THE CYBERTHREAT REPORT

June 2023

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

Presented by

Trellix ADVANCED RESEARCH CENTER

چکیده مدیریتی

به گزارش تهدیدات سایبری شرکت ترلیکس (Trellix) خوش آمدید!

این گزارش را مرکز تحقیقات پیشرفته ترلیکس (Trellix Advanced Research Center) ارائه کرده است. گزارشی که شامل شواهدی از فعالیت باج‌افزارها، گردانندگان APT، تهدیدات مبتنی بر ایمیل و استفاده مخرب از ابزارهای معتبر است.

آمار و اطلاعات ارائه شده در این گزارش، برگرفته از بیش از یک میلیارد حسگر ترلیکس و بررسی مستمر محققان این شرکت در خصوص فعالیت تهدیدات سایبری و مهاجمان آنها است.

هدف از ارائه این گزارش، تقویت سازوکارهای دفاعی با تکیه بر مخزن عظیم اطلاعات شرکت ترلیکس برای مقابله مؤثرتر با تهدیدات روز افزون و فوق پیچیده امروزی است.

ادغام شرکت‌های مک‌آفی اینترپرایز (McAfee Enterprise) و فایرآی (FireEye)، به‌عنوان دو قدرت امنیت فناوری اطلاعات تحت برند ترلیکس نویدبخش آینده‌ای روشن در مقابله با تهدیدات سایبری است. اطلاعات انبوه شرکت جدید ترلیکس و دامنه گسترده محصولات و مشتریان آن در سرتاسر جهان چشم‌اندازی دقیق را از وضعیت تهدیدات سایبری فراهم می‌کند.

گروه تحقیق و توسعه

شرکت مهندسی شبکه گستر - اولین شرکت فعال در حوزه ضدویروس در ایران

www.shabakeh.net

شبکه گستر
خدمات آگاهی رسانی

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 between January 1, 2023 and March 31, 2023.

Cyberthreats continue to evolve and multiply. At speed and at scale.

As SecOps teams race to defend information, assets, and operations, no single one of them has a full and complete view of the threat landscape.

Why? Gaining perspective requires a broad horizon. Multiple sources. Streams of data. Raw intelligence. Massive volumes of telemetry.

Real insight requires a strategic view across many organizations and industries. And regions. And attack surfaces.

Welcome to the June 2023 edition of The CyberThreat Report.

UNDERSTANDING THE RISKS, THREATS, AND VULNERABILITIES ATTACKERS ARE TARGETING – AND ACTIVELY HUNTING THEM

I spend a great deal of time speaking with board members, CEOs, CISOs, CIOs, CTOs, and other leaders responsible for the cyber defense of nations, governmental agencies, and private sector organizations across industries.

We cover a wide range of topics – from global research, innovation, and intelligence to their SecOps teams' latest cyber defense practices. We talk about their challenges, as Trellix recently documented in our Mind of the CISO thought leadership – e.g., too many different sources of information (35%), changing regulatory mandates and legal requirements (35%), growing attack surfaces (34%), a shortage of skilled staff (34%), and a lack of buy-in and use from other parts of the company (31%).[1]

Almost every one of these interactions, directly or implicitly, addresses the nature of the threat environment. What kinds of attacks are unfolding? What are the most impactful ransomware groups? Which vulnerabilities are targeted? Which nation-states appear to be most active? What threat trends are we tracking in email and network security?

> "As a board member, CEO, CISO, CIO, CTO, or SecOps team member, this knowledge – shared in this report and across Trellix's rich library of guidance, information and perspectives – is often critical to your mission."

At Trellix, we have a lot to share, because we are on the frontlines every day. We're tapping into a massive reservoir of security intelligence, insights, and data gleaned from more than one billion sensors worldwide. As a board member, CEO, CISO, CIO, CTO, or SecOps team member, this knowledge – shared in this report and across Trellix's rich library of guidance, information and perspectives – is often critical to your mission.

My colleague John Fokker, who leads the threat intelligence practice within Trellix's elite Advanced Research Center team, has compiled an excellent report here. Use these insights to help focus your team, tighten your processes, and get the right XDR technologies in place. And let us know where we can focus in future editions to help keep your organization safe, secure, and thriving.

Joseph (Yossi) Tal
SVP, HEAD OF TRELLIX ADVANCED RESEARCH CENTER

IN SUPPORT OF CYBERSECURITY'S FRONTLINE HEROES

I work with heroes. I'm not referring to my team, though they've been viewed as having superpowers throughout their various public and private sector careers.

I'm referring to you. I'm talking about the people and teams worldwide who rely on Trellix's advanced research capabilities – our systems, insights, and intelligence – to protect your organizations from cyberattacks. CISOs, CTOs and CIOs, yes, as well as our colleagues at agencies like Europol, the FBI and NSA, the Cybersecurity and Infrastructure Security Agency (CISA), Australia's Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK). Just as importantly – and perhaps even more so – I'm talking about every member of your SecOps team.

> "As you know intimately from your work every day, cybersecurity is evolving remarkably quickly. Breakthroughs in technology and a powerful shift toward XDR."

What do you think are game changers for your SecOps mission? According to the Trellix report my colleague Yossi mentioned above, cybersecurity leaders around the globe shared their point of view on these. They included better visibility (44%), stronger prioritization of what matters (42%), broader collaboration to address multi-vector attacks (40%), and improved accuracy (37%).[2]

Every one of these factors relies fundamentally on accurate insights, information, and data – like the contents of this report.

As you know intimately from your work every day, cybersecurity is evolving remarkably quickly. Breakthroughs in technology and a powerful shift toward XDR. Shifts in regulation, from laws to liability. Changes in the threat environment. There's a revolution under way, a transformation in how SecOps teams can stay "one step ahead" of the next generation in cyberattacks. Winning always starts with insights, with an understanding of our current state.

We're in this together. Trellix has your back. This report is for you.

John Fokker
HEAD OF THREAT INTELLIGENCE
AND PRINCIPAL ENGINEER
TRELLIX ADVANCED RESEARCH CENTER

[1] Trellix, "2023 Report: The Mind of the CISO," 2023.
[2] Trellix, "2023 Report: The Mind of the CISO," 2023.

Strategic Context: An Unsettled World

Interpreting the data in this report requires understanding "the bigger picture" on a global scale. That's because cyberthreats to organizations worldwide don't occur in a technical vacuum. Among the major drivers of cyber risk are wars and other forces majeures, large-scale shifts in economic cycles, and new vulnerabilities that can emerge any time a team introduces changes to factors such as business models, key partners, core processes, technology adoption, and regulatory compliance. A sampling of factors influencing our Q1 2023 threat data includes:

Russia's Invasion of Ukraine and Asymmetric Warfare Against the West: Cyberactivity for the purposes of espionage, warfare, and disinformation in service of political, economic, and territorial ambitions from major nation-states continues to escalate. Hackers are levying increasingly sophisticated cyberattacks against Western businesses, governments, and infrastructure.

Xi Jinping's Consolidated Control over China and its Geopolitical Aspirations: China's nationalist goals, assertive foreign policy, and corporate espionage practices continue to drive cyber risks as China-affiliated advanced persistent threat (APT) groups dominate the global landscape.

Developing Economies and Rapid Infrastructure Expansion: As many developing regions scale up infrastructure and technology as their economies grow, cybersecurity is often not top-of-mind – leading to many cyber-related vulnerabilities in critical infrastructure.

Global Inflation and its Economic and Political Impacts: This quarter included market volatility, financial and political crises, and pressures on spending priorities and cybersecurity budgets.

Continued Post-COVID Supply Chain Disruptions: New paths to market across regions required shifts in partners, transportation networks, information sharing, and – by extension – cyber risk. Because cyberthreats are impacting the supply chain daily, the need for zero-trust capabilities remains strong across industries.

The Myth of Apple's Superior Security Environment: This persists despite the fact MacOS environments can no longer be considered safe as threat actors start to leverage Golang-based malware at scale and broaden attack vectors to cover numerous operating systems.

Artificial Intelligence Arrives on the World's Stage, Promising Disruption: Cyber defense is helped and hurt by enhanced machine learning, natural language processing, and other advances. As global cyberthreats are evolving and occurring at a scale far faster than human teams can manage, artificial intelligence solutions become vital for enterprise cyber defense.

Cybersecurity: CISO Challenges and the SecOps Revolution

What is one of the most critical challenges for cybersecurity practitioners and SecOps teams? To digest threat intelligence intake – at speed and at scale – and push actionable insights immediately to threat-hunting teams and task forces across organizations.

Trellix's goal? Simplify that journey.

How? By providing the level of automation to get to the responses that organizations need to focus on, using our superior threat intelligence, threat hunting and security operation capabilities embedded into our XDR, host protection, network, and mail products.

This year's Q1 threat environment was also influenced by in-house factors, many of which reflect ongoing headwinds confronting cybersecurity leaders and frontline teams.

Outdated Technology: Many organizations continue to rely on legacy technology like SOAR and SIEM. In fact, 96% of CISOs say they need better solutions to protect their entity from cyber threats.[3]

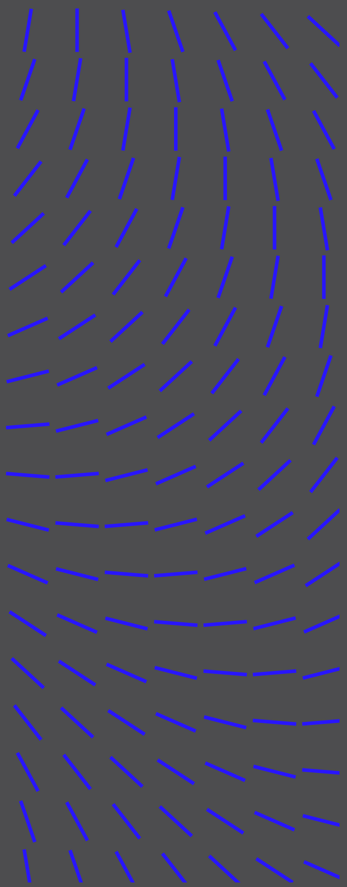
Sea of Security Tools: SecOps teams are flooded with alerts and lack what they need to prioritize their time. On average, organizations employ a confusing array of 25 security solutions and tools.[4]

Alert Fatigue: Inundated with alerts, SecOps teams struggle with prioritization, false positive, and missed alerts. According to IDC, 35% ignore alerts – perhaps, in part, because 45% are false positives.[5]

Insufficient Resources: With limited SecOps resources and expertise, it's hard to counter threats effectively. What's the average SOC analyst tenure? Approximately two years.[6]

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.



Application: How to Use This Information

It’s imperative that any Industry-leading assessment team understands, acknowledges and, where possible, mitigates the effect of bias – the natural, embedded, or invisible inclination to 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.

Central to this investigative ethic is the following:

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 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.

The Road Ahead: Guidance and Resources

What does the information contained in this report mean for cybersecurity heroes on the frontlines? Cybersecurity insights and data are only useful if they are transformed into action – and result in lower risk, improved decision-making, or more efficient or cost-effective SecOps activities. For additional guidance and resources, please visit www.trellix.com.

INTRODUCTION

Q1 2023 HIGHLIGHTS AT-A GLANCE

REPORT ANALYSIS, INSIGHTS, AND DATA

SECURITY INCIDENTS

RANSOMWARE

NATION-STATE ACTIVITY

VULNERABILITY INTELLIGENCE

EMAIL SECURITY

NETWORK SECURITY

CLOUD INCIDENTS

METHODOLOGY

RESOURCES

ABOUT TRELLIX ADVANCED RESEARCH CENTER & TRELLIX

[3] Trellix, "2023 Report: The Mind of the CISO," 2023
[4] Trellix, "2023 Report: The Mind of the CISO," 2023
[5] IDC Voice of the Analysts, 2021
[6] Ponemon Institute, 2020

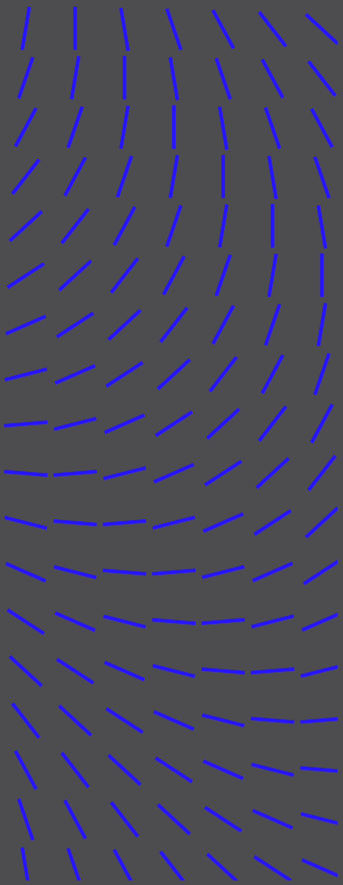
Q1 2023 HIGHLIGHTS AT-A-GLANCE

The Ransomware Landscape

- **The Ransomware Wave:** Ransomware continues to be king as the primary type of cyberattack across the globe. Socially engineered ploys to deceive and manipulate individuals into divulging confidential or personal information, such as phishing, are more prevalent than ever even as they become more sophisticated.
- **Cuba and Play Dominate:** Though we observed a decline in ransom-related cybercriminal activity at the start of the year, the most prevalent ransomware families in Q1 were Cuba (9%) and Play (7%).
- **LockBit Lingers:** Despite a reduction in activity two quarters in a row, LockBit continues to be the most aggressive ransomware in pressuring its victims to comply with ransom demands.
- **Magecart Group Potentially on the Rise?** Public reporting indicates this credit card theft and ecommerce scalping group's activity in Q1 2023 increased tremendously. This threat rarely operates at the same scale of activity as the other major nation-state-affiliated APTs, potentially indicating a re-emergence of Magecart Group worldwide.

Ransomware Tactics Evolving

- **Monetary Objectives:** It's unsurprising that the motivations for ransomware remain primarily financial; the insurance (20%) and financial services (17%) sectors logged the most detections of potential attacks.
- **Mid-Size Businesses Most Impacted:** Evaluation of our leak site data reveals the victims from these attacks are most commonly mid-sized businesses with only 51 to 200 employees (32%) and $10M to $50M in revenue (38%).
- **United States as Primary Target:** The U.S. (15%) was the country most affected by ransomware groups. It was also the country with the highest percentage of corporate victims (48%) who decided to "buy their data back" from the attackers – a rate six times greater than the next nation on the list, the United Kingdom.
- **Cobalt Strike as the Weapon of Choice:** Trellix telemetry identifies this tool as heavily favored by ransomware actors (28% of incidents). It appears to be growing in popularity and usage amongst these groups despite vendor Fortra's attempts in late Q4 2022 to make it harder for threat actors to use it.



Nation-State Red Flags

- **Leading Actors:** For the last six months, APT actors linked to China, including Mustang Panda and UNC4191, were the most active in targeting nation-states in Q1. China-affiliated threat actors dominated the global scene, generating 79.3% of all nation-state activity, followed by actors tied to North Korea, Russia, and Iran.
- **Most Active APT Group:** Mustang Panda persisted for the third quarter in a row as the most active APT group worldwide (72%) – denoting China's continued and growing malicious cyber efforts for the purpose of espionage and disruption.

Vulnerability Intelligence

- **Failure to Address Known Vulnerabilities:** Most of this quarter's most critical vulnerabilities consisted of known vulnerabilities not yet addressed.
- **Yesterday's News:** For a disclosed Apple vulnerability in February of this year, the bug had roots as far back as the FORCEDENTRY exploit, which was used by NSO Group as part of its Pegasus spyware disclosed in 2021.

Email Security

- **New Avenues of Attack:** Although Microsoft has started to block macro attachments for the Office platform, threat actors have quickly adopted other means of infections to continue targeting Windows devices – such as SEO poisoning, OneNote, and Zip attachments.
- **Untrustworthy Brands:** In addition to generic phishing emails, bad actors are increasingly leveraging legitimate brand names and services, like those from PayPal, Google, DWeb, and IPFS, to scam victims and steal their online credentials.

Rogue Access to the Cloud

- **A Shift in Tactics:** Cloud infrastructure attacks continue to rise as more and more businesses transition from on-prem infrastructure to more affordable and scalable options from Amazon, Microsoft, Google, and others.
- **Valid Accounts:** Though more sophisticated attacks with multi-factor authentication, proxies, and API execution are ascendant, the dominant attack technique continues to be through valid accounts, at more than twice the frequency of the second most used attack vector. This emphasizes that the risk of rogue access is real, as cybercriminals access and sell legitimate account or website logins to infiltrate and conduct attacks.

Security Incidents

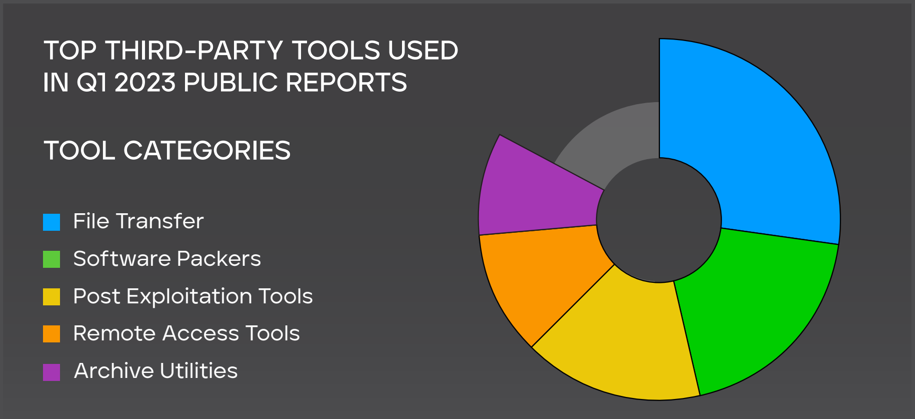
The security incidents discussed in this section are based on public reports. In the first quarter of 2023, windows binaries, third-party tools, custom malware, and penetration-testing tools continued to impact operations as threat actors exploited paths of least resistance. PowerShell and the Windows Command Shell continued to be abused to spawn tasks leading to persistence, deployment, and extraction.

TOP WINDOWS BINARIES USED IN Q1 2023 EVENTS

1. PowerShell
2. Windows CMD
3. Scheduled Task
4. RunDLL32
5. WMIC

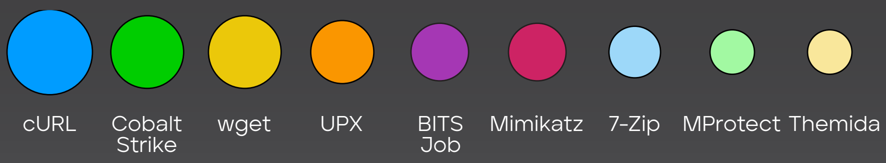
Scheduling tasks, inserting malicious DLL files, and commands executed through Windows management instrumentation rounded out the top 5. Whether executing by scripts or manual keyboard entry, threat actors continued to make use of the unprotected and unmonitored binaries already at their disposal.

In many cases, third-party tools, freeware, and penetration testing tools play a role in an attack lifecycle assisting threat actors in setting persistence, running scripts, discovering and collecting targeted information and escalating privileges to access assets or data that are otherwise inaccessible to restricted accounts. Additionally, when used for privilege escalation, an attacker can run installation processes with elevated privileges and access areas, assets, or data that are otherwise inaccessible to restricted accounts.



THIRD-PARTY TOOLS USED IN Q1 2023 PUBLIC REPORTS

SPECIFIC TOOLS



The more nefarious third-party tools such as Cobalt Strike, Mimikatz, and Sharphound are used both legitimately and by threat actors to gather passwords, set beacons, or elevate privileges. Once an attacker compromises an environment, they can use file transfer tools such a cURL to access remote payloads, or Rclone to exfiltrate data to cloud storage.

In the first quarter of 2023, the Magecart Group, APT29, and APT41 were the three most active threat groups and APTs to target users by geolocation and sectors as methods to collect monetary value, uncover government secrets, or inhibit infrastructure use. We were surprised to discover that the Magecart Group topped the list as it rarely operates at the scale of the other major nation-state-affiliated APTs. We will be monitoring the group's activity in the months ahead to gauge whether the current period's data signals the group's re-emergence on the global stage.

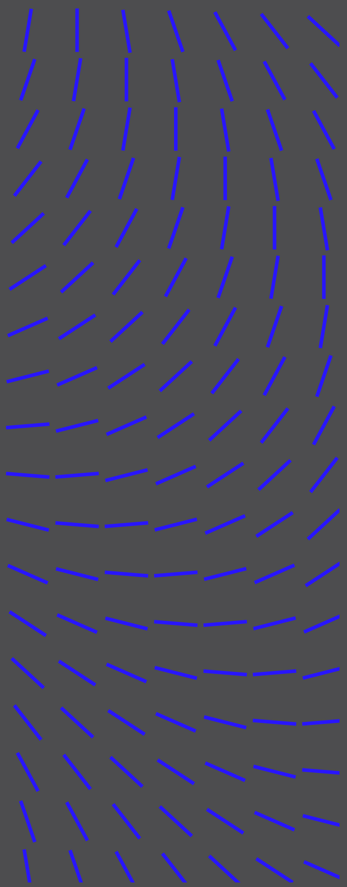
TOP THREAT ACTORS ACTIVE IN Q1 2023 PUBLIC REPORTS

1.	Magecart Group	5%
2.	APT29	4%
3.	APT41	4%
4.	Blind Eagle	4%
5.	Gamaredon Group	4%
6.	Lazarus	4%
7.	Mustang Panda	4%
8.	Sandworm Team	4%

Less sophisticated spray-and-pray techniques designed to snag anyone who might click or download plagued sectors in past global campaigns. Targeted attacks have evolved in sophistication, increasing in persistence against manufacturing, finance, and health sectors. Though the remaining two sectors, telecom and energy, appear to have been targeted less frequently in global

TOP SECTORS TARGETED IN Q1 2023 PUBLIC REPORTS

1.	Manufacturing	8%
2.	Finance	7%
3.	Health	6%
4.	Telecom	5%
5.	Energy	5%



events, both are equally important and organizations within them may not have reported a breach or remain unaware of an incident.

Reported events analyzed and vetted by our research team contain a wealth of information, correlations, or attributions of an individual threat actor, a threat group, or a more sophisticated APT. The tools, techniques, and procedures along with malware families include loader and downloader malware, RATs, information stealers, and ransomware. In the Q1 2023 events analyzed and available via Insights, we determined that Ukraine was targeted most frequently, followed closely by the U.S.

The Royal Ransom, Trigona, and Maui ransomware families were the heavy hitters in Q1 2023. Trellix recently published a detailed analysis of Royal Ransom and its inner workings with Windows and Linux executables. Although statistics represented emerged specifically from our Insights platform, many additional events occurred across the globally connected infrastructure – including known events either reported or kept private and events that have yet to be identified and remediated.

TOP COUNTRIES TARGETED IN Q1 2023 PUBLIC REPORTS

7%

In the public events available for analysis, we determined that Ukraine was the most targeted country by threat actors, followed closely by the United States.

1.	Ukraine	7%
2.	United States	7%
3.	Germany	4%
4.	South Korea	3%
5.	India	3%

TOP RANSOMWARE USED IN Q1 2023 PUBLIC REPORTS

1.	Royal Ransom	7%
2.	Trigona	4%
3.	Maui	4%
4.	Magniber	3%
5.	LockBit	3%

Ransomware

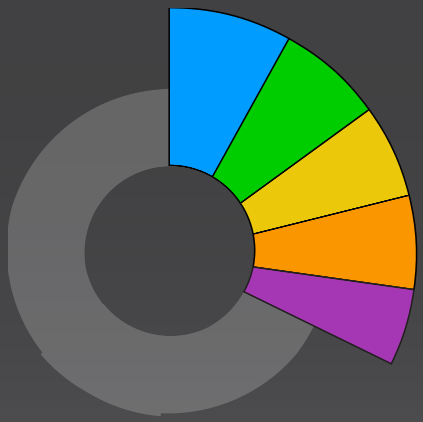
The statistics displayed below are those of the campaigns, not the detections themselves. Our global telemetry revealed indicators of compromise (IoCs) belonging to several campaigns from various ransomware groups.

It’s fairly common to see a drop in cybercriminal activity at the start of the year, especially in January. This trend could explain the notable decrease in activity for both Hive and Cuba. Furthermore, the FBI and Europol’s disruption of Hive’s activities in late January would have significantly interfered with their operations. LockBit continues to be a major family in the ransomware space – and is especially aggressive and seemingly successful at pushing victims to pay their ransoms.

TOP RANSOMWARE USED IN Q1 2023 EVENTS

8%

Cuba was the most active ransomware group, followed by Play and LockBit.

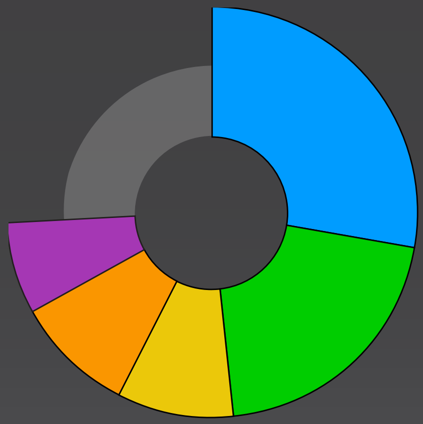


- 🟦 Cuba
- 🟩 Play
- 🟨 LockBit 3.0
- 🟧 Clop
- 🟪 Hive

RANSOMWARE TOOLS USED IN Q1 2023

28%

CobaltStrike was used in almost a third of all ransomware incidents in the quarter, only growing in usage despite recent updates to make it harder for threat actors to abuse the tool.



- 🟦 Cobalt Strike
- 🟩 Mimikatz
- 🟨 Empire
- 🟧 BloodHound
- 🟪 SystemBC

COUNTRIES MOST IMPACTED BY RANSOMWARE GROUPS Q1 2023

15% 🇺🇸

The United States continues to be the country most impacted by ransomware activity, closely followed by Turkey this quarter.

1.	United States	15%
2.	Turkey	14%
3.	Portugal	10%
4.	India	9%
5.	Canada	9%

SECTORS MOST IMPACTED BY RANSOMWARE GROUPS Q1 2023

1.	Insurance	20%
2.	Financial Services	17%
3.	Pharma	7%
4.	Telecom	4%
5.	Outsourcing & Hosting	4%

Ransomware groups extort victims by publishing their information on websites referred to as "leak sites," using the exposure to jumpstart stalled negotiations with victims or when payment of the ransom is refused. Our Trellix experts use RansomLook, an open-source tool, to collect data from the posts, and then normalize and enrich the results to provide an anonymized analysis of victimology.

It is important to note that not all ransomware victims are reported in the respective leak sites. Many victims pay the ransom and remain unreported. The metrics below are an indicator of the victim ransomware groups targeted for extortion or retaliation and should not be confused with the total number of victims.

RANSOMWARE GROUPS REPORTING MOST VICTIMS PER LEAK SITES Q1 2023

1.	LockBit	30%
2.	Hive	22%
3.	Clop	12%
4.	Royal Ransom	7%
5.	ALPHV	5%

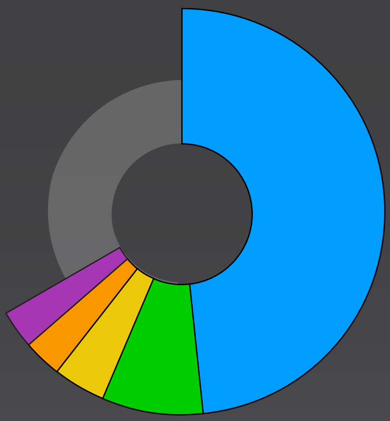
SECTORS MOST AFFECTED BY RANSOMWARE GROUPS PER LEAK SITES Q1 2023

1.	Industial Goods & Services	25%
2.	Retail	14%
3.	Technology	11%
4.	Health	8%
5.	Financial Services	6%

TOP COUNTRIES OF COMPANIES LISTED ON RANSOMWARE LEAK SITES Q1 2023

48%

of victim companies listed on ransomware groups' leak sites were based in the United States.



SIZE OF COMPANIES LISTED ON RANSOMWARE LEAK SITES Q1 2023

EMPLOYEE RANGE		
1.	51-200	32%
2.	1,000-5,000	22%
3.	11-50	15%
4.	201-500	15%
5.	501-1,000	15%

ANNUAL REVENUE		
1.	$10M-$50M	38%
2.	$1B-$10B	23%
3.	$1M-$10M	21%
4.	$100M-$250M	11%
5.	$500M-$1B	7%

Nation-State Activity

Insights on nation-state group activity gathered from multiple sources create a better picture of the threat landscape and help reduce 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.

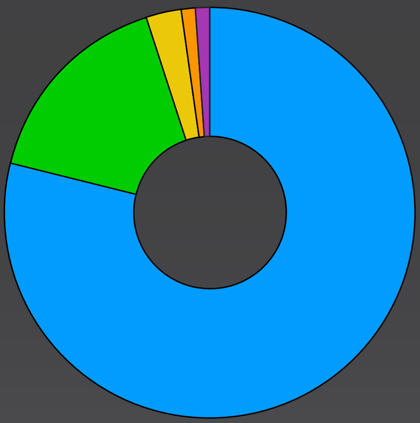
As noted above, these statistics are those of the campaigns, not the detections themselves. Due to various log aggregations, our customers' use of threat simulation frameworks, and high-level correlations with the threat intelligence knowledge base, the data is manually filtered to meet our analysis goals.

We continue to see China-affiliated threat actors dominate the global landscape, particularly with Mustang Panda driving a significant majority of detections in Q1 2023. Since they rely heavily on sideloading and other techniques for stealth, it's possible Chinese-affiliated APT groups rotate their malware tools less frequently compared to other threat actors. If so, this practice could lead to "projection bias" or an inflated estimate of the detections of Chinese-affiliated hashes.

MOST PREVALENT THREAT-ACTOR COUNTRIES BEHIND NATION-STATE ACTIVITY Q1 2023

79%

China accounted for a dominant majority of the Nation-State-related activity in Q1 2023.



MOST PREVALENT THREAT-ACTOR GROUPS Q1 2023

1.	Mustang Panda	72%
2.	Lazarus	17%
3.	UNC4191	1%
4.	Common Raven	1%
5.	APT34	1%

MOST PREVALENT MITRE ATT&CK TECHNIQUES USED IN NATION-STATE ACTIVITY Q1 2023

1.	LDLL Side-Loading	14%
2.	Deobfuscate/Decode Files for Information	11%
3.	Ingress Tool Transfer	10%
4.	Data from Local System	10%
5.	File and Directory Discovery	10%

MOST PREVALENT MALICIOUS TOOLS USED IN NATION-STATE ACTIVITY Q1 2023

38%

PlugX accounted for 38% of malicious nation-state activity in Q1 2023.

1.	PlugX	38%
2.	Cobalt Strike	35%
3.	Raspberry Robin	14%
4.	BLUEHAZE/DARKDEW MISTCLOAK	3%
5.	Mimikatz	3%

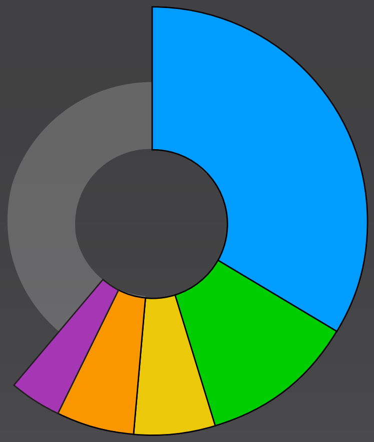
India is one of the leading countries in Asia and neighboring regions with capable cyber programs. Some groups, predominantly China-linked threat actors, have demonstrated great interest in India's technological, military, and political developments. A notable number of detections in India can be attributed to Mustang Panda.

COUNTRIES WITH MOST DETECTIONS OF NATION-STATE ACTIVITY Q1 2023

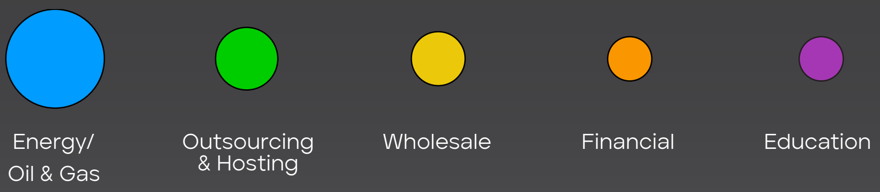
34%

The Philippines led the list of countries with the most detections of nation-state activity in Q1 2023.

- 🟦 Philippines
- 🟩 India
- 🟨 Myanmar
- 🟧 Cameroon
- 🟪 United States



SECTORS WITH MOST DETECTIONS OF NATION-STATE ACTIVITY Q1 2023



Vulnerability Intelligence

Trellix Advanced Research Center's experts in reverse engineering and vulnerability analysis continuously monitor the latest vulnerabilities in order to provide guidance to customers on how threat actors are leveraging them and how to mitigate the probability and impact of these attacks.

One of our most critical, but unsurprising, findings for 2023's first quarter is many of this period's most critical vulnerabilities consisted of bypasses to patches for older CVEs, supply chain bugs resulting from the utilization of outdated libraries, or long-patched vulnerabilities persisting far past their expected five minutes of fame.

Consider CVE-2022-47966 for example, a critical (9.8) vulnerability in Zoho's ManageEngine products that made the rounds this January. ManageEngine is used by thousands of companies worldwide, so we weren't surprised when exploitation of this vuln was detected in the wild. What astonished us was the root cause: utilization of Apache Santuario 1.4.1 – a version nearly old enough to vote – which contained a known issue allowing for XML injection. Zoho patched the vulnerability across its suite of products in October and then, almost three months later in Q1, CISA released an advisory warning of in-the-wild exploitation and urging vendors to patch.

Another example is CVE-2022-44877, a critical vulnerability in Control Web Panel (CWP). Although not directly related, this vulnerability has many of the same characteristics as our previous example: it is another 9.8 RCE that saw widespread active exploitation in January despite being patched back in October. The root cause was not exactly Black Hat-talk worthy, either: command injection using standard shell variable expansion in a URL parameter.

A third example is CVE-2021-21974, a vulnerability in VMware ESXi's OpenSLP service addressed back in February 2021, almost exactly two years before its sudden resurgence due to an in-the-wild exploitation. When we reported on this vulnerability in our February Bug Report, we noted around 48,000 internet-reachable servers were still running vulnerable versions of ESXi according to Shodan. Today, that number is still over 38,000 – a change of less than 22%.

Date	Number of Vulnerable ESXi Servers According to Shodan
Late February 2023	48,471
Late April 2023	38,047

We found a few examples of our own when researching Apple devices earlier this year: CVE-2023-23530 and CVE-2023-23531. These two vulnerabilities differ from the previous examples in that their impact is limited to local elevation of privilege and not RCE. This is not a reason to overlook their significance, however, as a very similar vulnerability was leveraged by the FORCEDENTRY exploit, which was used by NSO Group to deploy its Pegasus spyware back in 2021. In fact, the two CVEs we uncovered utilize the same primitive that served as the basis for the FORCEDENTRY exploit: an innocuous class called NSPredicate. Unfortunately, Apple's approach to mitigating FORCEDENTRY involved the use of an extensive denylist to shore up the ways NSPredicate was being abused – a mitigation which failed to address the underlying problem and allowed us to bypass it.

It is tempting to point to trends such as these and conclude vendors don't take security seriously or bemoan the regurgitation of old exploits by threat actors and researchers, but this isn't the right takeaway. Vulnerability researchers engage in variant analysis because an effective vulnerability researcher emulates the priorities of real threat actors, and finding a mitigation bypass or an old CVE in a rarely patched product consistently produces better ROI than reinventing the wheel. For organizations which rightfully recognize this trend, the takeaway should be this: while cutting-edge threat detection technologies are irreplaceable in the modern threat landscape, many victories can be won on the fundamentals, such as patching processes and supply chain vetting.

Email Security

Email security statistics are based on telemetry generated from several email security appliances deployed on customer networks around the world.

Phishing attacks that leverage legitimate brands to scam users and steal their credentials are on the rise, with DWeb, IPFS, and Google Translate heavily utilized in email attacks. Attackers also abused freemail and other comparable services, such as the two applications PayPal Invoicing and Google Forms, to mount vishing attacks and avoid detection. Similarly targeted during this period were new brands like Scribd, LesMills, and Google Play gift cards.

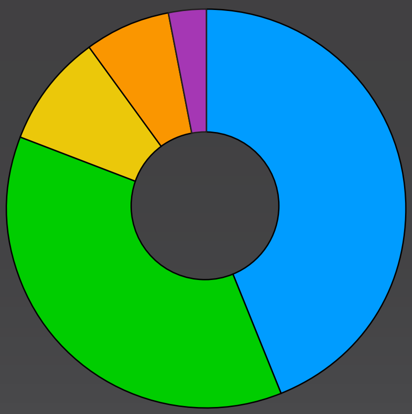
Furthermore, in terms of the specific malware used for these attacks, Formbook and Agent Tesla both saw notable increases in Q1 2023, compared to late last year. This may be driven by the fact both pieces of malware are easier to acquire and deploy, compared to Remcos, Emotet, and Qakbot.

MOST PREVALENT EMAIL MALWARE TACTICS Q1 2023

44%

Formbook accounted for almost half of email malware in Q1, closely followed by Agent Tesla.

- 🟦 Formbook
- 🟩 Agent Tesla
- 🟨 Remcos
- 🟧 Emotet
- 🟪 Qakbot



COUNTRIES MOST TARGETED BY EMAIL PHISHING Q1 2023

30%

The United States and Korea were the primary victims of email phishing attempts in Q1, receiving almost two thirds of all global phishing attempts.

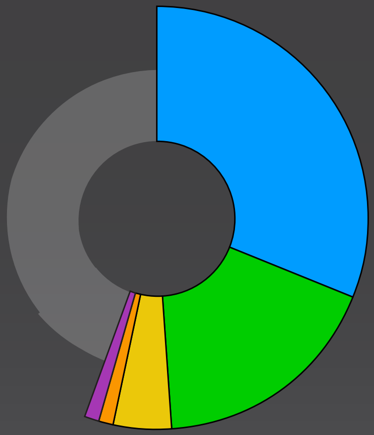
1.	United States	30%
2.	South Korea	29%
3.	Taiwan	10%
4.	Brazil	8%
5.	Japan	7%

PRODUCTS AND BRANDS MOST TARGETED BY EMAIL PHISHING Q1 2023

38%

Though hundreds of brands were targeted, Microsoft products accounted for the most by a long shot in Q1 2023.

🟦 Microsoft
🟩 Google Captcha
🟨 Outlook
🟧 Gcash
🟪 USPS



SECTORS MOST IMPACTED BY MALICIOUS EMAIL Q1 2023

1.	Government	11%
2.	Financial Services	8%
3.	Manufacturing	6%
4.	Technology	6%
5.	Entertainment	5%

HIGHLY ABUSED WEB HOSTING PROVIDERS Q1 2023

1.	IPFS	41%
2.	Google Translate	33%
3.	Dweb	16%
4.	AmazonAWS Appforest	3%
5.	Firebase OWA	3%

EVASION TECHNIQUES MOST USED IN PHISHING ATTACKS Q1 2023

79% 302 Redirect Based Evasion was the most prevalent evasion technique used by phishing attacks in Q1 2023.

46% Captcha-based attacks increased significantly in Q1 compared to Q4 2022.

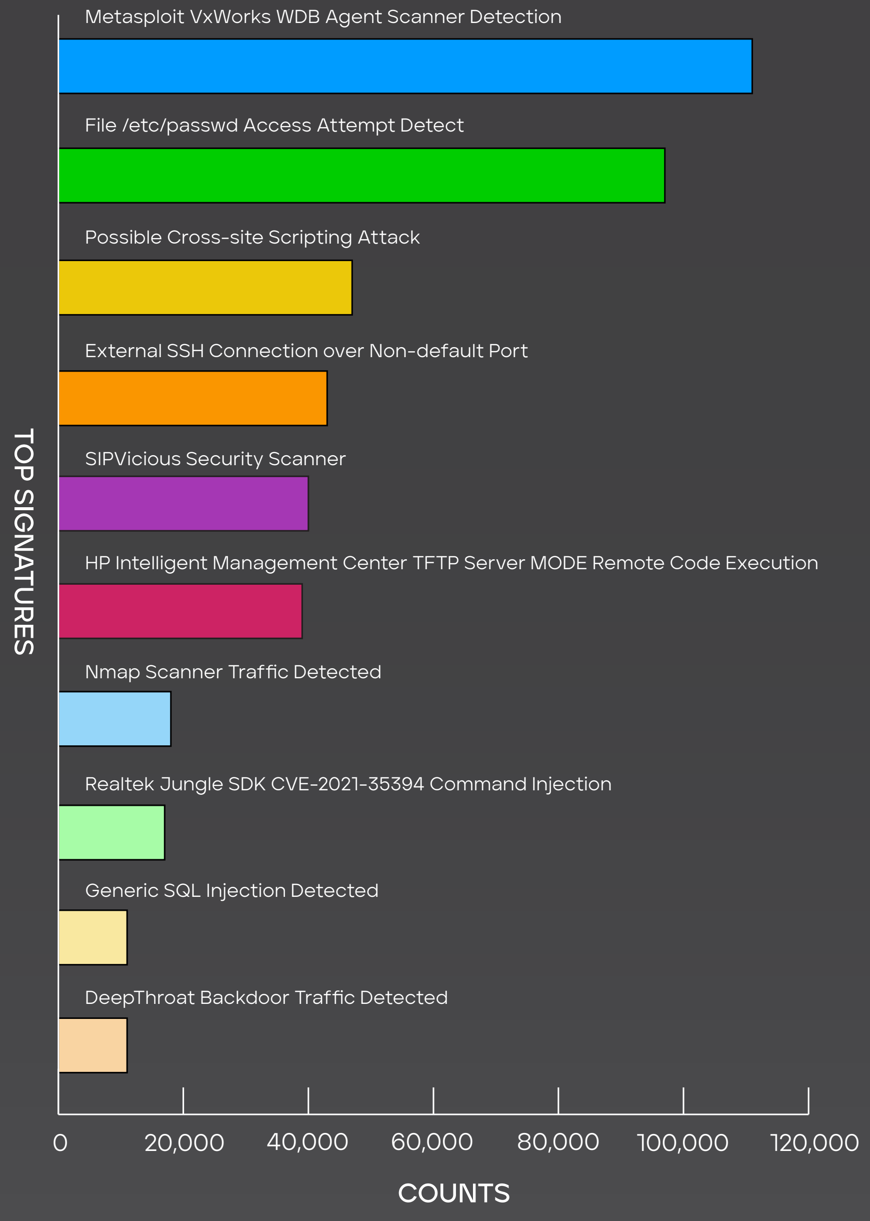
Network Security

In the course of detecting and blocking network-based attacks threatening our customers, the Trellix Advanced Research Center's network research team inspects different areas of the kill chain – from recon and initial compromise to C2 communication and lateral movement TTPs.

MOST NOTEWORTHY MALWARE CALLBACK TRENDS IN Q1 2023

Stop ransomware activity declined	94%
LockBit ransomware distributed by Amadey increased by	25%
Android malware activity increased by	12.5%
Ursnif activity increased by	10%
Smokeloader activity increased by a factor of	7X
Amadey activity increased by a factor of	4X
CobaltStrike activity increased by a factor of	3X
Emotet activity increased by a factor of	2X

MOST IMPACTFUL ATTACKS ON EXTERNALLY FACING SERVICES Q1 2023



Cloud Incidents

Cloud infrastructure attacks on services developed and delivered by Amazon, Microsoft, Google, and others continue to rise. The table below describes the cloud-based attack telemetry data by customer and cloud provider.

DETECTIONS BY MITRE ATT&CK TECHNIQUES Q1 2023

	AWS	Microsoft Azure	GCP
Valid Accounts	3,437	4,312	997
Modify Cloud Compute Infrastructure	4,268	0	17
Non-standard Port	115	0	17
Multi-factor Authentication	190	1,534	22
Network Service Discovery	141	93	0
Brute Force	25	1,869	22
Proxy	299	2,744	135
Account Discovery	264	68	787
Email Forwarding Rule	25	0	22
Execution through API	1,143	0	252

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 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 an extensive partner ecosystem, accelerated technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security.

INTRODUCTION

Q1 2023 HIGHLIGHTS AT-A GLANCE

REPORT ANALYSIS, INSIGHTS, AND DATA

SECURITY INCIDENTS

RANSOMWARE

NATION-STATE ACTIVITY

VULNERABILITY INTELLIGENCE

EMAIL SECURITY

NETWORK SECURITY

CLOUD INCIDENTS

METHODOLOGY

RESOURCES

ABOUT TRELLIX ADVANCED RESEARCH CENTER & TRELLIX

This document and the information continued herein describes computer security research for educational purposes only and the convenience of Trellix customers. Trellix conducts research in accordance with its Vulnerability Reasonable Disclosure Policy I Trellix. Any attempt to recreate part or all of the activities described is solely at the user's risk, and neither Trellix nor its affiliates will bear any responsibility or liability.

Trellix is a trademark or registered trademark of Musarubra US LLC or its affiliates in the US and other countries. Other names and brands may be claimed as the property of others.

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.