Trellix

ADVANCED THREAT RESEARCH REPORT

JAN 2022

McAfee ENTERPRISE

چکیده مدیریتی

به شماره جدید گزارش Advanced Threat Research و به شرکت جدید Trellix خوش آمدید!

این اولین گزارش ماهانه Advanced Threat Research است که تحت نام شرکت جدید Trellix منتشر می‌شود. شرکت Trellix از ادغام دو شرکت بزرگ امنیتی McAfee و FireEye تشکیل شده است.

اکنون که سال میلادی جدید ۲۰۲۲ را آغاز کرده‌ایم، مروری بر روند تهدیدات سایبری در یک سال گذشته و به ویژه ماه‌های پایانی سال ۲۰۲۱ خواهیم داشت.

در ماه‌های پایانی سال ۲۰۲۱، نقطه ضعف Log4j نه تنها عناوین اخبار را تحت الشعاع قرار داد، بلکه توان واکنش گروه‌های امنیتی را به چالش کشید. Log4j به عنوان حادترین ضعف امنیتی دهه‌های اخیر توصیف شده است. هر محصولی که کتابخانه Log4j را بکار گرفته بود، تحت تاثیر این ضعف امنیتی قرار داشت، از برنامه‌های کاربردی سازمان‌ها تا خدمات ابری شرکت‌های بزرگ بین المللی. گزارش مشروحی از این نقطه ضعف در این شماره ارائه شده است.

در اواخر سال ۲۰۲۱، برخی گروه‌های گرداننده باج‌افزار متلاشی شدند، دوباره فعال شدند، تغییر نام دادند و یا سرمایه جدید برای توسعه جذب کردند ولی در هر حال، همچنان یک تهدید رایج و مخرب علیه کاربران و سازمان‌های مختلف باقی مانده‌اند.

کارزارهای مرتبط با «تهدیدات مستمر و پیشرفته» (Advanced Persistent Threat - به اختصار APT) که در شش ماه گذشته فعال بوده و با روش‌ها و ابزارهای مختلف، هر کدام کشورها و کاربران خاصی را در جهان مورد هدف قرار داده‌اند، مورد بررسی و تحقیق قرار گرفته‌اند.

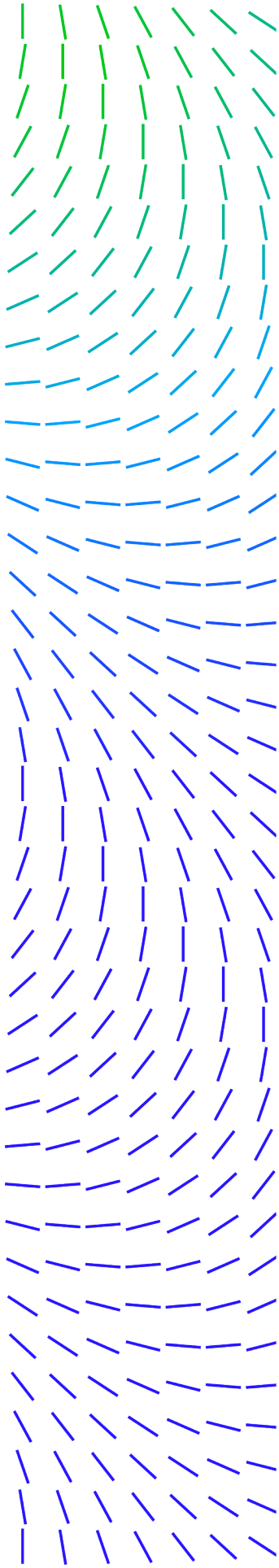
در این گزارش به روش مخرب «کسب روزی از زمین» (Living off the Land - به اختصار LotL) پرداخته شده و آمار مفیدی ارائه گردیده است. در روش LotL مجرمان سایبری از توابع و برنامه‌های عادی و سالم در سیستم قربانی برای انجام عملیات مخرب خود بر روی آن سیستم استفاده می‌کنند. این روش برای مخفی ماندن عملیات مخرب و شناسایی نشدن حملات بسیار موثر است.

همچنین در بخشی از این گزارش به نقاط ضعف کشف شده که از سوی تولیدکنندگان و سازندگان انواع محصولات اعلام و اصلاحیه‌هایی برای ترمیم آنها منتشر کرده‌اند، پرداخته شده ولی فارق از درجه‌بندی رسمی این نقاط ضعف (نظیر درجه CVSS و یا رتبه OWASP)، فقط بر اساس تجربه و شناخت کارشناسان Trellix برای شما اولویت‌بندی و توضیح داده شده‌اند.

در پایان گزارش نیز انواع تهدیدات سایبری بر اساس نوع بدافزار، منطقه فعالیت، نوع قربانیان و روش‌های بکار گرفته شده، دسته‌بندی و میزان فراوانی هر یک با نمودارهای رنگین نمایش داده شده‌اند.

گروه تحقیق و توسعه
شرکت مهندسی شبکه گستر - اولین شرکت فعال در حوزه ضدویروس در ایران
www.shabakeh.net

TABLE OF CONTENTS



In our new company's first threat report, we acknowledge the Log4j issue that dominated not only headlines, but the focus of defenders and enterprise security teams.

LETTER FROM OUR CHIEF SCIENTIST

Welcome to our new threat report and our new company.

As we look ahead in this new year, we must acknowledge a threatscape that left us all exhausted from a particularly challenging end to 2021. In our new company's first threat report, we acknowledge the Log4j issue that dominated not only headlines, but the focus of defenders and enterprise security teams. We also look back at the third and fourth quarters of 2021, but let's first detail our wealth of resources available to help you combat Log4j.

Fundamentally, as more details of the Log4j threat emerge, it's imperative to connect to our research and updated resources for help. Beyond the product status, we continuously monitor for any active campaigns leveraging this vulnerability and detailing the coverage status for the new payloads.

When details of the Log4j vulnerability appeared we very quickly responded with the availability of network-based signatures and a write-up of the vulnerability. We quickly followed up with additional assets detailed in this report.

To understand more about current Log4j threat activity, as well as, other prevalent threats, please see our valuable threat dashboard.

In addition, please check out our Trellix Threat Labs blogs featuring our latest threat content, videos and links to the security bulletin.

Of course, Log4j isn't the only threat to your enterprise's security. This report also spotlights the looming shadow and disruption of ransomware, and other prevalent threats and attacks observed in the wild.

Happy 2022 and welcome to a new company.

—Raj Samani

Fellow and Chief Scientist

Twitter: @Raj_Samani

Writing and Research

Alfred Alvarado
Christiaan Beek
John Fokker
Douglas McKee
Tim Polzer
Steve Povolny
Raj Samani
Leandro Velasco

LOG4J: THE MEMORY THAT KNEW TOO MUCH

In what is becoming a threatening tradition, Log4j, a new vulnerability affecting a widely used Log4j library was released just in time for the holidays. What has been described as the most serious cybersecurity flaw in decades called Trellix and the cybersecurity industry to action in the fourth quarter of 2021. The Log4j vulnerability threatened a potentially massive impact on any product which has integrated the Log4j library into its applications and websites including products and services from Apple iCloud, Steam, Samsung Cloud storage and many others.

Our team has been closely tracking Log4j since its discovery. We released a network signature KB95088 for customers leveraging Network Security Platform (NSP). The signature detects attempts to exploit CVE-2021-44228 over LDAP. This signature may be expanded to include other protocols or services, and additional signatures may be released to complement coverage.

Log4j Timeline

Here's a quick timeline of Log4j and our research:

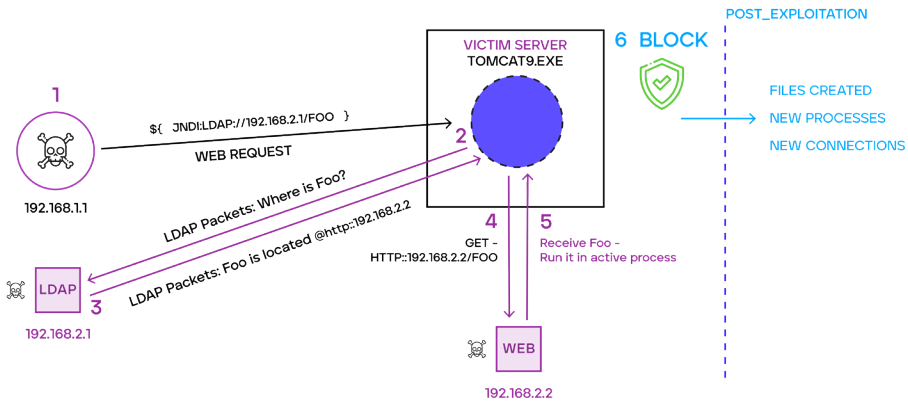
- **December 9** – The Log4j vulnerability (CVE-2021-44228) was released on Twitter along with a POC on Github for the Apache Log4j logging library. The bug was originally disclosed to Apache on November 24.
- **December 10** – Steve Povolny and Douglas McKee posted a Log4j blog with an overview of our immediate findings. Our initial goal was to determine the ease of exploitation using the public PoC, which we have reproduced and confirmed. This was done using the public Docker container, and a client-server architecture leveraging both LDAP and RMI, along with marshalsec to exploit Log4j version 2.14.1.
- **December 14** – Log4j version 1.2's vulnerability to similar attacks through the JMSAppender component was confirmed and CVE-2021-4104 issued.
- **December 18** – A new denial of service (DOS) vulnerability CVE-2021-45105 was discovered affecting versions 2.0-alpha1 through 2.16.0 of Log4j.

Consult our Trellix Threat Labs blogs and threats dashboard for our latest research on defending against Log4j. Our team gathers and analyzes information from multiple open and closed sources before disseminating intelligence reports.

Log4j Attack

Our team quicky researched and outlined what happens in the execution of a common web-based Log4j attack:

LOG4J FLOW OF EXECUTION



- Step 1 – An attacker sends a specially crafted string to the web server hosting the vulnerable application. This string, as we have seen, can be obfuscated to bypass network-based signatures.
- Step 2 – The application proceeds to deobfuscate this string to load it in memory. Once loaded into memory, the application initiates a LDAP connection to request the malicious class location's address.
- Step 3 – The attacker-controlled LDAP server responds with the location of the malicious Class file by indicating the HTTP URL address of where it's hosted.
- Step 4 – The vulnerable application initiates a download for the malicious class file.
- Step 5 – The vulnerable application will load and run the malicious class file from Step 4.

Trellix ATR Log4j Defenses

To protect an environment against attacks like Log4j, a layered strategy comprised of network security coupled by targeted endpoint memory scans allows defenders to effectively detect and prevent the attack execution flow against vulnerable systems exposed via network vectors. Our ENS Expert Rules and Custom Scan reactions are designed to enable defenders with such capabilities so they can apply precise countermeasure against these emerging threats.

CISA.gov also provides a Log4j scanner to help organizations identify potentially vulnerable web services affected by the Log4j vulnerabilities.

RANSOMWARE

In the third quarter of 2021, high-profile ransomware groups disappeared, reappeared, reinvented, and even attempted to rebrand, while remaining relevant and prevalent as a popular and potentially devastating threat against an increasing spectrum of sectors.

Even though ransomware activity was denounced and banned from numerous cybercriminal forums in Q2 2021, our team has observed activity among the same threat actors on several forums using alternate personas.

Trellix Aids In Ransomware Arrests and Ransom Seisures

In December 2021, Trellix provided research that assisted FBI and Europol in the arrest of REvil affiliates and the seizure of $2 million in ransom.

Notable Q3 2021 ransomware trends and campaigns included:

- BlackMatter – This ransomware threat, discovered near the end of July 2021, started with a strong group of attacks that threatened to reveal proprietary business data of U.S. based agricultural supply-chain company New Cooperative. New Cooperative reported supply chain management capabilities and animal feeding schedules were locked and estimated that 40 percent of grain production in the U.S. could be negatively affected. While BlackMatter claimed to utilize the best parts of other malware, such as GandCrab, LockBit and DarkSide, we seriously doubt the campaign is being run by a new group of developers. BlackMatter malware has too much in common with the DarkSide malware associated with the Colonial Pipeline attack.
- We released our belief that the Groove Gang is associated with the Babuk gang, either as a former affiliate or subgroup.
- REvil/Sodinokibi claimed responsibility for successfully infecting more than 1 million users through a ransomware attack on managed service software provider Kaseya VSA. REvil's reported ransom demand of $70 million was the largest publicly known ransom amount to date. The results of the attack included the forced closing of hundreds of supermarket stores for several days.
- LockBit 2.0 surfaced in July 2021 and eventually listed more than 200 victims on its data-leak site.

Government Response to Ransomware Threats

In Q3, the U.S. government initiated a proactive campaign to reduce ransomware's prevalence with the launch of StopRansomware.gov hub offering rewards up to $10 million for information identifying or locating state-sponsored threat actors involved in cyber activities against critical U.S. infrastructure.

For more on how these ransomware and new campaigns could threaten enterprise in the coming months, see our Trellix 2022 Threat Predictions.

Trellix Ransomware Research

To help enterprises better understand and defend against ransomware attacks in the threatscape, our team presents research and findings into the prevalence of a wide variety of ransomware threats including families, techniques, countries, sectors, and vectors.

Ransomware Family Detections

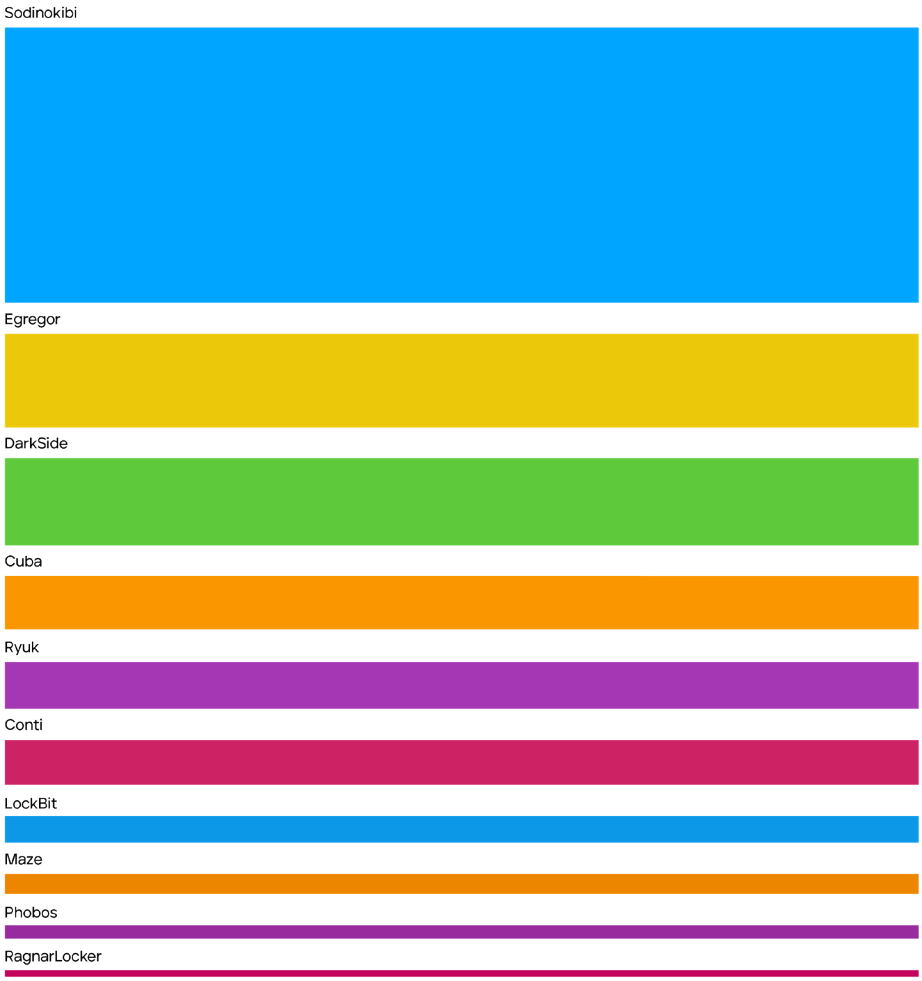


Figure 1. Sodinokibi (41%) was the most prevalent Ransomware Family detected in Q3 2021, followed by DarkSide (14%) and Egregor (13%).

See Ransomware Client Countries, Customer Sectors, and MITRE ATT&CK Techniques below.

ATTACK PATTERN TECHNIQUES

The team tracks and monitors APT campaigns and its associated indicators and techniques. Our team research reflects APT Threat Actors, Tools, Client Countries, Customer Sectors and MITRE ATT&CK Techniques from Q3 of 2021.

APT Threat Actors

Figure 2. APT41 (24%) and APT29 (22%) were the most prevalent APT Threat Actors in Q3 2021 and responsible for nearly half of APT activity monitored.

APT Tools

The team has identified indicators of compromise that belong to tracked APT campaigns with the following tools associated with them. APT groups are known for using common system utilities to bypass security controls and perform their operations:

Figure 3. Cobalt Strike (34%) was the most prevalent APT tool detected in Q3 of 2021 followed by Mimikatz (27%), Net.exe (26%), and PsExec (20%). Cobalt Strike attack suite abused by nation state actors was detected in over a third of APT activity.

See APT Client Countries, Customer Sectors, and MITRE ATT&CK Techniques below.

ADVANCED THREAT RESEARCH

Our team tracked threat categories in the third quarter of 2021. The research reflects percentages of detections in the type of ATR Malware used, Client Countries, Customer Sectors, MITRE ATT&CK techniques used in attacks and industry sectors.

ATR Tool Threats

Figure 4. Formbook (36%), Remcos RAT (24%), and LokiBot (19%) amounted to almost 80% of ATR Tool Threats detections in Q3 2021.

See ATR Client Countries, Customer Sectors, and MITRE ATT&CK Techniques below.

THREATS TO COUNTRIES, CONTINENTS, SECTORS AND VECTORS

Countries and Continents: Q3 2021

Notable country and continent increases of publicly reported incidents in the third quarter of 2021 include:

- North America recorded the most incidents among continents but saw a 12% decrease from Q2 to Q3 2021.
- The United States experienced the most reported incidents in Q3 2021, but incidents decreased 9% from Q2 2021.
- France recorded the highest increase (400%) of incidents reported in Q3 2021.
- Russia experienced the largest decrease (-79%) of Q3 2021 incidents compared to Q2 2021.

Attack Sectors: Q3 2021

Notable publicly reported incidents against sectors in the third quarter of 2022 include:

- Multiple Industries (28%) were targeted most often, followed by Healthcare (17%), and Public (15%).
- Notable sector increases from Q2 to Q3 2021 include Finance/ Insurance (21%) and Healthcare (7%).

Attack Vectors: Q3 2021

Notable publicly reported incidents against vectors in the third quarter of 2021 include:

- Malware was the technique used most often in reported incidents in Q3 2021 but reported malware incidents decreased 24% compared to Q2 2021.
- Sector increases from Q2 to Q3 2021 include Distributed Denial of Service (112%) and Targeted Attack (55%).

LIVING OFF THE LAND

Cybercriminals use Living off the Land (LotL) techniques that use legitimate software and functions in a system to perform malicious actions on that system. Based on third quarter events, Trellix has identified a trend in tools used by adversaries who are attempting to remain undetected. While state-sponsored threat groups and larger criminal threat groups have resources to develop tools in house, many turn to binaries and administratively installed software that may already be present on a target system to carry out distinct phases of an attack.

To identify native binaries or administratively used software during a reconnaissance phase for a high-profile target, adversaries may gather information on technologies used from job postings, customer testimonials advertised by vendors, or from an inside accomplice.

Native OS Binaries		Comments
Powershell (41.53%)	T1059.001	Powershell is often used to execute scripts and Powershell commands.
Windows Command Shell (CMD) (40.40%)	T1059.003	Windows Command Shell is the primary CLI utility for Windows and is often used to execute files and commands in an alternate data stream.
Rundll32 (16.96%)	T1218.011, T1564.004	Rundll32 can be used to execute local DLL files, DLL files from a share, DLL files obtained from the internet and alternate data streams.
WMIC (12.87%)	T1218, 1564.004	WMIC is a command line interface for WMI and may be used by adversaries to execute commands or vpayloads locally, in alternate data streams or on a remote system.
Excel (12.30%)	T1105	While not natively installed, many systems contain spread sheet software, adversaries may send attachments to user that contain malicious code or scripts that, when executed, may be used to retrieve payloads from a remote location.
Schtasks (11.70%)	T1053.005	An adversary may schedule tasks that maintain persistence, execute additional malware, or perform automated tasks.
Regsvr32 (10.53%)	T1218.010	Regsvr32 may be used by adversaries to register dll files, execute malicious code and bypass application whitelisting.
MSHTA (8.78%)	T1218.005	MSHTA may be used by adversaries to execute JavaScript, JScript and VBScript files that may be hidden in HTA files locally and in alternate data streams or retrieved from a remote location.
Certutil (4.68%)	T1105, 1564.004, T1027	Windows command utility is used to obtain certificate authority information and configure certificate services. Alternatively, adversaries may use certutil to gather remote tools and content, encode and decode files as well as access alternate data streams.
Net.exe (4.68%)	T1087 & Sub-techniques	Windows command line utility that allows an adversary to perform reconnaissance tasks such as identifying users, network, and services functionality of a victim machine.

Reg.exe (4.10%)	1003.002, 1564.004		Reg.exe may be used by adversaries to add, modify, delete, and export registry values which may be saved to alternative data streams. Additionally, reg. exe may be used to dump credentials from a SAM file.

Administrative Tools			Comments
Remote Services (15.21%)	T1021.001, T1021.004, T1021.005	AnyDesk ConnectWise Control RDP UltraVNC PuTTY WinSCP	Remote services tools, both native to Windows and third-party software may be used by adversaries along with valid accounts to gain access to a machine or infrastructure remotely, perform ingress transfer of tools and malware as well as exfiltrate data.
Archive Utilities (4.68%)	T1560.001	7-Zip WinRAR WinZip	Adversaries may use archive utilities to compress collected data in preparation to be exfiltrated as well as to decompress files and executables.
PsExec (4.68%)	T1569.002		PsExec is a tool used to execute commands and programs on a remote system.
BITSAdmin (2.93%)	T1105, T1218, T1564.004		BiTSAdmin is often used to maintain persistence, clean up artifacts and for invoking additional actions once a set criterion is met.
fodhelper.exe (1.17%)	T1548.002		Fodhelper.exe is a Windows utility that may be used by adversaries to run malicious files with elevated privileges on a victim machine.
ADFind (.59%)	T1016, T1018, T1069 & Sub-Techniques, T1087 & Sub-techniques, T1482		Command line utility that may be used by adversaries to discover active directory information such as Domain Trusts, Permission Groups, Remote Systems and Network Configurations.

BUG REPORT

Bugs on the Windshield

(Douglas McKee, Principal Engineer and Senior Security Researcher, and other bloggers track and analyze vulnerabilities in the monthly Bug Report.)

As the world attempted to drive 100 mph through the end of 2021, many "bugs" were splattered on our proverbial windshield. Some cleaned off easily, while some left a lasting stain. The team tracks and evaluates new vulnerabilities, aka bugs, each month upon their release and reports what we "feel" are going to be the most important. That's right, not CVSS score or OWASP ranking, but an old-fashioned gut check based on years of experience.

A Moment of Reflection

Looking at our top reported bugs from the last several months, a few stand out from the rest. Apache had a rough year with both its webserver (CVE-2021-41773) and Log4j component (CVE-2021-44228) hit hard with impactful bugs. Palo Alto also deserves an honorable mention with a bug found in their Global Protect VPN (CVE-2021-3064), having a unique impact during a global pandemic. Hold up, let's be real for a minute. The Apache Log4j vulnerability deserves more than an "impactful" rating as it is by far the biggest bug of 2021 and has potential to defend its title, for years to come. If you live under a rock and haven't heard of these I highly suggest reading our December Bug Report. Don't forget to check back every month for the latest and greatest vulnerability news.

So, what makes these bugs the worst of the bunch? Simply put, they can be leveraged remotely, without authentication on tools that sit on the edge of your network. These bugs can be the initial entry point to a network without requiring an attacker to "phish their wish," but instead be a gateway to a larger scale attack.

If your CISO likes playing Russian roulette and says you can only patch one product, we recommend prioritizing the Log4j vulnerability hands down as it is easy to execute and has seen active exploitation across malicious actors. Although the Palo Alto VPN flaw is serious, and VPNs have seen an increase in exploitation since 2020, it takes a back seat to Log4J and the other Apache vulnerabilities since it affects an older version of the VPN software and has yet to see active exploitation in the wild.

Termites

Some bugs, like termites, can slip through the cracks, but have a devastating effect.

A Microsoft Windows Installer Service local privilege escalation bug labeled as CVE-2021-41379, was the proverbial termite of November. Microsoft disclosed the bug as requiring local access and allegedly fixed it with an official patch, but the strategy backfired when the patch didn't work as expected.

With a failed patch and a publicly available POC, bad actors did not wait to compile this into their playbooks, as seen in Insights. Compounding the issue, our team has seen weaponized versions of this exploit being sold on the dark web.

However, if you're a monthly follower of the Bug Report, you know we always leave you with the Gold Standard and why should we stop now?

ADDITIONAL CUSTOMER SECTORS, CLIENT COUNTRIES AND MITRE ATT&CK TECHNIQUES

Ransomware Client Countries

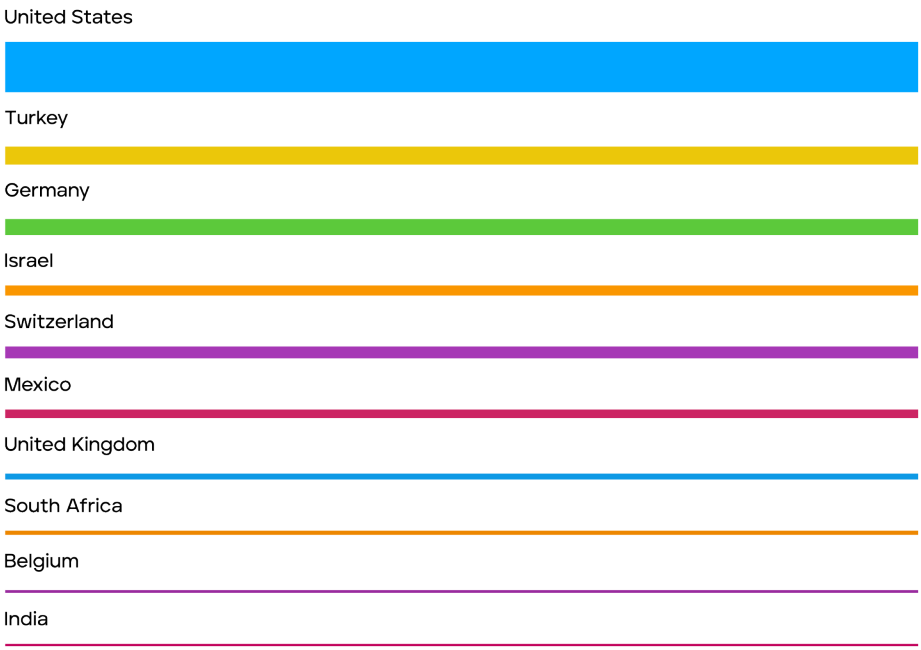


Figure 5. Clients based in the United States accounted for more than one third of the total Ransomware detections in Q3 2021.

Ransomware Customer Sectors

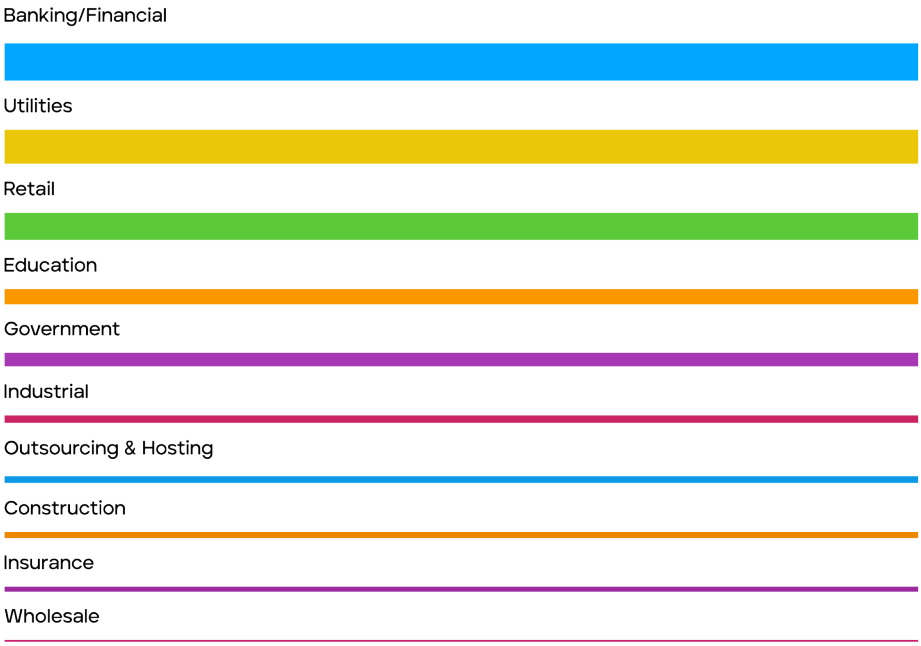


Figure 6. Banking/Financial (22%), Utilities (20%), and Retail (16%) accounted for almost 60% of total Ransomware Customer detections in Q3 2021.

Ransomware MITRE ATT&CK Techniques

Figure 7. Data Entry (2.6%), File and Directory Discovery (2.5%), and Obfuscated Files or Information (2.4%) topped the Ransomware MITRE ATT&CK Techniques detected in Q3 2021.

APT Client Countries

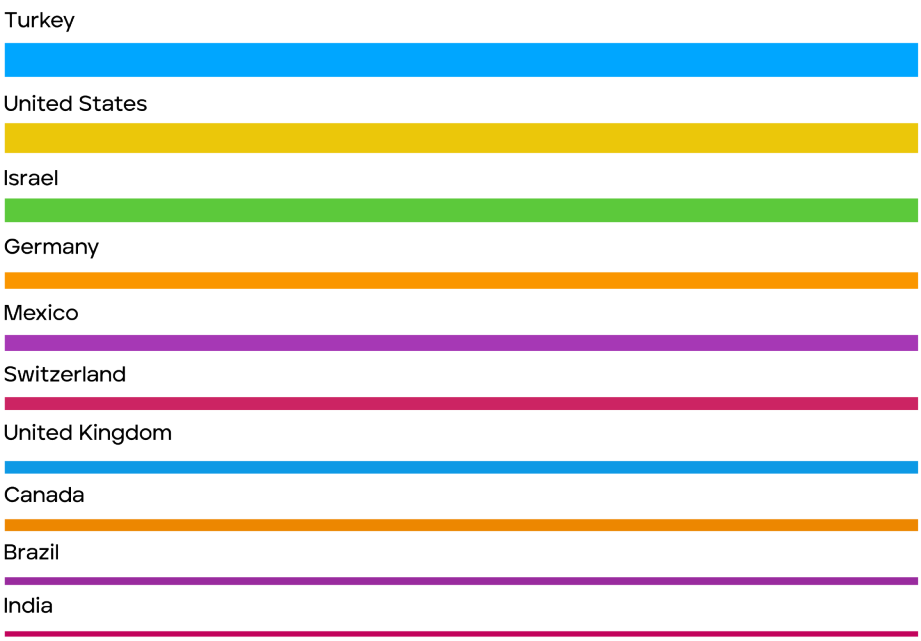


Figure 8. Client detections of Attack Pattern Techniques in Turkey accounted for 17% of total detections in Q3 of 2021, followed by the United States (15%) and Israel (12%).

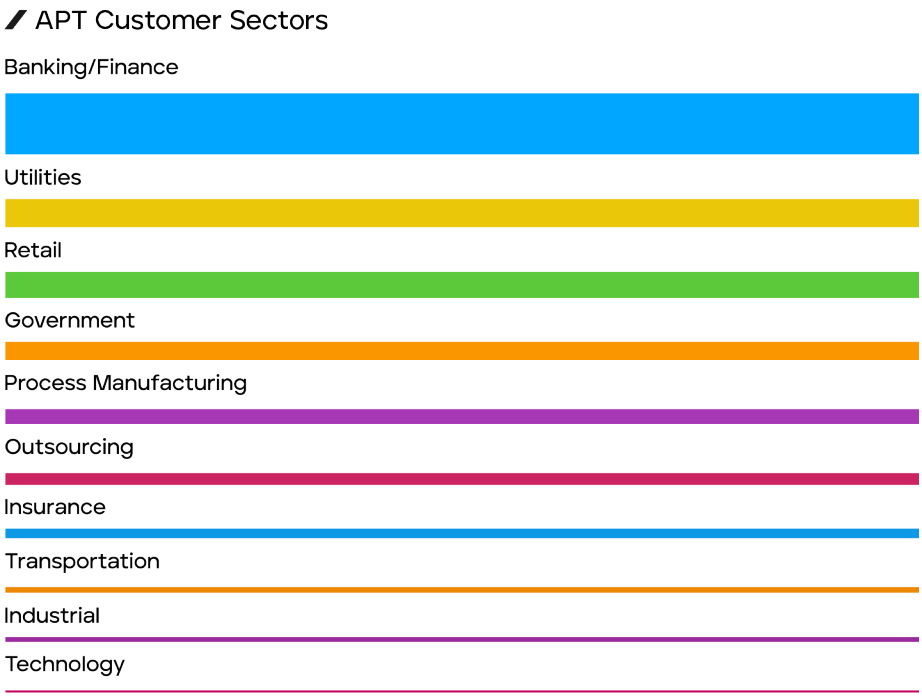


Figure 9. The most APT detections in Q3 2021 occurred in the Banking/Financial sector (37%) followed by Utilities (17%), Retail (16%), and Government (11%).

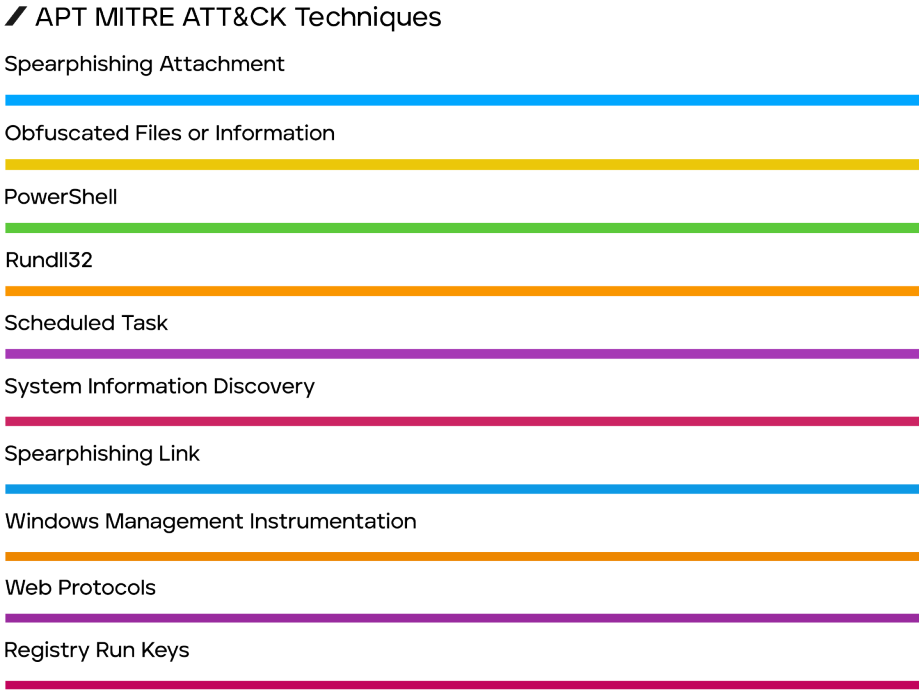


Figure 10. Spearphishing Attachment (16.8%), Obfuscated Files or Information (16.7%), and PowerShell (16%) were the most prevalent APT MITRE ATT&CK Techniques detected in Q3 of 2021.

ATR Client Countries

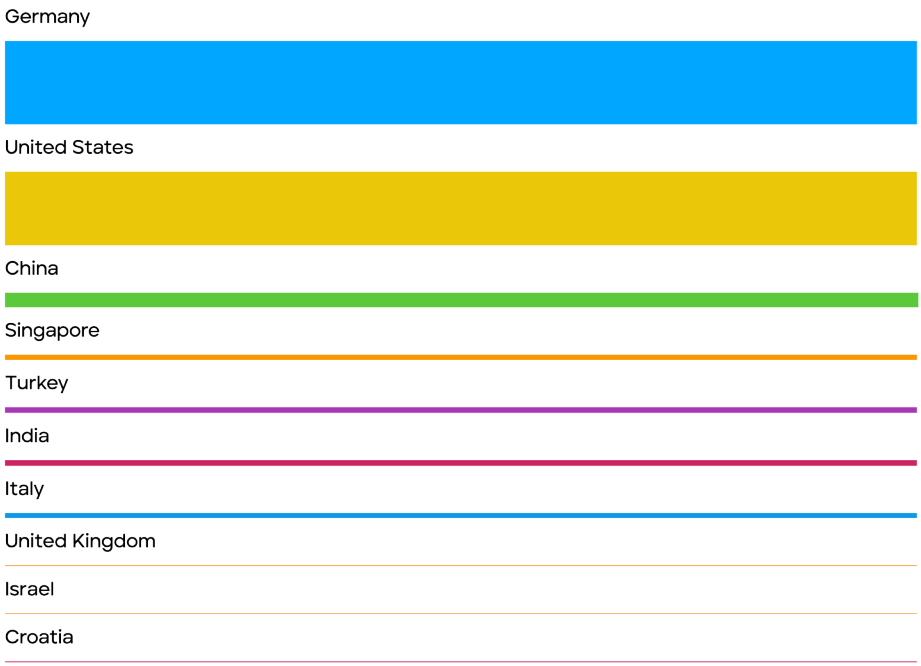


Figure 11. More than half of total ATR tool threats detected in Q3 2021 were in Germany (32%) and the United States (28%).

ATR Customer Sectors

Figure 12. Banking/Financial ATR customer sector detections (45%) were most prevalent by far in Q3 2021.

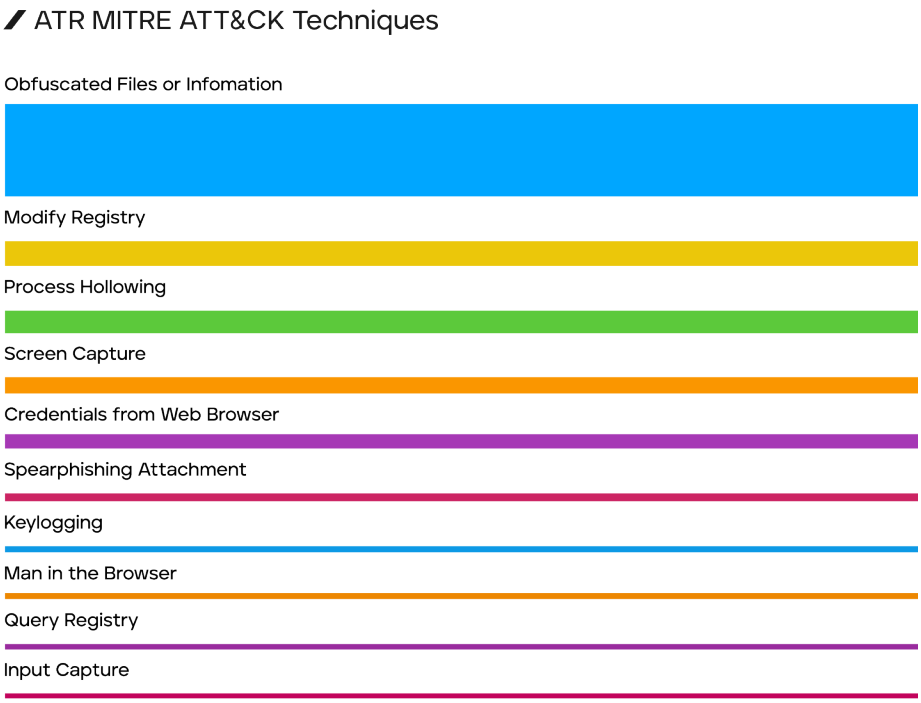


Figure 13. Obfuscated Files or Information amounted to 5% of all ATR MITRE ATT&CK Technique detections in Q3 2021.

RESOURCES

To keep track of the latest threats and research, see our team's resources:

Threat Center—Today's most impactful threats have been identified by our team.

Twitter:

Trellix Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

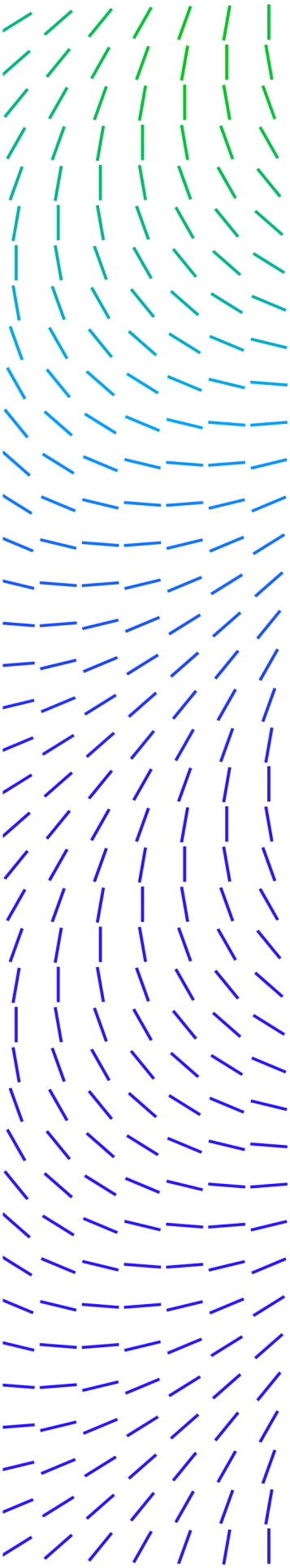
Douglas McKee

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers. More at www.trellix.com.

Trellix Threat Labs

Subscribe to Receive Our Threat Information



Trellix

6220 American Center Drive,
San Jose, CA 95002