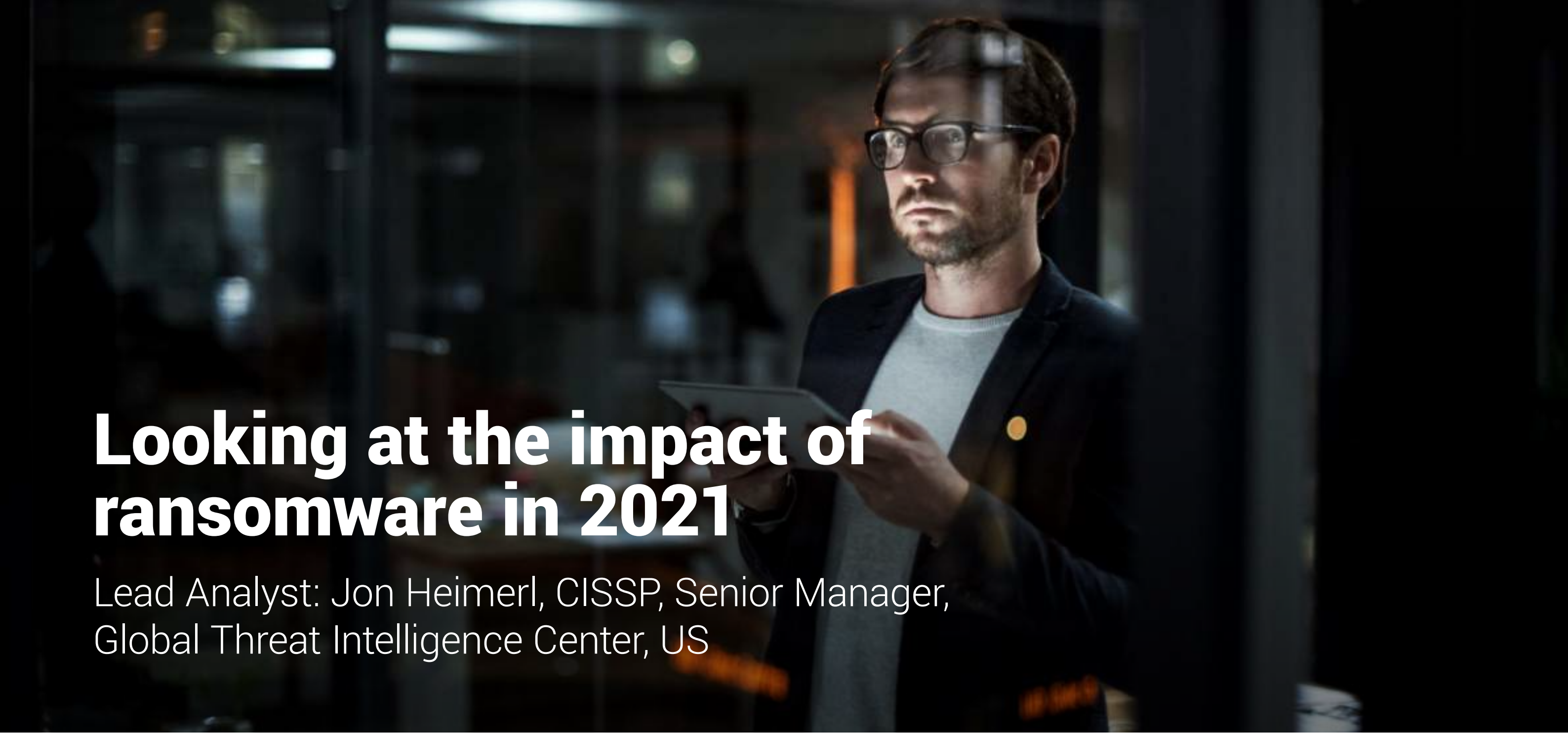
Global Threat Intelligence Center

Monthly Threat Report

August 2021

Contents



Looking at the impact of ransomware in 2021

Lead Analyst: Jon Heimerl, CISSP, Senior Manager, Global Threat Intelligence Center, US

Is ransomware exploding in 2021?

2021 has been full of news stories on the latest ransomware breach and associated demands – from a couple of hundred dollars, a 'fraction of a bitcoin,' to a USD 70 million demand. Media outlets and others have reported about the 'explosion' of ransomware, but is it really worse this year than ever?

Ransomware has been a problem for years, but not necessarily because of the volume of associated attacks. For the past several years, analysis for our annual Global Threat Intelligence Report (GTIR) has shown ransomware at about 3-4% of all detected malware. While that sounds like a low number, it's worth keeping in mind that 3-4% is still hundreds of thousands of detections.

In analysis for the 2021 GTIR, our analysts observed that ransomware had jumped to about 6% of all malware detections. This was an effective increase of nearly 50% in volume from 2019. Ransomware volume in 2021 experienced a surge of activity in January, then a return to more normal levels in February. Since that time, however, ransomware reports have increased about 50% over the year. If volume growth continues through the rest of the year, this would likely indicate that ransomware incidents will double by the end of the year, to closer to 12% of all malware detections, which would indicate millions of detections. This would mean ransomware could very well be increasing by 300% over levels from the end of 2019. One analyst suggests that by the end of 2021, organizations should expect a ransomware attack every 11 seconds.

Other industry sources indicate that ransomware detections and reports are up. Different analyst groups have access to different data sources, and analyse data in different ways, but most analysts tend to agree that ransomware attacks in 2021 have increased by at least 50% and by as much as 350% on the year. While there is no doubt that incidents are up dramatically from previous years, ransomware may very well not rank as the most common type of malware observed. But, as ransomware shows, it's not all about the 'volume' of those attacks.

> While 3-4% sounds like a low number, it's worth keeping in mind that **this is still hundreds of thousands of ransomware detections.**

Ransomware demands averaged about USD 5,000 in 2018. The average ransom paid was about USD 115,000 in 2019, and according to Palo Alto research, ballooned to over USD 312,000 in 2020, and the amount continues to rise.

- As victims and insurance companies pay ransoms, hostile threat actors have been emboldened to continue attacks and increase ransoms.
- There is a low barrier to entry for hostile threat actors, and the return on investment is high.
- Global acceptance of cryptocurrency has made it easier to process larger electronic payments that are easier to hide (early ransomware payments were often in the form of gift cards).

In the past, ransomware payments often did not result in unlocking data for the affected organization. Most industry analysts suggest that more than 95% of organizations who pay can recover at least some of their data. But that number may be misleading since, according to one firm, only 8% of victims were able to restore all of their data.

And it's important to remember that the ransom is not the only cost of a ransomware breach.

- Analysts typically report that the average downtime related to a ransomware breach is in the 12–21 day range, as organizations struggle with the aftermath, recover their data and resume normal operations.
- Analyst claims vary, depending on the source, but it appears 75-80% of organizations who pay a ransom are also attacked via ransomware again later.
- Since an attacker has access to an organization's environment to install malware, especially if they have exfiltrated their data and are threatening to publish it, it means the organization must report the breach under privacy laws like HIPAA and GDPR. In many cases, if the governing body finds the organization were not protecting the data with due care, the organization may also be responsible for regulatory fines and additional scrutiny, on top of any ransomware-related costs.

A ransomware breach is big – and big news

According to analysis performed for our 2021 GTIR, the most common type of malware detected in client environments during 2020 was some form of illicit cryptocurrency miner. The problem with an illicit cryptocurrency miner is that such attacks don't really scare people. A serious coin miner infection might cost an organization a couple of thousand USD per month in electricity, the occasional replacement system and some loss of availability as the miner consumes CPU cycles. And, even at that, the impact of such a breach may not be readily visible. The worse part of an illicit cryptomining attack is that a hostile threat actor was somehow able to install malware onto the organization's environment – it's still a breach.

On the other hand, ransomware breaches tend to be big. If you are victimized, you know it, and often, everyone else knows it too. Important organizational data is locked up and made unavailable for use. In modern ransomware, organizations are also facing the threat that the attacker will publish their private data if they don't pay – so anyone else who wants that data can also have it – for free. Ransomware attacks are often very public events, and can be crippling to organizations with time-sensitive operations and data, which is most organizations.

And the amount paid in ransom is not a good measure of the actual impact such a breach has on the organization. Average costs to recover from a ransomware breach are approaching USD 2 million globally. This is potentially worse for organizations who are bigger, have more data, have more sensitive data, or have a complicated infrastructure. It's not just a matter of 'restoring data.' 'Recovery' means restoring data and applications, rebuilding workstations and user systems, repeating any lost work, testing and analysis, analysing the root cause of the breach, patching and reconfiguring systems to prevent a repeat of the breach, and potentially the purchase of additional hardware, software and services to help strengthen the environment.

Consider that the barrier to entry for a hostile threat actor is low. If an attacker isn't ready to set up their own ransomware infrastructure, they can take advantage of another actor's ransomware-as-a-service (RaaS) options for minimal costs. Given that average payouts have risen past USD 300,000 per incident and are still growing, that is potentially a very attractive return on investment for the threat actor.

Ransomware attacks are profitable.

- Before it shut down, the GandCrab ransomware group collected more than USD 150 million profit on USD 2 billion in ransom.
- According to analysis by one researcher, DarkSide collected over USD 90 million in ransoms in the nine months before Darkside reported that they ceased operations in the aftermath of the Colonial Pipeline breach.
- REvil claimed they had made over USD 100 million in 2020.

Ransomware-as-a-service (RaaS)

Attackers popularized RaaS in 2016 soon after initial reports of ransomware as malware. A ransomware developer licenses third parties (other hostile threat actors) to use their ransomware infrastructure. The third party does not need to know anything about writing malware or require any actual technical knowledge – they simply gain the capability to launch ransomware attacks by licensing from the developer. RaaS access often includes technical support, user forums and other common 'as-a-service' functions. The only requirement of the end-user is that they pay the license fee, ranging from less than USD 100 per month to a couple of thousand dollars per campaign, along with a cut of the proceeds. This has lowered barriers to entry and enabled the spread of ransomware attacks as hostile threat actors licensed these services.

Some well-known RaaS solutions are NetWalker, Avaddon, Locky, DarkSide, REvil (Sodinokibi) and Dharma, but there are many others.

Double ransoms

Double ransoms may have been around since 2019, but they took off when Twisted Spider embraced the tactic with dedicated leak sites in early 2020. The standard ransomware process locks the target's data, but the attacker also gives an additional extortion demand that they will publish the victim's data for others to access if the victim does not pay. The technique not only encourages accelerated payment, but also compensates for targets who have protected backups and processes that would allow them to recover from a normal ransomware attack.

Maze, then Egregor, encouraged double ransoms throughout 2020 – at least until Egregor was shut down in February 2021. By the second half of 2021, the technique was much more commonplace, with most ransomware attacks currently including a double-ransom component. Threat actors like Twisted Spider began setting up their own hosted sites to release exfiltrated data. The technique continued evolving, and current threat actors often release part of the captured information as proof to the victims that they have the ability, and willingness, to release more. Ransomware families like NetWalker and RagnarLocker embraced the technique, but their data hosting sites also attracted attention from global law enforcement.

Some attackers have begun implementing 'triple ransoms,' also promising extended denial-of-service (DoS) attacks if negotiations do not progress and the victim does not pay the ransom in a timely manner. This technique is also growing in popularity.

Exactly what are we seeing?

No industry or organization is safe from ransomware. We have observed clients of all sizes and industries face ransomware challenges. While several threat actors have stated they are only targeting bigger organizations, other actors regularly target SMBs. Our 2021 GTIR reported that in 2020 the technology and healthcare industries were most targeted by ransomware. In the first half of 2021, a few industries have observed higher amounts of ransomware than others.

Industry	% of ransomware in 2021
Manufacturing	28%
Retail	28%
Healthcare	22%

Ransomware reports and detections tend to be very dynamic. Ransomware observations often come in waves as a threat actor starts a new campaign with one of the popular RaaS kits, or as one of the RaaS providers upgrades their service in some way. RaaS providers regularly close up shop, sometimes resurfacing with a different name. The result is that week-by-week, we may observe dramatically different volumes and variants. But, over time, some ransomware use stands out. For the first half of the year, we've observed more reports for some ransomware families.

Ransomware detections and reports evolve rapidly. Mespinoza, for instance, showed a spike in reports in January, then largely faded from view. The list of most active ransomware by the end of 2021 will likely appear dramatically different than it does now as threat actors evolve their products, disband old groups and form new ones.

What do I do about it?

A complete list of preventive, mitigating and remedial actions could span many pages and depend highly on the organization's exact circumstances. But, the following four high-level recommendations can help protect against ransomware in many cases:

1. **Conduct security awareness training** designed to help protect users from phishing attacks. A significant amount of malware is spread via phishing, and any reduction in this exposure can help.
2. **Regularly perform effective backups** of all data on all critical systems, with high frequency. Store some of these backups offline and do not readily overwrite backup media. Retaining the ability to restore data can help minimize the impact of ransomware.
3. **Patch critical and exposed systems aggressively.** Some ransomware is introduced to organizational environments by known vulnerabilities which have patches available. Keeping exposed systems patched can help reduce the potentially exposed vulnerabilities.
4. **Disable Remote Desktop Protocol (RDP) in your environment.** Many ransomware variants make extensive use of RDP as an infection source and control path. Removing RDP can remove that threat vector from your environment.

Otherwise, practicing good security hygiene, like using multifunction authentication and implementing aggressive network segmentation can help reduce your exposure. If you take such actions to reduce your exposure to vulnerabilities and attacks, you can potentially reduce your exposure to ransomware. Unfortunately, with the variety of threat actors, ransomware variants and specific techniques being employed, it seems there is little chance of fully eliminating your exposure.

> Ransomware attacks are often very public events, and can be crippling to organizations. Average ransomware breach recovery **costs are approaching USD 2 million globally.**

Ransomware variant	Percent on the year	Description
Avaddon	21%	Avaddon was a RaaS that both encrypted victim data and exfiltrated it for extortion. If the victim didn't pay, attackers posted the stolen data on the Avaddon data website. The Avaddon ransomware group added distributed denial-of-service (DDoS) attacks to help pressure victims to pay. Breaches tended to come through remote access login credentials or via Remote Desktop Protocol. Before encryption, Avaddon would verify the victim was not located in the Commonwealth of Independent States (CIS), made up of Russia and 11 countries that had been part of the former Soviet Union. Avaddon claims to have ceased operations and released decryption keys for 2,934 victims (with an average ransomware demand of USD 40,000, the maximum potential value of their pending ransoms could have been USD 117 million). It's not clear if they shuttered their business due to increased scrutiny from US and Australian law enforcement or if it was related to the ransomware and cybersecurity discussions between Presidents Biden and Putin.
DarkSide	6%	DarkSide was a RaaS that emerged in August 2020. DarkSide immediately set a trend of focusing on larger victims, along with larger ransoms, often into millions of dollars. It includes data exfiltration and a data leak 'blog' to help force victims to pay. DarkSide added a Linux variant in April 2021, along with the ability to DDoS targets. Breaches tend to come through phishing, remote accounts and Remote Desktop Protocol. DarkSide actively promoted their professionalism and customer service. They claimed to have lost access to their infrastructure and shuttered the business due to fallout from the Colonial Pipeline breach. They also claimed they would be providing decryptors for pending victims. According to analysis by one researcher, DarkSide collected over USD 90 million in ransoms in the nine months before Darkside reported that they ceased operations in the aftermath of the Colonial Pipeline breach.
Ragnarok	5%	Ragnarok is ransomware first circulated early in 2020. Ragnarok is known to have compromised targets via unpatched Citric ADC servers (CVE-2019-19781) and scan for additional systems using the EternalBlue vulnerability. It also attempts to disable Windows Defender, making the system more vulnerable. The ransom note left by the software claims the victim's data will be made public on the internet. Ragnarok excludes targets with Chinese, Russian or several CIS states set in the system's Windows language ID. Some configuration files are common, despite samples being found at different targets, which suggests attackers are not tailoring attacks to specific victims. Ragnarok is still very active, and reports have been increasing steadily over the past few months.
Nefilim	5%	Nefilim is ransomware that first appeared in March 2020. It shares a substantial amount of code with the NEMTY ransomware family, but any relationship between the actors behind the two ransomware is not clear. Nefilim threatens to publish the victim's sensitive exfiltrated information if they fail to meet the attacker's demands. Breaches tend to rely on vulnerable Remote Desktop Protocol services. The ransom note instructs victims to contact the operators via email instead of the usual payment portal. Nefilim has promised not to attack healthcare and other select organizations during the COVID-19 pandemic. Reports of Nefilim have been relatively steady so far throughout 2021.
Clop	4%	Clop ransomware first appeared around February 2019, so it's one of the older variants commonly detected throughout 2021. It's most commonly delivered via attachments in spam emails or by compromised websites providing malicious downloads. It has also been spread via additional compromises, ultimately providing access to the internal network's Active Directory. The threat actor behind Clop has expressed interest in targeting large network environments rather than smaller users. Clop excludes targets in Russia and CIS countries by checking the keyboard layout of the target host. The ransom note does not provide the actual ransom demand but includes instructions to contact the operator via email for additional instructions. Reports of Clop have been irregular, varying greatly from week to week. With members of Clop being arrested in Ukraine in June, the ransomware experienced a brief drop in activity, but it does not appear Clop has been seriously disrupted.
Conti	3%	Wizard Spider has been using Conti ransomware since about May 2020. It's known for its speed of encryption as well as several modern features, including the ability to target the local network via SMB shares. It appears some of these features are directly controlled by the threat actor via remote access. Reports of Conti have been rising steadily since February, but with 3% of total reports has not accumulated enough activity to make the top five for the year. Still, Conti is worth keeping an eye on for future activity. The growth of Conti as ransomware contributed to double-extortions, as Conti embraced the technique early on.

The state of application security – how do organizations find the silver bullet?

Lead Analyst: Setu Kulkarni, Vice President Corporate Strategy and Business Development, NTT Application Security, US

The threat landscape surrounding web, mobile and API-based applications is evolving rapidly. Consequently, there is a critical need for a frequent and periodic analysis of the overall state of application security.

For our July AppSec Stats Flash, we reviewed some major trends from the last six months to analyse the current state of application security and lay out our recommendations to make immediate improvements.

We track and analyse four major indicators in our monthly application security statistics report:

1. The **window of exposure** is a lagging indicator of how well the application and the application security program are performing. The **window of exposure** tells us about how long an application is vulnerable to exploits through serious, unaddressed vulnerabilities.
2. The **vulnerability types** are the descriptions of the most common vulnerability types and how they are changing.
3. The **time-to-fix by risk** tells us how long it's taking organizations to fix serious vulnerabilities.
4. The **remediation rate by risk** tells us how many of the serious vulnerabilities organizations are fixing.

We examined these metrics from 1 January 2021 to 30 June 2021 to identify the trends shaping the state of application security. The bottom line is that applications are more vulnerable than last year. The time required to fix serious vulnerabilities is increasing, remediation rates are decreasing and the types of vulnerabilities applications suffer from have not changed. In other words, hackers have it easy. Applications have become the path of least resistance for attackers to breach an enterprise. Here is a simple visual to summarize the state of application security:

Larger window of exposure x **Common vulnerability types** x **Long time to fix** x **Poor remediation strategies** = **Exponential business risk**

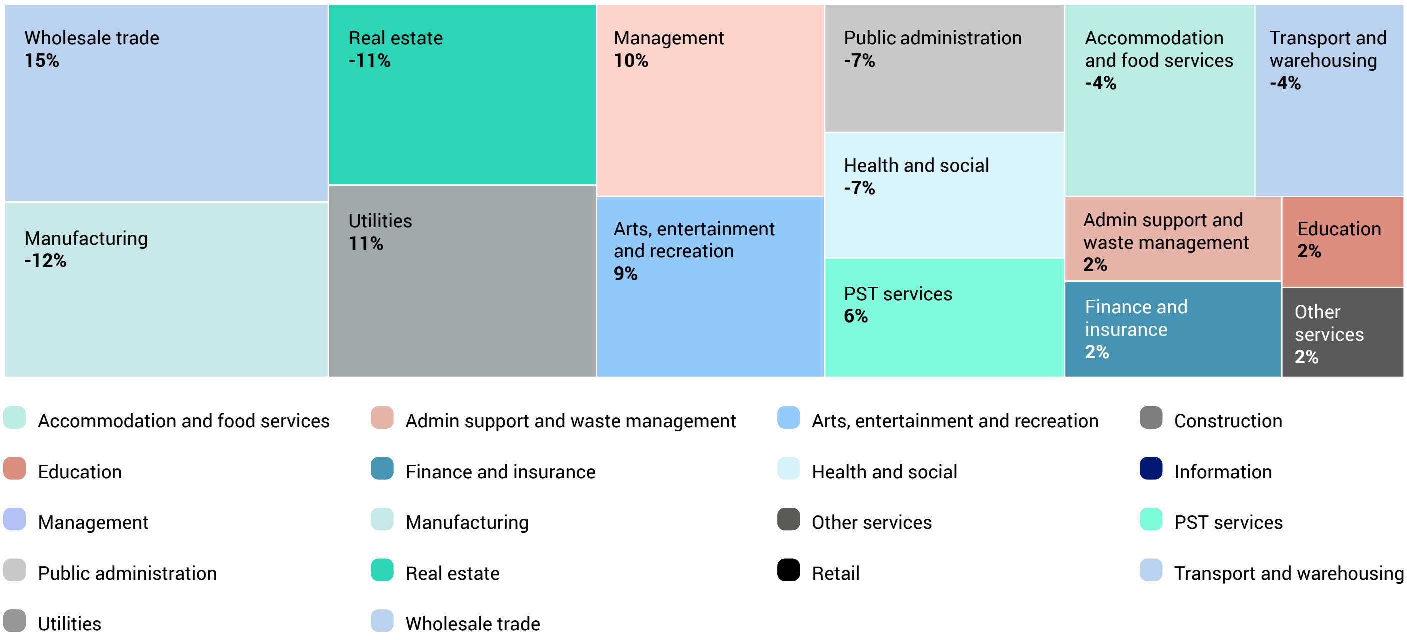
Window of exposure

While the overall window of exposure across industries remains unacceptably high, we find that for some industries, it's the best of times, and for others, it's the worst of times.

In particular, two industries are moving in the right direction:

1. **Manufacturing:** High volumes of activity related to persistent supply-chain type attacks seem to have forced a change in behaviour. Applications in this industry have seen a 15% decrease in their window of exposure for serious vulnerabilities throughout the year.
2. **Public administration:** Citizens are consuming public services online more than ever before. Along with the release of the Presidential Executive Order on cybersecurity, this has helped contribute to an increased focus on securing applications in the public administration industry. This has resulted in a 7% reduction in their window of exposure.

On the other hand, industries like wholesale trade (15% increase), utilities (11% increase), management or holding companies (10% increase) and education (2% increase) have an increasing window of exposure.



The bottom line is that the window of exposure for organizations continues to be a worrying sign of breach exposure. One way to reduce the window of exposure is to adopt a Two-Speed AppSec strategy to address the disparate needs of legacy applications and greenfield applications.

- **For legacy applications,** focus on detecting vulnerabilities in production and implementing a rapid-response type mitigation strategy.
- **For greenfield applications,** along with adopting a production testing strategy, implement the integration of AppSec vulnerability information into the software development cycle to remediate issues.

Vulnerability likelihood by class

The top five vulnerability classes have remained constant every month in 2021.

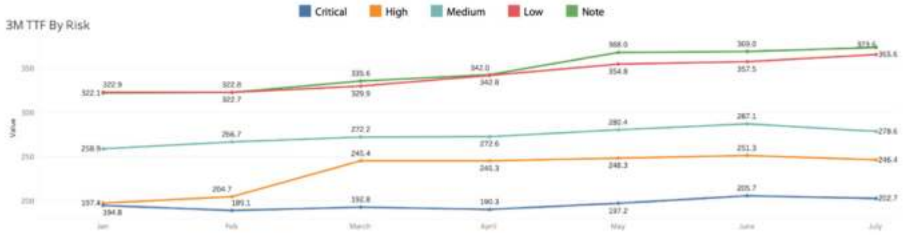
1. Information leakage
2. Insufficient session expiration
3. Cross-site scripting
4. Insufficient transport layer protection
5. Content spoofing

These pedestrian vulnerabilities continue to plague applications. The effort and skill required to discover and exploit these vulnerabilities are relatively low, making it easier for the adversary to take advantage of them.

> The effort and skill required to discover and exploit these vulnerabilities are relatively low, **making it easier for the adversary to take advantage of them.**

Time-to-fix by risk

Time-to-fix (TTF) has also seen a significant increase, pointing to a growing need to implement targeted campaigns to reduce the time it takes to mitigate critical and high-risk vulnerabilities.

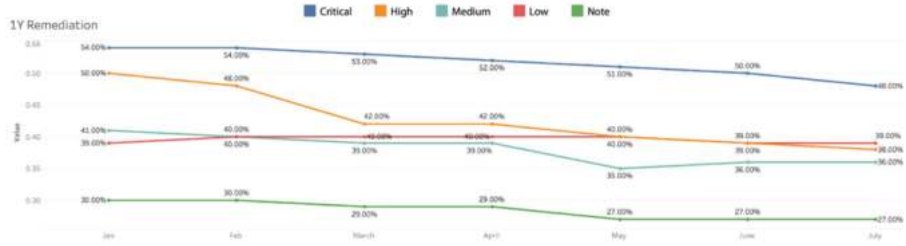


TTF for all vulnerability severities is increasing.

- As of the end of June, the average TTF for critical vulnerabilities increased from 197 days to 202 days in 2021.
- As of the end of June, the average TTF for high vulnerabilities increased from 194 days to 246 days in 2021.

Remediation rates by risk

The remediation rate for severe vulnerabilities has been declining so far in 2021. When combined with the observed increasing 'time-to-fix', this trend contributes to an overall increase in the window of exposure for applications.



Remediation rates across all vulnerability severities are decreasing.

- As of the end of June, remediation rates for critical vulnerabilities decreased from 54% to 48% in 2021.
- As of the end of June, remediation rates for high vulnerabilities decreased from 50% to 38% in 2021.

The way forward

The 'silver bullet' to improving the state of your applications' security is hidden in your AppSec testing metrics. It's important that you test applications in production to gather actionable AppSec testing metrics. Once you have that data, take a targeted approach to identify the most prevalent severe vulnerability and run an organization-wide campaign to eradicate that vulnerability. In doing so, ensure that your team is:

1. Acting on vulnerabilities by risk of attack, prioritizing the most severe vulnerabilities ahead of lesser severe vulnerabilities.
2. Educating all stakeholders in your software development lifecycle (SDLC) about the impact, and how to mitigate the most severe vulnerabilities plaguing your applications.
3. Planning to address these vulnerabilities as a matter of 'business as usual' instead of spinning up unsustainable one-off projects.

Two industries – manufacturing and public administration – **are moving in the right direction, reducing their windows of exposure.**

Five trending threat actor groups

Lead Analyst: Jeremy Bender, Security Intelligence Writer,
Global Threat Intelligence Center, US

At any one time, there are numerous threat actors and groups targeting specific industries, vulnerabilities and high-profile events. These threat actors range from mere annoyances lacking any technical sophistication to highly-competent, technically-advanced adversaries.

As part of our research efforts, our Global Threat Intelligence Center (GTIC) actively tracks the activities of high caliber, sophisticated threat actor groups.

In particular, the following five groups have been highly active over the past six months. These five groups are by no means the only advanced groups operating, or the only groups we monitor. However, these groups' activities and technical sophistication warrant the attention of all organizations.

APT35

APT35 (also known as Charming Kitten, Magic Hound and Phosphorus) is an Iranian state-sponsored group which has primarily been involved in information theft and espionage since 2014. Historically, the group has largely targeted US and Middle Eastern organizations – especially groups either based in or with business interests in Saudi Arabia – journalists, human rights advocates and academics.

APT35 has traditionally used watering-hole attacks, phishing emails and fake social media profiles to lure targets into attacks. Most recently, in July 2021, researchers publicized a campaign the group conducted targeting academics, experts on the Middle East and journalists. As part of the campaign, dubbed 'Spoofed Scholars,' APT35 compromised a legitimate website belonging to the London University School of Oriental and African Studies (SOAS). The group then used that site to send credential harvesting phishing messages to select targets.

Researchers believe APT35's end goal for Spoofed Scholars, as is typical for the group's campaigns, was to obtain information of specific interest to the Iranian government.

APT41

APT41 is a China-based APT group who has been active since at least 2012. Based on shared use of certain tools and malware variants, such as Winnti malware, as well as overlap in tactics, techniques and procedures (TTPs), researchers place APT41 under the Winnti Group Umbrella. APT41, and more broadly the Winnti Group, has targeted a range of industries for cyberespionage, however, the group has focused on organizations in the United States, Europe and Asia Pacific. Historically, the groups targeted the video game industry in order to steal code-signing certificates, though APT41 and the wider Winnti Group Umbrella have diversified their targets to include industries like healthcare, telecommunications and technology.

In July 2021, researchers discovered a new remote access trojan (RAT) dubbed 'BIOPASS' targeting online gambling companies in China via watering-hole attacks. Compromised websites serve the loader for BIOPASS to visitors by disguising it as a legitimate installer for Adobe Flash Player or Microsoft Silverlight. Researchers believe the BIOPASS RAT is in the development stage. While researchers have not definitively linked BIOPASS to APT41 or the Winnti Group Umbrella intrusion set, the TTPs used in the campaign overlap with APT41. It's worth noting that online gambling in China is illegal, leading some researchers to hypothesize BIOPASS may be part of a Chinese government crackdown on the industry within the country.

Wizard Spider

The Wizard Spider threat group is one of the most nefarious cybercriminal groups currently active. The group infamously operates the TrickBot banking trojan, whose infection chain includes the deployment of Ryuk ransomware. In such attacks, the Wizard Spider subgroup Grim Spider drops Ryuk as the final stage of the infection cycle. Wizard Spider has typically engaged in indiscriminate targeting and deployment of TrickBot, though the group does also partake in big-game hunting. In such operations, the group will specifically target certain high-profile entities for ransomware attacks in the hopes of larger payouts. In addition to Ryuk, Wizard Spider has also deployed Conti ransomware.

We participated with partner organizations in a disruption of the TrickBot infrastructure in the fall of 2020. However, Wizard Spider has since set up new TrickBot infrastructure and started using new tools, such as the BazarLoader, to continue operations. In July 2021, researchers discovered a new ransomware variant dubbed Diavol. While this ransomware does not yet have an undisputed connection to Wizard Spider, there are multiple clues indicating this variant may be linked to the group.

REvil

REvil (also known as Ransomware Evil and Sodinokibi) is a ransomware-as-a-service (RaaS) operation and gang which has been active since at least 2018. Like Wizard Spider, REvil engages in big game hunting. REvil also operates a dedicated leak site called Happy Blog, where the threat actors will post exfiltrated data from compromised organizations who refuse to pay the ransom. As a RaaS operation, the core REvil gang rents their infrastructure to affiliates who then carry out the actual attacks.

REvil has targeted a wide range of sectors, including critical infrastructure, finance, manufacturing, transportation, telecommunications and healthcare. REvil gained widespread media attention after an affiliate launched a supply-chain ransomware attack leveraging a vulnerability in Virtual System Administrator (VSA) servers belonging to IT management solutions provider Kaseya on 2 July 2021. Kaseya has since released patches to mitigate three vulnerabilities in their VSA software.

Following the Kaseya attack, all REvil's dark-web sites went offline. It's unclear why the group took down their sites, however, REvil's disappearance follows US President Biden speaking to Russian President Putin about the Kaseya attack. It's widely believed REvil is based in Russia, so theories for the group's disappearance include a law enforcement takedown or a self-directed takedown by the group to lay low for the time being.

APT29

APT29 (also known as Cozy Bear, Minidionis, Nobelium and The Dukes) is a Russian state-sponsored group engaged in cyberespionage since at least 2008. APT29 has been attributed to Russia's Foreign Intelligence Service (SVR). The group primarily targets organizations with the goal of advancing Russian foreign and security policy decision-making, and it has a target list spanning defense, energy, government, telecommunication, NGO, media and pharmaceutical organizations in Europe, North America, Asia Pacific, Africa and the Middle East.

Governments and researchers have attributed several high-profile compromises to the group, including the compromise of the Democratic National Committee in the summer of 2015. In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise to the SVR and cited APT29. APT29 also launched a notable email-based attack campaign in May 2021 leveraging a legitimate mass-mailing service to masquerade as a US-based development organization. This campaign distributed malicious URLs to more than 150 organizations across several industries. In June, the group launched additional password spray and brute-force attacks. This campaign was primarily aimed at IT companies and government organizations in the United States, the United Kingdom, Germany and Canada.

Summary

Threat actors, groups and APTs often come and go as groups decide to disband or their operations are disrupted. It's not uncommon to see activity of any single threat group wane or grow over days, weeks or even months, as can be seen by the apparent cease in activity from REvil. But most of these groups have displayed staying power that suggest they will continue to remain active threats for the foreseeable future. And if they don't, they will soon be replaced by someone just as active.

> The five threat group actors' **activities and technical sophistication** warrant attention from all organizations.

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs, and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2021 Global Threat Intelligence Report

Our 2021 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month. Sign up for our **Emerging Threat Advisory** and security bulletins for visibility of emerging threats and vulnerabilities that are being actively exploited across the world, sourced from our global threat intelligence platforms.

NTT