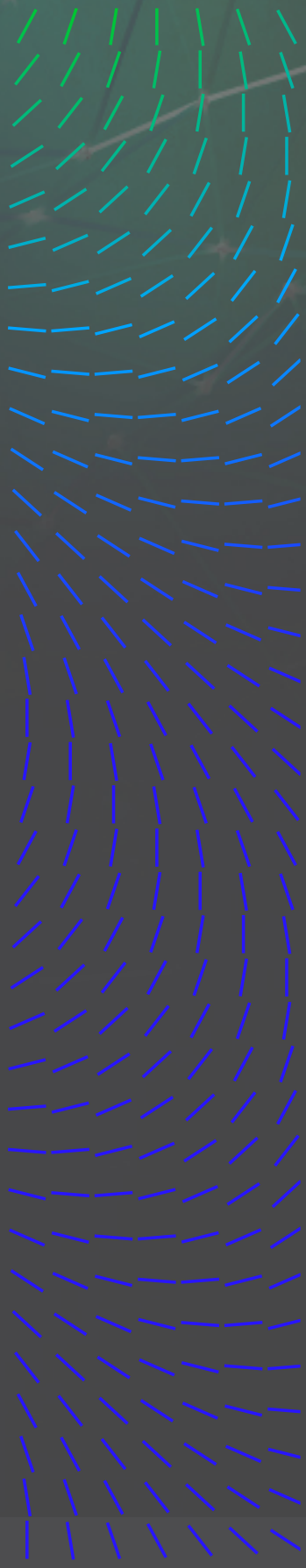
Presented by

Trellix ADVANCED RESEARCH CENTER

THE THREAT REPORT

February 2023

TABLE OF CONTENTS



Q4 2022 THREAT OVERVIEW

Threat actors remained formidable adversaries during the final months of 2022, and the Trellix Advanced Research Center countered by adding even more threat intelligence resources to our team of hundreds of elite security analysts and researchers.

"In other words: we've taken our threat intelligence to the next level. To bring calm to your SecOps chaos with simpler security. To make your security outcomes better with less stress. Threats continue to evolve. And so can you."

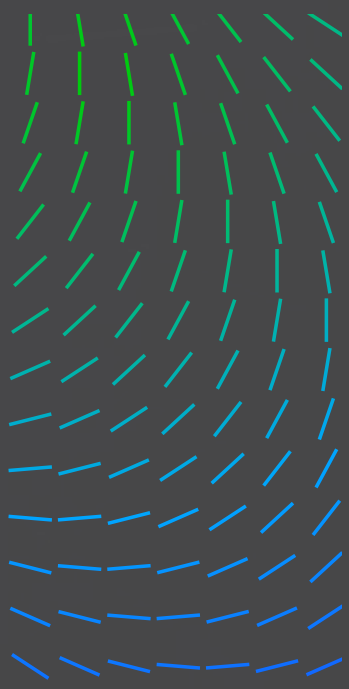
In this report, we share our industry-leading lineup of which threat actors, families, campaigns, and favorite techniques were prevalent during the last quarter. But there's more. We've also expanded our sources to glean data from ransomware leak sites, and security industry reports. And as Trellix resources grow, so do the categories of threat research including new content covering Network Security, Cloud Incidents, Endpoint Incidents, and Security Operations.

Since our last threat report, the Advanced Research Center engaged with research and findings across the globe including Gamaredon's link to greatly increased cyberattacks targeting Ukraine in Q4, patching 61,000 vulnerable open-source projects, and releasing insights into the new year's novel attacks with its 2023 Threat Predictions.

The following overview gleaned from these threat report improvements are examples of how the Advanced Research Center works to better enable customers and the security industry to realize better threat outcomes:

Ransomware

- Breakout research on LockBit 3.0's prominence as Q4's most impactful ransomware group
- Ransomware's continued prevalence across the globe, especially in the United States
- Ransomware targeting of sectors including Industrial Goods & Services



Nation States

- Nation states targeting sectors including Government and Transportation & Shipping
- Companies based in the United States impacted by nation-state activity

Living Off the Land (LOLBIN)

- Expanded insights into Cobalt Strike in the wild using Trellix Advanced Research Center's hunting methodology
- The high number of Cobalt Strike Team servers hosted at Chinese Cloud providers
- Windows Command Shell accounting for almost half of the top-10 most prevalent OS Binaries used in the reported campaigns

Threat Actors

- China, North Korea, and Russia topping the list of prevalent threat-actor countries

Email Security Trends

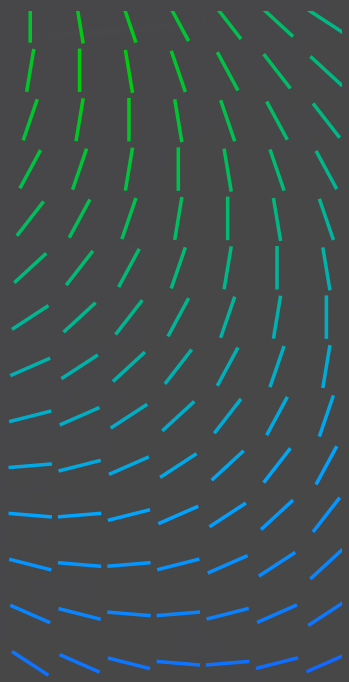
- The highly increased volume of malicious emails in Arab countries observed during the global football tournament
- Insights into phishing and vishing campaigns including impersonation techniques, and popular company themes used by vishing

Network Security

- The quarter's most impactful, significant, and relevant attacks, WebShells, tools, and techniques

Security Operations Telemetry Powered by Trellix XDR

- Prevalent security alerts, exploits, log sources, and MITRE ATT&CK Techniques
- Cloud incidents
- Techniques and detections for Azure, AWS, and GCP
- Top techniques and detections



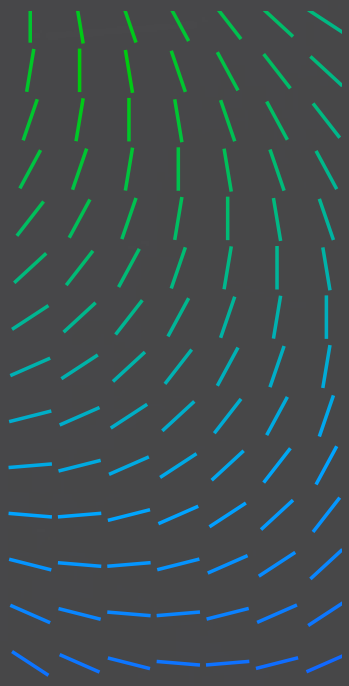
LETTER FROM OUR HEAD OF THREAT INTELLIGENCE

Our Advanced Research Center team is excited to share the first Threat Report of Q4 2022 data, closing off the year. You will find this report continues to evolve with the inclusion of new data from our product sensor array combined with insights from other data sources such as ransomware leak sites and our infrastructure tracking in the wild. At Trellix, we remain tenacious in our mission to protect our customers against evil, as threat actors and their motivation never stop and become more multifaceted. The need for global threat intelligence grows as the geopolitical and economic outlook remain complicated with a greater level of uncertainty.

On a global level the economic uncertainty created by the war in Ukraine has provoked a massive energy price shock not seen since the 1970s which is taking a heavy toll on the world economy. The return of war in Europe has also served as a wake-up call for those questioning the EU's approach to security and defense and its ability to defend its interests, particularly in cyberspace. The U.S. administration also recognized the need to address geostrategic competition, protect critical infrastructure, and combat foreign information manipulation and interference. SolarWinds, Hafnium, Ukraine and other events have prompted bipartisan action from the administration and Congress on new security standards and funding that significantly builds on the nation's commitments and the work of past U.S. governments. So how is this uncertainty impacting the cybersecurity of our businesses, our public and private institutions and democratic values?

In the last quarter, our team saw cyber as statecraft in the areas of espionage, warfare and disinformation actively used in service of political, economic, and territorial ambitions. The war in Ukraine has also seen the emergence of new forms of cyberattacks, and hacktivists became savvier and more emboldened to deface sites, leak information and execute DDoS attacks. Meanwhile traditional forms of cyberattacks continue. Socially engineered ploys to deceive and manipulate individuals into divulging confidential or personal information, such as phishing, remain prevalent.

Ransomware has continued to plague many organizations worldwide. Just like we observed during the COVID-19 pandemic, cyber criminals quick to profit from a time of crisis and uncertainty. As the threat landscape evolves, so will our research. Our mission will remain wholly focused on always improving the efficacy of our products and delivering actionable intelligence to our stakeholders to ensure they can protect what matters most. In this report, you will see how



important the work we do is to every member of the Advanced Research Center. There is not a researcher or expert on our team that doesn't approach each and every project we do with care and heart.

Let us know what you think of this extended report, and if there are areas you'd like to see our team dive into by reaching out to me or our team @TrellixARC on Twitter. We also look forward to seeing many of you at RSA in San Francisco in April.

John Fokker
Head of Threat Intelligence

METHODOLOGY

Trellix's backend systems provide telemetry that we use as input for our quarterly threat reports. We combine our telemetry with open-source intelligence around threats and our own investigations into prevalent threats like ransomware, nation-state activity, etc.

When we talk about telemetry, we talk about detections, not infections. A detection is recorded when a file, URL, IP address or other indicator is detected by one of our products and reported back to us.

For instance, we are aware a growing number of organizations are using efficacy testing frameworks that deploy real malware samples. This usage will show up as a detection but is definitely not an infection.

The process to analyze and filter false positives in the telemetry is in constant development, which can result in new threat categories when compared to previous editions.

New threat categories will also be added as more Trellix organization teams contribute to this quarterly report.

Privacy of our customers is key. It's important when it comes down to telemetry and mapping that out to the sectors and countries of our customers. Client-bases per country differ and numbers could show increases that require a deeper look into the data. An example: The Telecom sector often scores high in our data. It doesn't necessarily mean this sector is highly targeted. The Telecom sector contains ISP providers as well that own IP-address spaces that can be bought by companies. What does this mean? Submissions from the IP-address

space of the ISP are showing up as Telecom detections but could be from ISP clients that are operating in a different sector.

RANSOMWARE Q4 2022

In this section we provide the various insights we have collected about ransomware groups activity. This information is gathered from multiple sources to have a better picture of the threat landscape and reduce the observation bias and help us determine which ransomware family was most impactful in Q4 2022. The first source is a quantitative source and depicts the ransomware campaigns statistics extracted from the correlation of ransomware IOCs and Trellix customers telemetry. The second is a qualitative source and shows the analysis of the various reports published by the security industry that are vetted, parsed, and analyzed by the Threat Intelligence Group. Finally, the third source, is a new category, consist of the set of ransomware victims reports that are scraped from the various ransomware groups "leak sites," normalized, enriched, and lastly analyzed to provide an anonymized version of the results.

By providing these different points of view we aim to provide many pieces of the puzzle that comprise the current threat landscape. None of them is sufficient as they carry their own limitations. Nobody has access to all the logs of all the systems connected to the internet, not all security incidents are reported, and not all victims are extorted and included in the leak sites. However, the combination of the different views can lead to better understanding of the various threats, while reducing our own blind spots

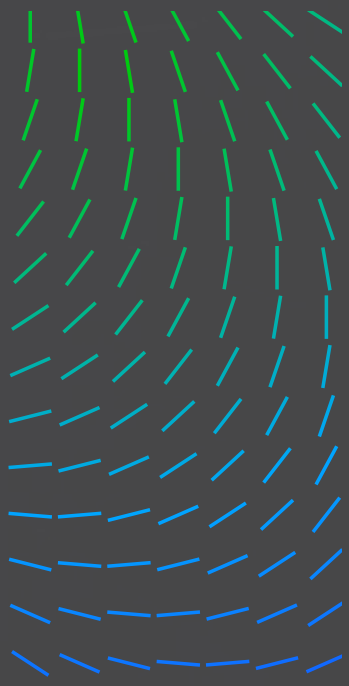
An informed judgment results from combining quantitative and qualitative data from sources while taking into account potential drawbacks and blind spots.

Ransomware Highlights from Q4 2022

Most Impactful Ransomware Group for Q4: LockBit 3.0

Through observation of Trellix's various sources, we can conclude that LockBit 3.0 was the most impactful ransomware group in Q4 2022. LockBit 3.0's significant standing is based on the following characteristics:

3RD LockBit 3.0 ranked third among the most prevalent ransomware groups in the quarter according to the ransomware telemetry analysis gleaned from the Trellix's global sensors.



2ND LockBit 3.0 ranked second – alongside Cuba Ransomware – among the most reported ransomware groups by the security industry, as analyzed by the various campaigns collected by the Threat Intelligence Group.

1ST The LockBit 3.0 leak site reported the most victims among ransomware groups in the quarter. Making LockBit the most eager to pressure their victims through naming and shaming.

Here are more LockBit categories and findings from Q4 2022:

SECTORS AFFECTED BY LOCKBIT 3.0 Q4 2022

29%

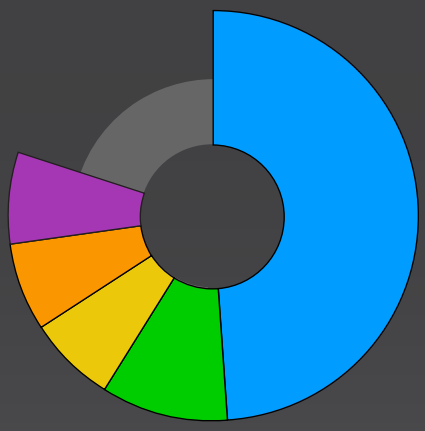
Industrial Goods & Services was the sector most affected by LockBit 3.0 in Q4 2022 according to the LockBit3 victim leak site.

- Industrial Goods & Services
- Retail
- Technology
- Healthcare
- Construction & Materials
- Personal & Household Goods
- Government

COMPANY COUNTRIES AFFECTED BY LOCKBIT 3.0 Q4 2022

49%

United States companies were most affected (49%) by LockBit 3.0 in Q4 2022, followed by companies in the United Kingdom according to the LockBit 3.0 victim leak site.



- United States
- United Kingdom
- Canada
- France
- Brazil

LockBit 3.0 Tools and Exploits

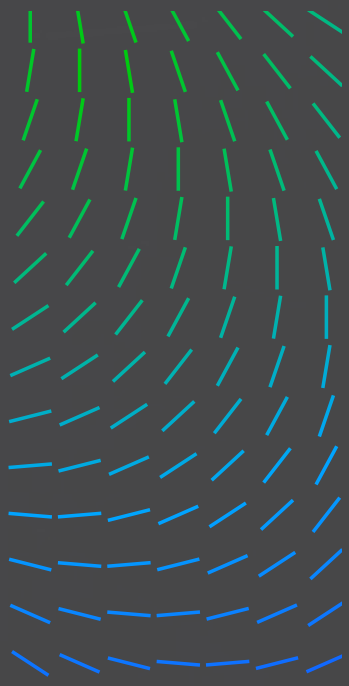
VULNERABILITIES KNOWN TO BE EXPLOITED BY LOCKBIT 3.0
CVE-2018-13379
CVE-2020-0787
CVE-2021-20028
CVE-2021-34473
CVE-2021-34523

MALICIOUS TOOLS USED BY LOCKBIT 3.0	
Amadey	Hakops
Blister	Neshta
BloodHound	SocGholish
Cobalt Strike	StealBit
Grabff	WinPEAS

NON-MALICIOUS TOOLS USED BY LOCKBIT 3.0			
BCDEdit	MiniDump	NSIS	Schtasks.exe
Cmd	MpCmdRun.exe	PCHunter	VSSAdmin
Fltmc.exe	Mshta	PowerShell	wevtutil
Fsutil	Mstsc	Process Monitor	WMIC
GMER	Netsh	Rundll32	RCLONE
MEGASYNC	Nltest		

Ransomware Through the Lens of Our Telemetry

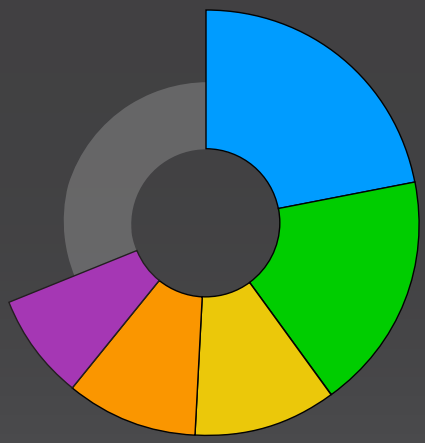
The following statistics are based on correlations between our telemetry and our threat intelligence knowledge base. Following an analysis phase, we identify a set of campaigns from the data over the selected time and extract their characteristics. The statistics displayed are those of the campaigns, not the detections themselves. Our global telemetry showed indicators of compromise (IoCs) that belong to several campaigns from various ransomware groups. The following ransomware families, with their respective tooling and techniques, represent the most prevalent families in the identified campaigns. Likewise, the countries, and sectors that follow represent the most impacted by the identified campaigns.



MOST PREVALENT RANSOMWARE FAMILIES Q4 2022

22%

Cuba was the most prevalent ransomware family in Q4 2022. Zeppelin was often used by Vice Society. Read more on Yanluowang's communication leaks



MOST PREVALENT MALICIOUS TOOLS USED BY RANSOMWARE GROUPS Q4 2022

41%

Cobalt Strike was the most prevalent malicious tool used by ransomware groups in Q4 2022.

1.	Cobalt Strike	41%
2.	Mimikatz	23%
3.	BURNTCIGAR	13%
4.	VMProtect	12%
5.	POORTRY	11%

MOST OBSERVED MITRE-ATT&CK TECHNIQUES USED BY RANSOMWARE GROUPS Q4 2022

1.	Data Encrypted for Impact	17%
2.	System Information Discovery	11%
3.	PowerShell	10%
4.	Ingress Tool Transfer	10%
5.	Windows Command Shell	9%

MOST PREVALENT NON-MALICIOUS TOOLS USED BY RANSOMWARE GROUPS Q4 2022

21%

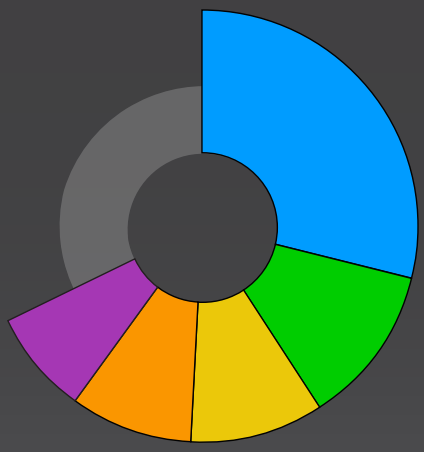
Cmd was the most prevalent non-malicious tool used by ransomware groups in Q4 2022.

1.	Cmd	21%
2.	PowerShell	14%
3.	Net	10%
4.	Reg	8%
5.	PsExec	8%

COUNTRIES MOST IMPACTED BY RANSOMWARE GROUPS Q4 2022

29%

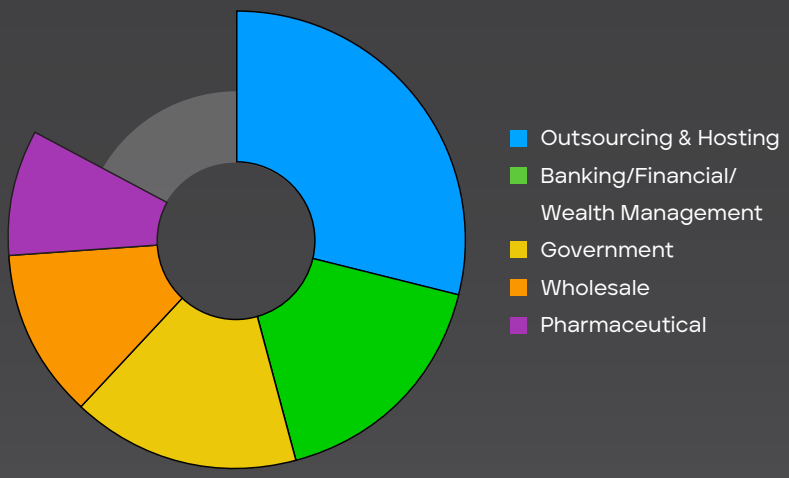
The United States was the country most impacted by ransomware groups in Q4 2022 according to Trellix telemetry.



SECTORS MOST IMPACTED BY RANSOMWARE GROUPS Q4 2022

29%

Outsourcing & Hosting was the sector most impacted by ransomware groups in Q4 2022 according to Trellix telemetry. This correlates with the average organization size of the victims listed on the ransomware leaks sites, these organizations often don't have their own assigned IP block and rely on third-party hosting providers.



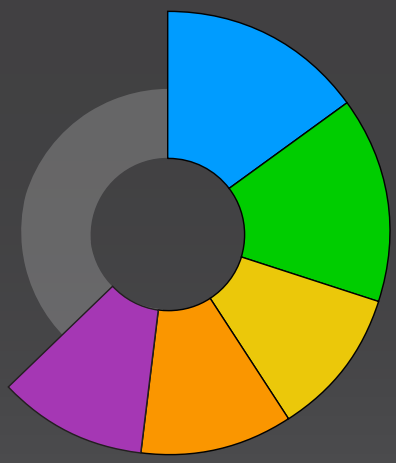
Ransomware Reported by the Security Industry

The following statistics are based on public reports as well as in-house research. Please note that not all ransomware incidents are reported. Many ransomware families have been active for a while and naturally are less noteworthy than novel families during specific quarters. Following these criteria, these metrics are an indication of ransomware families the security industry found most impactful and relevant in the quarter.

MOST REPORTED RANSOMWARE FAMILIES Q4 2022

15%

Black Basta ransomware and Magniber ransomware were the most reported ransomware families in Q4 2022 according to security industry reports.



TOP RANSOMWARE FAMILY ATTACK TECHNIQUES Q4 2022

19%

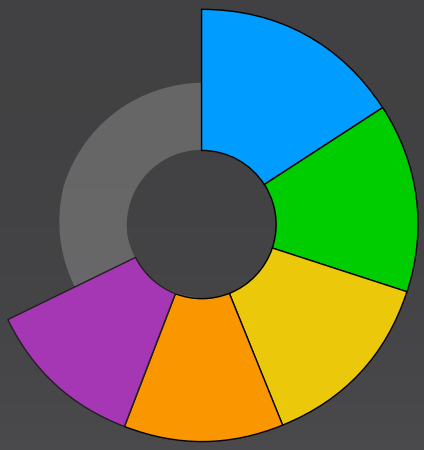
Data Encrypted for Impact was the most reported ransomware family attack technique in Q4 2022 according to security industry reports.

1.	Data Encrypted for Impact	19%
2.	Windows Command Shell	11%
3.	System Information Discovery	10%
4.	Ingress Tool Transfer	10%
5.	PowerShell	10%

TOP SECTORS TARGETED BY RANSOMWARE FAMILIES Q4 2022

16%

Health was the sector most targeted by ransomware families in Q4 2022 according to security industry reports.



- Health
- Finance
- Government
- Manufacturing
- Transport

COUNTRIES MOST TARGETED BY RANSOMWARE FAMILIES Q4 2022

19%

The United States was the country most targeted by ransomware families in Q4 2022 according to security industry reports.

- United States
- Germany
- Brazil
- Argentina
- Canada
- India
- Netherlands
- South Korea
- Switzerland
- United Kingdom

CVES USED BY RANSOMWARE FAMILIES Q4 2022

1.	CVE-2021-31207	16%
	CVE-2021-34474	16%
	CVE-2021-34523	16%
2.	CVE-2021-34527	13%
3.	CVE-2021-26855	9%
	CVE-2021-27065	9%

MALICIOUS TOOLS USED BY RANSOMWARE FAMILIES Q4 2022

44%

Cobalt Strike was the malicious tools used most by reported ransomware families in Q4 2022 according to security industry reports.

1.	Cobalt Strike	44%
2.	QakBot	13%
3.	IcedID	9%
4.	BURNTCIGAR	7%
5.	Carbanak SystemBC	7% 7%

NON-MALICIOUS TOOLS USED BY RANSOMWARE FAMILIES Q4 2022

21%

PowerShell was the non-malicious tool used most by reported ransomware families in Q4 2022 according to security industry reports.

1.	PowerShell	21%
2.	Cmd	18%
3.	Rundll32	11%
4.	VSSAdmin	10%
5.	WMIC	9%

Ransomware "Leak Sites" Victim Reports Q4 2022

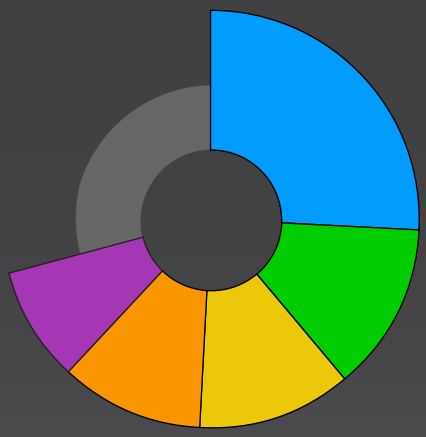
The data in this section was compiled by scraping the "leak sites" of various ransomware groups. Ransomware groups extort victims by publishing information about their victims on these websites. When negotiations stall or victims refuse to pay the ransom by the ransomware group's deadline, the ransomware group releases information stolen from the victims. We use the opensource tool ransomlook to collect the various posts, we then internally process the data to normalize and enrich the results to provide an anonymized version of the victimology analysis.

It is important to note that not all ransomware victims are reported in the respective leak sites. Many victims pay the ransom and are not reported. These metrics are an indicator of victims that ransomware groups extorted or retaliated against and should not be confused with the total amount of victims.

RANSOMWARE GROUPS REPORTING MOST VICTIMS Q4 2022

26%

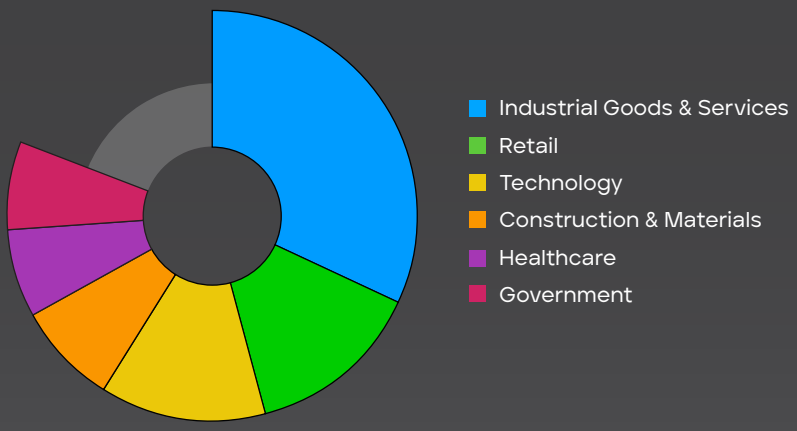
LockBit 3.0 accounted for 26% of the top-10 ransomware groups reporting the largest number of victims on their respective leak sites in Q4 2022.



SECTORS AFFECTED BY RANSOMWARE GROUPS PER LEAK SITES Q4 2022

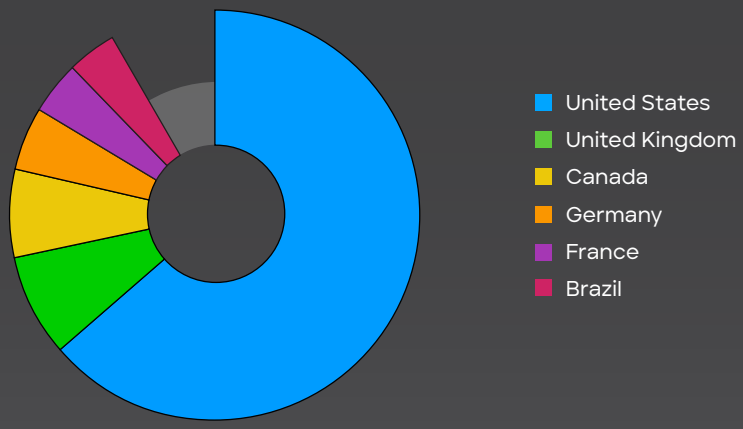
32%

Industrial Goods & Services was the most prevalent industry affected by ransomware groups per their leak sites in Q4 2022. Industrial Goods & Services encompasses all material products and intangible services mainly used for construction and manufacturing



COUNTRIES OF COMPANIES AFFECTED BY RANSOMWARE GROUPS PER LEAK SITES Q4 2022

63% of the top-10 companies reported by various ransomware groups in their corresponding leak sites in Q4 2022 were based in the United States, followed by the United Kingdom (8%) and Canada (7%).



NATION-STATE STATISTICS Q4 2022

This section provides insights we have collected on nation-state group activity. This information is gathered from multiple sources to create a better picture of the threat landscape and reduce the observation bias. First, we depict the statistics extracted from the correlation of nation state groups IOCs and Trellix customer telemetry. Secondly, we provide insights from various reports published by the security industry that are vetted, parsed, and analyzed by the Threat Intelligence Group.

Nation-State Highlights Q4 2022

- The United States and Germany experienced significant increases in nation-state attacks.
- China and Vietnam make an appearance in Q4 nation-state attacks.

Nation-State Statistics Through the Lens of Our Global Telemetry

These statistics are based on correlations between our telemetry and our threat intelligence knowledge base. Following an analysis phase, we identify a set of campaigns from the data over the selected time period and extract their characteristics. The statistics displayed are those of the campaigns, not the detections themselves. Due to

various log aggregations, our customers' use of threat simulation frameworks, and high-level correlations with the threat intelligence knowledge base, the data is manually filtered to meet desired criteria.

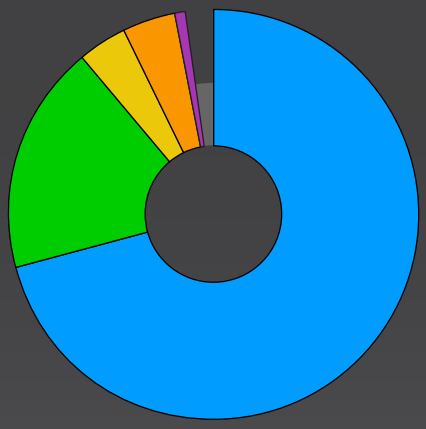
Our global telemetry showed indicators of compromise (IoCs) that are related to several campaigns from advanced persistent threat groups (APT). The following threat actor's countries and threat actors, together with their tooling and techniques, represent the most prevalent in the Identified campaigns. Likewise, the data on countries and sectors represent the most impacted by the identified campaigns.

Nation-State Telemetry Insights

MOST PREVALENT THREAT-ACTOR COUNTRIES BEHIND NATION-STATE ACTIVITY Q4 2022

71%

China was the most prevalent threat-actor country behind nation-state activity in Q4 2022.

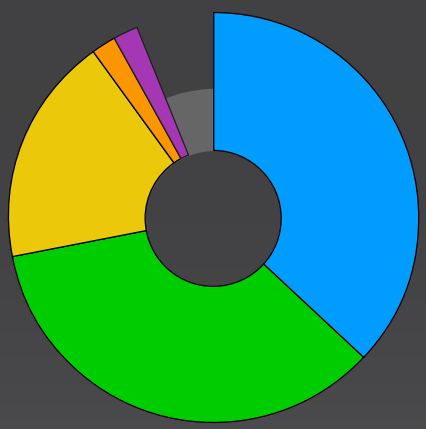


- China
- North Korea
- Russia
- Iran
- Lebanon

MOST PREVALENT THREAT ACTOR GROUPS Q4 2022

37%

Mustang Panda was the most prevalent threat actor group in Q4 2022 according to nation-state telemetry.



- Mustang Panda
- UNC4191
- Lazarus
- MuddyWater
- Kimsuky

MOST PREVALENT MITRE ATT&CK TECHNIQUES USED IN NATION-STATE ACTIVITY Q4 2022

1.	DLL Side-Loading	14%
2.	Rundll32	13%
3.	Obfuscated Files or Information	12%
4.	Windows Command Shell	11%
5.	Registry Run Keys/ Startup Folder	10%

MOST PREVALENT MALICIOUS TOOLS USED IN NATION-STATE ACTIVITY Q4 2022

1.	PlugX	24%
2.	BLUEHAZE	23%
3.	DARKDEW	23%
4.	MISTCLOAK	23%
5.	JSX Remote Access Trojan	2%

MOST PREVALENT NON-MALICIOUS TOOLS USED IN NATION-STATE ACTIVITY Q4 2022

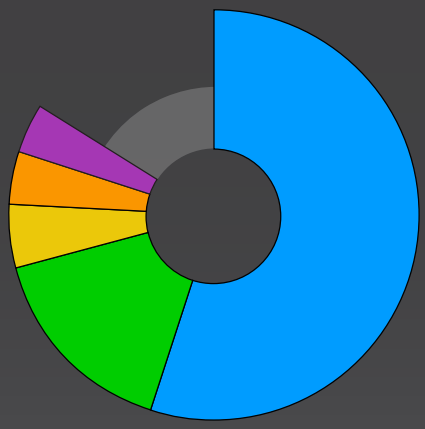
1.	Rundll32	22%
2.	Cmd	19%
3.	Reg	17%
4.	Ncat	12%
5.	Regsvr32	6%

COUNTRIES MOST IMPACTED BY NATION-STATE ACTIVITY Q4 2022

55%

The United States was the country most impacted by nation-state activity in Q4 2022.

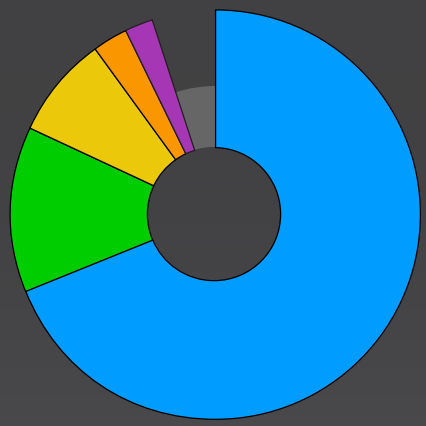
- United States
- Vietnam
- India
- Germany
- China



SECTORS MOST IMPACTED BY NATION-STATE ACTIVITY Q4 2022

69%

Transportation & Shipping was the sector most impacted by nation-state activity in Q4 2022.



Nation-State Incidents According to Public Reports Q4 2022

These stats are based on public reports and in-house research – not telemetry from customer logs. Please note that not all nation-state incidents are reported. Many campaigns follow the same TTPs that are already known and are less attractive to report. The industry tends to pick more novel campaigns where an actor either tried something new or made a mistake. These metrics are an indication of what the industry found insightful and relevant during Q4 2022.

THREAT-ACTOR COUNTRIES MOST REPORTED IN NATION-STATE CAMPAIGNS Q4 2022

37%

of the publicly reported nation-state campaigns in Q4 2022 originated in China

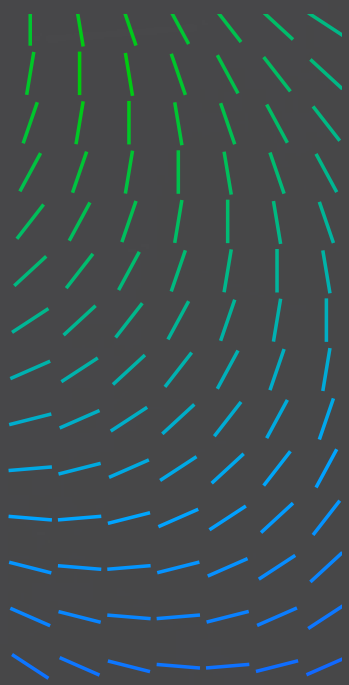
1.	China	37%
2.	North Korea	24%
3.	Iran	1%
4.	Russia	1%
5.	India	1%

MOST PREVALENT THREAT ACTORS OF REPORTED NATION-STATE ACTIVITY Q4 2022

33%

Lazarus was the most prevalent threat actor in reported nation-state activity in Q4 2022.

1.	Lazarus	33%
2.	Mustang Panda	17%
3.	APT34 APT37 APT41 COLDRIVER Patchwork Polonium SideWinder Winnti Group	each 1%



COUNTRIES MOST TARGETED BY REPORTED NATION-STATE CAMPAIGNS Q4 2022

16%

The United States was the country most targeted by reported nation-state campaigns in Q4 2022

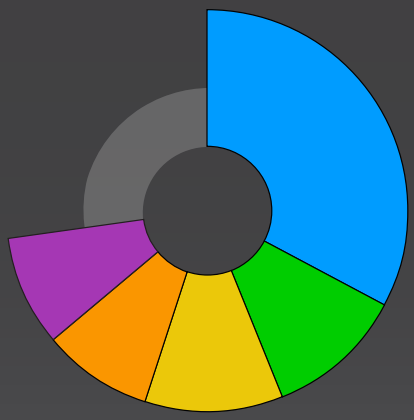
- United States
- United Kingdom
- Pakistan
- Russia
- Ukraine

SECTORS MOST TARGETED BY REPORTED NATION-STATE CAMPAIGNS Q4 2022

33%

Government was the sector most targeted by reported nation-state campaigns in Q4 2022, followed by Military (11%) and Telecom (11%).

- Government
- Military
- Telecom
- Energy
- Finance



MOST POPULAR MALICIOUS TOOLS USED IN REPORTED NATION-STATE CAMPAIGNS Q4 2022

1.	PlugX	22%
2.	Cobalt Strike	17%
3.	Metasploit	13%
4.	BlindingCan	9%
5.	Scanbox ShadowPad ZeroCleare	each 9%

MOST POPULAR NON-MALICIOUS TOOLS USED IN NATION-STATE CAMPAIGNS Q4 2022

1.	Cmd	32%
2.	Rundll32	20%
3.	PowerShell	14%
4.	Reg	8%
5.	Schtasks.exe	7%

MOST POPULAR MITRE ATT&CK TECHNIQUES USED IN REPORTED NATION-STATE CAMPAIGNS Q4 2022

1.	Ingress Tool Transfer	13%
2.	System Information Discovery	13%
3.	Obfuscated Files or Information	12%
4.	Web Protocols	11%
5.	Deobfuscate/Decade Files or Information	11%

OBSERVED VULNERABILITIES EXPLOITED IN REPORTED NATION-STATE CAMPAIGNS Q4 2022

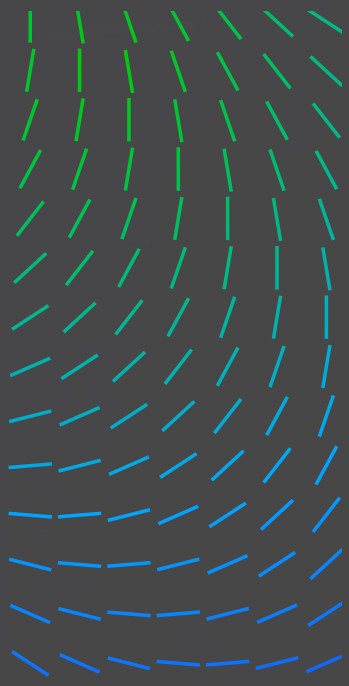
CVE-2017-11882
CVE-2021-44228
CVE-2018-0802
CVE-2021-26855
CVE-2021-27065
CVE-2021-34473
CVE-2021-34523
CVE-2015-2545
CVE-2017-0144
CVE-2018-0798
CVE-2018-8581
CVE-2019-0604
CVE-2019-0708
CVE-2019-16098
CVE-2020-0688
CVE-2020-1380
CVE-2020-1472
CVE-2020-17141
CVE-2020-17143
CVE-2021-21551
CVE-2021-26606
CVE-2021-26857
CVE-2021-26858
CVE-2021-28480
CVE-2021-28481
CVE-2021-28482
CVE-2021-28483
CVE-2021-31196
CVE-2021-31207
CVE-2021-40444
CVE-2021-45046
CVE-2021-45105
CVE-2022-1040
CVE-2022-30190
CVE-2022-41128

LIVING OFF THE LAND (LOLBIN) & THIRD-PARTY TOOLS Q4 2022

Observations and tracking through our Trellix Insights Global Threat Intelligence platform have garnered the following intelligence and visibility into the Q4 2022 threat landscape:

LOLBIN HIGHLIGHTS Q4 2022

- Living Off the Land continues to play a role from initial access, execution, discovery, persistence, to impact.
- Q4 2022 data shows a continued trend of command and scripting techniques being executed via Windows Command Shell or PowerShell is the most commonly (ab)used technique.



- Use by cybercriminals is prevalent among threat actors including the well-seasoned APTs, the financially motivated groups as well as the hacktivists.

The newcomers, the one-offs and the script kiddies that stumble on to the threat landscape are also making use of the already present binaries incorporated in the popular exploitation framework, as they attempt to go unnoticed and hack a Gibson or exploit a vulnerability.

Living off the Land techniques continue to be (ab)used to carry out nefarious tasks from initial access, execution, discovery, persistence, to impact. According to data collected throughout the fourth quarter of 2022, we can see a continued trend of command and scripting techniques being executed via Windows Command Shell and PowerShell is the most commonly (ab)used technique.

MOST PREVALENT OS BINARIES Q4 2022

47%

Windows Command Shell accounted for 47% - almost half – of the 10 most prevalent OS Binaries in Q4 22, followed by PowerShell (32%) and Rundl32 (27%).

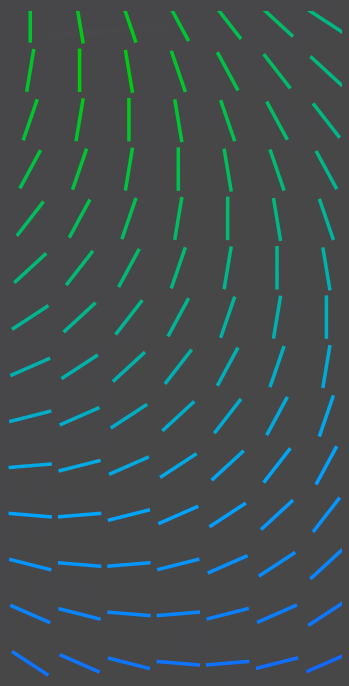
1.	Windows Command Shell	47%
2.	PowerShell	32%
3.	Rundl32	27%
4.	Schtasks	23%
5.	WMI	21%

Use by cybercriminals is prevalent among threat actors including the well-seasoned advanced persistent threats, the financially motivated groups as well as the woke hacktivists.

Events processed through our Trellix Insights platform where threat actors made use of Windows binaries led to the deployment of additional malware such as an information stealer, a remote access trojans or ransomware. Binaries such as MSHTA, WMI, or WScript may have been executed to retrieve the additional payloads from attacker-controlled resources.

TOP THIRD-PARTY TOOLS Q4 2022

1.	Remote Access Tools	58%
2.	File Transfer	22%
3.	Post Exploitation Tools	20%
4.	Network Discovery	16%
5.	AD Discovery	10%



Remote access and control tools are consistently among the highest tools abused by threat actors, however tools used by security practitioners continue to be abused for malicious intent. Threat actors may use them to initiate keep alive beacons, automate exfiltration or to gather and compress targeted information.

Among free and open-source tools, software packers are abused by threat actors to repackage a legitimate software to include malicious content or to pack malware in hopes of bypassing detections and to hinder analysis.

COBALT STRIKE INSIGHTS OF Q4 2022

The Advanced Research Center's Threat Intelligence Group monitors the usage of Cobalt Strike Team servers (Cobalt Strike C2s) in the wild by combining payload and infrastructure hunting methodologies. Here we present notable insights identified during the analysis of the gathered Cobalt Strike beacons:

15%
TRIAL COBALT STRIKE LICENSES

Only 15% of the Cobalt Strike Beacons identified in the wild had a Trial Cobalt Strike license. This version of Cobalt Strike includes most of the known features of this post exploitation framework. However, it adds "tells" and removes the in-transit encryption to make the payload easily detectable by security products.

87%
RUNDLL32.EXE

Rundll32.exe, the default process used for spawning sessions and running Post-exploitation Jobs, was found in 87% of the beacons identified.

5% HOST HTTP HEADER

At least 5% of the observed Cobalt Strike Beacons used the Host Http header, an option that facilitates domain fronting with Cobalt Strike. Domain Fronting is a technique that abuses Content Delivery Networks (CDNs) hosting multiple domains. Attackers hide an HTTPS request to a malicious website under a TLS connection to a legitimate website.

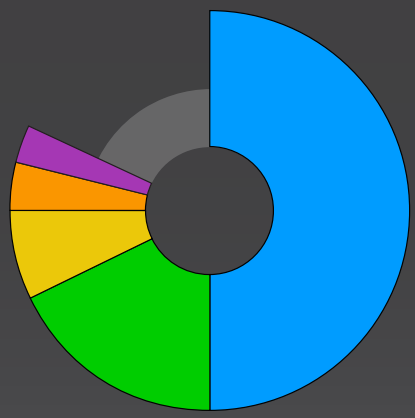
22% DNS BEACONS

DNS beacons accounted for 22% of the identified Cobalt Strike beacons. This payload type communicates back to the attacker's Cobalt Strike team server, which is the Domain's authoritative server, via DNS queries to conceal its activity.

TOP COUNTRIES HOSTING COBALT STRIKE TEAM SERVERS Q4 2022

50%

Half of the Cobalt Strike Team servers detected in Q4 2022 were hosted in China largely due to the size of cloud hosting available in China



GOOTLOADER Q4 2022

Gootloader is a modular malware that may at times be referred to interchangeably with another malware identified as "GootKit" or "GootKit Loader." The current modular features of the Gootloader malware are now being used to distribute additional malware payloads including REvil, Kronos, Cobalt Strike, and Icedid.

In recent events, Gootloader had been seen using search engine optimization (SEO) to lead unsuspecting users to compromised or fake site used to host an archive file containing a JS (JavaScript) file payload. This technique however requires the unsuspecting user to open the archive and execute the contents that in turn executes the malicious JS code via the Windows Scripting Host. Upon successfully execution, Gootloader will initiate C2 communications and retrieve additional malware.

Gootloader is a suspected malware as a service (MaaS) offered to subscribers which allows threat actors to load several additional payloads, therefore Gootloader poses a significant threat to enterprise environments.

Through our internal Gootloader tracker we identified a recent variant, spotted in the wild on November 18, 2022, and witnessed older variants going silent as of November 13, 2022. Modifications to the latest variant consist of:

- Removal of registry manipulation functionality
- Increased remote network requests to 10 URLs rather than three

- Ability to directly invoke PowerShell scripts via CScript
- Persistence for every user logon.

Our Gootloader Tracking Process

The new Gootloader variant is evolved using multiple obfuscation layers. Each nested stage after unpacked uses variables loaded from its earlier stage that make the analysis more challenging. The collected samples yielded by our YARA hunting efforts, are fed into a static JavaScript and PowerShell analyzer to extract IOCs such as remote Command and Control (C&C, C2) servers and unique ID signatures. These IOCs can be used to identify and track specific instances of Gootloader in the wild.

The extracted Gootloader IOCs are then processed by querying Trellix URL reputation team's database to identify which are malicious, potentially compromised legitimate domains, and legitimate domains being used as decoys to impair analysis.

Gootloader Telemetry Insights

The statistics displayed are those of the campaigns identified from the correlation of the IOCs extracted and our customers' logs, not the detections themselves. In the case of Gootloader, most of the detections are based on domain hits. Since Gootloader uses decoy domains the stats shown should be interpreted as malicious with medium level confidence.

COUNTRIES MOST VICTIMIZED BY GOOTLOADER Q4 2022

37%

The United States was the country most victimized by Gootloader in Q4 2022.

1.	United States	37%
2.	Italy	19%
3.	India	11%
4.	Indonesia	9%
5.	France	5%

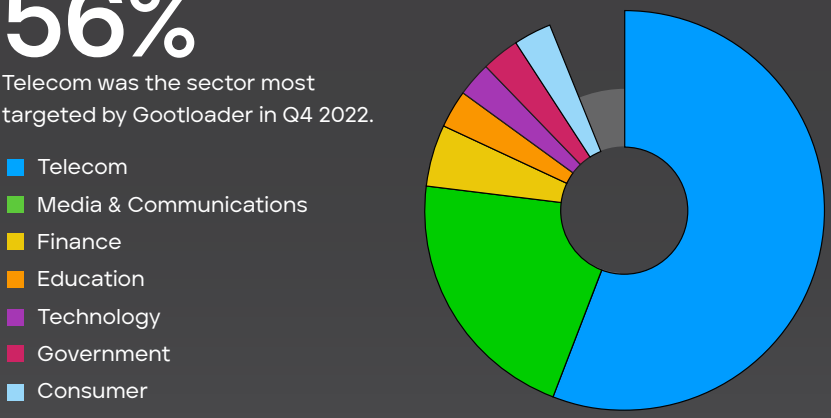
MOST POPULAR MITRE ATT&CK TECHNIQUES USED BY GOOTLOADER Q4 2022

1. Deobfuscate/Decode Files or Information
2. JavaScript
3. Obfuscated Files or Information
4. PowerShell
5. Process Hollowing

SECTORS MOST TARGETED BY GOOTLOADER Q4 2022

56%

Telecom was the sector most targeted by Gootloader in Q4 2022.



Most Popular MITRE Attack Techniques Used by Gootloader Q4 2022

Deobfuscate/Decode Files or Information

JavaScript

Obfuscated Files or Information

PowerShell

Process Hollowing

Reflective Code Loading

Registry Run Keys / Startup Folder

Rundll32

Scheduled Task

VULNERABILITY INTELLIGENCE Q4 2022

Our vulnerability dashboard collates the analysis of the latest high impact vulnerabilities. The analysis and triage are performed by the Advanced Research Center's industry experts on vulnerabilities. These researchers, who specialize in reverse engineering and vulnerability analysis, continuously monitor the latest vulnerabilities and how threat actors are utilizing these in their attacks to provide remediation guidance. This concise and highly technical expert advice allows you to filter the signal from the noise and to focus on the most impactful vulnerabilities that can affect your organization allowing you to react fast.

VULNERABILITY INTELLIGENCE HIGHLIGHTS Q4 2022

41% Lanner accounted for 41% of vulnerable products and vendors impacted by unique CVEs in Q4 2022.

29% IAC-AST2500A Firmware version 1.10.0 was the most reported CVE used by products in Q4 2022

MOST IMPACTFUL VULNERABLE PRODUCTS, VENDORS AND CVES Q4 2022

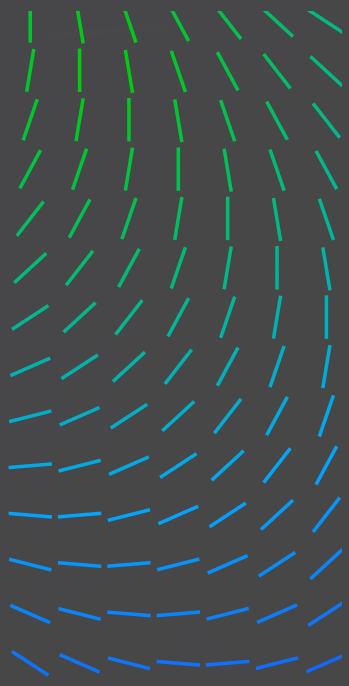
1.	Lanner	41%
2.	Microsoft	19%
3.	BOA	15%
4.	Oracle	8%
5.	Apple Chrome Citrix Fortinet Linux	each 5%

REPORTED CVES BY PRODUCTS Q4 2022

29%

IAC-AST2500A Firmware version 1.10.0 was the most reported CVE used by products in Q4 2022, followed by BOA Server (10%), IAC-AST2500A (6%), and Exchange (6%).

Reported CVEs Products	Unique CVEs
IAC-AST2500A, Firmware version 1.10.0	9
BOA Server	3
Exchange	3
IAC-AST2500A	2
tvOS	1
iPadOS	1
iOS	1
Windows	1
Safari	1
SQLite Up to and including 3.40.0	1
Oracle Access Manager, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	1
MacOS	1
Linux Kernel before 5.15.61	1
Internet Explorer	1



Reported CVEs Products	Unique CVEs
FortiOS (sslvpnd)	1
Citrix ADC/Citrix Gateway	1
Chrome, Versions before 108.0.5359.94/.95	1
BOA Server, Boa 0.94.13	1

REPORTED CVES Q4 2022

CVE-2022-1786
CVE-2022-26134
CVE-2022-27510
CVE-2022-27518
CVE-2022-31685
CVE-2022-32917
CVE-2022-32932
CVE-2022-33679
CVE-2022-34718
CVE-2022-35737
CVE-2022-3602
CVE-2022-3786
CVE-2022-37958
CVE-2022-40684
CVE-2022-41040
CVE-2022-41080
CVE-2022-41082
CVE-2022-41128
CVE-2022-41352
CVE-2022-42468
CVE-2022-42475
CVE-2022-4262
CVE-2022-42856
CVE-2022-42889
CVE-2022-43995
CVE-2022-46908
CVE-2022-47939

EMAIL SECURITY TRENDS Q4 2022

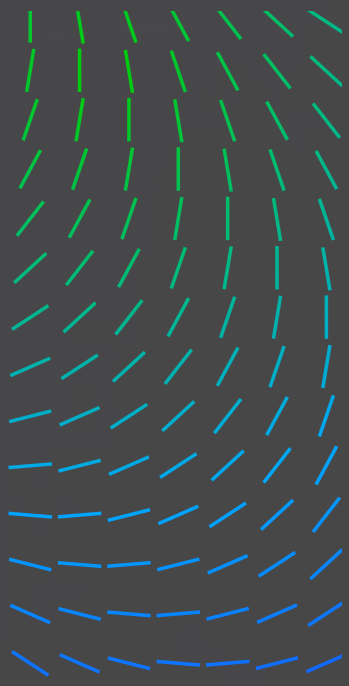
Email security statistics are based on telemetry generated form the several email security appliances deployed on customers networks around the world. The detection logs are aggregated and analyzed to produce the following findings:

EMAIL SECURITY TRENDS HIGHLIGHTS Q4 2022

100% The volume of malicious emails in Arab countries was observed to have increased by 100% in October when compared to August and September.

40% Qakbot was the malware tactic most used, accounting for 40% of campaigns targeting Arab countries

42% Telecom was the sector most impacted by malicious emails in Q4 2022, accounting for 42% of malicious email campaigns targeting industries.



87% Phishing emails using malicious URLs was by far the most prevalent attack vector in Q4 2022.

64% Impersonation hits increased 64% from Q3 to Q4 2022.

82% of all CEO fraud emails were sent using free email services.

78% of all Business Email Compromise (BEC) attacks were using common CEO phrases.

142% Vishing attacks were prominent in Q4 2022, increasing 142% from Q3 2022.

MOST PREVALENT EMAIL MALWARE TACTICS Q4 2022

40%

Oakbot was the most prevalent email malware tactics used in Q4 2022.

1.	Qakbot	40%
2.	Emotet	26%
3.	Formbook	26%
4.	Remcos	4%
5.	QuadAgent	4%

PRODUCTS AND BRANDS MOST TARGETED BY EMAIL PHISHING Q4 2022

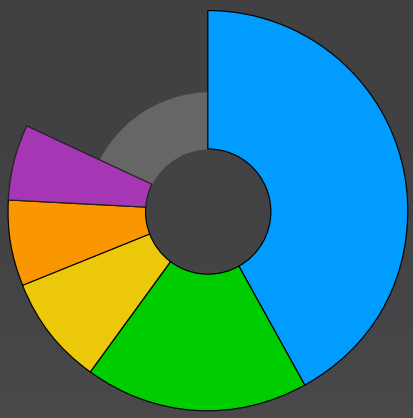
1.	Generic	62%
2.	Outlook	13%
3.	Microsoft	11%
4.	Ekinet	8%
5.	Cloudfare	3%

SECTORS MOST IMPACTED BY MALICIOUS EMAIL Q4 2022

42%

Telecom was the sector most impacted by malicious email in Q4 2022.

- Telecom
- Government
- Education
- Finance
- Services/Consulting



EMAIL IMPERSONATION TRENDS HIGHLIGHTS Q4 2022

82% of all CEO fraud emails were sent using free email services.

78% of all Business Email Compromise (BEC) attacks were using common CEO phrases.

64% increase in malicious emails impersonating CEOs and other business leaders from Q3 to Q4 2023.

Top CEO phrases used in BEC attacks in Q4 2022:

"I need you to carry out a task for me immediately."

"I need you to get a task done so kindly forward me your cell phone number."

"Send me your phone number, You need to get something done for me right now."

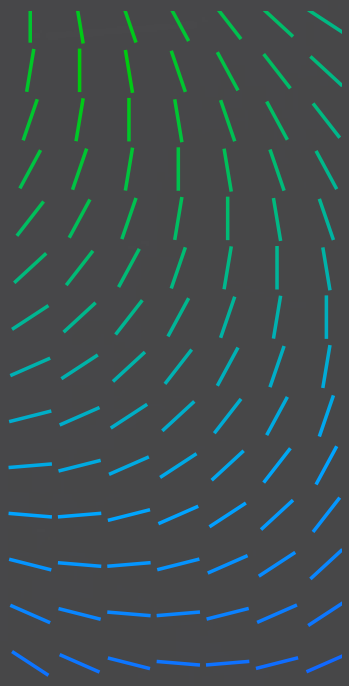
"Please send me your cell number and keep an eye out for my text. I need a task completed."

"Please review and confirm your cellphone number and keep a lookout to my text for instructions."

"Did you receive my previous email? I have a Profitable deal for you."

IMPERSONATION COMPARISON Q4 2022

64% Impersonation hits increased 64% from Q3 to Q4 2022



PHISHING CAMPAIGN INSIGHTS Q4 2022

Web Hosting Providers Increasingly Used to Scam & Steal

In Q4, we observed a rise in the use of legitimate web hosting providers for scamming users and stealing credentials. There are three service providers which were mostly abused. These are dweb.link, ipfs.link, translate.goog. We also noticed significant volumes from other service provider domains such as ekinet, storageapi_fleek, and selcdn.ru. Apart from these there were a couple of other service provider domains like ekinet, storageapi_fleek, selcdn.ru. Attackers are continuously using new and popular hosting services to host phishing pages and bypass anti-phishing engines. One reason why attackers have increased their interest in using legitimate web hosting providers: these services can't be blacklisted by any detection system since their main goal is to host legit files and share content

ATTACK VECTORS MOST USED IN PHISHING EMAILS

87%

Phishing emails using malicious URLs was by far the most prevalent attack vector in Q4 2022

1.	URL	87%
2.	Attachment	7%
3.	Header	6%

HIGHLY ABUSED WEB HOSTING PROVIDERS Q4 2022

154%

While Dweb was the most abused web hosting provider in Q4 2022, Google Translate showed the largest increase (154%) from Q3 to Q4 2022.

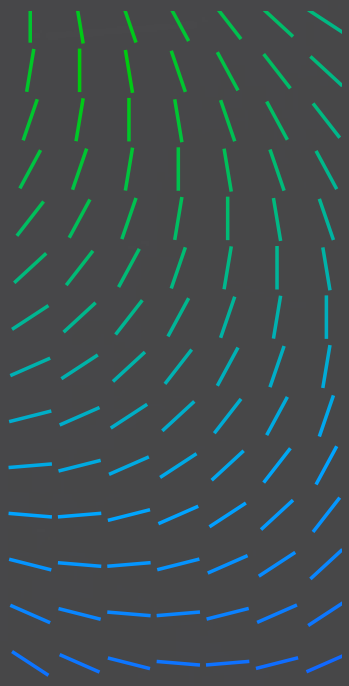
1.	Dweb	81%
2.	Ipfs	17%
3.	Google Translate	10%

EVASION TECHNIQUES MOST USED IN PHISHING ATTACKS Q4 2022

63%

302 Redirect Based Evasion was the most prominent in Q4 2022.

- Geo-based evasion phishing attacks increased significantly in Q4.
- Captcha based attacks have also increased in Q4.



VISHING INSIGHTS Q4 2022

Vishing is another form of phishing, and designed to entice victims to connect with attackers mostly using an email, text message, phone call, or direct-chat messages.

142% Vishing attacks were prominent in Q4 2022, increasing 142% from Q3 2022.

85% Free email services have become a favorite for bad actors using vishing. A large percentage of Q4 2022 vishing attacks we detected (85%) were sent using a free email service.

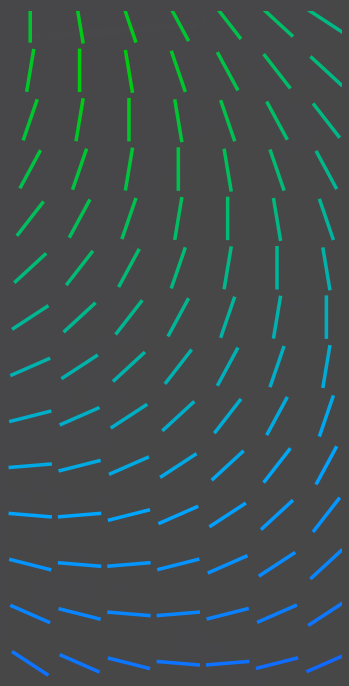
Norton, McAfee, Geek Squad, Amazon, and PayPal were the most popular themes used by vishing campaigns in Q4.

NETWORK SECURITY Q4 2022

The Trellix ARC network research team focuses on detecting and blocking network-based attacks that threaten our customers. We inspect different areas of the kill chain - from recon, initial compromise, C2 communication as well as lateral movement TTPs. Our ability to leverage the strengths of our combined technologies allows us visibility to better detect unknown threats.

Most Popular MITRE ATT&CK Techniques Used Against Network Security Q4 2022

- T1083 - File and Directory Discovery
- T1573 - Encrypted Channel
- T1020 - Automated Exfiltration
- T1210 - Exploitation of Remote Services
- T1569 - System Services
- T1059 - Command and Scripting Interpreter: Windows Command Shell
- T1047 - Windows Management Instrumentation
- T1087 - Account Discovery
- T1059 - Command and Scripting Interpreter
- T1190 - Exploit Public-Facing Application



Most Impactful Attacks on External-Facing Services Q4 2022

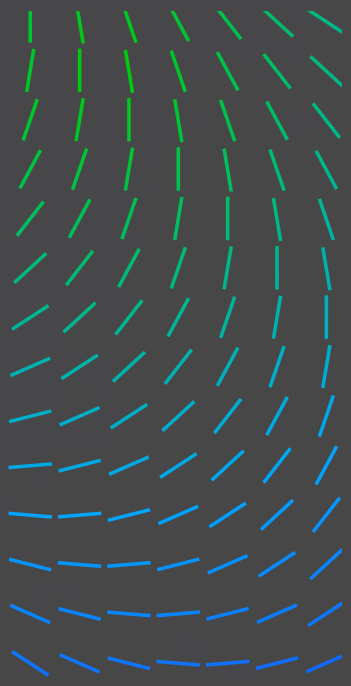
There are many network scans that are performed every day to probe external facing machines to find a potential threshold to a customer environment. Old exploits continually look for unpatched systems.

- File /etc/passwd Access Attempt Detect
- Possible Cross-site Scripting Attack
- SIPVicious Security Scanner
- Nmap Scanner Traffic Detected
- Scanning Activity - Shellshock, webserver Probing
- Bash Remote Code Execution (Shellshock) HTTP CGI (CVE-2014-6278)
- Oracle WebLogic CVE-2020-14882 Remote Code Execution Vulnerability
- Directory Traversal Attempt
- Apache Struts 2 ConversionErrorInterceptor OGNL Script Injection
- Apache Log4j CVE-2021-44228 Remote Code Execution

Most Significant WebShells Used as Initial Network Foothold Q4 2022

The following WebShells are typically found used to attempt to control a vulnerable web server.

- China Chopper WebShell
- JFolder WebShell
- ASPXSpy WebShell
- C99 WebShell
- Tux WebShell
- B374K WebShell / RootShell Family



Most Relevant Tools, Techniques, and Procedures Once Inside the Network Q4 2022

The following WebShells are typically found used to attempt to control a vulnerable web server.

We have seen a high volume of TTPs that attackers use during lateral movement including the usage of old vulnerabilities and tools like SCShell and PSExec.

- SCshell: Fileless Lateral Movement Using Service Manager
- Windows WMI Remote Process Call
- Invocation Of CMD Shell via WMIEXEC Over SMB
- EternalBlue Exploit Detected
- Microsoft SMBv3 CVE-2020-0796 Attempt
- Apache Log4j CVE-2021-44228 RCE
- Remote Domain/Enterprise Admin Account Enumeration
- Suspicious PowerShell Remoting
- Suspicious Network Reconnaissance Using WMIC
- Enumeration command detected in batch file
- SMB PSEXEC Activity

SECURITY OPERATIONS TELEMETRY POWERED BY TRELLIX XDR

These stats are based on telemetry generated from different sensors across our customer base. The detection logs are aggregated and analyzed to produce the following sections:

Most Impactful Security Incidents Q4 2022

Below section shows the most prevalent security alerts for the fourth quarter of 2022:

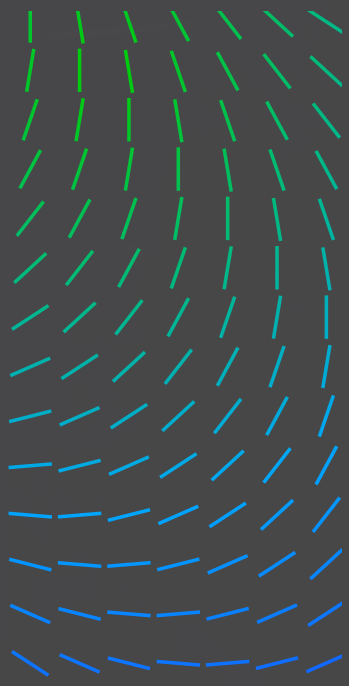
EXPLOIT - LOG4J [CVE-2021-44228]

OFFICE 365 ANALYTICS [Abnormal Logon]

OFFICE 365 [Allowed Phish]

EXPLOIT - FORTINET [CVE-2022-40684]

EXPLOIT - APACHE SERVER [CVE-2021-41773 - Attempt]



WINDOWS ANALYTICS [Brute Force Success]

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]

EXPLOIT - F5 BIG-IP [CVE-2022-1388 Attempt]

MOST USED MITRE ATT&CK TECHNIQUES Q4 2022

1.	Exploit Public-Facing Applications (T1190)	29%
2.	Application Layer Protocol: DNS (T1071.004) Phishing (T1566)	14% 14%
3.	Account Manipulation (T1098.001) Brute Force (T1110) Drive-by Comparison (T1189) User Execution: Malicious File (T1204.002) Valid Accounts: Local Accounts T1078,003)	each 7%

TOP LOG SOURCES DISTRIBUTION Q4 2022

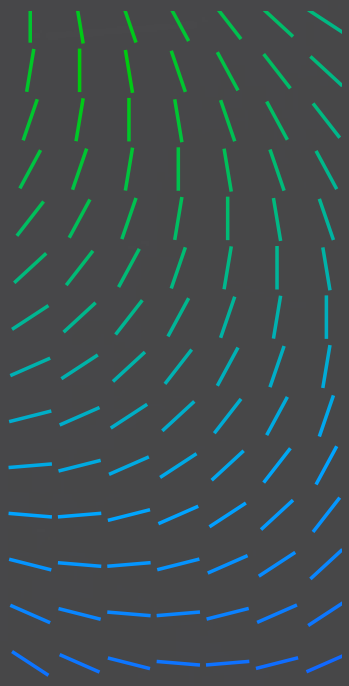
1.	Network	40%
2.	Email	27%
3.	Endpoint	27%
4.	Firewall	6%

EXPLOITS OBSERVED Q4 2022

MOST PREVALENT EXPLOITS OBSERVED IN Q4 2022

30% Log4j was the most prevalent exploit observed in Q4 2022.

1.	Log4j (CVE-2021-44228)	30%
2.	Fortinet (CVE-2022-40684)	16%
3.	Apache Server (CVE-2021-41773)	15%
4.	Atlassian Confluence (CVE-2022-26134)	14%
5.	F5 Big-IP (CVE-2022-1388 Attempted)	13%
6.	Microsoft Exchange (ProxyShell Exploit Attempt)	11%



CLOUD INCIDENTS Q4 2022

Attacks on cloud infrastructure are always on the rise as many companies transition from on-prem infrastructure. Gartner analysts predict more than 85% of organizations will embrace a cloud-first principle by 2025.

While analyzing the telemetry of Q4, 2022, we have observed:

- Detections related to AWS lead the way possibly due to AWS's status as a key leader in the cloud marketplace.
- Most of the attacks were focused on getting initial access by Bruteforce/Passwordspray to valid accounts which points to initial infection vector in the cloud attack surface.
- With the majority of the enterprise accounts having had Multi Factor Authentications enabled, the successful bruteforces makes the adversaries land on MFA platforms, resulting in a spike of MFA related detections.

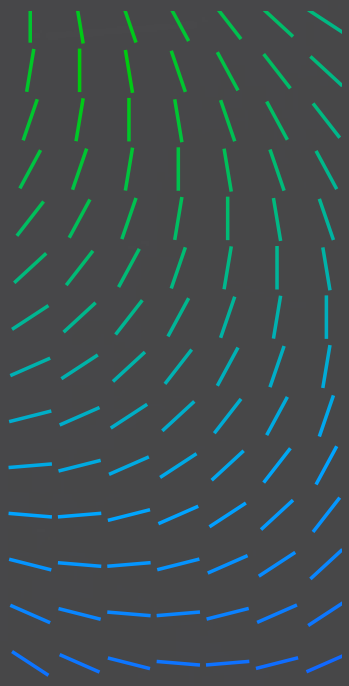
Below sections briefly describes the cloud-based attack telemetry data across our customer base breakdown by the various cloud providers.

MITRE ATT&CK TECHNIQUES DISTRIBUTION FOR AWS Q4 2022

1.	Valid Accounts (T1078)	18%
2.	Modify Cloud Compute Infrastructure (T1578)	12%
3.	Account Manipulation T1098)	9%
4.	.Cloud Accounts (T1078.004)	8%
5.	Brute Force (T1110) Impair Defenses (T1562)	each 6%

TOP MITRE ATT&CK TECHNIQUES FOR AZURE Q4 2022

1.	Valid Accounts (T1078)	23%
2.	Multi-Factor Authentication (T1111)	19%
3.	Brute Force (T1110)	14%
4.	Proxy (T1090)	14%
5.	Account Manipulation (T1098)	5%

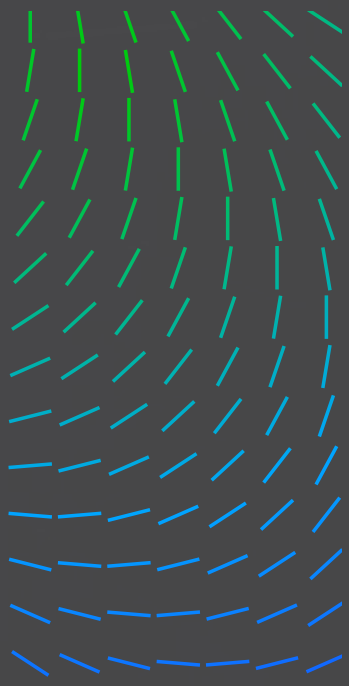


TOP AWS DETECTIONS BY MITRE ATT&CK TECHNIQUES Q4 2022

MITRE Technique	Rule
Account Manipulation (T1098)	AWS-Privileged Policy Attached To IAM Identity AWS S3 - Delete Bucket Policy
Valid Accounts(T1078)	AWS Analytics Abnormal Console Login AWS Analytics Abnormal API Key Usage AWS Guardduty anomalous user behavior AWS Guardduty anonymous access granted
Impair Defenses (T1562)	AWS Cloudtrail Policy Changes to Cloudtrail AWS Cloudtrail DeleteTrail
Credentials In Files (T1552.001)	Alert possible stealing of AWS secret keys
Modify Cloud Compute Infrastructure (T1578)	AWS Cloudtrail Delete S3 Bucket AWS CloudTrail Put S3 Bucket ACL AWS Cloudtrail Put Object ACL

TOP AZURE DETECTIONS BY MITRE ATT&CK TECHNIQUES Q4 2022

MITRE ATT&CK Technique	Rule
Valid Accounts(T1078)	Azure AD Risky sign-in Azure login from unusual location Azure login by account not seen in 60 days
Brute Force (T1110)	Azure Multiple authentication failures Graph brute force attack against azure portal Graph distributed password cracking attempts
Multi-Factor Authentication (T1111)	Azure mfa denied due to fraud alert Azure mfa denied due to user blocked Azure mfa denied due to fraud code Azure mfa denied due to fraud app
External Remote Services (T1133)	Azure sign in from tor network
Account Manipulation (T1098)	Azure Unusual User password reset

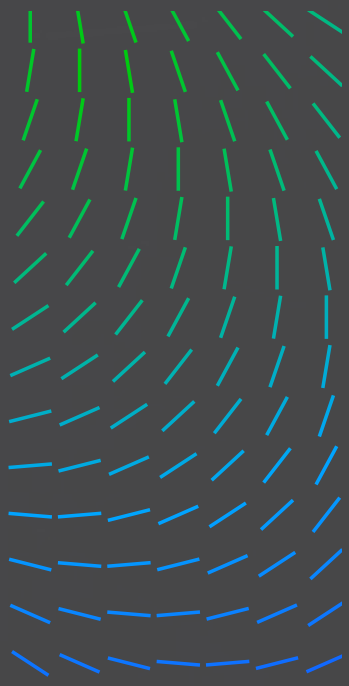


MITRE ATT&CK TECHNIQUES DISTRIBUTION FOR GCP Q4 2022

1.	Valid Accounts (T1078)	36%
2.	Execution through API (T0871)	18%
3.	Account Discovery (T1087.001) Account Manipulation (T1098) Impair Defenses (T1562) Modify Cloud Compute Infrastructure (T1578) Remote Services (T1021.004)	each 9%

TOP GCP DETECTIONS BY MITRE ATT&CK TECHNIQUES Q4 2022

MITRE ATT&CK Technique	Rule
Valid Accounts(T1078)	GCP Creation of Service Account GCP Analytics Abnormal Activity GCP Creation of Service Account Key
Remote Services (T1021.004)	GCP firewall rule allows all traffic on ssh port
Account Manipulation (T1098)	GCP Organization IAM Policy Changed
Account Discovery (T1087.001)	Alert ["gcps net user"]
Transfer Data to Cloud Account (T1527)	GCP Logging Sink Modified
Modify Cloud Compute Infrastructure (T1578)	GCP Deletion Protection Disabled



WRITING AND RESEARCH

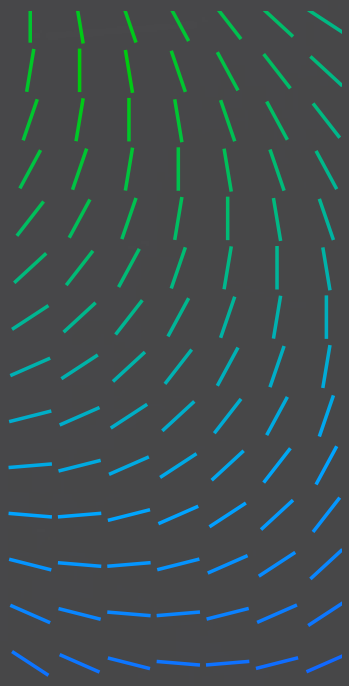
Alfred Alvarado
Henry Bernabe
Adithya Chandra
Dr. Phuc Duy Pham
Sarah Erman
John Fokker
Lennard Galang
Sparsh Jain
Daksh Kapoor
Maulik Maheta
João Marques
Tim Polzer
Srini Seethapathy
Rohan Shah
Vihar Shah
Swapnil Shashikantpa
Shyava Tripathi
Leandro Velasco

RESOURCES

To keep track of the latest and most impactful threats identified by the Trellix Advanced Research Center view these resources:

TWITTER

Trellix ARC

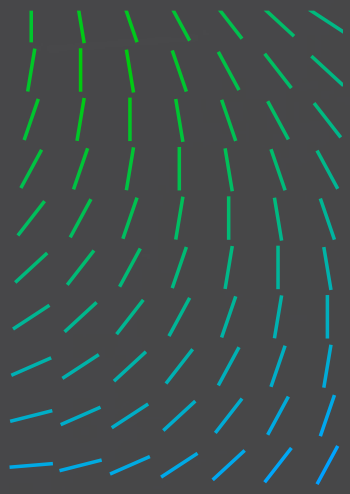


ABOUT THE TRELLIX ADVANCED RESEARCH CENTER

The Trellix Advanced Research Center has the cybersecurity industry's most comprehensive charter and is at the forefront of emerging methods, trends, and actors across the threat landscape. The premier partner of security operations teams across the globe, The Trellix Advanced Research Center provides intelligence and cutting-edge content to security analysts while powering our leading XDR platform.

ABOUT TRELLIX

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



Visit Trellix.com to learn more.

Trellix

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.

072022-05