fever pitch. When that happens, expect a flurry of cybercriminal extradition, takedowns, and arrests among law enforcement worldwide and a slowdown in infrastructure attacks. We also predict that 2022 will see the genesis of international cyberlaw, which may even include treaties with adversarial nation-states. There are four other significant predictions:

1. **The anatomy of an MSP will be different in 2022**
   As private equity has entered the channel, deep financial pockets and mergers and acquisitions have given way to a new super-MSP. While the industry will continue to see small and nimble MSPs, market dynamics have changed forever. The challenge for these larger MSPs worldwide will be hiring talent, and a balance between in-house and outsourced teams will start to play out.
2. **Federal regulators and legislators will create and define clarity on ransomware payments for the first time**
   The voluntary standard of the NIST Cybersecurity Framework is not sufficient in the eyes of regulators and legislators, so mandatory compliance is likely on the horizon. Financial regulators have testified to Congress multiple times around cybercrime, ransomware threat actors, and the changes organizations need to enact to drive better cybersecurity. Additionally, there is new legislation in committee describing MSPs and their role in the supply chain. These things will culminate in more cybersecurity legislation in the coming years.
3. **The SMB market is going to spend more in 2022**
   Hiring challenges will only increase for MSP. They'll compete against multi-national corporations for the same talent, meaning MSPs will have to pay more for talent, do more with less, or both. Additionally, the cost of doing business will rise with changes in mandates for cyber insurance. The challenge for MSPs will show their clients how what worked in the past won't work in the future, and the increased efforts and expertise of the MSP will cost SMBs more money. This means that investments in cyber detection, response, and automation will be more important than ever to an MSP looking to protect its margins and grow throughout 2022.
4. **Threat actors will change tactics in response to law enforcement success to stay under the radar**
   Double and triple extortion has become normal behavior for most ransomware operators in 2021. In 2022, we predict that threat will continue this behavior but add a new tactic: stealing and extorting data without deploying ransomware. We expect that government activity will slow attacks on critical infrastructure, and financially (as opposed to politically) motivated threat actors will avoid these types of attacks.

   Lastly, in 2022, many ransomware operators will shift from "Big Game Hunting" to focusing on mid-tier organizations. These attacks can have a decent-sized payout, but they will not get as much public attention when compromised.

Take a closer look at significant cyberthreat events in 2021, continuing trends, predictions about the future of cybersecurity, and action items for MSPs.

[Read the full report]

Executive Summary

2022 MSP Threat Report

More ConnectWise Resources

ConnectWise CRU Feeds
The ConnectWise Cyber Research Unit feeds contain lists of threat intelligence indicators discovered by the CRU using the ConnectWise SIEM or found during threat hunting. This data is threat intelligence the CRU has been collecting for years and using internally at ConnectWise for threat hunting and threat analysis assistance. We use this intelligence daily, searching for these indicators in our partner's network data to find new threats and filter out false positives. This feed is updated daily. You can also see the latest details with MITRE ATT&CK Mappings with Mitigations.

Sign up for the CRU feeds now >> https://github.com/ConnectWise-Software/ConnectWise-CRU

ConnectWise Cybersecurity Management
The ConnectWise Cybersecurity Management solution includes software and support services that enable TSPs to protect their client's critical assets. With tools for 24/7 threat detection monitoring, incident response, and security risk assessment, ConnectWise removes the complexity of building an MSP-powered cybersecurity stack while lowering the costs of support staff.

Learn more >> www.connectwise.com/platform/security-management