# THE CYBERTHREAT REPORT

June 2024

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

**INSIDE:**




Presented by

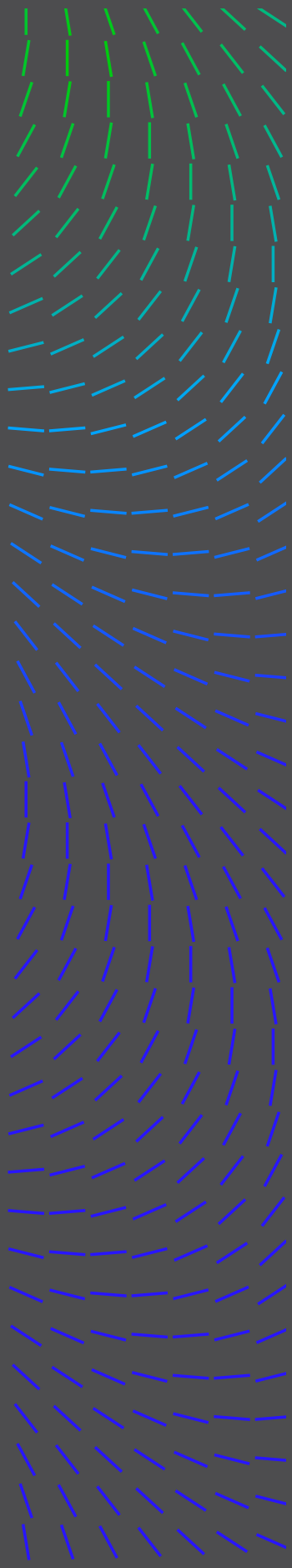
Trellix ADVANCED RESEARCH CENTER

An EDR evasion tool was just successfully used to shut down endpoint detection and response capabilities at another organization in your industry.

The cybersecurity race to outpace attackers and stop them from using legitimate security tools for bad is getting more complicated.

As CISO, you have to move with agility, speed, confidence and control. Your CEO and Board are waiting to know more about your logging and alert tools. You task your team to identify gaps, and you have a plan to address them.

The cybersecurity race is a triathlon. You're competing in SecOps, Technology and Intelligence. The race is on, and it's a game of endurance.



> As defense mechanisms become more sophisticated, so too do the offensive tools and tactics nation-state and cyber criminal actors.

## 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 October 1, 2023, and March 31, 2024.

1. Rapid and Significant Changes in the APT Landscape
2. LockBit Shakes Up Ransomware Ecosystem
3. EDR Killers Emerge
4. U.S. Presidential Election Themed Scams
5. GenAI and the Cybercriminal Underground

## FORWARD

Operational threat intelligence and the ability to add context for your environment to global threats has never been more important to the role of the CISO.

As we're tasked to do more with less, CISOs and their SecOps teams require threat intelligence to anticipate threats, identify and prepare for the most relevant threats targeting your organization, align programs and budget against the most likely threats and actors, and finally, to move from a reactive to proactive posture.

As "Customer Zero" for Trellix, I have never seen more potential for intelligence to shape the way responders move and strategize.

Take this content, digest it, and put it to use in your strategic planning, budget rationalization, board education and operational support.
I hope this insight is educational, informative and beneficial, and acts as a stepping stone to better guide and influence how you plan, prepare, and persist against APTs.

Harold Rivas
CISO, TRELLIX

**TABLE OF CONTENTS**

# PREFACE

With this report, and all of our reports, we aim to provide structure around intelligence and context to what we're observing.

## The landscape

The last six months have been unprecedented - a state of polycrisis remains and it has accelerated cybercriminal and threat actor activity globally. We're seeing radical shifts in behavior, including:

- The ransomware ecosystem is a-typical following law enforcement action,
- Autonomous groups are selling their wares in penetration testing and alternative attack methods to ransomware gangs,
- Warfare in Israel has triggered direct state-sponsored attacks and hacktivism, and
- Threat actors are looking to be more sophisticated, and they have access to cheap and free GenAI-based tools that empower them to become experts overnight, and
- EDR Evasion and termination tools become more important to threat actors.

## A cat and mouse game

With larger implementation of endpoint detection and response (EDR) solutions, we're seeing the cat and mouse game of cybersecurity get more complex. The increase of threat actors using criminal tools to dismantle EDR has piqued our interest and is a sharp course change from the use of traditional malware-based tools.

As defenders, we have to change course, too. EDR has proven effective at detecting malware, ransomware and the activity of APT groups, but if EDR is taken offline, what's an organization and their CISO to do? You need logging, you need alerting, and you need operational threat intelligence to keep from being blind to unusual behavior in your system. There's a new layer of gameplay.

We work diligently to share threat intelligence with the community - a core value of ours to keep ahead of adversaries - and track campaigns and threat groups at scale.

The landscape is shifting more than ever. Our aim is to support our customers and the industry at large with the intelligence needed to sharpen defenses, make countermeasures, and identify gaps.

In this cat and mouse game, we have to play to win.

John Fokker
HEAD OF THREAT INTELLIGENCE, TRELLIX

TABLE OF CONTENTS

# INTRODUCTION: THE CYBERTHREAT REPORT: JUNE 2024

## Geopolitical Events Impacting the Cyber Domain

Research from the Trellix Advanced Research Center into activity from October 1, 2023 - March 31, 2024 has revealed a shift in threat activities, with a noticeable increase in geopolitically motivated cyber threat operations. Notably, major regional and global events – such as military exercises, political or economic summits, political conventions, and elections – drove cyber threat activities.

Trellix analysts assess with moderate confidence that threat actors focused on these events to collect relevant intelligence about counterparts, probe networks proactively to obtain information for situational awareness, or preposition on IT networks strategically for future attacks.

- **Presidents Biden and Xi meet in San Francisco:** In November 2023, Trellix telemetry detection data indicated an uptick in malicious activity from China-associated APT actor groups only days before the meeting between U.S. President Biden and China's President Xi in San Francisco as part of the Asia-Pacific Economic Cooperation (APEC) meeting. The number of threat activities decreased significantly following the Biden-Xi summit and throughout the APEC summit.

  As the APEC summit came to an end, the level of threat activity fell to its lowest point in the month of November 2023. This pattern of threat activity from China-associated threat actor groups likely suggests that China's state-sponsored threat actor groups were heavily influenced by geopolitical events such as APEC. It may also indicate that China's APT groups may have deliberately withdrawn their hacking activity during a major political event possibly to preserve their public image and international reputation.
- **Israel-Hamas war:** Threats from Iranian-linked APT threat actor groups have also been driven by political developments surrounding the Israel-Hamas war. In the United States, Trellix global telemetry data shows periodic surges of malicious activity from Iranian-linked APT threat actor groups in the last six months (with the exception of late November and December 2023). Specifically, our global telemetry shows a reduction in threat activity from Iranian-linked APT groups targeting U.S. organizations during the periods of Israel hostage exchange and ceasefire agreements in late November 2023 and December 2023, when the U.S. pushed for a humanitarian ceasefire in the Gaza Strip as Iran is an open supporter of Hamas. Additionally, Trellix global telemetry indicates that Iranian-linked APT threat actor groups has employed a variety of TTPs, including phishing, information stealer, backdoors, downloader, malicious webshells, and commonly exploited vulnerabilities to target organizations in Israel during the reporting period.

**TABLE OF CONTENTS**

- **Military drills:** In addition, multinational military exercises to enhance combat readiness can trigger increased malicious activities. Most recently, in March 2024, Trellix global telemetry data shows repeated surges in threat activities in South Korea during the U.S.-South Korean large-scale joint military exercises, known as Freedom Shield, from March 4 to March 14, 2024. These military drills are designed to reflect the "Korea Theater of Operations" and counter North Korea's evolving nuclear threat. Specifically, threat detections in South Korea exceeded over 150,000 detections on March 7 and March 13, 2024, respectively, which is around seven times the usual 20,000 daily detections in the country.
- **Russia-Ukraine war:** Continued kinetic warfare in the region has been accompanied by cyber initiatives large and small. Most notably, Russian-linked actors have been observed leveraging new and more advanced wiper malware to wipe thousands of virtual servers and PCs by attacking Ukrainian telecom provider Kyivstar. The attack to KyivStar is one of the highest-impact disruptive cyberattacks on Ukraine since Russia invaded the country in 2022.

## Highlights At-a-Glance

While this report serves as a repository for research from across our business, key themes persist:

1. **Rapid and Significant Changes in the APT Landscape**
    a. **Russia-Linked Sandworm Escalates:** As geopolitical tensions rise, so does APT activity across the entire ecosystem. While APT threats grow overall, Russia-linked Sandworm Team was detected 40% more in the period observed in this report.
    b. **China Remains Prolific:** China-linked threat groups remain the most prolific originator of APT activities with Trellix observing more than 21 million detections of threat activities from China-aligned threat actor groups. Over 23% of the detections of malicious activities are directed at the government sector worldwide.
    c. **VoltTyphoon Activity Spikes:** As a relatively new China state-sponsored APT group, Volt Typhoon stands out because of its unique behavior pattern and targeting practices. Since mid-January 2024, Trellix telemetry detected over 7,100 malicious activities associated with Volt Typhoon, with periodic spikes throughout the period from January through March 2024.

TABLE OF CONTENTS

2. **LockBit Shakes Up Ransomware Ecosystem**
    a. **Imposters Impact Gang Reputation:** Following a global law enforcement action, Operation Cronos, Trellix observed imposters pretending to be LockBit, all while the group frantically tried to save face and restore the lucrative operation.
    b. **U.S. Remains Most Targeted:** The United States remained the most targeted by ransomware groups, followed by Turkey, Hongkong, India and Brazil.
    c. **Transportation and Shipping Most Hit:** Ransomware actors threatened the transportation and shipping sector the most in Q4 2023 and Q1 2024. The sector generated 53% and 45% of global ransomware detections, respectively, and was followed by the finance industry.
    d. **Law Enforcement Action Leads to Sentencing:** Before finalizing this report, global law enforcement disclosed the true identity of LockBit's ring leader. Further action against ransomware criminals took place on May 1st. The REvil affiliate that attacked Kayesa and many other organizations was sentenced to 13 years in prison and repayment of $16 million USD.
3. **EDR Killers Emerge**
    a. **D0nut Ransomware Gang Appears:** The emergence of the D0nut ransomware gang was particularly noteworthy for their innovative use of an EDR killer tool, showcasing an advanced tactic to circumvent endpoint detection and enhance the effectiveness of their attacks.
    b. **Spyboy's EDR Evasion Tool Used to Target Telecom:** A EDR "killer" tool by developer Spyboy called "Terminator" was used in a new campaign in January 2024. The tool is used to circumvent EDR solutions, and 80% of detections were targeted at the telecom sector.
4. **U.S. Presidential Election Themed Scams**
    a. **Phishing Remains Ripe:** As the world looks to see the outcome of November's presidential election in the U.S., scams leveraging election imagery and curated to secure donations have been observed.

**TABLE OF CONTENTS**

5. **GenAI and the Cybercriminal Underground**
    a. **Free AI-Powered Tools:** Trellix observed a free ChatGPT 4.0 Jabber tool available in the cybercriminal underground, which both allows the developer to enable threat actors to adopt GenAI into their operations and to create a GenAI knowledge base to learn from other cyber criminals or even steal their ideas and tools.
    b. **InfoStealer Adoption Rises:** Two InfoStealers with GenAI-based features were observed to be used by cybercriminals. MetaStealer and LummaStealer are equipped with GenAI to evade detection and to detect bots among the list of logs, respectively. GenAI capabilities make these criminal tactics harder to find and harder to stop.

## Methodology: How We Gather and Analyze Data

Experts from our Trellix 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.

TABLE OF CONTENTS

## REPORT ANALYSIS, INSIGHTS, AND DATA

### Nation States and Advanced Persistent Threats (APT)

From October 2023 through March 2024, Trellix observed a 17% increase in APT-backed detections compared to the previous six months. This is notable as our last report identified a staggering 50% increase in these detections. The APT ecosystem is fundamentally different from a year ago – more aggressive, cunning and active.

In the rapidly evolving cyber threat landscape, Advanced Persistent Threat (APT) groups continue to pose a significant and sophisticated challenge to global cybersecurity.

We aim to thoroughly analyze activities associated with Advanced Persistent Threats (APT) detected from Q4 2023 through Q1 2024. This analysis focuses on the origins of these threats, their main targets, and the tools used in their operations. We compare these findings to data from the first half of 2023 (Q2 to Q3) using two key metrics: percentage variance and proportional contribution variance.

- Percentage variance: This metric helps us see if the activity of a specific APT group, the targeting of certain countries, or the use of particular tools has gone up, gone down, or stayed the same over time. Understanding this helps us track how the behaviors of these threat actors change and how the overall landscape of cyber threats is evolving.
- Proportional contribution variance: This metric adds context by not just showing the raw change in activity, but how this change stands against the backdrop of the entire cybersecurity threat environment. For example, even if detections of a particular actor have increased significantly, this might still represent a small part of the total cyber threats if the overall threat environment has become much busier. Conversely, if their detections have decreased, but the rest of the threat environment has slowed down even more, this actor could be becoming relatively more significant.

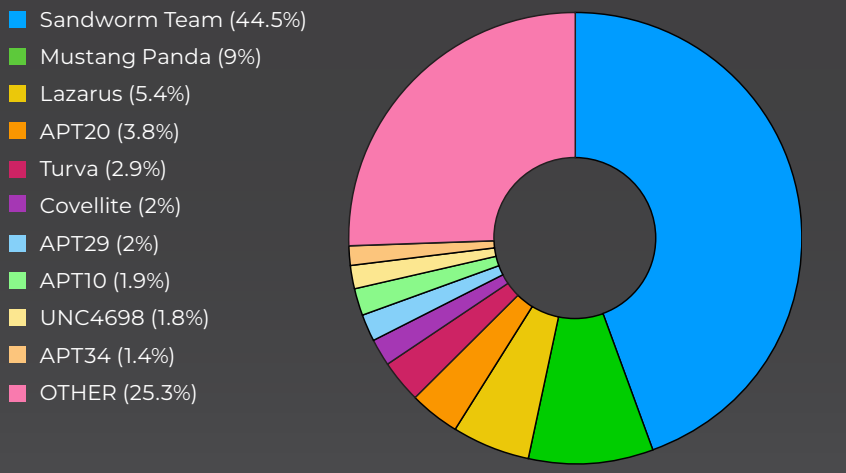
By employing these metrics, we aim to provide a nuanced understanding of the shifts in APT activities, enabling us to draw insights into their strategic objectives, preferred methodologies, and the cybersecurity challenges they pose. The following sections delve into these findings, shedding light on the intricate world of APTs and the continuous efforts required to safeguard against their sophisticated threats.

**TABLE OF CONTENTS**

## Active nation states and APT groups

Further, the period spanning from October 2023 - March 2024 witnessed significant fluctuations in the activities of various APT groups. These fluctuations not only underscore the dynamic nature of cyber threats but also highlight shifts in the operational focus and techniques employed by these sophisticated actors.

### TOP 10 APTS BASED ON DETECTIONS BETWEEN THE LAST QUARTER OF 2023 AND THE FIRST QUARTER OF 2024.




### CHANGES IN CYBER THREAT GROUP ACTIVITY: VARIANCE AND PROPORTIONAL CONTRIBUTION

| Advanced Persistent Threats | Percentage Variance | Proportional Contribution Variance |
|---|---|---|
| Sandworm Team | 1669.43% | 40.34% |
| Mustang Panda | -2.19% | -6.14% |
| Lazarus | 66.87% | 0.07% |
| APT28 | 18.67% | -1.49% |
| Turla | 2.95% | -1.74% |
| Covellite | 85.30% | 0.23% |
| APT29 | 123.98% | 0.53% |
| APT10 | 80.46% | 0.17% |
| UNC4698 | 368.75% | 1.14% |
| APT34 | 96.73% | 0.23% |
| Other | -28.99% | -33.33% |

TABLE OF CONTENTS

- **Shift in tactics:** Sandworm Team, historically known for its disruptive cyber operations, has seen a staggering increase in detections by 1669%, with a proportional contribution variance of 40%. This monumental rise suggests an unprecedented escalation in their cyber activities from the Russia-linked group.
- **Aggressive expansion of operations:** APT29, a group with a history of extensive cyber espionage, showed a significant uptick in activity, with detections increasing by 124%. Similarly, APT34 and Covellite also demonstrated substantial increases in detections, by 97% and 85% respectively, indicating heightened operational tempos or the initiation of new campaigns.
- **Homeostasis:** In contrast, groups like Mustang Panda, Turla, and APT28 saw minimal changes in their activity levels, with Mustang Panda showing a slight decrease of -2% and Turla a modest increase of 3% in detections.
- **New actors emerge:** Noteworthy is the emergence of UNC4698, which saw a 363% increase in detections, suggesting the rise of a potentially significant new player in the APT landscape.

### WHAT DO WE KNOW ABOUT UNC4698?

Not a lot is known about this group, but researchers have been able to recognize their behavior as group activity and don't know yet how to attribute it.

Having said that, what is known about UNC4698 is that its focus is on industrial espionage, gathering sensitive operational data which could be used to support economic or national security objectives of the sponsoring state, presumably linked to China due to the nature and regional focus of the attacks.

Its usual targets are oil and gas organizations in Asia.

They are also known to employ a specific malware that goes by the name of 'SNOWYDRIVE'.

UNC4698 employs a variety of tactics, techniques, and procedures (TTPs) centered around the use of malware delivered via USB flash drives. Here are some key TTPs associated with this threat actor:

- **Initial Access via Infected USB Devices:** The primary method of infection involves USB drives that contain malicious software designed to create a backdoor on the host system.

TABLE OF CONTENTS

## WHAT DO WE KNOW ABOUT UNC4698?

- **Execution through Malicious Files:** The malware typically includes a dropper that writes malicious executables and DLLs to disk. These files often masquerade as legitimate software to avoid detection and are executed to establish further control.
- **Persistence and Registry Modification:** UNC4698 ensures persistence on the infected systems by modifying the Windows registry. This allows the malware to start automatically whenever the system boots up.
- **Command and Control (C2) Communication:** The malware sets up a method for remote communication, allowing the attackers to issue commands and control the compromised systems from afar.
- **Lateral Movement via Removable Media:** The malware can copy itself to other USB devices connected to the infected machine, which helps in spreading the infection to other systems.

Lesser-known or unidentified groups, saw a 62% increase in detections, indicating a diverse and growing array of threats beyond the well-documented APT entities. This increase of 8% in their proportional contribution to the total detections highlights the constant evolution and diversification of cyber threats.

### APT groups and countries of origin

**TOP 10 APT ASSOCIATED COUNTRIES BASED ON DETECTIONS CORRELATED TO CAMPAIGNS, BETWEEN THE LAST QUARTER OF 2023 AND THE FIRST QUARTER OF 2024**

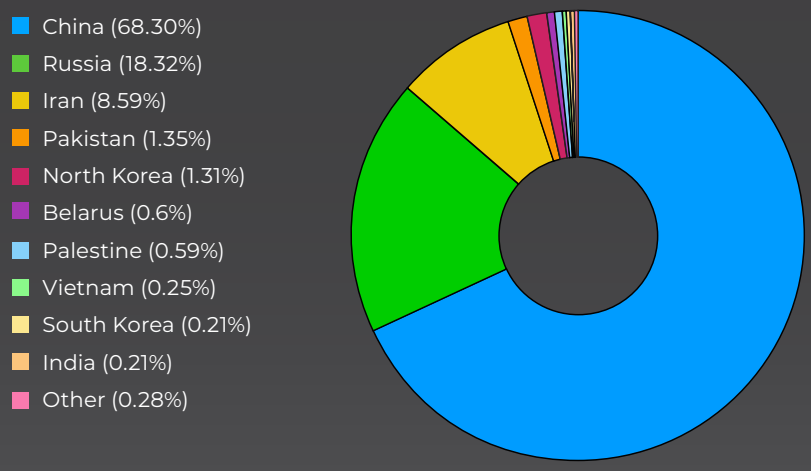



TABLE OF CONTENTS

When looking at countries of origin, Trellix telemetry from October 2023 through March 2024 also observed notable shifts in the landscape of state-sponsored cyber activities.

China-linked threat groups remain the most prolific originator of APT activities

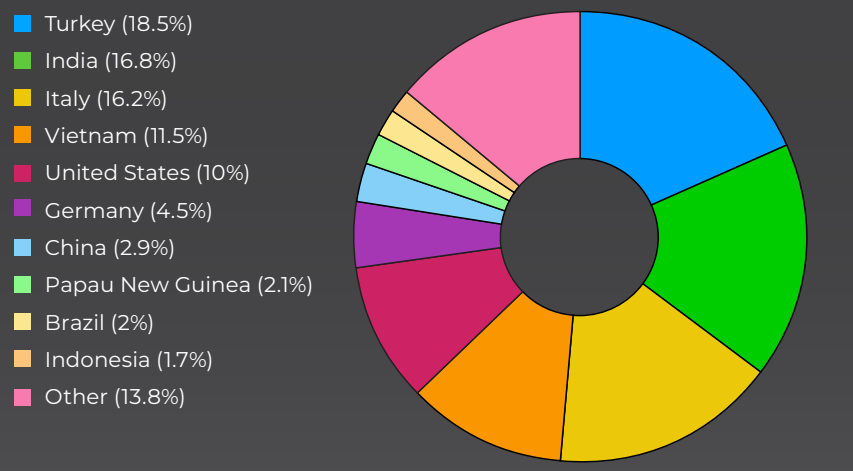
- **Substantial escalation in operations:** Geopolitical motivations and cybersecurity capabilities are evolving across different nations. Our telemetry observed the following:
  a. Russia-linked threat groups have shown a significant increase in APT detections, up by 31%, with its proportional contribution rising by 4%. This indicates a substantial escalation in cyber operations, possibly reflecting broader strategic objectives or responses to global cybersecurity dynamics.
  b. Iran-linked threat groups have also markedly ramped up cyber activities, with an 8% increase in detections and a 3.89% rise in proportional contribution. This highlights a significant expansion in Iran's cyber operations, in line with its geopolitical aims and involvement in the Israeli-Hamas war.
- **Broader diversification:** China remains the most prolific originator of APT activities, with detections slightly increasing by 1%. However, its proportional contribution to the overall detections has seen a slight decrease of -1%, which might suggest a broader diversification of APT origins during this period. February of this year also saw reports of significant efforts from China-backed APT Volt Typhoon targeting U.S. critical infrastructure; more on this in the following section.
- **Shift in strategy:** Conversely, groups linked to North Korea, Vietnam, and India have seen dramatic decreases in their APT activities, with North Korea-linked detections dropping by -82%, Vietnam by -80%, and India by -82%. The significant downturn in North Korea's proportional contribution (-6%) is particularly notable, possibly indicating a shift in focus, strategy, or capabilities.
- **More countries emerging:** Pakistan-linked and Belarus-linked groups have seen considerable increases in their APT activities, with detections up by 55% and an astonishing 2019%, respectively. These increases, particularly the exponential rise associated with Belarus, underscore the emergence of new or previously underrecognized actors in the APT arena.

  The category of "Other" shows a 121% increase in detections, indicating that APT activities are not limited to the most frequently cited countries. This diversity highlights the global nature of cyber threats and the necessity for a wide-ranging and adaptive cybersecurity posture.

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

TABLE OF CONTENTS

## TARGETED COUNTRIES AND REGIONS WITH APT ASSOCIATED DETECTIONS




### Targeted Countries and Regions

This section focuses on the countries regions where Trellix detected APT related activity by APT groups from Q4 of 2023 through Q1 of 2024, revealing significant shifts in focus and strategy among these sophisticated cyber actors.

> The data underscores the global nature of cyber threats and the varying levels of attention different nations receive from APT groups.

The Trellix Advanced Research Center assesses with a moderate level of confidence that the following factors impacted activity detected in certain countries and regions

Turkey has seen an unprecedented surge in APT-related detections

**Operational objectives:**
Detections in threats targeting Turkey increased by a staggering 1458%, translating to a 16% rise in its proportional contribution to the total detections. This remarkable increase indicates a significant shift in cyber threat focus towards Turkey, possibly reflecting broader geopolitical tensions or specific operational objectives of the APT groups.

- **Strategic importance:** India and Italy have also experienced considerable increases in detections, with detections up by 614% and 308%, respectively. These countries' rising prominence in the list of targets may point to their growing strategic importance in the cyber domain, whether due to economic, political, or technological factors

TABLE OF CONTENTS

- **Broadening landscape:** Interestingly, Vietnam and the United States, while still generating significant APT detections, have shown different trends. Vietnam's detections increased by 9%, yet its proportional contribution decreased by -9%, indicating a broadening of the targeting landscape. The United States saw a moderate increase of 15% in detections but experienced a -7% drop in its proportional contribution, suggesting a diversification in the targeting strategies of APT groups.
- **Geopolitical developments:** Germany, China, Papua New Guinea, and Brazil have all seen increases in detections, with Germany and China witnessing significant proportional contribution changes. This diversification in targeting reflects the strategic and opportunistic adjustments APT groups make in response to global cybersecurity postures and geopolitical developments.
- **Enhancement of national security:** Conversely, Indonesia experienced a notable decrease in detections by -48%, coupled with a -4% drop in its proportional contribution. This reduction might suggest a temporary deprioritization or a successful enhancement of national cybersecurity measures.
- **Consolidation of focus:** The "Other" category, representing a collective of various other countries where Trellix detected APT related activity, saw a -23% decrease in detections and a -21% decline in proportional contribution. This decrease highlights a possible consolidation of focus by APT groups on specific high-interest targets during this period.

We see potential for the landscape to continue changing rapidly due to geopolitical trends.

## Malicious tools

**TOP 10 MALICIOUS TOOLS DETECTED BETWEEN THE LAST QUARTER OF 2023 AND THE FIRST QUARTER OF 2024.**

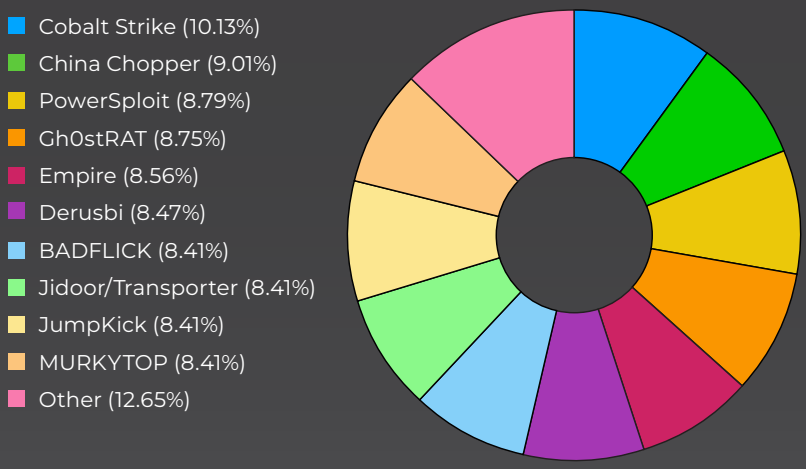



TABLE OF CONTENTS

The analysis of malicious tools used in APT campaigns from Q4 2023 to Q1 2024 reveals notable trends in the preferences and operational tactics of cyber threat actors. The variance in detection rates and their proportional contributions provides insights into the evolving cyber threat landscape and the shifting dynamics of tool usage among these sophisticated groups.

The following trends were observed:

- **Offensive tools getting stronger:** Cobalt Strike remains a tool of choice for many Threat groups, despite a 17% decrease in detections. Its relatively small decrease in proportional contribution variance (+1%) suggests it retains its popularity and effectiveness in cyber operations, underlining the challenge of defending against versatile and widely used offensive tools.
- **Reliance on web shells, PowerShell and Remote Access attacks:** China Chopper, PowerSploit, and Gh0st RAT also saw significant decreases in detections, by 23%, 24%, and 24%, respectively. Despite these decreases, their slight changes in proportional contribution variance indicate they remain integral to the toolkit of a threat actor. These tools, known for their capabilities in web shell attacks, PowerShell exploits, and remote access, highlight the continued reliance on proven, versatile tools for cyber operations.
- **Less detectable tools:** Empire, Derusbi, BADFLICK, JJdoor/Transporter, JumpKick, and MURKYTOP experienced similar downward trends in detections, all exceeding a 25% decrease. This uniform decline could reflect a broader shift in the tools preferred by threat groups or an adaptation to countermeasures and detection techniques, prompting a move towards newer, less detectable tools.
- **Constant innovation:** The category of "other" malicious tools saw a significant increase in detections, up by 30%, and a notable increase in its proportional contribution variance by 6.00%. This increase underscores the constant innovation and adaptation among threat actors, as they explore new tools and techniques to evade detection and achieve their objectives.

The evolving preferences in malicious tool usage signify the adaptive nature of cyber threat actors in response to cybersecurity developments.

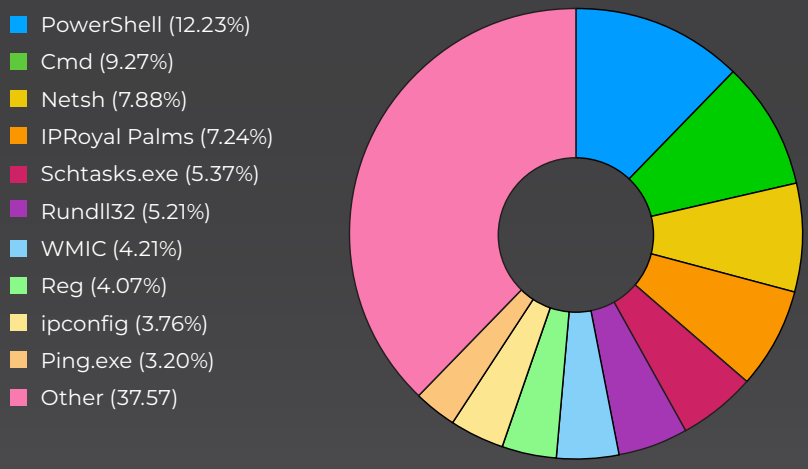
> As defense mechanisms become more sophisticated, so too do the offensive tools and tactics of APT groups.

The shift towards a broader range of tools, as indicated by the increase in "Other" detections, highlights the necessity for continuous research, threat intelligence, and adaptive defense strategies to mitigate the risk posed by these evolving cyber threats.

**TABLE OF CONTENTS**

## Non-malicious tools

**TOP 10 NON-MALICIOUS TOOLS DETECTED BETWEEN THE LAST QUARTER OF 2023 AND THE FIRST QUARTER OF 2024.**




> This practice, known as “living off the land,” complicates detection efforts and underscores the sophistication of these threat actors.

The use of non-malicious tools in cyber operations by APT groups from Q4 2023 to Q1 2024 highlights an important aspect of modern cyber threats: the leveraging of legitimate system tools for malicious purposes. This practice, known as “living off the land,” complicates detection efforts and underscores the sophistication of these threat actors. The statistics reveal significant variances in the usage of these tools, reflecting their strategic importance in cyber operations

- **Versatility:** PowerShell has seen a dramatic increase in detections, up by 105%, with a proportional contribution variance of 1%. This surge underscores its versatility and power in automating a wide range of malicious activities, from reconnaissance to payload delivery.
- **Focus on network manipulation:** Netsh and IPRoyal Pawns have both seen significant increases in detections, by 99% and 102%, respectively. These tools are often used for network configuration and proxy traffic, indicating a strategic focus on network manipulation and evasion techniques.
- **Automation to scale:** Schtasks.exe has experienced the highest percentage variance among the tools listed, at 138%. This reflects the growing reliance on scheduled tasks for persistence and execution of malicious payloads without direct user intervention.

TABLE OF CONTENTS

- **Tactical shifts:** Conversely, Rundll32 and WMIC have seen increases in their use but faced decreases in proportional contribution variances, indicating a shift in the tactical preferences of APT groups despite these tools' continued utility.
- **Tool diversification:** Cmd, the good old command-line interpreter on Windows systems also experienced a substantial increase in usage, with detections up by 65%. Despite its increased use, its proportional contribution variance has decreased by -2.5%, suggesting a broader diversification in tool usage among APT groups.

  The "Other" category, representing a variety of less commonly used or more specialized tools, saw a 42% increase in detections. However, it experienced a significant decrease in proportional contribution variance (-21%), highlighting the expanding arsenal of tools at the disposal of cyber threat actors.

The evolving landscape of non-malicious tool usage by APT groups illustrates the complexity of detecting and defending against sophisticated cyber threats. The strategic selection and application of these tools reveal a deep understanding of the targeted environments and the efforts to remain undetected.

> **CISO TIP:** Cybersecurity defenses must, therefore, advance beyond traditional malware detection to include behavioral analysis and anomaly detection to counteract the misuse of legitimate tools in cyber operations.

Data collected through the Trellix ATLAS global sensors, coupled with strategic Insights from industry vetted reporting, delivered by the Trellix Advanced Research Center allows our customers to identify threat actors targeting their respective sectors and use our behavioral analysis to detect anomalous behavior within their environment.

**TABLE OF CONTENTS**

## Conclusion

The analysis of Advanced Persistent Threat (APT) activities from Q4 2023 to Q1 2024 has illuminated the dynamic and increasingly complex nature of the cyber threat landscape. Our examination of the statistics related to APT group origins, targeted countries, malicious and non-malicious tool usage reveals several key trends that underscore the evolving strategies of cyber threat actors.

APT groups continue to demonstrate high degrees of

1. Adaptability and sophistication
2. Leveraging a mix of malicious tools
3. Exploiting legitimate system utilities to conduct espionage, disrupt operations, and steal sensitive information.

The significant variances observed in the targeting and operational tactics of these groups reflect not only their strategic objectives but also their response to global cybersecurity developments and defensive measures.

The dramatic shifts in targeting practices, with certain countries experiencing substantial increases in APT-related activities, highlight the geopolitical motivations driving these cyber operations. Similarly, the changes in tool usage, including the notable rise in "living off the land" tactics, emphasize the ongoing challenge of detecting and countering APT threats within a landscape where legitimate and malicious activities are increasingly intertwined.

Moreover, the diversification in APT origins and the broadening of their targeting strategies indicate a global proliferation of cyber capabilities and the need for a unified and collaborative approach to cybersecurity.

> It is clear that no nation or organization is immune to the reach of these sophisticated threat actors.

**TABLE OF CONTENTS**

## Volt Typhoon: A Chinese Associated Nation-State Group

Nation-state threat actor groups continue to pose a grave threat to commercial and public sector organizations worldwide during the last quarter of 2023 and the first quarter of 2024. These adversaries, often well-equipped and adept at sophisticated cyber-enabled threats, relentlessly target networks over prolonged periods with superior talent and resources compared to their cybercriminal or hacktivist counterparts.

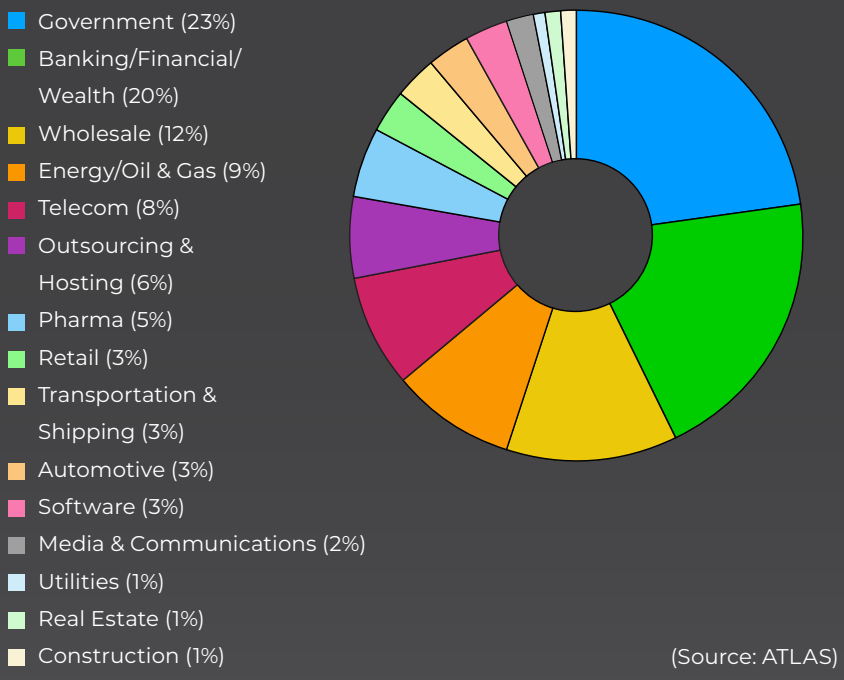
**23%**

Over 23 percent of the detections of malicious activities are directed at the government sector worldwide

Over 21 million detections of threat activities from China-aligned threat actor groups

Specifically, based on Trellix telemetry detections, China-associated nation-state-sponsored threat actor groups have posed increasing threats to the government sector worldwide. Our data show over 21 million detections of threat activities from China-aligned threat actor groups from Oct. 2023 - March 2024.

### GLOBAL DETECTIONS FROM CHINA-AFFILIATED APT GROUPS




(Source: ATLAS)

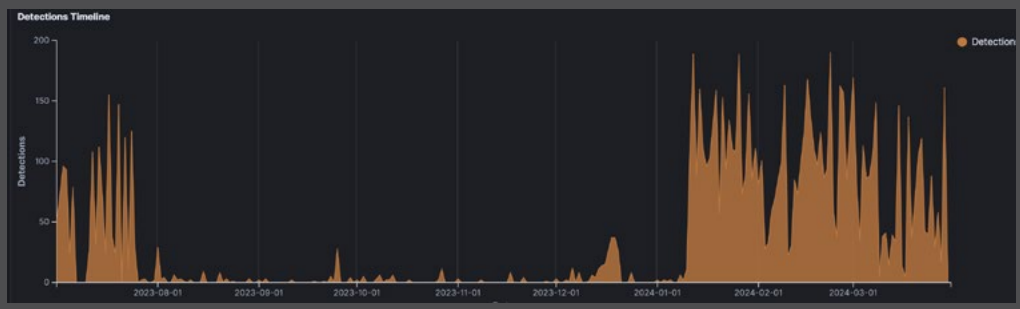
TABLE OF CONTENTS

## Overview

As a relatively new China state-sponsored APT group, Volt Typhoon stands out because of its unique behavior pattern and targeting profiles, which deviate from the conventional cyber espionage and intelligence collection of other China-associated APT groups. Previous open-source reporting suggests that this Chinese APT group has pre-positioned itself on industrial controls IT networks to facilitate lateral movement to disrupt operational technology (OT) assets and functions in the event of geopolitical crisis or war. Trellix telemetry data shows that since resuming its operations in January 2024, Volt Typhoon has repeatedly targeted the global government sector, including the United States, while employing living-off-the-land techniques.

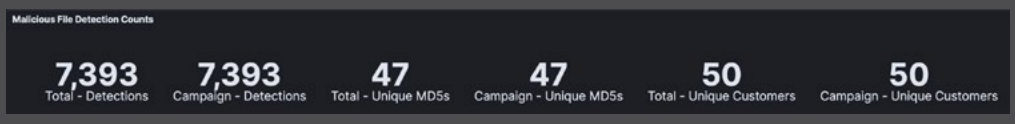
## Operational timeline

Trellix global telemetry data shows that Volt Typhoon was first detected in mid-2021, but became largely dormant with little or no activity from August 2023 through January 2024. This break period may result from a culmination of threat investigations in the months following the first vendor report on Volt Typhoon published in May 2023 that attracted global attention. It could also be due to Volt Typhoon possibly shifting its attack infrastructure during this period due to public exposure, so few threat activities were detected.




Volt Typhoon detection timeline from July 2023 to March 2024 (Source: Trellix ATLAS)

Volt Typhoon resumed operations around mid-January 2024 based on Trellix telemetry data. Since mid-January 2024, Trellix telemetry detected over 7,100 malicious activities associated with Volt Typhoon, with periodic spikes throughout the period from January through March 2024.




Volt Typhoon detection details from January to March 2024

TABLE OF CONTENTS

## Tactics, techniques and procedures (TTPs)

Our detection data suggest that since returning to operations in mid-January 2024, Volt Typhoon has consistently leveraged a number of native Windows tools and functionality to execute commands for malicious reasons. These tools, known as living-off-the-land (LOTL) tools—which are dual-use tools that are legitimate software and functions available in the system—have become increasingly popular among China-based nation-state actor groups, including Volt Typhoon. Netsh.exe is one of these tools that can be used for various malicious purposes, such as disabling firewall settings or setting up a proxy tunnel to allow remote host access to an infected host. Ldifde is another tool leveraged by Volt Typhoon threat actors for information collection.

After gaining access to a domain controller, attackers may use Ldifde.exe to export sensitive data or perform authorized changes to the directory. Similarly, Volt Typhoon threat actors also use ntdsutil for malicious attempts. Ntdsutil is a legitimate tool that allows administrators to perform database maintenance; however, it can also be used to create a dump of the Active Directory to harvest credentials and exfiltrate sensitive data.

The Volt Typhoon threat actor continued to use open-source tools, such as FRP, Impacket, and Mimikatz, in their threat operations. Trellix telemetry also detected Volt Typhoon using the following LOTL tools and commands between February and March 2023:

- Comsvcs
- Dnscmd
- Ldifde
- MiniDump
- Net
- Netsh
- NTDSUtil
- Reg
- ping
- Powershell
- PsExec

TABLE OF CONTENTS

The top MITRE ATT&CK tools leveraged by Volt Typhoon observed in our telemetry are as follows:

- Initial Access – T1190: Exploit Public-Facing Application
- Execution – T1106: Native API
- Persistence – T1546: Event Triggered Execution
- Privilege Escalation - T1546: Event Triggered Execution
- Defense Evasion – T1070.001: Clear Windows Event Logs
- Defense Evasion – T1070: File Deletion
- Defense Evasion – T1027: Obfuscate Files or Information
- Credential Access – T1003.003: NTDS
- Credential Access – T1003: OS Credential Dumping
- Credential Access – T1110: Brute Force
- Credential Access – T1555: Credentials from Password Stores
- Discovery – T1069.002: Domain Groups
- Discovery – T1069.001: Local Groups
- Discovery – T1083: File and Directory Discovery
- Discovery – T1057: Process Discovery
- Discovery – T1010: Application Window Discovery
- Collection – T1560: Archive Collected Data
- Collection – T1560.001: Archive via Utility
- Command and Control – T1090.002: External Proxy
- Command and Control – T1105: Ingress Tool Transfer
- Command and Control – T1132: Data Encoding

## Ransomware Landscape Evolution

In Q4 2023, the cyber threat landscape witnessed an escalation in ransomware attacks, with new families from the year making an increasingly significant impact.

- **EDR killer tools:** Among these, the emergence of the D0nut ransomware gang was particularly noteworthy for their innovative use of an EDR killer tool, showcasing an advanced tactic to circumvent endpoint detection and enhance the effectiveness of their attacks. More on this in the following section.
- **Vulnerability exploitation:** This period also saw a continuation of the trend towards exploiting critical vulnerabilities to facilitate ransomware deployment. Notably, CVE-2023-4966, referred to as Citrix Bleed, was exploited by LockBit 3.0 affiliates, highlighting the ongoing vulnerability of critical infrastructure to sophisticated cyber attacks. Additionally, the exploitation of CVE-2023-22518 in Confluence Data Center and Server underscored the attackers' focus on infiltrating widely-used business platforms to deploy ransomware. The Cactus ransomware campaign, which targeted

TABLE OF CONTENTS

Qlik Sense installations by exploiting newly discovered vulnerabilities, further demonstrated the attackers' agility in adapting to security landscapes and exploiting emerging vulnerabilities. Making Q4 2023 an active quarter for ransomware groups.

However the status quo was about to be shaken up in Q1 2024 by a noteworthy Law Enforcement action.

## Operation Cronos: Law enforcement action to disrupt LockBit

Starting February 19, 2024 an international law enforcement action, Operation Cronos, unfolded. It gracefully disrupted the infamous LockBit Gang, giving the long standing crime group a taste of their own medicine. Law Enforcement didn't only display the well known takedown notices but eventually had complete control of the crime group's leaksite and displayed some leaks of their own by exposing the crime group to the world. Several indictments we presented and active affiliates received a friendly welcome message when they logged in to the LockBit backend, making it crystal clear that their identities were known.

These actions were aimed at not only disrupting LockBit's operation, but also damaging their reputation and breaking the trust within the gang.

At the time of finalizing this report, Operation Cronos got another plot twist. Global law enforcement went for round two by disclosing the true identity of LockBit's ring leader. This wasn't the only victory for law enforcement; on May 1st the REvil affiliate that attacked Kayesa and many other organizations was sentenced to 13 years in prison and has to repay $16 million USD in damages. More info on how Trellix Advanced Research Center assisted in the REvil case can be read here.

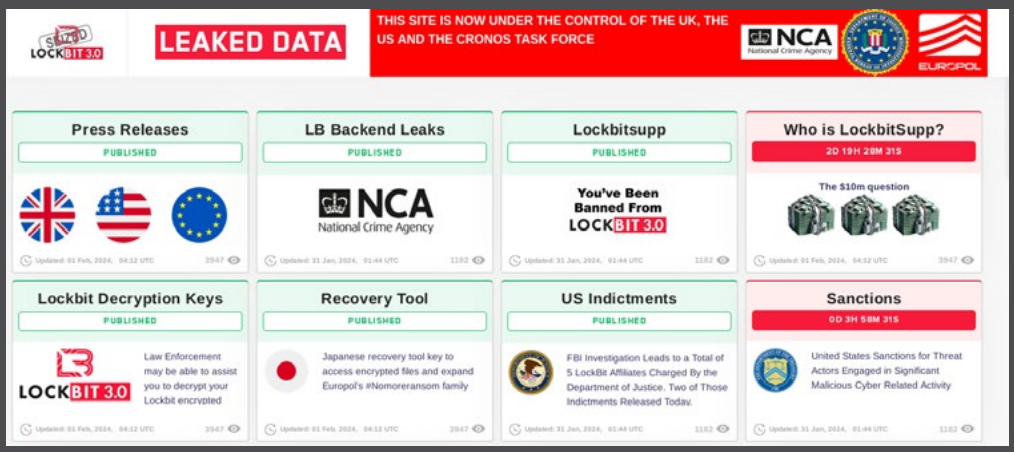



TABLE OF CONTENTS

Last year, our February report identified LockBit as the most aggressive with ransom demands. These cybercriminals use a variety of techniques to execute their campaigns, including exploiting vulnerabilities found as far back as 2018. Through 2023, LockBit consistently remained the most prevalent ransomware group with the largest number of victims posted on their name-and-shame site. They primarily targeted North American and European organizations across various sectors, impacting the Industrial Goods & Services sector the most. In 2023 LockBit kept continuously evolving and introducing new tools and methods to their ransomware program. Notable events include LockBit working on development of LockBit Green encryptor based on the leaked code of Conti ransomware as well as LockBit variants targeting MacOS. Furthermore, we witnessed LockBit RaaS offering in 2023 a new home for affiliates of other RaaS programs such as ALPHV and NoEscape whose operations got shut down.

In the aftermath of the disruptive actions, we witnessed LockBit frantically trying to save face and restore the lucrative operation. This was to be expected given the publicity of LockBit's criminal activities, however in the cybercriminal underground, a server is easier restored than years of trust. It remains to be seen how much information law enforcement has obtained on LockBit's operation, persona and its affiliates.

> This uncertainty creates a huge risk for any cyber criminal willing to engage with LockBit and their (former) team.

It became very clear after the law enforcement actions that it is a dog-eat-dog world amongst criminals. The Trellix Advanced Research Center observed other actors using the leaked LockBit Black version to impersonate the well-known brand for their own financial gain.

Imposters or not, the victims they made were real, all these events made the last two quarters definitely fit for a movie script.

### A global look at ransomware

During our research into ransomware activity in the first quarter of 2024, we investigated multiple sources: leak sites, telemetry, and public reporting. A few words about each of the categories.

- **Leak sites:** These sites are designed to show proof of extorted victims who have not paid the demanded ransom, allowing for a look into the criminal gang's activity. Additionally, it is important to note that the leak sites do not necessarily accurately reflect the landscape. Given that they are operated by criminals, not all statements are truthful nor correct. Further, if the gangs keep their word, the victims who pay the ransom are not listed, thus giving an incomplete picture. The data used in this report refers to overall trends from leak sites and does paint a meaningful picture.

TABLE OF CONTENTS

- **Telemetry:** Telemetry is derived from the Trellix sensor ecosystem and detections denote when a file, URL, IP address, or other indicator is detected by one of our products and reported back to us. This is not to say that every detection is an infection, as customers test the detection of certain files to fine tune their internal rules, which also show up in the aggregated logging. As such, this data remains useful when looking at the bigger picture, as trends still show.
- **Public reports:** Reports from vendors and individuals have been processed by our Advanced Research Center to analyze features and distill trends. There is an inherent bias for each report, an example of which can be the dominant geographical presence of a vendor compared to another vendor. This difference might cause one reporting entity to report on something while another entity might report on something else. Given the variety of biases for the included reports, we do not apply a specific filter.

## Active ransomware groups

When looking at the aggregated leak site posts from Q1 2024, many show signs of activity. On occasion, we see leak sites post general announcements, but the majority are "proof" of extortion or leaks of victim data. They'll also often post one victim multiple times which can cause inflation due to a victim being counted more than once in data.

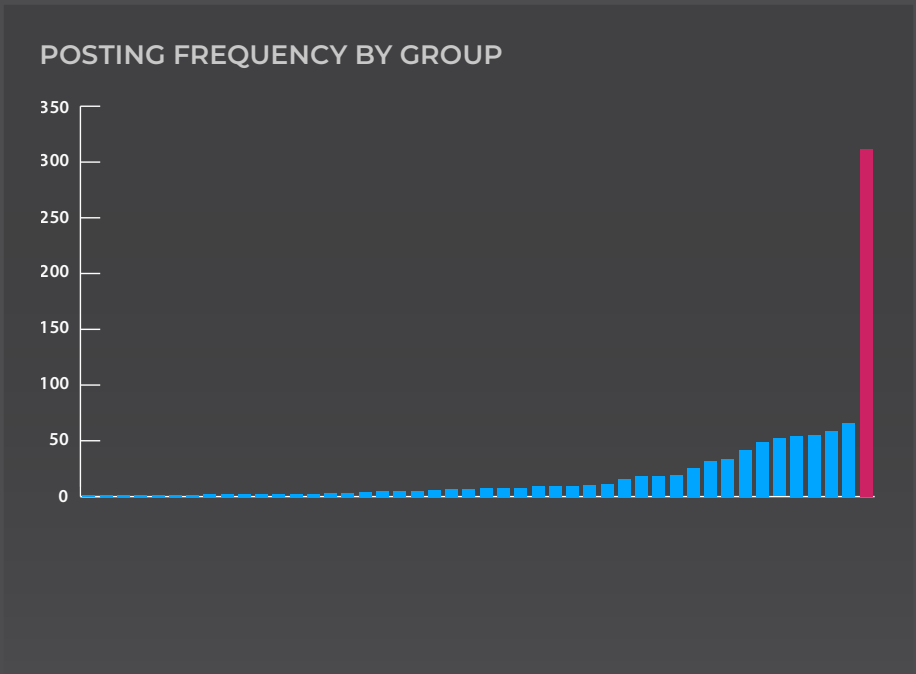
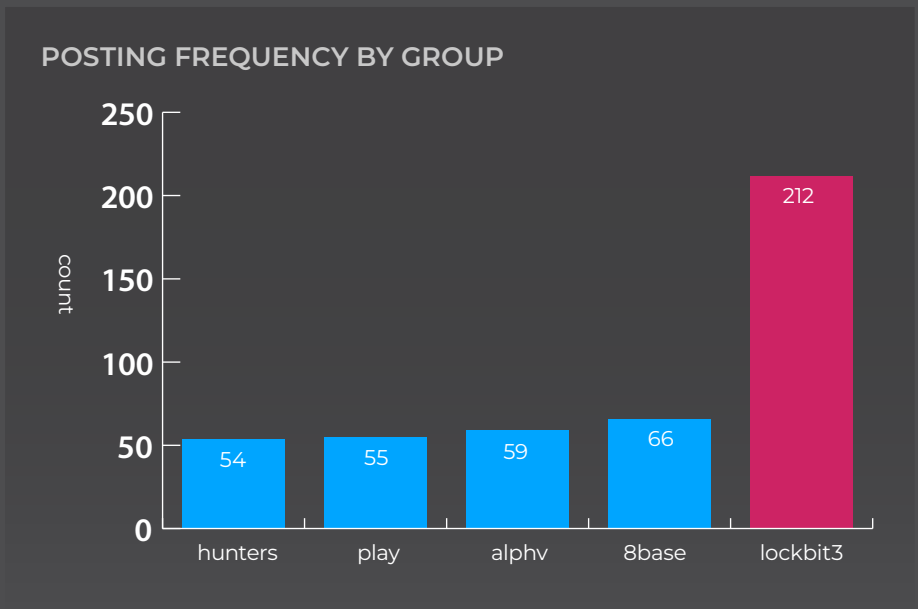



TABLE OF CONTENTS

When looking at the frequency of the five most active ransom gang leak sites, the graphs are dwarfed by LockBit's activity. The activity of the gangs aside from LockBit average over 50 posts in a quarter, meaning the average time between the posting of two victims is less than two days. As stated above, these numbers reflect non-paying victims, meaning that the actual number of victims is likely to be higher although there is no method to define how many.




## Targeted countries and regions

Building on the continuous activity of ransomware gangs, we can see ransomware detections within Trellix telemetry. The United States generates the most detections, followed by Turkey, Hong Kong, India and Brazil.

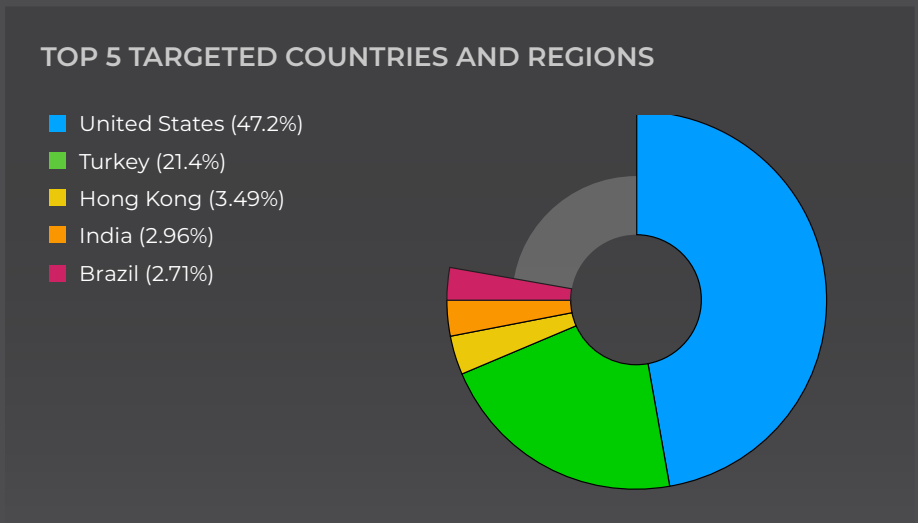


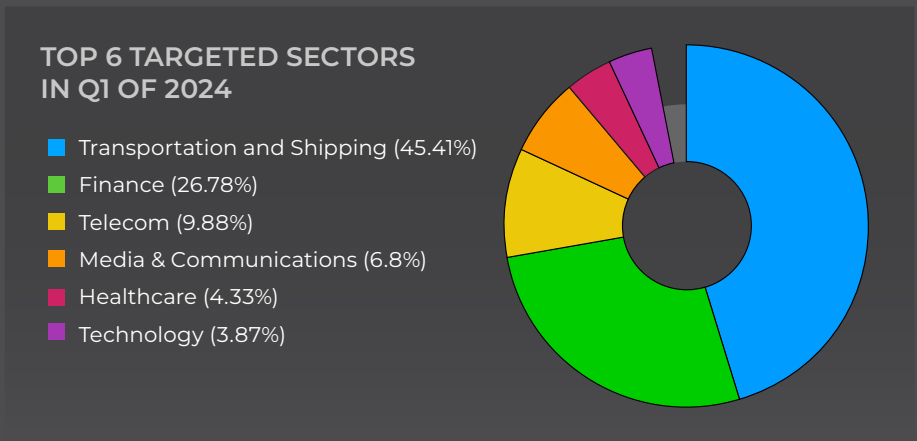

TABLE OF CONTENTS

Given that ransomware is a threat for all sectors in nearly every geography, the detection metrics make sense with respect to the population of customers.

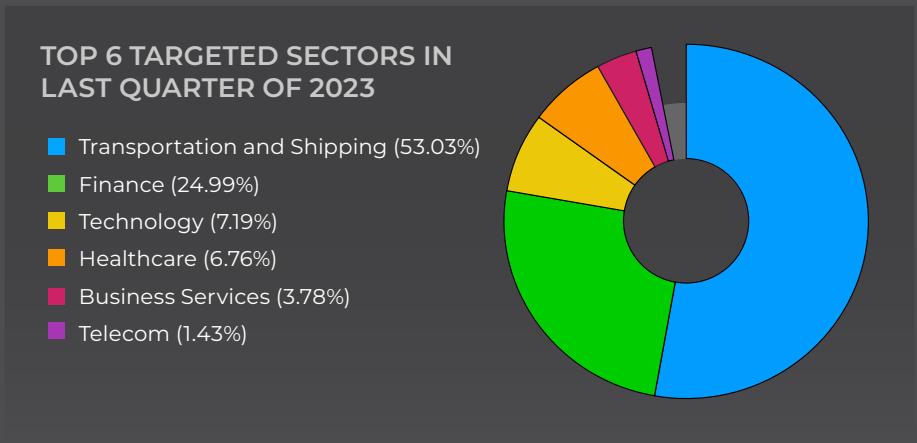
In the quarter prior, telemetry looks rather similar, barring the increase of detections in India and China. We have no indication that there was a specific campaign against these regions and suspect malware testing was done and caused a higher number of detections in said regions.

## Targeted sectors

The aggregation of global telemetry per sector shows that half of the detections come from the transportation and shipping industry, and just over a quarter comes from the financial services. These two sectors make up more than 72% of all detections, which is logical: the availability of their services is of the utmost importance. If a transportation company cannot move goods around due to a ransomware attack, their operational process cannot continue, causing a huge financial burden. Likewise, the financial industry is built on trust, while the leakage of sensitive data and/or downtime of the company due to a ransomware attack, hurts financial companies in their core.




In the last quarter of 2023, the top targeted sectors were slightly different, albeit without differences in the top two sectors. Those two were responsible for an even larger share, totalling at a combined 78% of all detections for the given period. The technology and healthcare sectors decreased in the first quarter of 2024, compared to the prior quarter, but the difference itself cannot be attributed to one or more specific events.




## Tools and techniques

The last of the three mentioned sources are public reports. Based on the collected reports, MITRE techniques, associated tools and commandlines can be distilled.

> **CISO TIP:** These can be used by organization blue teams from a detection perspective: by focusing on the most used techniques and tools, multiple types of attacks from different actors can be mitigated, starting by the most effective. Additionally, red and purple teaming exercises can focus on these techniques to test what detection measures are in-place.

This table below shows the most frequent techniques, listed in descending order.

| MITRE ATT&CK Techniques | Unique Campaigns |
|---|---|
| Data Encrypted for Impact | 31 |
| File and Directory Discovery | 23 |
| PowerShell | 23 |
| Ingress Tool Transfer | 21 |
| System Information Discovery | 21 |
| Obfuscated Files or Information | 19 |
| Modify Registry | 18 |
| Windows Command Shell | 17 |
| Deobfuscate/Decode Files or Information | 16 |
| Service Stop | 16 |

Given ransomware's objective, the data encryption and file and directory discovery techniques unsurprisingly rank at the very top. When comparing these techniques with the most prevalent techniques from the fourth quarter of 2023, one will notice that most

TABLE OF CONTENTS

of the top techniques in the list are similar, although their specific place might differ.

| MITRE ATT&CK Techniques | Unique Campaigns |
|---|---|
| Data Encrypted for Impact | 45 |
| PowerShell | 29 |
| Obfuscated Files or Information | 25 |
| File and Directory Discovery | 24 |
| Windows Command Shell | 24 |
| Inhibit System Recovery | 23 |
| Exploit Public-Facing Application | 21 |
| Ingress Tool Transfer | 21 |
| Process Discovery | 21 |
| Service Stop | 21 |

Much like in the above section on APTs, attackers continue to leverage legitimate tools for crime. The used tools influence the observed techniques, as a tool is a means to an end, which is a technique in this case. For example, PowerShell and the Windows Command Shell are often used to execute additional commands on the system, such as the removal of the shadow copies, which is the main contributor to the "Inhibit System Recovery " Technique. This is also the reason as to why they are the top used tools, as shown in the image below.

| CLI Tool Name (attr) | Unique Campaigns |
|---|---|
| Cmd | 7 |
| PowerShell | 6 |
| VSSAdmin | 5 |
| wevtutil | 4 |
| curl | 4 |
| Rundll32 | 4 |
| Reg | 4 |
| Schtasks.exe | 3 |
| BCDEdit | 3 |
| wget | 2 |

TABLE OF CONTENTS

The usage of VSSAdmin, BCDEdit, and wevutil are signs that the ransomware is ensuring the victim's system cannot recover to a normal state, as it would be in prior to the attack. The usage of reg shows the changes to the registry, which can be done for a variety of reasons. Malware often uses the registry for persistence, but ransomware isn't keen on persistence, as it has no purpose once the encryption finishes. Instead, it can alter other settings, to allow certain actions which normally wouldn't be possible. Rundll32 is often used to either load and run a dynamic link library, but often it is also the target of process injection.

Much like the quarter prior to the one above, PowerShell and the command prompt top the list for the exact same reason. VSSAdmin and BCDEdit are present as well, though the Windows Event Util (wevtutil) is not present in the top tools list. Given the few occurrences of all mentioned tools, with the highest frequency being 13 in either of the quarters, it is no surprise that not all campaigns use the same tools. A small deviation can lead to the exclusion of such tools.

| CLI Tool Name (attr) | Unique Campaigns |
|---|---|
| Powershell | 13 |
| Cmd | 9 |
| WMIC | 6 |
| Net | 6 |
| echo | 5 |
| VSSAdmin | 4 |
| msiexec | 3 |
| Schtasks.exe | 3 |
| Rundll32 | 3 |
| BCDEdit | 3 |

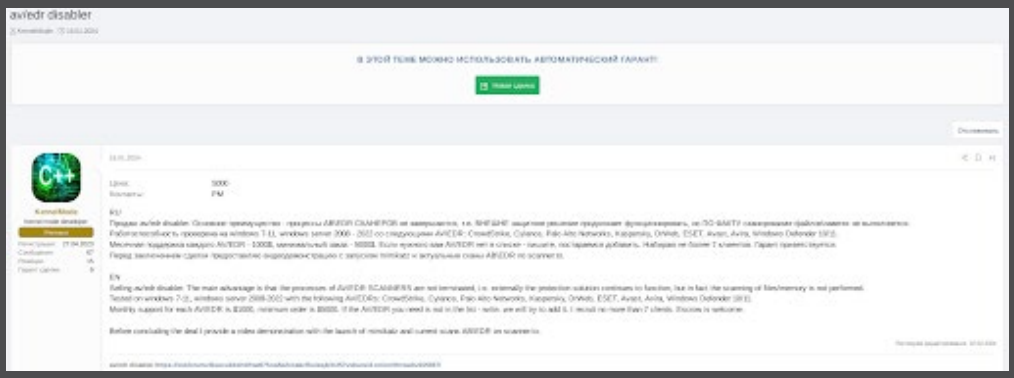
The threat of ransomware remains.

**TABLE OF CONTENTS**

## The Emergence of EDR Killer and Evasion Tools

The global adoption of EDR solutions by many organizations has proven to better detect, understand, and respond to more sophisticated attacks. Threat actors nowadays often rely on living-off-the-land binaries (LOLBins) and more complex attack methods, but with the presence of EDR technology it has become more difficult for attackers to remain undetected.

Security however, remains a cat and mouse game, and attackers are trying to find ways to evade or disable EDR solutions. This movement has given birth to a whole wave of EDR killer and evasion tools/ techniques, some of which are being offered on cybercriminal underground forums. We saw earlier, for example, that the D0nut ransomware gang has gained prominence thanks to their own EDR killer.




EDR disabler advertisement on the XSS underground forum

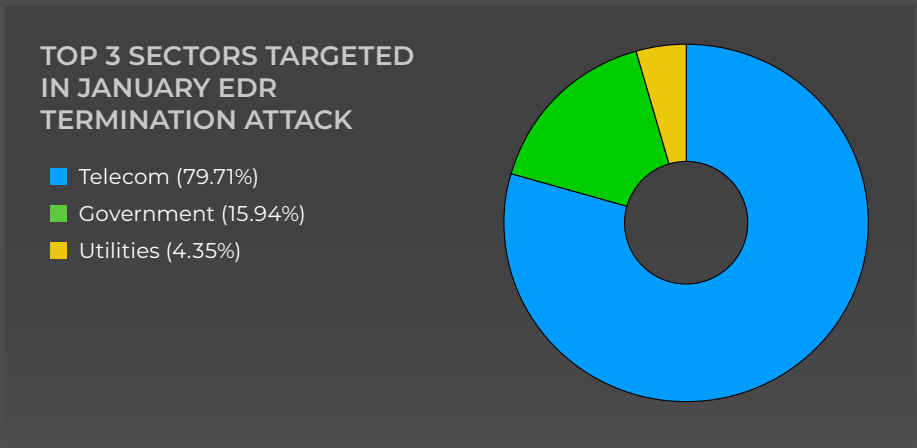
### January campaign using Spyboy's EDR Terminator tool

One common technique is by exploiting vulnerable drivers to achieve privileged code execution is referred to as a Bring Your Own Vulnerable Driver (BYOVD) attack.

An example of this method is the EDR "Terminator" tool that was offered by a threat actor called Spyboy. The Terminator tool leverages a legitimate but vulnerable Windows driver belonging to the Zemana anti-malware tool to execute arbitrary code from within the Windows Kernel likely exploiting CVE-2021-31728. Terminator appeared online in mid-2023 and Trellix issued a detailed knowledge base article around product coverage which can be found here.

From January 11 - 17, 2024, the Trellix Advanced Research Center noticed an unusual set of detections of Spyboy's Terminator in Trellix telemetry – a new campaign. This Terminator campaign spiked for three days during the six day period and was detected multiple times at a single government organization, a national utilities company and a satellite communications company. Given the specific targets Trellix assesses with a high level of confidence that the attack was related to the Russian-Ukrainian conflict.

TABLE OF CONTENTS




Trellix ATLAS Detections targeting Ukraine for the EDR Terminator campaign in January

## More EDR killers observed

Earlier in 2023, a tool with a similar purpose was described by Sophos – AuKill. It also used a vulnerable driver it brought (BYOVD). The drivers used in the EDR Terminator and AuKill cases are different, but both are benign drivers. In contrast, some campaigns in 2022 saw similar tooling use custom malicious drivers which were loaded.

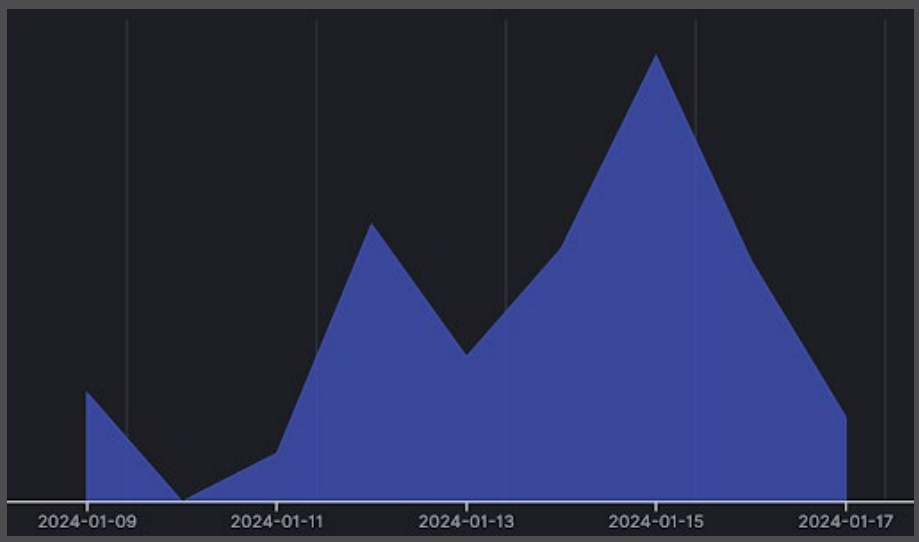



TABLE OF CONTENTS

Abusing benign drivers for such a purpose makes it harder to detect such attacks, and coincides with the aforementioned LOLBin usage. Although a binary and a driver differ technically, the intent and motive are similar, if not identical. The HermeticWiper from 2022 also comes to mind with regards to using a benign driver. In that case, the driver was used to wipe a machine, rather than disabling the antivirus. A further overlap with the usage of the EDR Terminator mentioned above, and the attribution of the HermeticWiper, is the usage by a pro-Russian actor.

We've also seen an example of the Discord CDN being used for malware distribution at one of our LATAM customers. Our team has observed Discord continue to be used in malware attacks in this way.

> **CISO TIP:** It is absolutely essential every SOC is monitoring their EDR closely. Alert and logging needs to be set up so if EDR tools are turned off, the SOC is notified immediately and appropriate action can be taken. Shutting down of EDR tools can be an indicator of tampering, and moving quickly is critical to limiting an attacker's access to your network. It is also critically important to use a defense-in-depth strategy, allowing other tools like your Network Detection and Response (NDR) platform to detect potential incidents. and moving quickly is critical to limit the access an attacker gets to your network.

**TABLE OF CONTENTS**

## Email Remains Ripe for Attackers

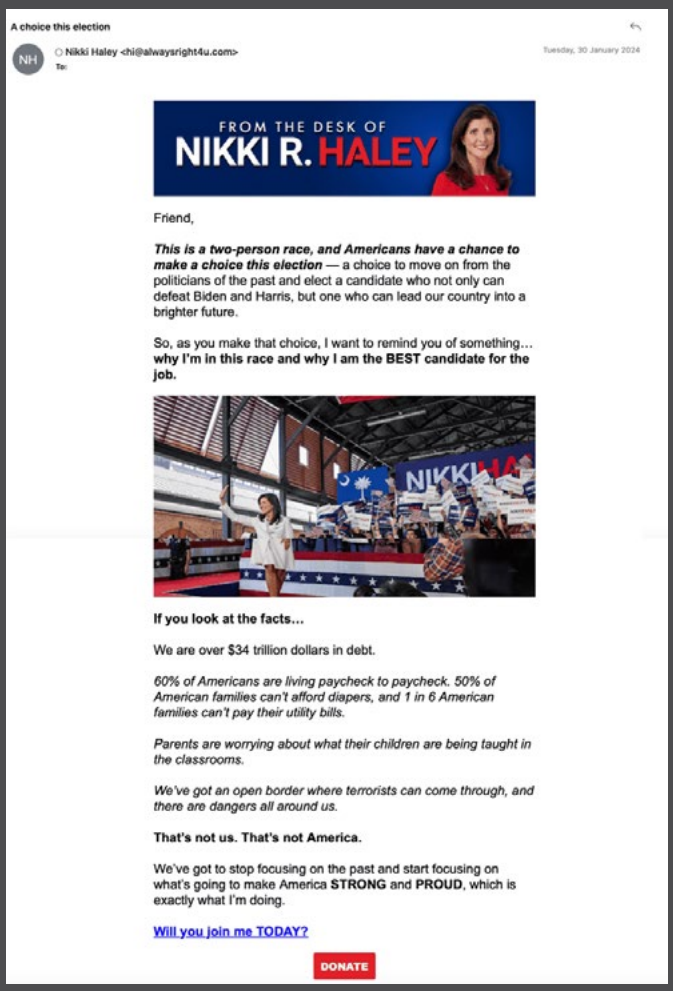
Trellix processes two billion email samples and 93 million email attachments per day. With this, comes an immense amount of data and opportunity to observe new techniques leveraged by attackers targeting victims via email.

### Election donation scams

Election donation phishing scams exploit individuals' goodwill and support for political candidates by leveraging patriotic sentiments and using famous political candidates names. In Q1 2024, our researchers found cybercriminals abusing legitimate marketing services to create convincing donation pages adorned with images of candidates alongside American flags, urging recipients to donate.

These scams utilize authentic marketing service URLs to deceive recipients, leading them to believe the emails are legitimate. However, the emails are sent to capitalize on people's generosity. Links within the emails direct users to donation pages, where they're prompted to enter financial details or send contributions to the senders' accounts or wallet addresses.

Our email researchers observed the following malicious emails leveraging election donations.


A choice this election

NH Nikki Haley <hi@alwaysright4u.com>

To:

Tuesday, 30 January 2024

FROM THE DESK OF NIKKI R. HALEY

Friend,

***This is a two-person race, and Americans have a chance to make a choice this election*** — a choice to move on from the politicians of the past and elect a candidate who not only can defeat Biden and Harris, but one who can lead our country into a brighter future.

So, as you make that choice, I want to remind you of something… **why I'm in this race and why I am the BEST candidate for the job.**

**If you look at the facts…**

We are over $34 trillion dollars in debt.

*60% of Americans are living paycheck to paycheck. 50% of American families can't afford diapers, and 1 in 6 American families can't pay their utility bills.*

*Parents are worrying about what their children are being taught in the classrooms.*

*We've got an open border where terrorists can come through, and there are dangers all around us.*

**That's not us. That's not America.**

We've got to stop focusing on the past and start focusing on what's going to make America **STRONG** and **PROUD**, which is exactly what I'm doing.

Will you join me TODAY?

DONATE



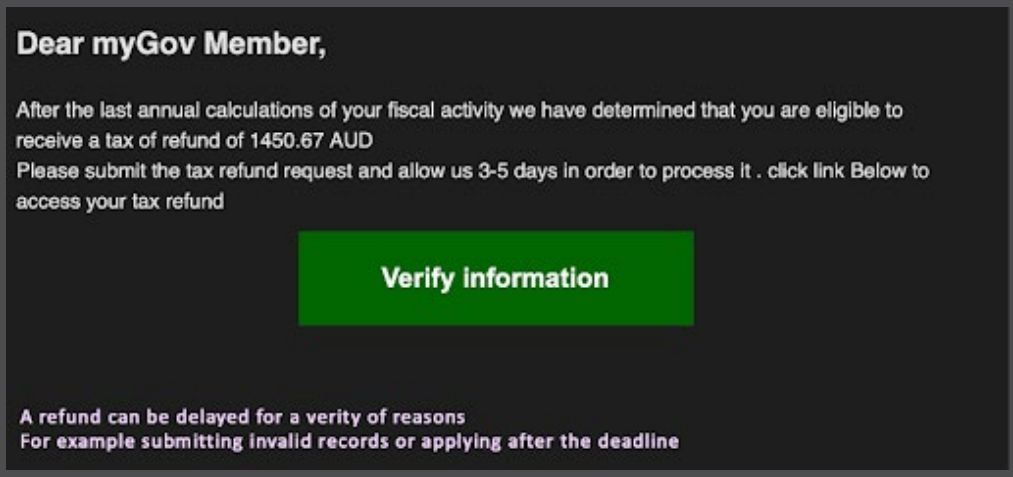
## Taxation phishing

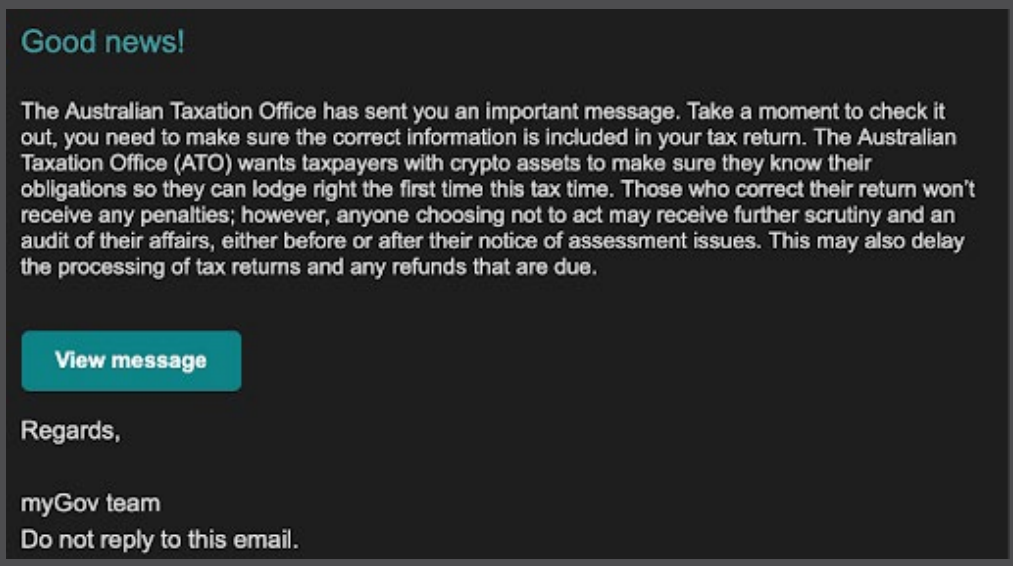
In the context of taxation, phishing attacks are particularly concerning. Scammers pose as government agencies, tax authorities, or reputable tax preparation services to trick individuals into divulging personal information. They may claim that you owe back taxes, have unfiled returns, or are eligible for a tax refund. Their ultimate goal is to obtain your Social Security number, bank account details, or other valuable data. The email contains links that appear to lead to official government or tax service websites but instead redirect you to fraudulent sites designed to steal data.

Trellix also observed a surge in such emails pretending to be from the Australian Tax Authority in the first quarter of 2024 and successfully detected them.

TABLE OF CONTENTS

Below is one sample from the campaign where we see clearly that attackers are creating urgency to click the link relating to taxation refund.




## The GenAI Arms Race: Findings from the Cybercriminal Underground

AI and machine learning are no longer only accessible to organizations with the deepest pockets. ChatGPT and the like can be used by anyone, including criminals, and so, AI has become an arms race between the good actors and the bad actors. AI is powerful and should be responsibly leveraged to further business goals, but it is imperative organizations do not let the attackers gain the advantage. We need to use newfound capabilities to outsmart cyber criminals as their tactics become honed, and their weapons become more dangerous.

TABLE OF CONTENTS

**CISO TIP:** The role of the CISO has become even more essential as they're looked upon to navigate this evolving landscape. With cyberattacks on the rise, AI pressures mounting, and responsibilities growing, it's no surprise 90% of CISOs find themselves under increased pressure. Keeping pace with AI and GenAI is vital, and almost all CISOs agree their organizations could do more. Read more in Trellix's latest report, Mind of the CISO: Decoding the GenAI Impact.

Threat actors are attracted to GenAI because of its accelerated capabilities and affordability. Most significantly, it provides expertise: bad actors can craft spear phishing emails in any language with perfect grammar, logos, and login info. They can find, write, and test exploits 10x faster without elite skills.

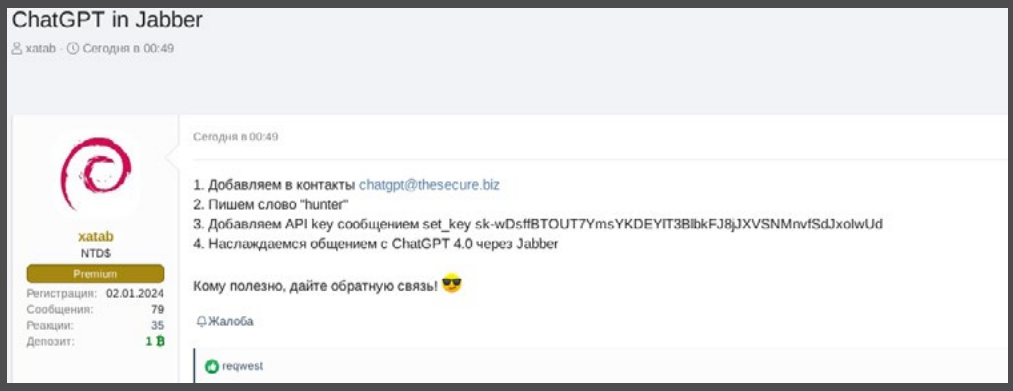
Our Advanced Research Center team regularly scours the cybercriminal underground to follow trends. GenAI is gaining steam with cybercriminals and they are sharing their successes and selling their tools. Since our last report, we've observed the following since the start of 2024.

### 'ChatGPT in Jabber' project possibly used by a Russian criminal APT group

In January, we observed an XSS underground forum's premium actor **xatab** searching for a developer to create "ChatGPT 4.0 in Jabber" along with an API and instructions on how to use it.

Besides the Cyber criminal embrace of LLM integrations It is also possible that **xatab**'s intention/motivation behind the "ChatGPT in Jabber" project is to intercept & collect threat actors correspondence, eavesdrop on their requests to gain intelligence & knowledge on what cybercriminals are interested in and what are the main topics & scopes of their illicit activities aided by GenAI.

We observed the following -




**xatab** shared on the XSS forum instructions and the API key for "ChatGPT in Jabber"

TABLE OF CONTENTS

```
Python
1. Add to your contacts chatgpt@thesecure.biz
2. Write a keyword "hunter"
3. Add API key in the message: set_key <OPENAI_API_KEY>
4. Enjoy the conversation with  ChatGPT 4.0 via Jabber

If useful share your feedback!
```

On January 31, 2024, **xatab** offered $2,000 for their 'ChatGPT in Jabber' project on the XSS forum. Based on the recent XSS complaint raised by an actor **germans** who built the requested bot and got ignored by **xatab** at first, it seems that **germans** agreed to develop the ChatGPT bot in Jabber for $1500. The bot was created for both Exploit forum (@exploit[.]im) and XSS (@thesecure[.]biz) Jabber servers and **xatab** posted it on both Exploit and XSS darknet forums supposedly to test it and get feedback from the forum members. The bot may be based on the xmppgpt project.

The **xatab** actor has multiple posts on Exploit/XSS forums where they advise they are an APT team (known in certain circles experienced pentesters) interested in hiring a broker of corp accesses of US/UK/Canada/Australia organizations for fruitful cooperation. They offered 20% of the revenue share for every access and they deposited one BTC to both Exploit and XSS forums to show their intention/seriousness of their offer.

By providing free ChatGPT 4.0 to cybercriminal community **xatab** is achieving two things:

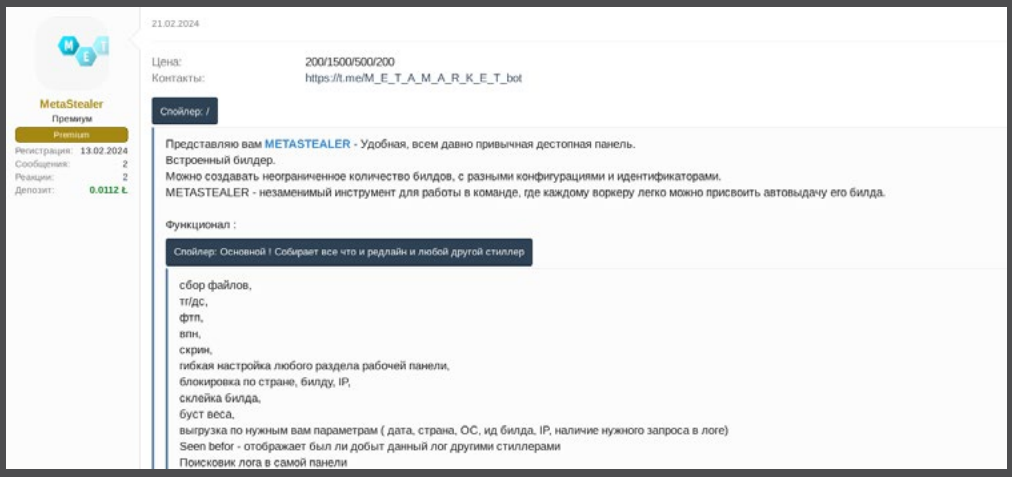
1. Serving  facilitator and enabler who is eager to help threat actors to innovate and adopt GenAI in their operations
2. Attempt to create a GenAI knowledge base/pool to learn from other cyber criminals or even steal their innovative ideas and tools

Trellix has tested the "ChatGPT in Jabber" project as per the given instructions and it seems to work as advised by the threat actor.

## GenAI adoption in InfoStealers

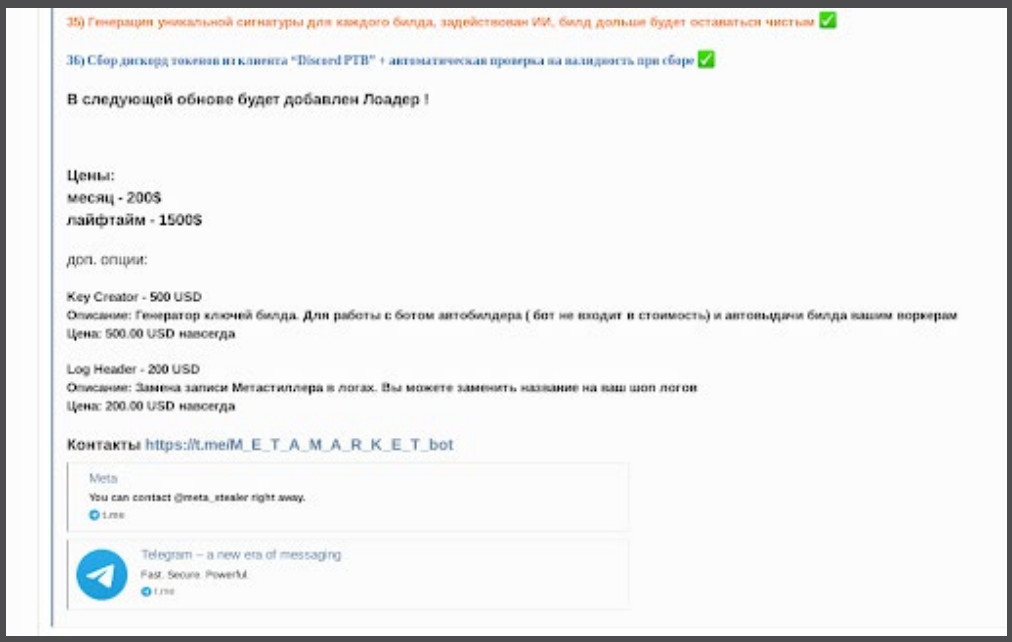
On February 21, 2024 our researchers observed a threat actor MetaStealer advertising a new, revamped version of **MetaStealer** on XSS forum. MetaStealer is an infostealer which first appeared in 2021 and is believed to be a spinoff of well-known infostealer Redline. There have been multiple versions of **MetaStealer** seen in the wild, however the recent version spotted by Trellix has a GenAI-based feature to further avoid detection.

TABLE OF CONTENTS




**MetaStealer** shared on the XSS forum revamped version of METASTEALER

In the below screenshot, the orange text under 35) translates as "Generation of unique signatures for every build, AI is used here, the build remains clear (or undetected) for a longer time," suggesting the developers of MetaStealer embedded a new GenAI based feature into their stealer which allows them to create unique builds of MetaStealer to evade detection and stay under the radar of AV/EDR systems for a longer period of time than before.

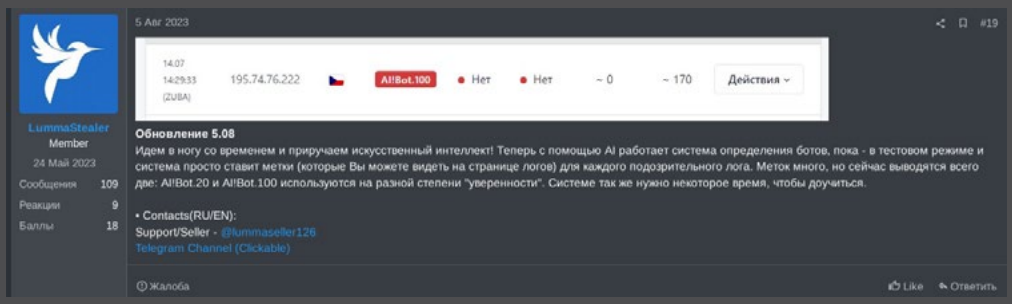



Revamped METASTEALER has an embedded GenAI based feature for defense evasion

Another example is a well-established infostealer called LummaStealer. Since August 2023, we've observed the LummaStealer team testing an AI-based feature which enables their infostealer users to detect bots among the list of logs. The AI-based system embedded into LummaStealer is potentially a custom neural network which is trained to detect if a suspicious user log is a bot or not. LummaStealer

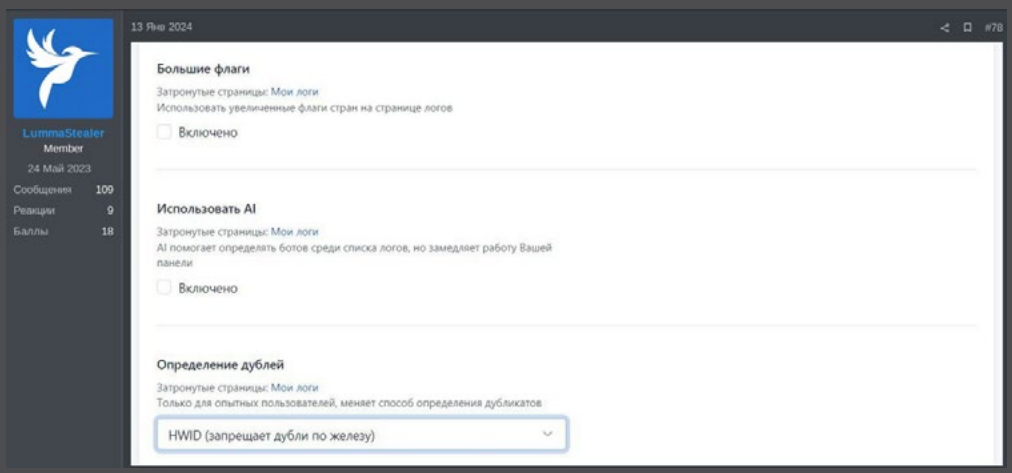
TABLE OF CONTENTS

uses a label **AI!Bot.<number>** to categorize the detected log as a bot, where <number> seems to be in a range of 0-100, representing the bot detection certainly:




LummaStealer post on the RAMP forum where the actor advised their infostealer has an AI based feature to detect bots among the list of stealer logs

**LummaStealer** advised its users the neural network was still being trained and it will take some time for it to improve the detection accuracy. Moreover, in January 2024, **LummaStealer** advised the GenAI based feature by default is disabled as it slows down the work of the LummaStealer panel.

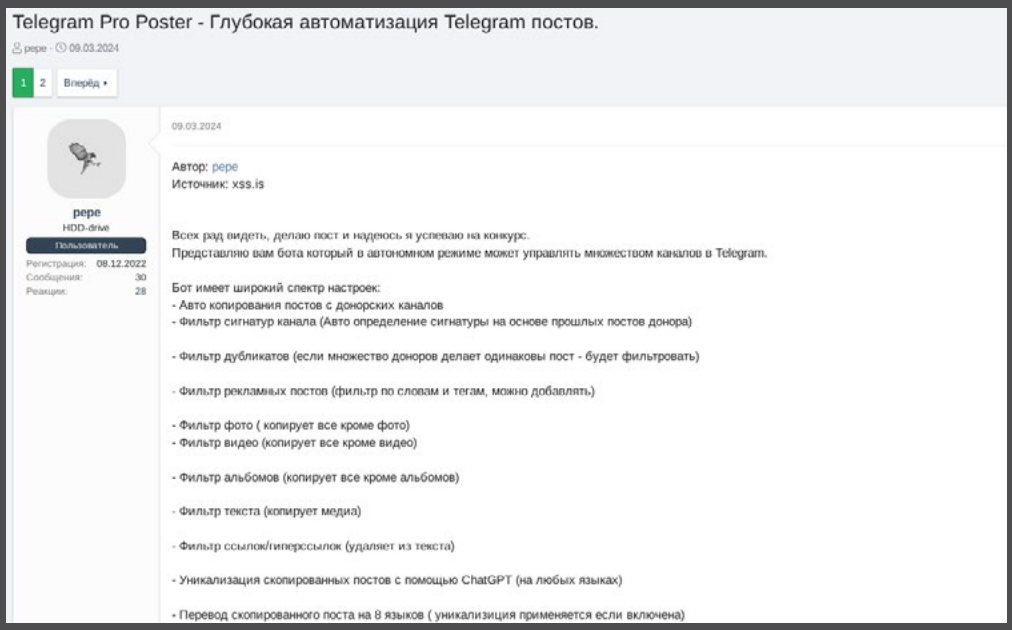



LummaStealer post on the RAMP forum where the actor advised the AI based bot detection is disabled by default

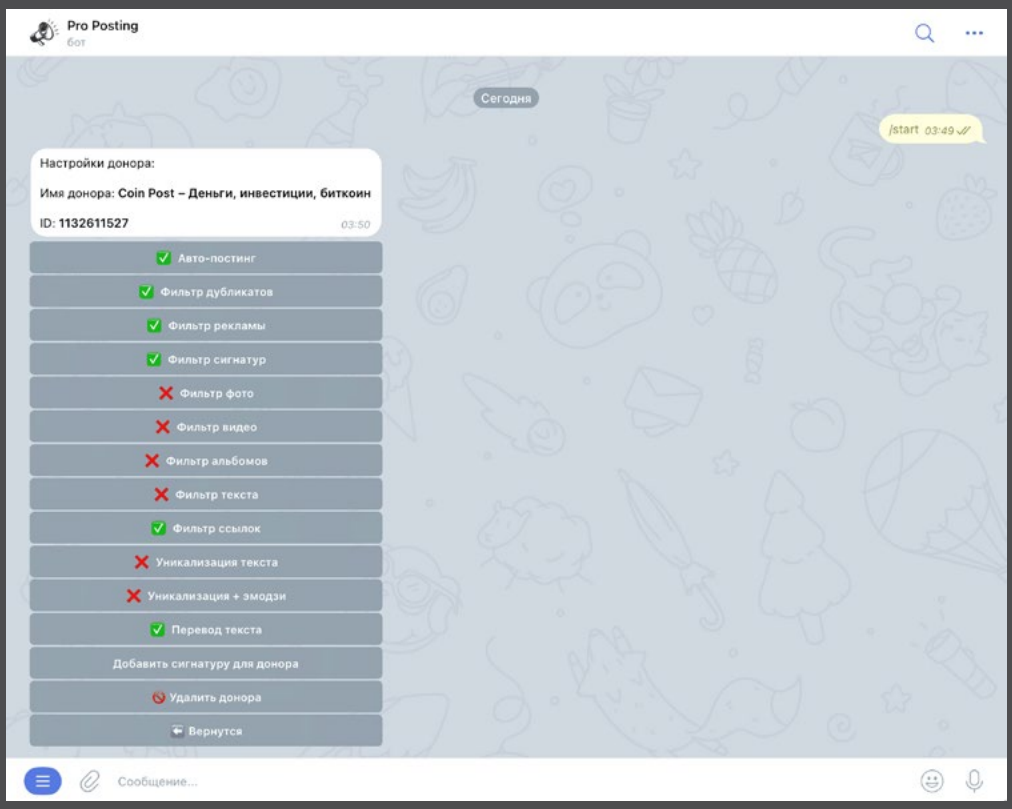
### 'Telegram Pro Poster' bot project

In early March 2024 Trellix observed a threat actor pepe posting their "Telegram Pro Poster' project on the XSS forum as a part of an underground competition of malicious tools/software. Telegram Pro Poster is a bot for "deep automation of Telegram posts." This Python-based bot allows users to manage multiple (unlimited amount of) Telegram channels in an autonomous way by automatically copying the posts from "donor" Telegram channels into the target channels. Amongst numerous post filtering features, this bot has two GenAI embedded features for translating telegram messages and paraphrasing a given post using ChatGPT.

TABLE OF CONTENTS




XSS forum post on Telegram Pro Poster GenAI-based bot




Telegram Pro Poster's filtering features including 'unique-alisation' features disabled by default

Trellix has obtained the source code of the Telegram Pro Poster and identified the following pieces of code which are responsible for translating copied posts from the donor channels via ChatGPT API into eight following languages prior to sending it to the target Telegram channels:

TABLE OF CONTENTS

```
Unset
API_ID = 99999999 #APP TELEGRAM ID
API_HASH = "HASH" # APP TELEGRAM HASH
BOT_TOKEN = "API" # BOT API
DATABASE_PATH = 'database.db'
OPEN_AI_KEY = 'API KEY' # OPEN AI KEY


language_codes = {
    'Ukranian': 'украинский',
    'Russian': 'русский',
    'English': 'английский',
    'Indian': 'индийский',
    'Italian': 'итальянский',
    'Brasilian': 'бразильский',
    'Germany': 'немецкий',
    'Indonesian': 'индонезийский'
}
...
def gpt_translate(input_text, language):
    print(f'Перевожу этот текст: {input_text}')
    if len(input_text) > 10:
        openai.api_key = OPEN_AI_KEY
        language = language_codes[language]

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": f"Когда ты получаешь текст то ты
должен перевести его на {language}."},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        return unique_text
    else:
        return input_text
```

The second feature called “unique-alization” by default is disabled, however when it is turned on, it uses OPEN_AI_KEY to request ChatGPT to paraphrase the given text into a desired language and optionally add an emoji.

```
Python
def unique_text(input_text, is_emoji_need):
    print(f'Уникализирую этот текст: {input_text}')
    if len(input_text) > 5:
        openai.api_key = OPEN_AI_KEY

        if is_emoji_need:
            content_text = "Перефразируй текст и добавь эмодзи: "
        else:
            content_text = "Перефразируй текст:"

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": content_text},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        token_count = response['usage']['total_tokens']
        return unique_text

    else:
        return input_text
```

**TABLE OF CONTENTS**

The XSS community of cybercriminals are already sharing their positive feedback on the "Telegram Pro Poster project" saying it is an interesting project and in competent hands this tool will certainly be useful. Another threat actor advised in the XSS forum thread that they are seeing this bot already being adopted in practice by various Telegram channels.

## AFTERWORD

### The race is on

Operational threat intelligence provides insights into the nature, intent, and timing of specific cyber threats. It's more detailed and contextual than tactical intelligence, including information about threat actors' tactics, techniques, and procedures (TTPs).

Organizations can use operational intelligence to understand the broader context of cyber attacks, such as the motivations behind them or the methods used, helping security teams anticipate and prepare for specific types of attacks.

In my work with customers, I know that the most important objective of every CISO is to limit risk to their organization. Applying operational threat intelligence is a tangible way to limit that risk as it allows CISOs and their SecOps teams to look ahead and get their footing. It empowers them to identify gaps in their security measures across their entire surface of the organization and get in the minds of their opponents, looking to knock them off track.

We share our threat intelligence to give you a solid, fact-based platform supporting some of the most important decisions you'll make. Our purpose is to help you substantially improve your cyber defense and beat attackers to the next leg of the race - however you choose to.

Let's go!

Ashok Banerjee,
CHIEF TECHNOLOGIST, TRELLIX

TABLE OF CONTENTS

## METHODOLOGY

**Collection:** Trellix and the 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.

- **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 their SecOps teams (1) understand the most recent trends in the cyberthreat environment, and (2) use this perspective to improve their ability to anticipate, prevent, and defend their organization from cyberattacks in the future.

### 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.

TABLE OF CONTENTS

- 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.

TABLE OF CONTENTS

## RESOURCES

Threat Report Archives

The Mind of the CISO

### FOLLOW TRELLIX ARC ON X

Trellix ARC

View CyberThreat Report Archives

Trellix Advance Research Center

TABLE OF CONTENTS

## ABOUT THE TRELLIX ADVANCED RESEARCH CENTER

The Trellix Advanced Research Center is at the forefront of research into the emerging methods, trends, and tools used by cyber threat actors across the global cyber threat landscape. Our elite team of researchers serve as the premier partner of CISOs, senior security leaders, and their security operations teams worldwide. The Trellix Advanced Research Center provides operational and strategic threat intelligence through cutting-edge content to security analysts, powers our industry leading AI powered XDR platform, and offers intelligence products and services to customers globally. More at https://www.trellix.com/en-us/advanced-research-center.html.

## 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, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 40,000 business and government customers with living security. More at https://trellix.com.

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.

**TABLE OF CONTENTS**



Copyright © 2024 Musarubra US LLC