THE CYBERTHREAT REPORT

November 2023

Insights Gleaned from a Global Network of Experts, Sensors, Telemetry, and Intelligence

INSIDE:

- Ransomware Activity Following APT Trends
- Polyglot Malware Takes the Stage
- Underground Development of Malicious AI

Presented by

Trellix ADVANCED RESEARCH CENTER

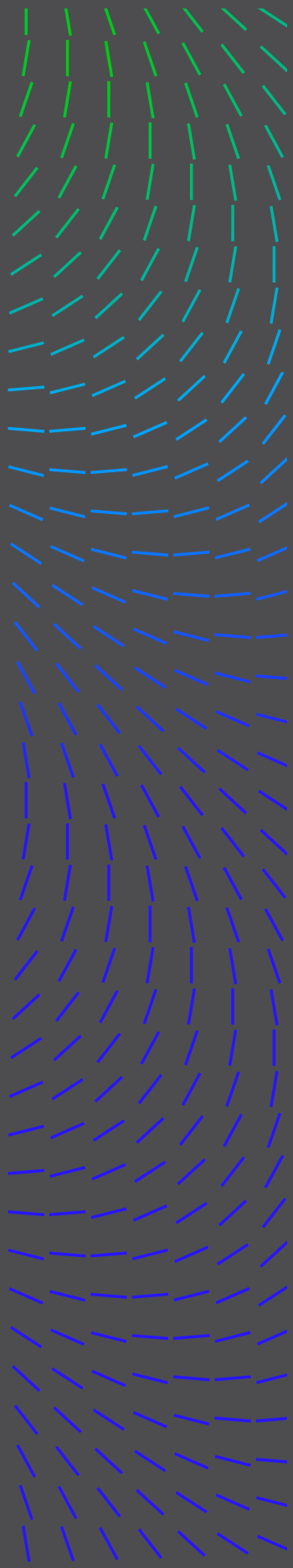
An espionage actor linked to China, UNC4841, compromises an industry peer's global network by exploiting CVE-2023-2868.

As CISO, you direct your SecOps team to start patching immediately – and ultimately avoid serious impact to your systems.

But your anxious board wants to see you in person. They need assurance. They don't understand cybersecurity – and you can't just walk in and say "hey, we've patched 500 vulnerabilities."

The narrative starts with cyber threats. Your story starts with intelligence. Insights gleaned from a million sensors.

Welcome to your November 2023 edition of The Trellix CyberThreat Report.



THE CYBERTHREAT REPORT

Authored by Trellix's Advanced Research Center, this report (1) highlights insights, intelligence, and guidance gleaned from multiple sources of critical data on cybersecurity threats, and (2) develops expert, rational, and reasonable interpretations of this data to inform and enable best practices in cyber defense. This edition focuses on data and insights captured primarily between April 1, 2023 and September 30, 2023.

A CRITICAL PARTNERSHIP

What's out there? What's incoming? How do we get ahead of it?

These questions are ones we live and breathe every day. You as CISOs, and your SecOps teams. And our Advanced Research Center experts, as well as myself. Like you, we bounce between urgent after-hour war-room calls with CEOs and boards and intensive, weekend-long search-and-counter missions tracking down ransomware gangs or malicious payloads.

Our missions depend deeply on one another.

- You oversee your organization's information, technology, and cybersecurity. And we are your eyes and ears at the leading edge of the cyber risks you manage.
- We share similar credentials – such as intelligence at a national security level, military or law service, special operations, counterterror, and espionage as well as senior-level expertise in areas such as network architecture design and system administration.

Working independently and together, your teams and ours represent the first line of defense for essentially every organization in the world.

The consequences of cyberattacks continue to evolve.

Preventing these incidents and impacts starts with intelligence. Understanding the threat environment. Translating raw telemetry into actionable insights on threat actors, vulnerabilities, and attacks.

We publish the Trellix Cyberthreat Report for you. In this 2023 Q4 edition you'll find insights on four fronts shaping the threat environment: (1) nation-state activity and APTs, (2) the continuing evolution of ransomware, (3) shifts in threat actor behavior, and (4) the emerging threat of generative AI.

Intelligence shapes the battlefield. In cybersecurity, that starts here.

John Fokker
TRELLIX HEAD OF THREAT INTELLIGENCE

INTRODUCTION

A Geopolitical Recession: Wars, Unrest, and Instability

Global context always matters in cybersecurity. Wars and conflicts inflame passions. Fragile relationships between nations fuel mistrust and misdeeds. Economic instability opens opportunities for some to prey on others. A sampling of factors influencing our Q4 2023 threat data and analysis includes the following.

- **Russia-Ukraine War and the Uncertainty of Post-War Russia** – Pro-Russian hackers have continued to ramp up attacks on Ukraine concentrating primarily on its critical infrastructure, government facilities, and military command and control centers. Hacktivist attacks have already expanded to target UN, NATO, and the West including cyber strikes against critical infrastructure and financial systems[1] in the U.S. and Europe. We expect these to continue to become more sophisticated after the war as the weakened nation chafes against its isolation.
- **China and its Cyber Espionage Threat and IP Theft Capabilities** – China's highly organized approach to intellectual property (IP) theft has now matured into "the most sustained, scaled, and sophisticated theft of intellectual property…that is unprecedented in human history," according to U.S. FBI Director Christopher Ray.[2] Some global leaders also fret that the China-owned platform TikTok could be used for mass data collection and influence operations. Meanwhile, the nation continues to ramp up cyberattacks against Taiwan.
- **Rogue States Iran and Korea and Their Cyberattack Sophistication** – These two autocratic nations are committed to undermining democracy worldwide. Last month, Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technologies on the National Security Council, remarked that North Korea is already experimenting with AI-enhanced cyberattacks.[3] At the same time, Iranian state-backed groups are aggressively targeting defense, satellite, and pharmaceutical enterprises.[4]
- **The Israel-Hamas War and Heightened Tensions Across the Middle East** – Although this armed war erupted in early October, just after the September 30 cutoff date for data and analysis addressed in the current edition of this report, its significance for cybersecurity requires highlighting it. The still-raging war has

[1] Cybersecurity and Infrastructure Security Agency, Russia Cyber Threat Overview and Advisories.
[2] The Register, "Five Eyes intel chiefs warn China's IP theft program is now at 'unprecedented' levels," October 2023.
[3] U.S. Dept. of State, "Digital Press Briefing with Anne Newberger." October 2023.
[4] CNN, "Iranian hackers target secrets held by defense, satellite and pharmaceutical firms," September 2023.

dramatically increased tensions between supporters on either side of the long-standing Israel-Palestinian dispute across the Middle East and Europe and threatens to spread to other nations in the region.

- **Artificial Intelligence as a Cyber Weapon** – Over the last few months, malicious actors have begun to incorporate artificial intelligence (AI) into the mechanics of mounting an attack, from identifying systems already infected with predatory payloads, generating higher quality emails, responding to complex questions on hijacked chat bots, solving problems, and generating new code. As advanced generative AI tools become more easily accessible, cybercriminals can launch attacks much more easily and cost effectively – without technical knowledge.
- **Political Tension, Hacktivism, and Misinformation** – As we predicted at the end of 2022,[5] political hacktivism (politically or socially motivated hacking by activists) is increasing – fueled in great measure by widening political polarization in the U.S leading up to the 2024 presidential election as well as other countries, such as Canada, Switzerland, Brazil, and New Zealand. Some of these groups are adopting cyber tactics and tools to amplify their messages, propagate misinformation, and cause disruption.

Methodology: How We Gather and Analyze Data

Trellix's world-class experts from our Advanced Research Center gather the statistics, trends, and insights that comprise this report from a wide range of global sources, both captive and open. The aggregated data is fed into our Insights and ATLAS platforms. Leveraging machine learning, automation, and human acuity, the team cycles through an intensive, integrated, and iterative set of processes – normalizing the data, analyzing the information, and developing insights meaningful to cybersecurity leaders and SecOps teams on the frontlines of cybersecurity worldwide. For a more detailed description of our methodology, please see the end of this report.

[5] Trellix, "Trellix Predicts Heightened Hacktivism and Geopolitical Cyberattacks in 2023," December 2022.

Application: How to Use This Information

It's imperative that any industry-leading assessment team and process understand, acknowledge and, where possible, mitigate the effects of bias – the natural, embedded, or invisible inclination to either accept, reject, or manipulate facts and their meaning. The same precept holds true for consumers of the content.

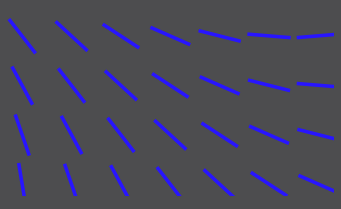
Unlike a highly structured, control-base mathematical test or experiment, this report is inherently a sample of convenience – a non-probability type of study often used in medical, healthcare, psychology, and sociology testing that makes use of data that is available and accessible.

- In short, our findings here are based on what we can observe and, pointedly, do not include evidence of threats, attacks, or tactics that evaded detection, reporting, and data capture.
- In the absence of "complete" information or "perfect" visibility, this is the type of study best suited to this report's objective: to identify known sources of critical data on cybersecurity threats and develop rational, expert, and ethical interpretations of this data that inform and enable best practices in cyber defense.

How to Understand the Analysis in this Report

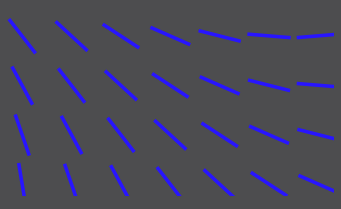
Understanding the insights and data in this report requires briefly reviewing the following guidelines:

- **A Snapshot in Time:** 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, tracking what we can leads to a better understanding of the various threats, while reducing analytical and investigative blind spots.
- **False Positives and False Negatives:** Among the high-performance technical characteristics of Trellix's special tracking and telemetry systems to collect data are mechanisms, filters, and tactics that help counter or remove false positive and negative results. These help to elevate the level of analysis and the quality of our findings.
- **Detections, not Infections:** 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.



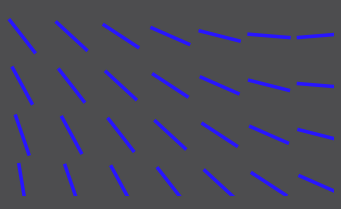
- **Uneven Data Capture:** Some data sets require careful interpretation. Telecommunications data, for example, includes telemetry from ISP clients operating in many other industries and sectors.
- **Nation-State Attribution:** Similarly, determining nation-state responsibility for various cyberattacks and threats can be very difficult given the common practice among nation-state hackers and cybercriminals to spoof one another, or disguise malicious activity as coming from a trusted source.

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.



Q4 2023 HIGHLIGHTS AT-A-GLANCE

1. **Socioeconomics, Nation-States, and APTs**
   - **Geopolitics Driving Threat Activity:** As geopolitical conflict escalates in nations like Russia, Ukraine, China, Taiwan, and Israel, activity from APT groups and hacktivists is intensifying worldwide. Activity from nation-state associated groups has increased by 50%+ in six months.
   - **Targeted Countries and Regions:** Nation-state actors are increasingly engaging in digital espionage, disinformation campaigns, and cyberwarfare. In addition to China and the U.S., recent waves of attacks have started targeting countries like India, Turkey, and Vietnam.
   - **The Return of Edge Device Attacks:** Traditional threats to devices at the edge of networks are increasing again as threat actors, including APT groups, return to this frontier. Major incidents include recent attacks involving Ivanti, MOVEit, and Barracuda Networks.
2. **Subtle Shifts in the Ransomware Landscape**
   - **Smaller Families Making Big Moves:** Ransomware remains the "malware king," but smaller digital adversaries are emerging more prominently – such as Agrius, BI00dy, and FusionCore.
   - **Ransomware Activity Following APT Trends:** India, Turkey, Israel, and Ukraine are enduring high attack volumes, suggesting that ransomware and APT practices may be converging.
3. **Evolution of the Cybercriminal Underground**
   - **Actor Collaboration:** Major threat actors are starting to work together, driven by practical goals, such as the sharing or selling of zero-day vulnerabilities and exploits – and politics.
   - **Coordinating and Sharing Zero-Day Vulnerabilities:** Cybercriminals are changing tactics. Rather than concealing their most promising vulnerability discoveries, they are selling them on the open market. Thus, the proliferation of zero-day exploits is higher than ever.
   - **Newer Malware Languages Take the Stage:** New programming languages like Nim, Rust, and Golang offer attractive features for cybercriminals. Golang-based malware in particular is becoming popular, primarily for ransomware (32%), backdoors (26%), and Trojan horses (20%).



4. **The Emergence of Malicious AI**

- **"Script Kiddies" Are Back:** Generative AI tools, like ChatGPT, are helping threat actors small and large overcome considerable challenges. With greater efficiency, they can now scale faster and improve targeting.
- **Development of Blackhat LLMs:** ChatGPT knockoffs designed for cybercriminals already exist. The acceleration and sophistication of phishing attacks in recent years suggest bad actors are already starting to leverage some of these tools.

REPORT ANALYSIS, INSIGHTS, AND DATA

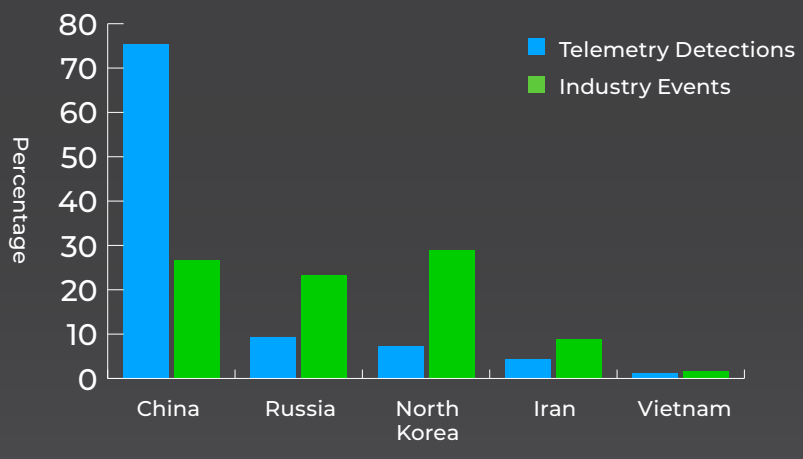
Nation States and Advanced Persistent Threats (APT)

Nation-state actors are increasingly engaging in digital espionage, disinformation campaigns, and cyberwarfare. In fact, as hostilities escalate between various entities, such as Russia and Ukraine, China and Taiwan, Israel and Hamas, and many others, threat activity worldwide from both APT groups and hacktivists has intensified at a significantly higher rate than in 2022 and before. Within the last six months alone, activity from nation-state associated groups has increased by more than 50%.

Active Nation States and APT Groups

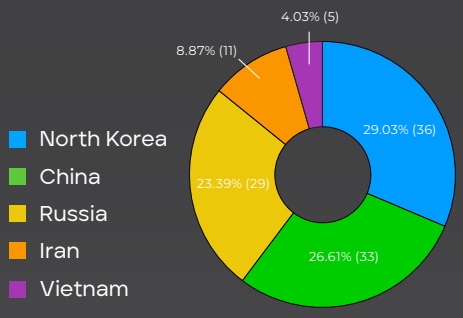
Based on the telemetry alone, the most prominent nation-states represented were China, Russia, and North Korea. Based on public events alone, the most prominent nation-state threat actor was North Korea, with 36 reports of affiliated groups including Lazarus, Kimsuky, APT37, and BlueNoroff. The second most represented nation-state was China, with 33 reported events, many of them involving Mustang Panda. Threat actors affiliated with Russia represented the third most common nation-state groups, with 29 reported events involving Gamaredon, APT28, APT29, and others.

NOTABLE THREAT ACTOR COUNTRIES, Q2 TO Q3*



* Percentage of total APT detections tracked by Trellix telemetry and industry-reported events.

TOP THREAT ACTOR COUNTRIES BY INDUSTRY EVENTS, Q2 TO Q3*



* Percentage of total APT detections tracked by industry-reported events.

TOP THREAT ACTOR COUNTRIES BY TELEMETRY DETECTIONS, Q2 TO Q3*

1.	China	75.46%
2.	Russia	9.38%
3.	North Korea	7.37%
4.	Iran	4.28%
5.	Vietnam	1.17%

* Percentage of total APT detections tracked by Trellix telemetry.

The APT groups most frequently identified in Q2 and Q3 reported events included the China-sponsored Mustang Panda, North Korea-backed Lazarus, and Russia-affiliated Gamaredon groups. This doesn't necessarily mean these groups were the most active threat actors, as the global telemetry data reflects, but does point to highly impactful attacks and breaches.

Like many China-backed APT actors, Mustang Panda is driven by strategic intelligence-gathering in other regions. Thus, the group deploys a more methodical approach, prioritizes the use of custom tools and malware, and pursues a disciplined focus on specific sectors and targets. As a result, Mustang Panda is comparatively more likely to be identified and reported.

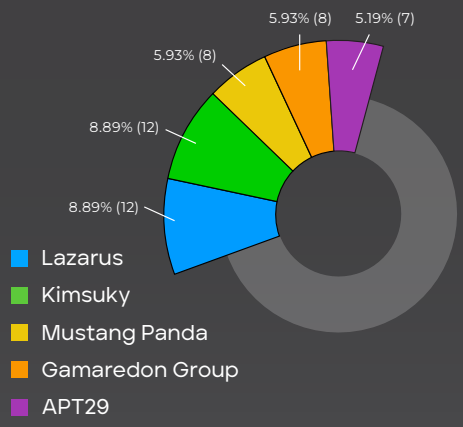
Like many APT groups associated with North Korean, on the other hand, Lazarus is highly represented on both sides. This is because the group (which is likely the author of the cyber espionage campaign Operation Dream Job) is more heavily driven by financial

TOP THREAT ACTOR GROUPS BY TELEMETRY DETECTIONS, Q2 TO Q3*

1.	APT40	42.28%
2.	Mustang Panda	15.93%
3.	Lazarus	5.12%
4.	APT10	2.82%
5.	Gamaredon Group	2.66%

* Percentage of total APT detections tracked by Trellix telemetry.

TOP THREAT ACTOR GROUPS BY INDUSTRY EVENTS, Q2 TO Q3*



* Percentage of total APT detections tracked by industry-reported events.

motives, leverages a broader array of tools, and targets a wider set of organizations in addition to its strategic priorities – such as attacking military infrastructure, from defense industries to top nuclear engineers, in the United States, Israel, Australia, and Russia.

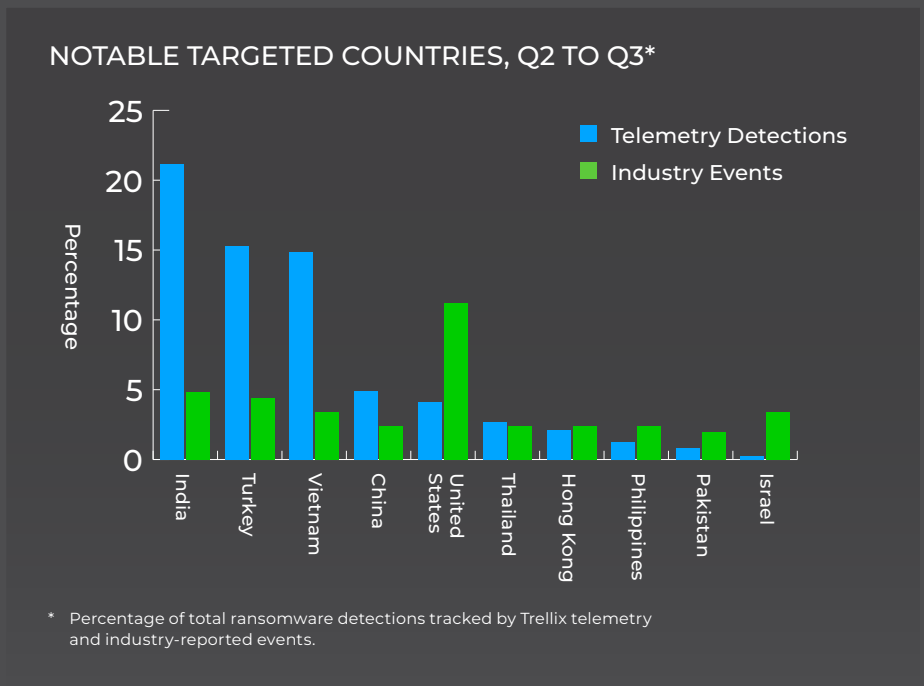
Targeted Countries and Regions

Comparing the global telemetry and industry reports helps highlight trends that reflect some of the world's military conflicts and socio-economic tensions in 2023. Russian-backed APT groups continue to execute coordinated cyberattacks on Ukrainian organizations and agencies. At the same time, while China rattles its sabers up and down the Taiwan Strait, Chinese-affiliated actors are assaulting Taiwan with cyberattacks. In a similar manner, North Korean APT groups are targeting South Korea.

Threat data involving other countries also reflects global events. Though not yet demonstrably tied to larger geopolitical conflicts or developments, it appears that major, established actors are refocusing or expanding their activities to target specific regions.

- **The Israel-Hamas War:** Though hostilities didn't begin until October, and thus aren't reflected in the data underlying this report, industry reports and detections in that region increased notably in the preceding months. While it is unclear whether this activity was a precursor of the incidents to follow, we can say the activities from Pakistani, Iranian and Saudi Arabian APT groups certainly helped further destabilize the region.
- **The India-Pakistan Axis:** For instance, APT36, a threat group affiliated with Pakistan, has a long history of targeting Indian defense and government entities. Over the last two quarters, however, the group's activity reflects a rising focus on the education sector in what may be a strategic attempt to monitor and perhaps compromise India's advances in research and technology. Several other APT groups are targeting India, driven perhaps by India's hosting and presiding over the G20 Summit in December 2022.
- **Turkey and the Middle East:** APT activity has also increased with attacks on Turkey, another G20 member. GoldenJackal's focus appears to be associated with the group's expanding interest in attacking countries in the Middle East. Also, SideWinder – which used to focus principally on Pakistan and Sri Lanka – has switched its attention to Turkey, though why isn't clear.

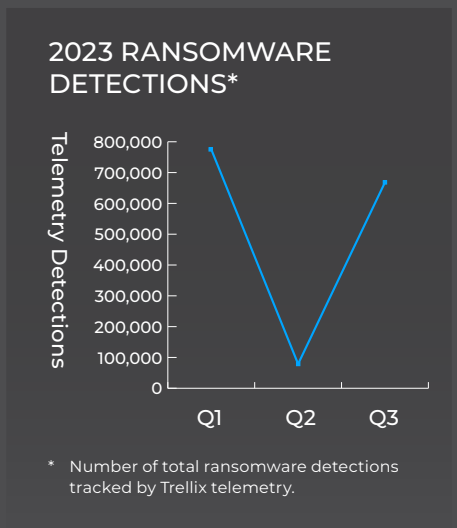
We will be tracking these new patterns closely in the months ahead.



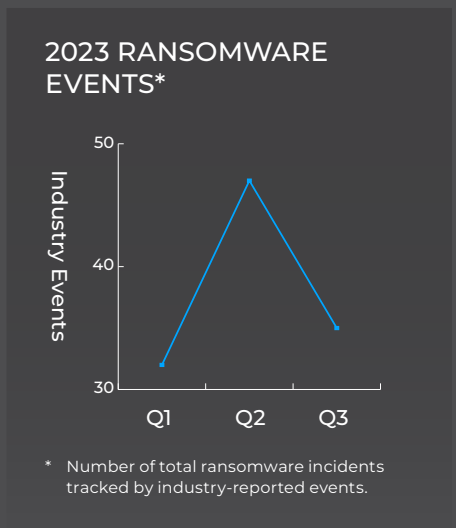
* Percentage of total ransomware detections tracked by Trellix telemetry and industry-reported events.

RANSOMWARE LANDSCAPE EVOLUTION

Ransomware continues to be the most common type of cyberattack worldwide. Global detections and industry-reported incidents, particularly in Q2 reflect unusual variations in ransomware families, as well as countries and industries targeted. Data for Q1 is provided for context.



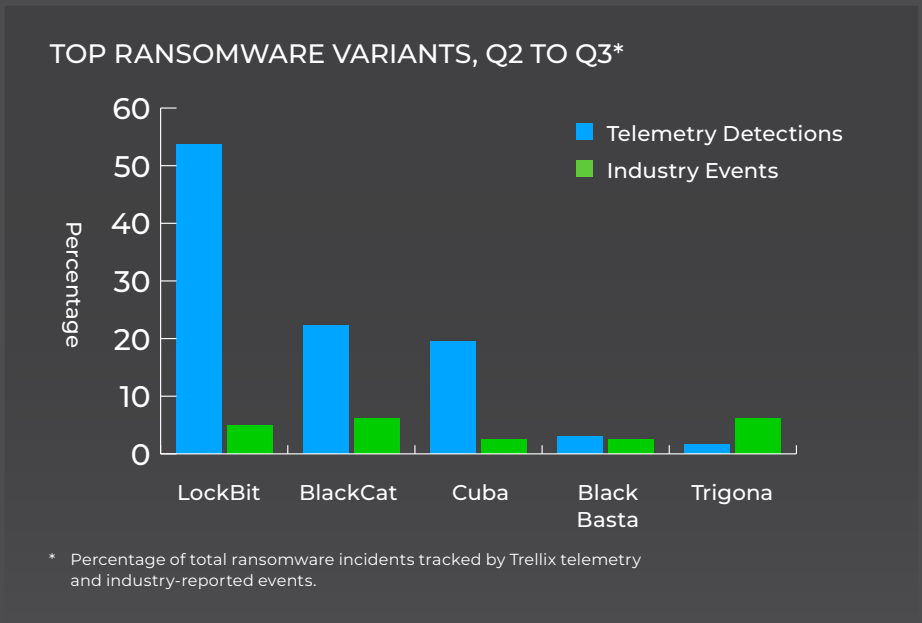
* Number of total ransomware detections tracked by Trellix telemetry.



* Number of total ransomware incidents tracked by industry-reported events.

Active Nation States and APT Groups

Analysis of Q2 and Q3 activity indicates that the “usual suspects” are at the top of the list. LockBit was detected far more often (54%) than other variants, followed by BlackCat (22%) and Cuba (20%). The most common industry-reported events, however, were BlackCat and Trigona (both at 6%).



* Percentage of total ransomware incidents tracked by Trellix telemetry and industry-reported events.

At the start of the year, threat actors prominent in 2022, like LockBit and Royal, continued to dominate the landscape.

However, in Q2, lesser-known actors emerged prominently on the scene. BlackCat was the most commonly detected variant (51%), followed by the Black Basta, Trigona, Rorschach, and Cyclance families. Rorschach (6%) and Black Basta (4%) were also the most frequently reported variants. Trigona (9%) was too, for a short while, until a group known as the Ukrainian Cyber Alliance apparently wiped Trigon's servers.

In Q3, we observed a "return to form" as the major players regained their prominence in both global telemetry and industry events. The most common were LockBit (60% of detections, 9% of reports), BlackCat (22% of detections, 9% of reports), and Cuba (19% of detections, 6% of reports).

THE BIG HEADLINE: Cl0p AND MOVEit

The largest ransomware incident during this period was the MOVEit attack by Cl0P, a data exfiltration exploit that impacted 2,500+ organizations. Cl0P leveraged a specific CVE against the managed file transfer software MOVEit, which allowed it to exfiltrate data at scale.

Despite the attack's sophistication, Cl0P seemed to struggle with handling the volume of data and communicating with victims. This factor, as well as the resources and time Cl0p invested for minimal return, calls into question the attackers' objective.

SMALLER ACTORS: ARE THEY TAKING THE STAGE?

Ransomware actors and groups are rapidly taking advantage of affiliate relationships, enhanced collaboration, and more vigorous communications across the cybercriminal underground. They can now execute sophisticated, wide-scale attacks today far more easily than in the past.

CONVERGENCE? A NEW TREND TO TRACK

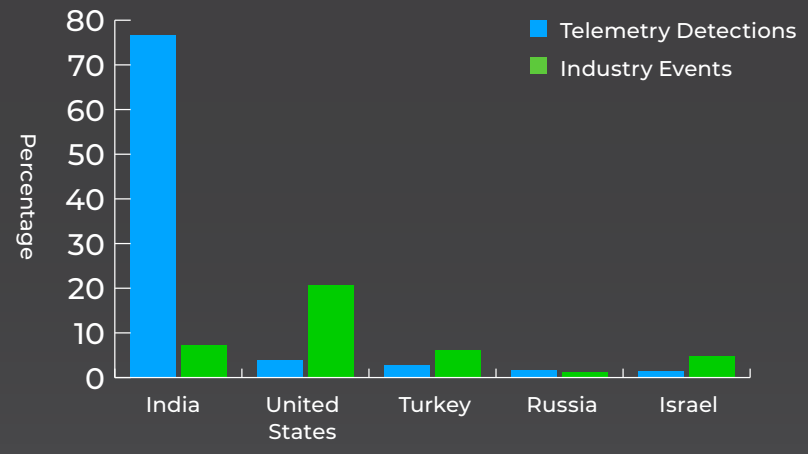
The countries enduring the highest ransomware activity correlate unsettlingly closely with the APT nation-state trends.

This may just be a coincidence. Or it could be an early sign that the goals, targets, and attack methods of ransomware actors and APT groups are starting to converge.

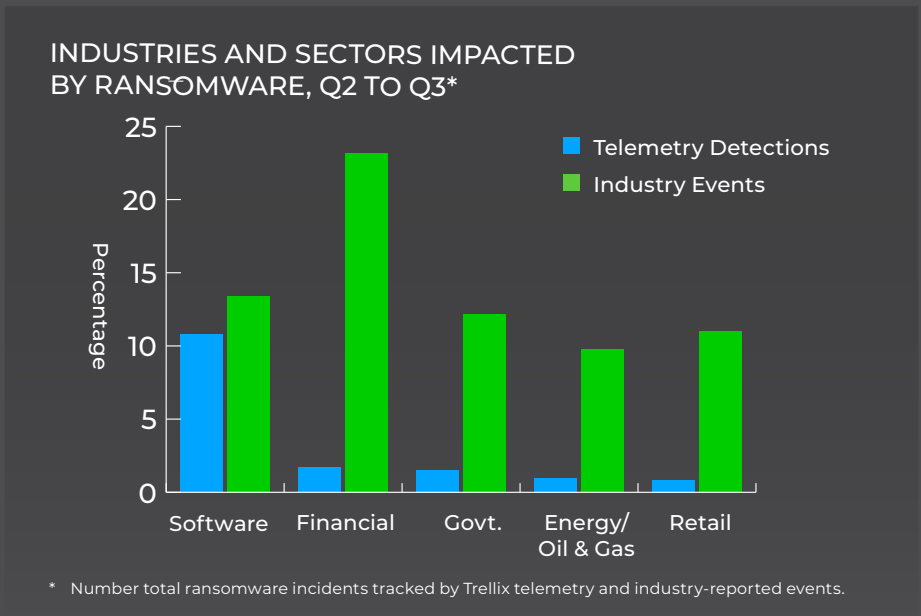
Targeted Countries and Regions

Geographically, for Q2 and Q3, we observed some surprising activity. India accounted for the vast majority (77%) of ransomware detections and ranked high among reported industry events (7%). The next two nations with the most detections and events were the United States and Turkey. Israel, Ukraine and Russia also ranked highly for ransomware activity during this period.

GEOGRAPHIC DISPERSION OF RANSOMWARE, Q2 TO Q3*



* Percentage of total ransomware incidents tracked by Trellix telemetry and industry-reported events.



* Number total ransomware incidents tracked by Trellix telemetry and industry-reported events.

THREAT ACTOR BEHAVIORAL SHIFTS

Actors' Collaboration

In the second half of 2023, a troubling trend emerged – one we have been anticipating for a while. Threat actors are starting to collaborate. This new behavior is driven by both practical goals, such as the sharing or selling of zero-day vulnerabilities and exploits, as well as political ones. These collaborations take many forms depending on the groups' shared interests, motivations, and political beliefs.

By leveraging each other's complementary skills, these groups are maximizing their advantages. Rather than focusing solely on politically motivated attacks involving Distributed Denials of Service (DDoS), website defacement, and data leaks, they have shifted their focus to ransomware activities, incorporating a double extortion scheme.

ABOUT "THE FIVE FAMILIES"

One very prominent new collaboration – an extended network referred to as "The Five Families" – is a great example of threat actors joining forces to increase the speed, operational efficiency, and impact of their cyberattacks.

The loosely organized coalition of 2,000+ members consists of the Stormous ransomware group as well as Blackforums underground forum group.

Other collaborations are driven by political goals. We have observed a distinct increase in the number of hacktivist collectives operating in the digital limelight of the Russia-Ukraine conflict. Actors like the following are pooling their resources and efforts, especially those who are pro-Russian.

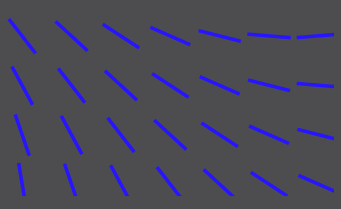
- **Darknet Parliament:** This group is targeting the Western world's banking system by launching attacks on the SWIFT payment infrastructure.
- **Net Worker Alliance:** This collective is another set of pro-Russian groups that have formed an alliance, driven by their common adversaries, NATO countries, and the West, in general.

Similarly, enhanced collaboration among threat actors is emerging on the periphery of the Israel-Hamas conflict. Immediately after the war erupted in October, our team observed a massive increase in cyberactivity. Since the start of the conflict, we have identified almost 80 pro-Palestinian groups targeting Israeli organizations with cyberattacks, and over two dozen pro-Israeli actors engaging in opposing activities. Among the hundreds of attacks between these parties so far, notable incidents include the compromise of the personal data of Israel Defense Forces soldiers and its sale on the dark web; the leak of stolen credentials associated with several key Palestinian government offices; and cyber attacks and compromises that have helped both sides target the other's critical infrastructure.

Zero-day Proliferation

During the latter part of 2023, we have continued to observe underground threat actors actively promoting zero-day exploits targeting vulnerabilities in both Windows and Linux systems. Some of the noteworthy vulnerabilities actively discussed on the dark web include the following:

- **Local Privilege Escalation (LPE):** Underground forums feature many advertisements for zero-day LPE vulnerabilities for Windows operating systems.
  - **Function and Impact:** These enable threat actors to escalate user privileges to SYSTEM or Domain administrators. They often come bundled with features such as User Account Control (UAC) bypass, and the ability to disable antivirus software.
  - **Examples of Exploits Sold:** These include zero-day exploits for CVE-2023-36874, CVE-2023-29336, and CVE-2023-36874, among others.



- **Remote Code Execution (RCE):**
  On the dark web, we have observed the sale of RCE zero-day exploits that affect various software applications and systems.
  - **Function and Impact:** These vulnerabilities have been found to impact Citrix products, the Discord application, Veeam software, and network appliances from vendors such as Draytek,
    TP-Link, and SonicWall.
  - **Examples of Exploits Sold:** One particularly notable zero-day RCE vulnerability was associated with the qTox client, which is widely adopted by threat actors for encrypted instant messaging. The discovery of this vulnerability caused concern within the cybercrime community as it risked exposing the real identities of threat actors. As a result, many either discontinued the use of the TOX messaging platform entirely or switched to alternative TOX clients.

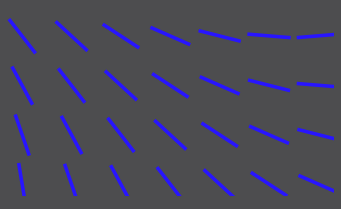
Vulnerabilities that allow for RCE and LPE are some of the most attractive for threat actors to exploit. While selling such exploits is not a novel practice – and several specialized actors have designed their entire business model around their development and sale – the prevalence of these zero-day exploits in the underground has notably increased.

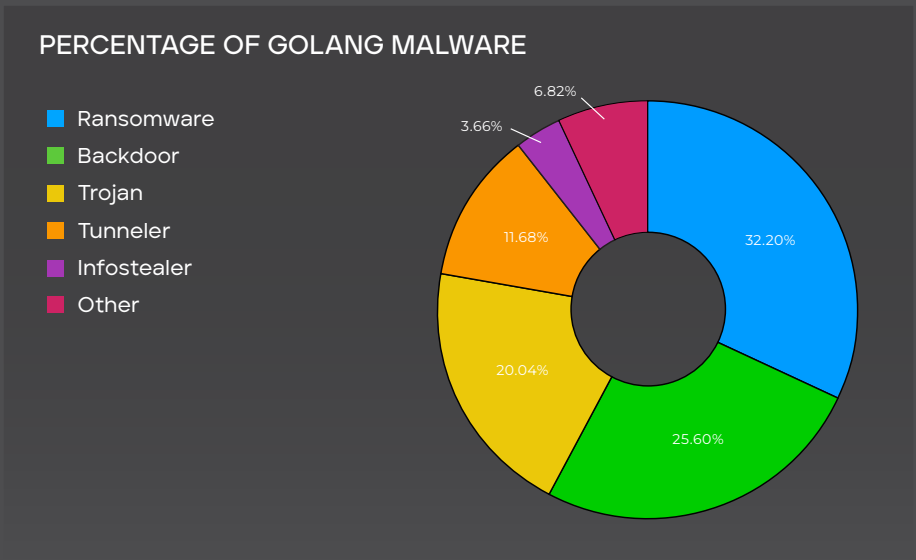
In effect, zero-day vulnerabilities discovered today are swiftly distributed among the underground network of threat actors, and rapidly end up in the hands of the most sophisticated and dangerous groups. Zero-day vulnerabilities are a more urgent threat than ever before, with major threat actors ready and waiting for the next big vulnerability they can exploit (e.g., the next Log4J, MOVEit or BlueKeep) to cause immense damage and lucrative financial windfalls.

Polyglot Malware

In recent years, there has been a noticeable rise in the use of newer programming languages such as Golang (or Go, as it is formally known), Nim, and Rust to develop malicious software. While the volume is still low compared to older languages like Python or C++, threat actors are clearly embracing this new capability.

These languages are attractive to cybercriminals for many reasons. Nim's focus on performance and expressiveness makes it useful for creating intricate malware. Rust's memory management features are attractive to ransomware groups concerned about the encryption efficiency of their samples. Go's simplicity and concurrency capabilities have made it a favorite for crafting lightweight and speedy malware. In 2023, we have observed that Golang-based malware is increasingly popular among bad actors – and have identified several emerging patterns we will be tracking closely in the months ahead.





At the beginning, cybercriminals used to employ Golang primarily to build infostealer samples that help elicit confidential data from victims, a practice that now represents only 3.66% of detections. This year, cybercriminals using Golang as ransomware represent nearly a third of detections (32%). The fact that malware authors have used Golang to build ransomware at this scale is a troubling shift in complexity and maturity. Backdoor and Trojan samples are prevalent among Golang samples, representing about 25% and 20% respectively. These types of malware tend to be distributed using fake software to infect any user who downloads it.

Particularly noteworthy, however, are incidents where APT actors have developed malware using Golang among their methods and tactics. For instance, earlier this year, security researchers uncovered a new attack in Ukraine by Sandworm. The APT group's SwiftSlicer wiper was developed using Golang. Several other incidents have been observed such as the Russian state-sponsored group APT28 distributing a Go-based version of their Zebrocy malware, and China-affiliated Mustang Panda APT deploying a new Go-based loader in several recent attacks. These observations underline how cybercriminals are adapting to the threat landscape using new technologies.

Edge Devices

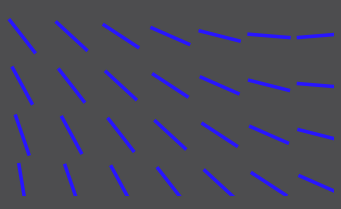
There is a significant and somewhat stealthy shift in the threat landscape underway, centering on the often-overlooked realm of edge devices. While the attack surface is definitely expanding thanks to the number and diversity of connected devices in enterprises, edge devices like routers and access points – no matter which sector they operate in – are becoming the new frontier for threat actors, including APT groups.

Detections of malware attacking these types of edge devices continue to rise across all vendors of access point devices. Threat actors leverage vulnerabilities on these devices for many purposes – such as creating a foothold supporting network investigation; establishing webshells or backdoors on the network; escalating privileges; utilizing the devices for DDoS botnet purposes; and even conducting strategic cyberespionage for nation-states.

What sets the threats to edge devices apart from normal is their subtlety. It's not about the easily foreseen IoT vulnerabilities, but rather the less conspicuous challenges posed by the devices themselves. Edge devices have their unique complexities. However, they cannot detect intrusions. Unlike traditional network components, they cannot simply be connected to another IDS or IPS. The gateways to our digital world are, by design, the first and last lines of defense. This makes them both the target and the blind spot. The evolving tactics of threat actors and the wealth of edge device architectures present with formidable challenges.

During 2023, we encountered several incidents in which APTs and sophisticated ransomware families leveraged edge device vulnerabilities for significant attacks:

- **Ivanti Endpoint Manager Mobile**
  CVE-2023-35081 and CVE-2023-35078 were both flaws in Ivanti Endpoint Manager Mobile. The former was a path traversal vulnerability, while the latter was an authentication bypass vulnerability. Though these have since been patched, they were exploited in the wild in July 2023 for a set of attacks targeting Norway and its government sector. The specific identity of the threat actor is still unknown but, based on targets, many experts, including our teams, suspect it to be an APT.
- **Barracuda Email Security Gateway**
  CVE-2023-2868 was a Barracuda Email Security Gateway remote command injection zero-day vulnerability. This flaw was exploited by many pieces of malware, stretching back to October 2022, before it was addressed through the BNSF-36456 patch in May 2023. UNC4841, an espionage actor linked to the People's Republic of China, was observed extensively leveraging this exploit to attack education, government, and research organizations across China, Hong Kong, and Taiwan.



- **Progress MOVEit Transfer**
  CVE-2023-34362 was an SQL injection vulnerability found in a MOVEit transfer web application. This vulnerability was exploited by the Cl0p ransomware family in May and June 2023. The group targeted the financial, education, energy, healthcare, technology, and government sectors in countries that included Belgium, Canada, France, Germany, Luxembourg, Switzerland, the United Kingdom, and the United States. The group's actions following the data exfiltration, however, indicate that their primary goal was likely aligned closer to APT activity than a ransom payout.

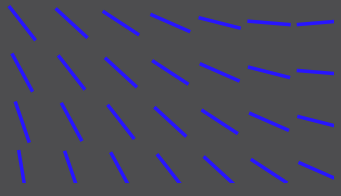
THE THREAT OF GENERATIVE AI

Benefits to Cybercriminals

With the advancement and evolution of artificial intelligence (AI) technology and new large language models (LLMs), we've seen new solutions and applications leveraging these innovations for cybersecurity. But, while these LLMs exhibit remarkable technological potential for positive applications, their dual-use nature also makes them vulnerable to malicious exploitation by threat actors. Leading generative AI applications like GPT-3.5, GPT-4, Claude and PaLM2 have achieved unparalleled capabilities in generating coherent text, answering intricate queries, solving problems, and coding, among other natural language tasks.

Our team harbors, however, significant and reasonable security concerns on how cybercriminals can misuse them for a large-scale attack. Unlike earlier less sophisticated AI systems, today's AI applications offer a potent and cost-effective tool for hackers, eliminating the need for extensive expertise, time, and resources. These AI applications are capable of mitigating considerable challenges encountered by cybercriminals – both smaller actors looking to increase the scale of their activities and larger groups aiming to improve targeting or efficiency. Some examples common to phishing attacks include:

- **Proficiency Prerequisites** – Cybercriminals with limited expertise and modest technical skills can proficiently use AI tools to write malware for their attacks. These applications allow attackers to dedicate their attention to advanced strategizing and execution, offering a more streamlined approach that enhances the overall impact of their malicious activities.
- **Quality for Quantity** – Crafting personalized phishing emails is a labor-intensive task – especially for spear-phishing. However, leveraging generative AI for this purpose produces emails that mimic human composition while requiring minimal engagement from the attacker. They can allow attackers to generate substantial volumes of convincing phishing emails, with a high level of spelling accuracy, in short periods of time.



- **Operational Workload** – These tools adeptly manage substantial volumes of unstructured data during the initial data-gathering stage in addition to operating continuously. They can significantly reduce the per-user expenditure of an attack, making it financially viable for cybercriminals to broaden their target audience. As the cost of cognitive resources continues to decrease, this expense becomes even more trivial.
- **Automated Social Engineering** – Cybercriminals are increasingly turning to technology to automate social engineering. Bots are used to gather data and deceive victims into sharing sensitive information like OTPs. This approach reduces the need for extensive human involvement and minimizes post-attack traces. Consequently, underground markets have emerged, offering automated social engineering tools, including OTP/SMS bots and LLM-based web crawlers.

Blackhat LLMs in the Wild

The availability of free and open-source software is what originally led to the rise of "script kiddies," individuals with little-to-no technical expertise using pre-existing automated tools or scripts to launch attacks on computer systems or networks. Though they are sometimes dismissed as unskilled amateurs or Blackhat wannabes, the growing availability of advanced generative AI tools and their potential for malicious malware usage means that almost any threat actor can pose a significant and growing threat to the market.

SOCIAL ENGINEERING SCAMS ARE NOW MORE LIKELY TO INVOLVE AI-GENERATED VOICES

As these can now closely mimic human speech patterns and nuances, differentiating between real and fake voices is becoming more difficult.

AI-generated voices can also be programmed to speak multiple languages, allowing scammers to target victims across diverse geographic regions and linguistic backgrounds – automating and amplifying their fraudulent activities' reach and effectiveness.

Cybercriminals can leverage LLM tools to improve the key stages of a successful phishing campaign by gathering background information, extracting data to craft tailored content, and generating phishing emails at scale for low marginal costs. Though little conclusive proof yet exists suggesting that this is already starting to occur, with malicious LLMs utilized in the wild for attacks, certain trends in activity imply it is a real possibility. The speed and scale at which phishing attacks are growing, with hundreds of millions of new attacks each quarter, indicates that attackers are using LLM tools to assist in their activities.

Weaponized generative AI is only the beginning though. More advanced tools are emerging, utilizing generative AI to outsmart endpoint security, creating signature-eluding malware, and posing

a persistent strategic threat to cybersecurity. Future malicious generative AI apps will offer comprehensive defense evasion and near-total anonymity and difficulty in attribution, challenging security teams in tracing attacks. This will extend dwell times, facilitating "low and slow" APT-style attacks. Inevitably, generative AI will democratize these capabilities for all attackers, making behavior interpretation, anomaly detection, and comprehensive endpoint monitoring essential.

AFTERWORD

Threat Insights and Intelligence – from Trellix: The Story Starts Here

We share our cyberthreat intelligence to give you a solid, fact-based platform supporting some of the most important decisions you'll make in the year ahead. Our purpose is to help you substantially improve your cyber defense and response capabilities in 2024 and beyond – however you choose to leverage the information in this report.

Application: How to Use This Information

- **Strategic planning:** Use it to inform and educate your CEO and board on this year's escalation in the complexity, lethality, and anonymity of cyberthreats. Trellix supports many CISOs and other security leaders with developing use cases tailored to their organization.
- **Financial validation:** Share it as an independent and objective rationale for cyber defense projects and expenses you made during 2023.
- **Budget rationalization:** Incorporate it as a justification for upgrading your existing threat detection and incident response capabilities with better technology.
- **Operational support:** Have your SecOps team read this as a critical resource as well as a perspective on the broader, strategic context of their work.

Each of these application avenues starts with cybersecurity intelligence. Intelligence helps you shape the battlefield. It helps communicate the "story" to your CEO and your board. What you're doing and why. What you need to do and what it costs. Why their support for your agenda is so critical.

That story starts here.

For additional guidance and resources, please visit www.trellix.com.

METHODOLOGY

Collection: Trellix and our seasoned, world-class experts from the Advanced Research Center gather the statistics, trends, and insights that comprise this report from a wide range of global sources.

- **Captive Sources:** In some cases, telemetry is generated by Trellix security solutions on customer cybersecurity networks and defense frameworks deployed around the world in both public and private sector networks, including those delivering technology, infrastructure, or data services. These systems, which number in the millions, generate data from a billion sensors.
- **Open Sources:** In other cases, Trellix leverages a combination of patented, proprietary, and open-source tools to scrape sites, logs, and data repositories on the internet, as well as the dark web, such as "leak sites" where malicious actors publish information about or belonging to their ransomware victims.

Normalization: The aggregated data is fed into our Insights and ATLAS platforms. Leveraging machine learning, automation, and human acuity, the team cycles through an intensive, integrated, and iterative set of processes – normalizing the data, enriching results, removing personal information, and identifying correlations across attack methods, agents, sectors, regions, strategies, and outcomes.

Analysis: Next, Trellix analyzes this vast reservoir of information, with reference to (1) its extensive threat intelligence knowledge base, (2) cybersecurity industry reports from highly respected and accredited sources, and (3) the experience and insights of Trellix cybersecurity analysts, investigators, reverse engineering specialists, forensic researchers, and vulnerability experts.

Interpretation: Finally, the Trellix team extracts, reviews, and validates meaningful insights that can help cybersecurity leaders and SecOps teams (1) understand the most recent trends in the cyber threat environment, and (2) use this perspective to improve their ability to anticipate, prevent, and defend their organization from cyberattacks in the future.

RESOURCES

Threat Report Archives

The Mind of the CISO

Trellix Advanced Research Center Discovers a New Privilege Escalation Bug Class on macOS and iOS

A Royal Analysis of Royal Ransom

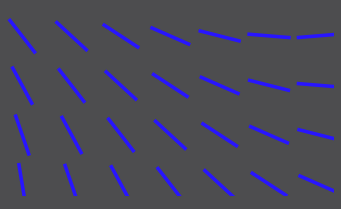
Feeding Gophers to Ghidra

TWITTER

Trellix ARC

View CyberThreat Report Archives

Trellix Advance Research Center



ABOUT THE TRELLIX ADVANCED RESEARCH CENTER

As the cybersecurity industry's most comprehensive charter, the Trellix Advanced Research Center is at the forefront of emerging methods, trends, and actors across the global threat landscape and serves as the premier partner of CISOs, senior security leaders, and their security operations teams across the world. The Trellix Advanced Research Center provides intelligence and cutting-edge content to security analysts while powering our leading XDR platform. Furthermore, the Threat Intelligence Group within the Trellix Advanced Research Center offers intelligence products and services to customers globally.

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 confidence in the protection and resilience of their operations. Trellix, along with its extensive partner ecosystem, has accelerated technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security.

Visit Trellix.com to learn more.

Trellix

072022-05