EXECUTIVE BRIEFING



EXECUTIVE BRIEFING

Key Insights from the 2022 Threat Detection Report

Welcome to Red Canary's 2022 Threat Detection Report executive summary. Based on in-depth analysis of over 30,000 confirmed threats detected across our customers' environments, this research arms security leaders and their teams with actionable insight into the threats we observe, techniques adversaries most commonly leverage, and trends that help you understand what is changing and why. This is our most expansive report to date, but our intention remains the same:

The Threat Detection Report exists to help you understand and detect threats.

This executive summary serves as a high-level introduction to a dozen key **trends**, the top ten **threats**, and the most prevalent **techniques** that we've observed in our customers' environments. The full report goes into significant detail for each of these sections including recommendations on how to detect, mitigate, and simulate specific threats and techniques. We recommend you share the full report with your team and discuss how the ideas, recommendations, and priorities map to your security controls and your overall strategy.

A full version of the report is available at redcanary.com/threat-detection-report





A dozen key trends

Red Canary performed an analysis of emerging and significant trends that we've encountered in confirmed threats, intelligence reporting, and elsewhere over the past year. We've compiled the most prominent trends of 2021 in this report to show major themes that may prelude into 2022.

The technique and threat sections of this report are focused on detection data and identifying prevalent ATT&CK techniques and threats in those detections. The trends section takes us one step beyond that data and allows us to narrate events that might not be prevalent but may be emergent or otherwise deserve your attention.





Ransomware

Ransomware continued to dominate the 2021 threat landscape, and we observed operators take new approaches.

Supply chain compromises

Supply chain compromises were a major theme, starting with SolarWinds, Kaseya and NPM package compromises mid-year, and ending with Log4j.

Vulnerabilities

Adversaries exploited vulnerabilities affecting popular enterprise platforms to drop web shells, spread ransomware, and more.

Affiliates

The threat landscape continued its trend toward a Softwareas-a-Service (SaaS) economy, muddying the already murky waters of attribution.

Crypters-as-a-service

Crypters like HCrypt and Snip3 joined the ranks of other "as-a-Service" threats.

Common webshells

Adversaries exploited web applications with help from web shells such as China Chopper, Godzilla, and Behinder.

User-initiated initial access

We observed an uptick in threats that occurred after users sought out content which, often unbeknownst to them, was malicious.

Malicious macOS installers

Malicious installers led to rotten Apples and adware, as macOS systems continued to be targeted.

Remote monitoring and management abuse

Adversaries continue to use and abuse legitimate remote monitoring and management (RMM) software to move data and control infected hosts.

Linux coinminers

Coinminers once again dominated the Linux threat landscape.

Abusing remote procedure calls

Intrusions leveraging remote procedure calls (RPC) made waves, particularly PetitPotam and PrintNightmare.

Defense validation and testing

Confirmed testing comprised almost one quarter of our detections in 2021, with many coming from open source tools.



Trend 1: Ransomware

Throughout 2021, ransomware remained one of the top threats to every organization. While some groups focused on traditional encryption, 2021 also marked the rise of additional tactics. Key trends include:

- **Double extortion:** A significant ransomware trend in 2021 was the increase in adversaries expanding their threats beyond data encryption. Multiple ransomware groups pivoted to stealing and exfiltrating data before encrypting it, then demanding payment to prevent the data from leaking publicly. While this practice isn't new (it dates back to at least 2019), what was significant in 2021 was the number of groups who adopted this approach—to the point where it became the standard.
- **Affiliate model:** Ransomware groups usually rely on multiple affiliates to give them initial access to an environment before they encrypt files or take other actions. These affiliates frequently use crimeware such as Bazar and Qbot to gain initial access to an environment, later passing off access to ransomware groups.
- **New ransomware groups:** Defenders must also contend with new groups emerging and others seemingly disappearing (often to be reincarnated in a different form as another group). Some of the ransomware families we bid farewell to in 2021 were Egregor, Sodinokibi/REvil, BlackMatter, and Doppelpaymer. New ransomware families include BlackByte, Grief, Hive, Yanluowang, Vice Society, and CryptoLocker/Phoenix Locker. Many new ransomware families displayed close similarities to old families that "disappeared," leading analysts to assess that known adversaries simply resurfaced using a new name.

Trend 2: Supply chain compromises

Supply chain compromises were prevalent in 2021, and these incidents aren't going away any time soon. A supply chain compromise occurs when an adversary compromises a software developer, hardware manufacturer, or service provider and uses that access to target customers who use the affected software, hardware, or service. Major supply chain compromises from 2021 include SolarWinds, Kaseya, Node Package Manager (NPM) compromises, and Log4j:

SolarWinds: Adversaries compromised SolarWinds, accessed the update infrastructure for its Orion IT management software, and sent backdoored updates to the company's thousands of customers in December 2020, affecting organizations well into 2021. The trojanized Orion platform updates included a legitimately signed dynamic link library (DLL) file,



and some featured backdoor functionality that, after a dormancy period lasting as long as two weeks, initiated communication with command and control (C2) servers. Adversaries identified targets of interest for further exploitation and conducted follow-on activity such as installing additional malicious binaries. These malicious binaries were used to install a backdoor where adversaries could access the victim organizations' accounts.

SolarWinds disrupted many networks, and it took months for enterprises to investigate and respond. The incident shined a light on supply chain risks and initiated a renewed focus that will remain relevant in 2022 and beyond.

- Kaseya: In July 2021, adversaries exploited vulnerabilities in Kaseya VSA IT Management software in a campaign ultimately designed to deploy Sodinokibi ransomware, also known as REvil. VSA is popular among managed service providers (MSP) that use it to remotely administer IT systems. The adversaries exploited zero days to gain remote control over the MSPs' VSA installations, which they used to infect the MSPs' customers' endpoints with ransomware. Kaseya estimated that about 50 direct customers who were running Kaseya VSA systems—and between 800 and 1,500 other businesses—were impacted by this breach. While the damage was not as bad as it could have been, this incident further highlights the importance of tracking supply chain threats. It also resulted in significant attention from the U.S. government, which later indicted the adversaries allegedly responsible for the attack.
- NPM package compromises: NPM is a repository for publishing node.js projects, including libraries that developers download and incorporate into their software. In October 2021, adversaries compromised an open source JavaScript library with more than 7 million weekly downloads and used it to distribute password stealers and coinminers. At the time, the NPM registry did not require author accounts to use multifactor authentication (MFA), which led to an unknown adversary hijacking the registry accounts of multiple package authors. After hijacking, the adversary published malicious versions of the legitimate packages that contained malware. Victims included package authors and end users of applications relying on those packages. One package, `ua-parser-js`, was downloaded around 8 million times a week at the time and is used by Google, Amazon, Facebook, IBM, and Microsoft. This was just one of several mNPM compromises throughout the year.
- Log4j: Log4j is a popular Java logging library underlying many third-party applications that was hit with a remote code execution vulnerability in December 2021. The primary threats initially exploiting this vulnerability were coinminers and botnets, though the community feared exploitation would expand because of Log4j's massive intrusion surface. In some scenarios, the Log4j library was affected by a remote code execution vulnerability. Though it took adversaries a few weeks to ramp up targeting,



in late December 2021 and early 2022, internet-facing VMware Horizon servers using vulnerable versions of Log4j became a target for multiple operators. Adversaries were likely attracted to VMware Horizon because it is widely used and often internet-facing. We anticipate the continued targeting of internet-facing applications using vulnerable versions of Log4j for months to come.

Trend 3: Vulnerabilities

Several high-profile vulnerabilities made it into the collective consciousness of the security community in 2021. ProxyLogon and ProxyShell targeted Microsoft Exchange servers and affected a massive number of systems, sometimes leading to ransomware deployment. The exploitation of vulnerabilities in Kaseya's VSA appliance software also led to ransomware deployment on some of the thousands of organizations that used Kaseya software for remote administration of endpoints. In the latter half of the year, adversaries exploited multiple vulnerabilities in Zoho's ManageEngine suite of products. PrintNightmare and an MSHTML vulnerability caused a ruckus among the security community and media; however, their actual impact appears to have been limited.

An important nuance to call out is that vulnerabilities are just flaws in code—a threat must exploit that vulnerability. Given the frequency with which vulnerabilities are disclosed and the ease with which adversaries can exploit newly reported weaknesses, particularly in common applications, Red Canary focuses on identifying and detecting the behavior we observe surrounding the exploitation of a vulnerability. We recommend other organizations do the same. Understanding the threats and the ways in which adversaries operate in compromised networks allows defenders to protect against malicious activity regardless of the means by which their environment is accessed

Trend 4: Affiliates

The term "affiliate" has been increasingly used to describe the cybercrime ecosystem's evolution into a Software-as-a-Service (SaaS) economy. Borrowed from the subscription-based software specialization strategy, an "affiliate" refers to the provider-customer relationship of malicious services. In the cybercrime ecosystem, several SaaS variants have emerged, from Phishing-as-a-Service (PhaaS) to Access-as-a-Service to Crypter-as-a-Service to Ransomware-as-a-Service (Raas). It has never been easier to find an adversary for hire.

This service specialization across the phases of an intrusion has led to a proliferation of partnering, muddying the waters of what was once a relatively consistent collection of tactics across campaigns. As adversaries swap subscribers and pass off payloads, identifying and anticipating the progression of a compromise becomes more challenging.



Trend 5: Crypters-as-a-Service

Crypters are used to make malware harder to detect by security tools. They achieve this by masquerading as legitimate programs prior to execution.

Throughout 2021, Red Canary observed operators using crypters HCrypt and Snip3 to obfuscate and deliver various remote access trojans (RAT). Like other "as-a-Service" threats, the developers sell or lease these crypters to affiliates who use them to carry out campaigns, expanding the threat landscape and creating new economies of scale. The "as-a-Service" ecosystem lowers the technical barrier to entry, allowing operators to purchase capabilities rather than develop them.

Trend 6: Common web shells

In 2021, adversaries exploited web applications with help from web shells such as China Chopper, Godzilla, and Behinder.

Web shells are malicious scripts designed to maintain persistent access to compromised web servers and facilitate remote code execution. Some are simple, allowing adversaries to issue a single command in a text box on a web page, while others include extensive capabilities where the adversary's imagination is the limit. Web shells execute with the same user account privileges as the exploited web application. If the application runs as an administrator, sensitive databases and systems may be accessible. Most web shells have simple or non-existent authentication mechanisms. Adversaries often leave web shells on public-facing web servers with no authentication mechanisms so they can return to the systems later. In some incidents, responders may find many web shells on a single server or evidence of multiple adversaries using an abandoned web shell. Web shells should be removed as soon as possible to prevent further access.

Trend 7: User-initiated initial access

Over the past year, we observed a rise in what we refer to as "user-initiated activity": cases where victims downloaded a malicious executable after engaging with content they purposefully sought out. This often occurs without the victim's knowledge, particularly in cases where adversaries poison search engine results to direct victims to compromised websites. This allowed adversaries to use a range of initial access mechanisms to gain a foothold into victims' environments. Much of the activity we saw was consistent with our expectations, with many detections resulting from malicious emails, attempts to harvest victims' credentials, and breaches by way of a trusted party. Several of our top 10 threats—SocGholish, Yellow Cockatoo, and Gootkit—rely on variants of user-initiated activity for initial access.



Understanding initial access can help defenders protect their environments early on. Prioritizing detections related to initial access saves money, time and effort; lessens pain points for users; and reduces impact to a business. From an intelligence perspective, understanding common patterns in initial access and follow-on activity helps build confidence in determining if relationships exist between threats that cooccur in an environment.

Though user-initiated activity can be just as dangerous as adversary-initiated activity, it can be more challenging to triage because it often involves unwanted software or riskware, which many organizations deem lower-risk. However, it is critical to respond to this type of activity immediately, as follow-on threats can include infostealers and ransomware.

Trend 8: Malicious macOS installers

We've come a long way from hearing cries of "Macs don't get viruses!," and in 2021, the information security community saw more and more malware targeting macOS systems. In contrast to Windows systems, we observe far fewer malicious documents or email attachments on macOS systems. Instead, the majority of malware we observe on macOS stems from malicious installers that trick victims into thinking they're downloading legitimate content. Most macOS threats we observe are malicious adware. Malicious adware is an unwanted program designed to show advertisements on a victim's screen, often within a web browser.

Trend 9: Remote monitoring and management abuse

Adversaries regularly abuse remote monitoring and management (RMM) tools because they're widely used for legitimate reasons and seem benign. Along with the ability to blend in while moving laterally, these tools offer adversaries a reliable way to communicate with and pass information in and out of infected hosts.

In 2021 we identified an uptick of ransomware operators abusing RMM to remotely control victim machines and deploy additional malicious payloads. RMM has typically been used by help desk technicians to resolve issues on client computers. These software suites allow users to remotely control hosts, providing adversaries with a user-friendly graphical interface, secure network connections via cloud hosted infrastructure, and host persistence. This makes it a challenge for defenders to catch the early stages of intrusions. It became increasingly clear to us throughout the year that being able to initially detect abnormal installation and execution of these tools can help thwart ransomware or slow further deployment of malicious payloads.



Trend 10: Linux coinminers

While coinminers affect all operating systems, they made up the majority of the threats we saw in Linux environments in 2021, just as we've seen in years prior. As Log4j vulnerabilities consumed the information security news cycle in December 2021, researchers reported adversaries exploiting Log4j to deliver XMRig payloads and other coinminers. Being able to detect and respond to common threats like coinminers will help any blue team detect a wide range of activity—even when it emanates from unknown exploits.

The coinmining binaries that we observed most commonly were XMRig payloads, which were often delivered by adversaries who targeted unpatched endpoints. Due to its popularity, XMRig artifacts provide excellent opportunities for detection, including several discussed in the full Threat Detection Report.

Trend 11: Abusing remote procedure calls

Remote procedure calls (RPC) facilitate local and remote communication between client and server programs. Many Windows services leverage RPCs for communication, and many RPCs expose functions to end users. Depending on privilege levels and the security checks that are (or are not) performed when these functions are implemented, adversaries can abuse RPCs to perform many malicious actions.

Two methods of RPC abuse stood out in 2021: PetitPotam and PrintNightmare. Both emerged over the summer, and adversaries quickly adapted them from theoretical proofs of concept for privilege escalation into real-world attacks. Both were reportedly leveraged in ransomware campaigns, underscoring the urgency behind these threats.

Trend 12: Defense validation and testing

We see a lot of testing. In fact, 23.4 percent of all the confirmed threats we detected in 2021 were confirmed by customers to be testing. We're all for testing (as you can hopefully tell by our work with **Atomic Red Team**). However, when comparing the top 10 detection analytics that appeared in detections marked by customers as testing to those that fired in detections not marked as testing, only three analytics overlapped. Here are some patterns we observed in testing detections during 2021:

Common testing tools: Unsurprisingly, a large volume of the testing detections we observed were from common breach and intrusion simulation tools and open source testing tools. Throughout 2021, we also frequently observed Mimikatz, BloodHound, Impacket, Cobalt Strike, and



Metasploit in testing—so much so that testing detections involving these tools helped all of them make it into our top 10 threats this year.

- Credential theft methods: We frequently observe credential theft during testing, which is a positive because adversaries frequently do this as well.
 However, we've noticed that testers often focus narrowly on just two approaches for credential dumping.
- Noisy discovery commands: Another pattern in our testing detections is quick execution of a series of discovery commands such as ipconfig, whoami, and others. This is in opposition to what we see from many adversaries, who often perform fewer discovery commands in a more targeted way.



Top 10 threats

The following chart illustrates the specific threats Red Canary detected most frequently across our customer environments in 2021. We ranked these threats by the percentage of customer organizations affected to prevent a single, major malware outbreak from skewing the metrics.

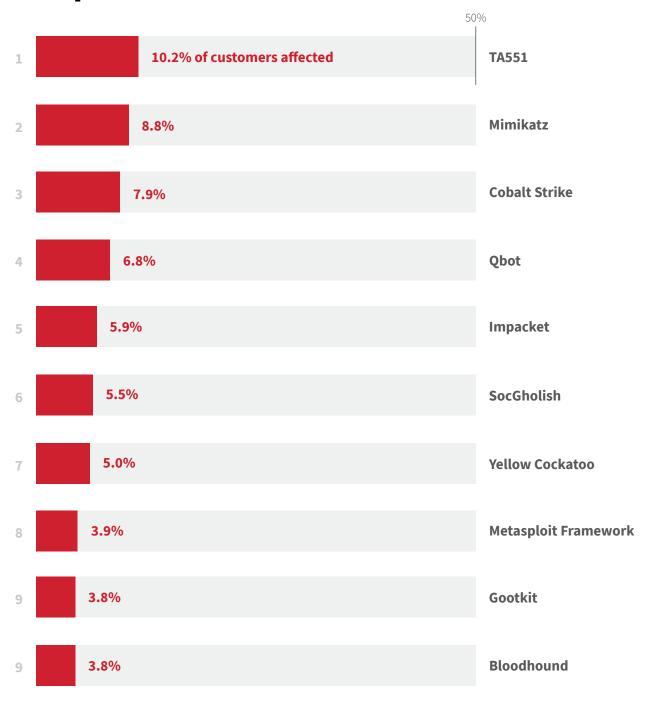
As discussed in our **Methodology section** in the full report, we chose to define "threats" broadly as malware, tools, threat groups, or activity clusters. Eight of our top 10 threats are malware families or tools, while one (TA551) is a threat group named by another team (Proofpoint) and another an activity cluster created by Red Canary (Yellow Cockatoo). This is expected because distinct malware families and tools are often more straightforward to identify, while associating activity to threat groups or activity clusters requires longer-term analysis that may extend beyond the year.

This was our second year tracking top threats. When compared to the top threats in 2020, the overall percentage of customers affected by each threat was down. For example, in 2020, 15.5 percent of customers were affected by TA551, compared to 10.2 percent of customers in 2021. While it's unclear whether this is anything more than a natural ebb and flow of activity, we suspect one factor is the overall increase in detection volume we observed in 2021.





Top threats



These are the most prevalent threats occurring in our customer environments, so we can assume they are prevalent elsewhere. The full report includes advice for responding to each threat and offers detection opportunities so you can better defend your organization. Some defenders may be able to take our detection guidance and apply it directly, while others may not. Regardless, defenders without a detection engineering function can still make use of the actionable analysis of each threat written by our Intelligence team experts.





Most Prevalent Techniques

The purpose of understanding techniques is to help you detect malicious activity in its early stages so you don't have to deal with the consequences of a serious security incident.

The following chart represents the most prevalent MITRE ATT&CK® techniques observed in confirmed threats across the Red Canary customer base in 2021. We have a library of roughly 3,000 detection analytics that we use to surface potentially malicious and suspicious activity across our customers' environments. These are mapped to corresponding MITRE ATT&CK techniques whenever possible, allowing us to associate the behaviors that comprise a confirmed threat detection with the industry standard for classifying adversary activity.





TOP TECHNIQUES

NAME	TECHNIQUE RANK (SUB-TECHNIQUE RANK)	% OF CUSTOMERS AFFECTED
T1059: Command and Scripting Interpreter	1	53.4%
• T1059.001: PowerShell	(1)	(35.0%)
 T1059.003: Windows Command Shell 	(2)	(28.1%)
T1218: Signed Binary Proxy Execution	2	34.8%
• T1218.011: Rundll32	(3)	(23.3%)
T1047: Windows Management Instrumentation	3	15.4%
T1003: Credential Dumping	4	18.3%
• T1003.001: LSASS Memory	(6)	(13.3%)
T1105: Ingress Tool Transfer	5	20.4%
T1055: Process Injection	6	21.7%
T1053: Scheduled Task/Job	7	14.7%
T1053.005: Scheduled Task	(4)	(12.2%)
T1027: Obfuscated Files or Information	8	19.4%
T1036: Masquerading	9	22.1%
• T1036.003: Rename System Utilities	(7)	(15.6%)
T1036.005: Match Legitimate Name or Location	(11)	(7.9%)
T1574: Hijack Execution Flow	10	8.4%
• T1574.001: DLL Search Order Hijacking	(5)	(7.8%)

^{*}Note: We chose not to include analysis for each technique in the PDF supplement to the report, but, as always, they're available in full on the Threat Detection Report website.





Examined holistically, the list of prevalent techniques showcased in this report suggests that if you can detect threats relatively early in the intrusion lifecycle, you're much less likely to face the consequences of a significant cyber attack. This principle has saved many of our customers from immeasurable grief over the years.

To that point, we mostly detect adversaries as they're setting the stage for later, more impactful actions. We catch them attempting to abuse native operating system utilities to execute code or bring in custom tooling. We catch them elevating their privilege levels to get deeper access to compromised systems. We catch them establishing persistence so they can maintain their presence. We catch them manipulating our customers' defensive controls to evade prevention or detection. These are necessary means to an end—whether the goal is to conduct espionage, a ransomware attack, or something else altogether. When we disrupt these means, we prevent their ends. This is precisely why exfiltration and impact techniques (e.g., ransomware) don't rank highly on our list.

If your organization is able to follow the visibility, collection, and detection guidance in this report, you can effectively improve your defense-indepth against the adversary actions that often lead to a serious incident. Of course, this is easier said than done. There are countless prerequisites to operationalizing this report, ranging from configuration challenges to developing plumbing that allows you to move telemetry from its source to its destination—whether that's a SIEM or some other aggregation point.

However, this analysis is still useful for practitioners or leaders who aren't immediately ready to operationalize it. For leaders, the most prevalent techniques can help you identify gaps as you develop a road map for improving coverage. You can assess your existing sources of collection against the ones listed in this report to inform your investments in new tools and personnel.

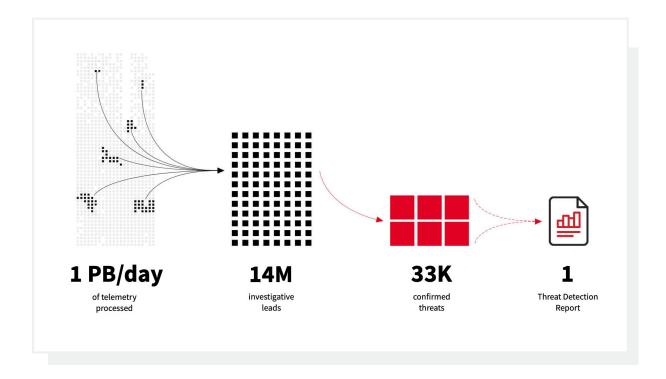
As a practitioner, you'll gain a better understanding of common adversary actions and what's likely to occur if an adversary gains access to your environment. You'll learn what malicious looks like in the form of telemetry and the many places you can look to find that telemetry. You'll gain familiarity with the principles of detection engineering by studying our detection opportunities. At a bare minimum, you and your team will be armed with hyper-relevant and easy-to-use Atomic Red Team tests that you can leverage to ensure that your existing security tooling does what you think it's supposed to do.

Learn more about our top techniques at redcanary.com/threat-detection-report



Methodology

Since 2013, Red Canary—the pioneers in managed detection and response (MDR)—has delivered high-quality threat detection to organizations of all sizes. Our platform collects as much as a petabyte of security telemetry every day and leverages a library of roughly 3,000 detection analytics to surface potential threats that are analyzed by our Cyber Incident Response Team (CIRT). Confirmed threats are tied to corresponding MITRE ATT&CK® techniques and specific threats to help our customers clearly understand what is happening in their environments. A significant portion of the Threat Detection Report is a summary of confirmed threats derived from this data.



To understand our data, you need to understand how we detect malicious and suspicious behavior in the first place. We gather telemetry from our customers' environments and feed it through a constantly evolving library of detection analytics. Our detection analytics are mapped to one or more ATT&CK techniques and sub-techniques, as appropriate. When telemetry matches the logic in one of our detection analytics, an event is generated for review by our detection engineers.

When a detection engineer determines that one or more events for a specific endpoint surpasses the threshold of suspicious or malicious behavior, they create a confirmed threat documenting the activity on that endpoint. These confirmed threats inherit the ATT&CK techniques that were mapped to the analytics that first alerted us to the malicious or suspicious behaviors.



Conclusion

Thank you for devoting your time to reading this executive summary of the 2022 Threat Detection Report. We understand there are lots of reports floating around the information security community, and we take pride in our work to muffle the noise, opting instead for curated and actionable content.

We hope the information encompassed in this executive summary entices you to dig deeper into the full report which offers insights into how to improve your security posture and what you can do if you encounter any of the most prevalent threats, trends, and techniques. We will continue to update the **Red Canary blog** with relevant resources related to the Threat Detection Report and many other valuable resources you can use to take action.

If you have any questions or concerns, or just want to chat, please feel free to reach out to us at info@redcanary.com or visit us at redcanary.com.

A full version of the report is available at redcanary.com/threat-detection-report

