OCTOBER 2024

Cyber Threat Advisory

Third-party cyberattacks exploit supplier access to compromise sensitive information and critical systems.

sdgc.com

Table of Contents

Key Cybersecurity Trends

CXO Summary

Microsoft Redesigning EDR Access Kernel

Microsoft plans to redesign the way anti-malware (EDR) products interact with the Windows kernel in direct response to the global IT outage caused in July by a faulty CrowdStrike update.

Microsoft wants vendors to adopt what it calls Safe Deployment Practices (SDP) while rolling out updates to the large Windows ecosystem.

Adversarial Use of AI—Is AI Threat a Deep Fake or Is Deepfake the AI Threat?

One of the most surprising aspects of generative AI models is their versatility. When fed enough high-quality training data, mature models can produce output that approximates human creativity. The implication is that the long-awaited upsurge in gen-AI generated phishing is imminent—the criminals seem to have been learning how best to use this new opportunity.

United Nations Convention on Cybercrime

Nearly 200 nations approved the United Nations Convention against Cybercrime on Thursday afternoon at a special committee meeting that capped months of complicated negotiations. The treaty—expected to win General Assembly approval within months—creates a framework for nations to cooperate against internet-related crimes, including the illegal access and interception of computer information, electronic eavesdropping, etc.

Nearly 200 nations approved the United Nations Convention against Cybercrime

CRITICAL THREAT ALERT

Focus of the Month: Attack on Machine Learning Models

Data poisoning attacks pose a significant threat to the integrity and reliability of AI and ML systems. A successful data poisoning attack can cause undesirable behavior, biased outputs, or complete model failure. As the adoption of AI systems continues to grow across all industries, it is critical to implement mitigation strategies and countermeasures to safeguard these models from malicious data manipulation.

Current Trends and Developments in Attacks on Machine Learning Models: Types of Attacks

1. **Adversarial Patch Attacks:** Techniques are being developed to create adversarial patches that are less noticeable to humans, making them more difficult to detect and more effective in real-world scenarios, such as fooling autonomous vehicles and facial recognition systems.
2. **Transferability Attacks:** Attacks generated for one model can often be transferred to other models, making it difficult to defend against a wide range of attacks, such as attacks on models without requiring access to their architecture or training data.
3. **Mislabeling Attacks:** By intentionally providing incorrect labels for training data, attackers can manipulate an AI model to learn biased or inaccurate relationships, ultimately compromising its performance.
4. **ML Supply Chain Attacks:** AI systems often depend on external components and data, which can create security risks. These vulnerabilities, including backdoors, can be introduced through supply chain attacks at any stage of the AI development process.
5. **Backdoors:** Attackers can manipulate AI models by introducing hidden vulnerabilities, or 'backdoors,' into their training materials or algorithms. These backdoors can be triggered to cause the model to generate malicious results when fed specific input.

The following strategies should, therefore, be implemented to mitigate the risks of such attacks.

- **Training Data Validation:** Before starting model training, all data should be validated to detect and filter out any suspicious or potentially malicious data points. This helps safeguard against the risk of threat actors inserting and later exploiting such data.
- **Adversarial Sample Training:** Introducing adversarial samples during the model's training phase is a vital proactive security defense measure to stop many data poisoning attacks. This enables the ML model to correctly classify and flag such inputs as inappropriate.
- **Diversity in Data Sources:** Using multiple data sources enables an organization to diversify its ML model training data sets, significantly reducing the efficiency of many data poisoning attacks.
- **Continuous Monitoring and Auditing:** Like all information systems, AI systems need strict access controls to prevent unauthorized users from accessing them. Apply the principle of least privilege and set logical and physical access controls to mitigate risks associated with unauthorized access. Continuous monitoring and auditing should also focus on the model's performance, outputs and behavior to detect potential signs of data poisoning.

Monthly Highlights

83% of Organizations Experienced at Least One Ransomware Attack in the Last Year

Ransomware has become a widespread issue, with 83% of organizations reporting at least one ransomware attack in the past year. Among these, 46% experienced four or more attacks, and 14% faced 10 or more. Of those affected, 61% said the attack caused downtime of at least 24 hours, according to Onapsis.

Additionally, 89% of organizations impacted by ransomware noted that their Enterprise Resource Planning (ERP) systems were affected at least once. Recognizing the critical nature of the issue, 93% of respondents agreed on the necessity of having a dedicated ERP security solution.

Concerns are growing around AI-powered threats. Gartner's research in the first quarter of 2024 identified AI-enhanced malicious attacks as the top emerging risk. Mariano Nunez, CEO of Onapsis, pointed out that the increasing impact on ERP applications is alarming, and the threat is expected to worsen with AI-driven attacks. He emphasized that attackers are targeting ERP systems because downtime at large organizations can result in millions of dollars in losses per hour, and existing security solutions are proving inadequate.

When it comes to handling ransomware, 69% of organizations admitted to communicating with the attackers. Regarding ransom payments, organizations were divided: 34% always pay, 21% occasionally pay, and 45% never pay. Many organizations seek external help, with 83% of those who paid the ransom at least once having worked with a ransomware broker.

Concerns are growing around AI-powered threats. Gartner's research in the first quarter of 2024 identified AI-enhanced malicious attacks as the top emerging risk.

Ransomware has become such a pervasive problem that 96% of organizations have made changes to their security strategies. In response to ransomware threats:

- 57% invested in new security solutions
- 54% invested in employee training
- 53% increased their internal cybersecurity staff
- 36% hired an external threat research team

Cyber Threats That Shaped the First Half of 2024

Global cybercrime continues to grow with no signs of slowing down and is projected to strengthen annually over the next five years.

To assess the most pressing cybersecurity threats for the first half of 2024, the Critical Start Cyber Research Unit (CRU) analyzed 3,438 high-priority alerts generated by 20 EDR (Endpoint Detection and Response) solutions and reviewed 4,602 reports related to ransomware and database breaches across 24 industries in 126 countries.

Scammers, previously focused on large corporations, are now targeting smaller businesses with weaker cybersecurity measures.

Key findings from the first half of 2024 reveal an alarming trend of cyberattacks targeting specific industries:

- Manufacturing and industrial products remained the most targeted sector, with 377 confirmed ransomware and database leak incidents.
- Professional services experienced a 15% rise in ransomware attacks and database leaks compared to 2023, with 351 cases reported. Legal services and supply chains have become high-value targets due to the sensitive intellectual property and data they hold.
- Healthcare and life sciences saw a dramatic 180% increase in ransomware and database leak incidents in February 2024 compared to the same period in 2023. This spike coincided with the attack on Change Healthcare and other healthcare providers.
- Engineering and construction remained a consistent target, with the U.S. facing a 46.15% surge in cyberattacks during the first half of 2024 compared to the previous year.
- Technology companies experienced a 12.75% decrease in ransomware and database leaks compared to the first half of 2023.

Security experts have noted the continued rise in ransomware and database leak activities, emphasizing the need for robust security strategies. She stressed the importance of MDR (Managed Detection and Response) solutions that integrate asset inventory, endpoint security, and MITRE ATT&CK mitigations to reduce the attack surface and build a resilient security infrastructure.

The report also highlighted emerging concerns for businesses, including:

- **Business Email Compromise (BEC) Attacks:** Scammers, previously focused on large corporations, are now targeting smaller businesses with weaker cybersecurity measures.
- **Deepfakes and Social Engineering:** A significant rise in deepfake attacks was observed, with a 3,000% increase in fraud attempts.
- **Abuse of Open-Source Repositories:** Attackers are increasingly exploiting these repositories to execute repo confusion and supply chain attacks.

A Macro Look at the Most Pressing Cybersecurity Risks

Forescout's 2024 H1 Threat Review provides an in-depth analysis of vulnerabilities, threat actors, and ransomware attacks during the first half of 2024, comparing them to the same period in 2023.

"Attackers are exploiting any weak spot in IT, IoT, and OT devices. Organizations that lack awareness of what's connected to their networks or whether those devices are secured are leaving themselves exposed," stated Barry Mainz, Forescout CEO. He emphasized that organizations need to improve network visibility, implement proactive security measures, and consider upgrading outdated VPN solutions. A comprehensive approach, including visibility into all connected devices and strong access controls, is critical to defend against the growing and evolving threats.

Key Findings

Vulnerabilities Increased by 43%

- Reported vulnerabilities surged by 43% compared to H1 2023, totaling 23,668 in H1 2024.
- The daily average of new Common Vulnerabilities and Exposures (CVEs) was 111, or 3,381 per month—7,112 more than in the same period last year.
- 20% of these exploited vulnerabilities targeted VPNs and network infrastructure.

Ransomware Groups and Attacks on the Rise

- Ransomware incidents rose by 6%, reaching 3,085 cases, up from 2,899 in H1 2023, with an average of 441 attacks per month or 15 per day.
- The U.S. accounted for half of all attacks, up from 48% in 2023.
- The most targeted sectors were government, financial services, and technology.
- The number of active ransomware groups increased by 55%.

Top Targets—U.S., Germany, and India

- Out of 740 threat actors tracked by Forescout, 387 were active in H1 2024.
- The U.S., Germany, and India were the most frequently targeted, with the U.S. seeing twice the number of attacks as Germany and India.
- 50% of these active groups were cybercriminals (including ransomware gangs), while 40% were state-sponsored actors, primarily from China, Russia, and Iran.

State-Sponsored Actors Using Hacktivist Fronts

- State-sponsored groups are increasingly posing as hacktivists to attack critical infrastructure.
- Notable groups like Predatory Sparrow and Karma Power were responsible for significant attacks under the pretense of hacktivism.
- This trend may be driven by the desire to obscure state-sponsored cyberwarfare activities.

Massive Targeting of VPN and Network Infrastructure

- In H1 2024, 15 new CVEs in the CISA Known Exploited Vulnerabilities (KEV) catalog targeted infrastructure and security appliances from companies like Ivanti, Citrix, Fortinet, Cisco, Palo Alto Networks, Check Point, and D-Link.
- These vulnerabilities accounted for nearly 20% of new entries in the CISA KEV.
- Attackers frequently used zero-day or newly disclosed vulnerabilities that remained unpatched.
- Forescout research identified routers and wireless access points as the riskiest IT devices in 2024.

Key Cyber Insurance Stakeholders Urge Government to Help Close $900B in Uncovered Risk

Marsh McLennan and Zurich Insurance Group have issued a white paper advocating for a public-private partnership to address the growing gap in cyber insurance coverage, with the White House developing a plan to address the issue.

Key Points

- Marsh McLennan and Zurich Insurance Group have called for government intervention to manage the increasing risk of catastrophic cyber events and to bridge a multibillion-dollar gap in the current cyber insurance market.
- The cyber insurance market has grown significantly and is projected to exceed $28 billion in gross written premiums by 2027, more than doubling the amount written in 2023, according to the firms' white paper.
- Despite this growth, there remains a protection gap of approximately $900 billion between insured and economic losses due to cyberattacks. Many small and medium-sized businesses are underinsured or lack coverage entirely.

Industry Concerns

The white paper highlights growing concerns about catastrophic cyber risks, particularly after the widespread outage in July caused by a faulty CrowdStrike software update, which affected 8.5 million Microsoft Windows devices. The estimated direct losses for Fortune 500 companies from this incident reached $5.4 billion, with insured losses expected to total $1 billion.

Concerns about large-scale cyber incidents have been prominent since the NotPetya attacks in 2017. Greg Eskins, head of the Global Cyber Insurance Center at Marsh Specialty, noted that systemic or "connected risks" have been a concern for regulators, underwriters, brokers, and multinational companies for years.

The industry is pushing for incentives to enhance resilience and better support small and mid-sized businesses that lack sufficient coverage. In 2022, Marsh McLennan urged the U.S. Treasury Department's Federal Insurance Office (FIO) to examine catastrophic insurance risk as a critical issue.

Government Efforts

Governments and industries around the world are closely monitoring the effects of cyberattacks on major sectors and national economies. In early 2024, the U.S. Treasury's Federal Insurance Office partnered with the National Science Foundation to study the impact of terrorism and catastrophic cyber events on the global insurance market.

A spokesperson from the Treasury Department confirmed that the FIO is working with the National Cyber Director and the Cybersecurity and Infrastructure Security Agency (CISA) to address catastrophic cyber risks, though further details have not yet been disclosed.

The White House also confirmed its involvement, noting that it is working on plans to address these challenges as part of the National Cybersecurity Strategy. According to a spokesperson for the Office of the National Cyber Director, the government is developing a policy proposal to strengthen the cyber insurance market, particularly in managing catastrophic risks, in collaboration with the Treasury's Federal Insurance Office and CISA.

Google Cloud Platform RCE Flaw Let Attackers Execute Code on Millions of Google Servers

This week, security researchers disclosed a critical remote code execution (RCE) vulnerability in Google Cloud Platform (GCP) that could have allowed attackers to execute malicious code on millions of Google servers. The vulnerability, named "CloudImposer" by Tenable Research, has since been patched by Google.

The issue was found in GCP's Cloud Composer service, a managed workflow orchestration tool built on Apache Airflow. It originated from a risky package installation process that left the service vulnerable to dependency confusion attacks.

Tenable researchers discovered that Google used the "–extra-index-url" argument when installing private Python packages in Cloud Composer. This argument tells the package manager to check both private and public repositories, potentially allowing attackers to inject malicious packages from public sources.

"CloudImposer could have enabled attackers to launch a large-scale supply chain attack by compromising GCP's Cloud Composer service, which is responsible for orchestrating software pipelines," said Liv Matan, a security researcher at Tenable.

The vulnerability affected several GCP services, including App Engine, Cloud Functions, and Cloud Composer. Exploiting it could have allowed attackers to upload malicious packages to the public PyPI repository, which would then be installed on Cloud Composer instances with elevated permissions. This would have given attackers the ability to execute arbitrary code, steal service account credentials, and potentially move laterally within GCP's services.

Due to the widespread nature of the vulnerability, a single compromised package could have impacted millions of servers across Google's infrastructure and customer environments.

Tenable noted, "Supply chain attacks in the cloud are far more damaging than on-premises. A single malicious package in a cloud service could affect millions of users."

Google has since resolved the vulnerability by ensuring that the affected Python package is installed only from a private repository. Additionally,

Organizations using GCP services are urged to review their package installation processes and implement safeguards,

they implemented extra security measures like checksum verification to ensure package integrity.

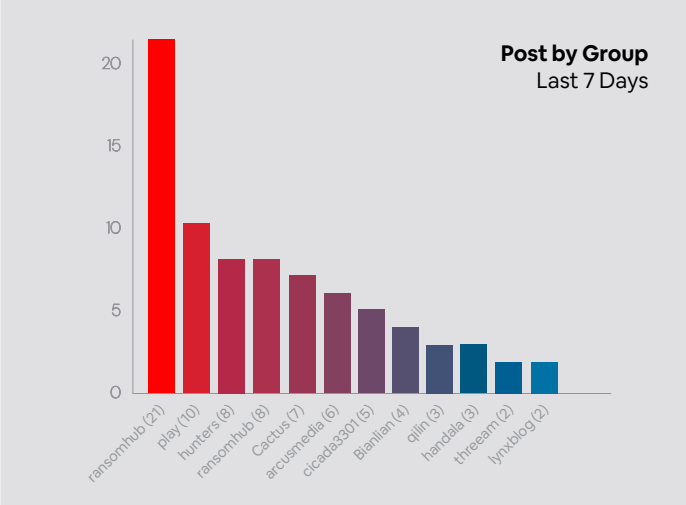
In response to Tenable's findings, Google updated its documentation, recommending the use of the safer "–index-url" argument instead of "–extra-index-url" for package installations. Google also advises customers to manage multiple package sources through GCP's Artifact Registry virtual repository.

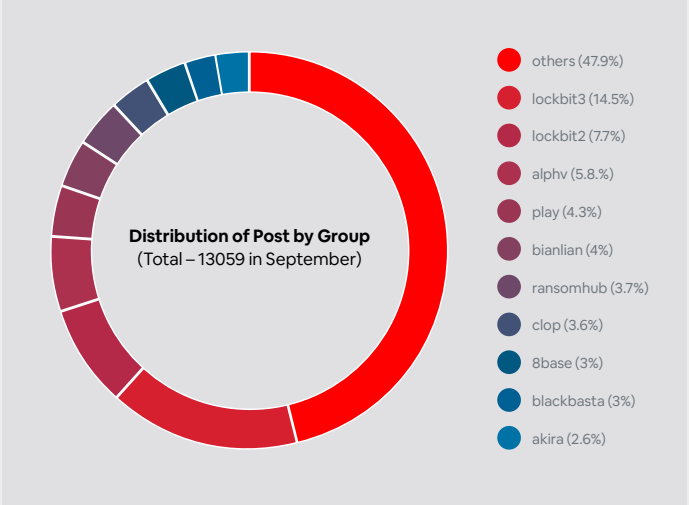
This discovery highlights the ongoing challenges of securing cloud environments and software supply chains. It emphasizes the importance for both cloud providers and customers to adopt strong security practices around package management and dependency resolution.

Organizations using GCP services are urged to review their package installation processes and implement safeguards, such as version pinning, checksums, and private repositories, to prevent dependency confusion attacks.

The CloudImposer vulnerability underscores the complexity of modern cloud environments and the potential for seemingly minor misconfigurations to have significant security impacts. As cloud adoption grows, addressing supply chain risks like these will remain a top priority for the industry.

Ransomware Tracker





Articles

Earth Baku Expands Operations: Targeting Europe, Middle East, and Africa with Sophisticated Cyber Espionage Tactics

Executive Summary

Earth Baku, a threat actor associated with APT41, has expanded its operations from the Indo-Pacific region to Europe, the Middle East, and Africa (EMEA). The group targets critical sectors in these regions using advanced malware and sophisticated post-exploitation techniques. This article provides a detailed analysis of their updated tools, tactics, and procedures (TTPs) and offers recommendations for defending against this evolving threat.

Detection

Geographic Expansion

Earth Baku's activities have been detected beyond the Indo-Pacific, now impacting regions in Europe, the Middle East, and Africa, including Italy, Germany, UAE, and Qatar. There are also signs of threat activities in Georgia and Romania.

Figure 1. Map chart for Earth Baku's scope of potential impact

Targeted Sectors

- Government
- Media and Communications
- Telecom
- Technology
- Healthcare
- Education

Indicator of Compromise (IOCs)

- Unusual activity on public-facing IIS servers
- Deployment of the Godzilla web shell
- Presence of advanced loaders such as StealthVector and StealthReacher
- Detection of reverse tunneling tools like iox, Rakshasa, and Tailscale
- Use of MEGAcmd for data exfiltration
- IOCs from Earth Baku's latest campaign

[SHA256]	[Detection name]
7e63c6b9ab3b32beffbc1eb23d6ca7cc59616b0722f0dd4f0d893c0a1724f5d7	Trojan.Win64.STEALTHVECTOR.ZYLH
8405d742405d3a6d3bda6bc49630dd5f3604a3d6ae27cbd533e425f8abbaafdc	Trojan.Win64.STEALTHVECTOR.ZYLH
a50f85c71b69563ba42bf04c937e1063244ca4957231d3adac76f1c96ab42d3c	Trojan.Win64.STEALTHVECTOR.ZYLH
ab56501167fe689fe55f6e6ddc3bb91952299bd5c3ef004b02bf1c3b4061c7cf	Trojan.Win64.STEALTHVECTOR.ZALG
ec10a9396dca694fe64366e0dab82d046cf92457f97efd50a68ceb85adef6b74	Trojan.Win64.STEALTHVECTOR.E
73eaba82ef1c502448e533007e92b1afa879b09f85f28b71648668ea62839ff5	Trojan.Win64.STEALTHVECTOR.ZYLH
0faddbe1713455e3fc9777ec45adf07b28e24f4c3ddca37586c2aa6b539898c0	Trojan.Win64.STEALTHVECTOR.ZYLH
1c88150ec85a07c3db5f18c5eedcb0b653467b897af01d690ed996e5e07ba8e3	Trojan.Win64.STEALTHVECTOR.ZYLH
3e52c310c6556367ff9e18448bc41719e603d1cbbdafdcba736c6565529617b6	Trojan.Win64.STEALTHVECTOR.ZYLH
07aa971f0791b06dd442d4c7a49c1d3d27a1cbb16602f731e870b5ef50edf69e	Trojan.Win64.STEALTHVECTOR.ZYLH
166b6dcdac31f4bf51e4b20a7c3f7d4f7017ca0c30fa123d5591e25c3fa66107	Trojan.Win64.STEALTHVECTOR.ZBLG
21fc0f50d545c0a373380934dc61c423c8a31d8c3e6eae4f8a35149ad9962d88	Trojan.Win64.STEALTHVECTOR.E
7586e58a569c2a07d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565a	Trojan.Win64.STEALTHREACHER.ZYLH
22a50cea6ad67a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86	Trojan.Win64.STEALTHREACHER.ZYLH
c6a3a1ea84251aed908702a1f2a565496d583239c5f467f5dcd0cfc5bfb1a6db	Trojan.Win64.STEALTHREACHER.ZBLH
073b35ecbd1833575fbfb1307654fc532fd938482e09426cfb0541ad87a04f75	Trojan.Win64.STEALTHREACHER.ZYLH
7463700ec5768d4af6549028465f978059611555aa8e22e2b7c664b1cdbfa9ae	Trojan.Win64.STEALTHVECTOR.ZYLH
cdcbd9c25e06ac6da5497fa19459d0007449ec1a3e6bc591334db6fb3598aecb	Trojan.Win64.STEALTHVECTOR.ZYLH
7f24bc080281d250ec88493e5803e488721a17c9382cd54ba8dfbcb785f23a88	Trojan.Win64.STEALTHVECTOR.ZYLH
e4360c0aa995e6e896b22bb7725a6c9b189be8606e7cbbc8b6e80c606358649d	Backdoor.Win64.COBEACON.ZYLH
83de8917bf0ac1d670acf27431015215db872b7291979312dd65e30d99806abb	Backdoor.Win64.COBEACON.ZALH
ec5a96f42aeccdf9a3ae4c3650689606c8539fd65c0b47f30887afecb901be43	Backdoor.Win64.COBEACON.ZYLH
c02accc26a389397fb172f83258baa8a974986ffd706ba708a3b0a679f61be56	Backdoor.Win64.SNEAKCROSS.ZBLG
e5f1360d4c299bb32e33e081115f2b520251a983af2ebc649b4b9b70308246fe	Backdoor.Win64.COBEACON.ZBLF.enc

[Type]	[URL/IP address]
Domain	www[.]mircoupdate[.]https443[.]net
Domain	icy-bar-c375.microsoft-updates.workers[.]dev
Domain	www.sitennews[.]com
Domain	update-chrome.realgodad.workers[.]dev
Domain	track.cdn78544[.]ru
Domain	www.cdn7854.workers[.]dev
Domain	shrill-tooth-b557.vgfjuic.workers[.]dev
IP address	5.182.207[.]28
IP address	78.108.216[.]20
IP address	212.87.212[.]115

Prevention

Entry Points

- Earth Baku exploits vulnerabilities in public-facing applications, particularly IIS servers, to gain initial access.
- Organizations should prioritize securing these entry points by applying the latest patches and hardening configurations.

Figure 2. The infection vector of recent campaigns

Security Measures

- **Principle of Least Privilege:** Restrict access to critical systems and data to reduce the risk of lateral movement by attackers.
- **Patch Management:** Regularly update systems to address vulnerabilities and consider virtual patching for unsupported systems.
- **Network Monitoring:** Implement continuous monitoring to detect unusual activity, especially on critical public-facing applications.
- **Incident Response Plans:** Develop and regularly test incident response plans to quickly address any breaches.

Remediation

Post-Exploitation Tools

After gaining access, Earth Baku uses tools like StealthVector, StealthReacher, and SneakCross to maintain persistence and exfiltrate data.

Persistence Mechanisms

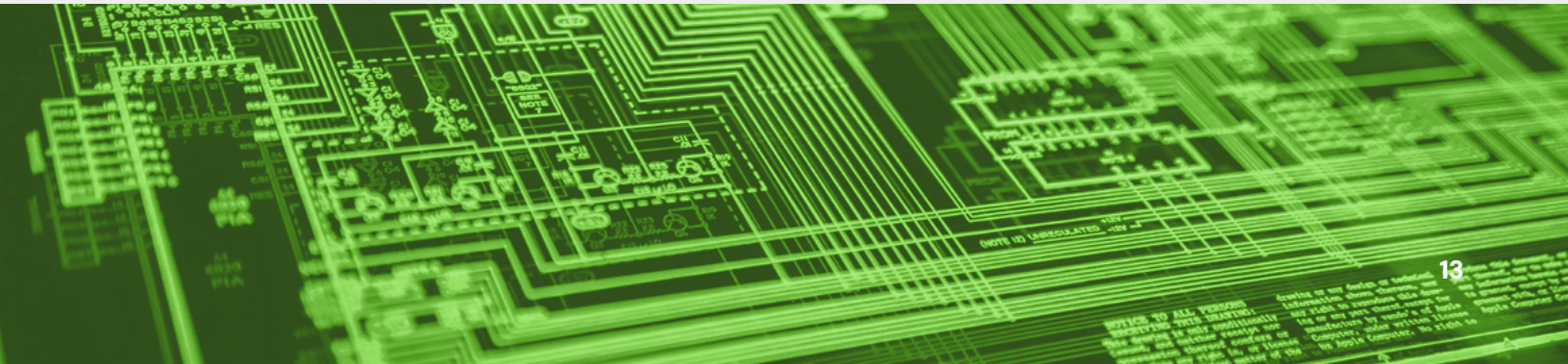
Reverse tunnels via a customized iox tool, Rakshasa, and Tailscale to maintain control over compromised systems.

Exfiltration Techniques

MEGAcmd tool is deployed for data exfiltration to MEGA cloud storage.

Recommended Actions:

- **Forensic Analysis:** Conduct a thorough forensic analysis to identify and remove all malicious tools and backdoors.
- **Reverse Engineering:** Analyze the loaders and backdoors like StealthVector and SneakCross to develop detection signatures.
- **Data Recovery:** Ensure that data backups are intact and restore affected systems from clean backups if necessary.
- **Security Audits:** Perform comprehensive security audits to identify any remaining vulnerabilities or backdoors.



BlackByte Ransomware Group: Evolving Tactics and New Exploits Targeting VMware ESXi and Beyond

Executive Summary

The BlackByte ransomware group, a known offshoot of the Conti ransomware gang, continues to refine its tactics, techniques, and procedures (TTPs). Recent investigations by Security Researchers reveal that BlackByte is leveraging new vulnerabilities, such as CVE-2024-37085 in VMware ESXi, alongside their established use of vulnerable drivers to bypass security protections. This report details BlackByte's latest activities, their new self-propagating ransomware encryptor, and actionable recommendations for defending against these advanced threats.

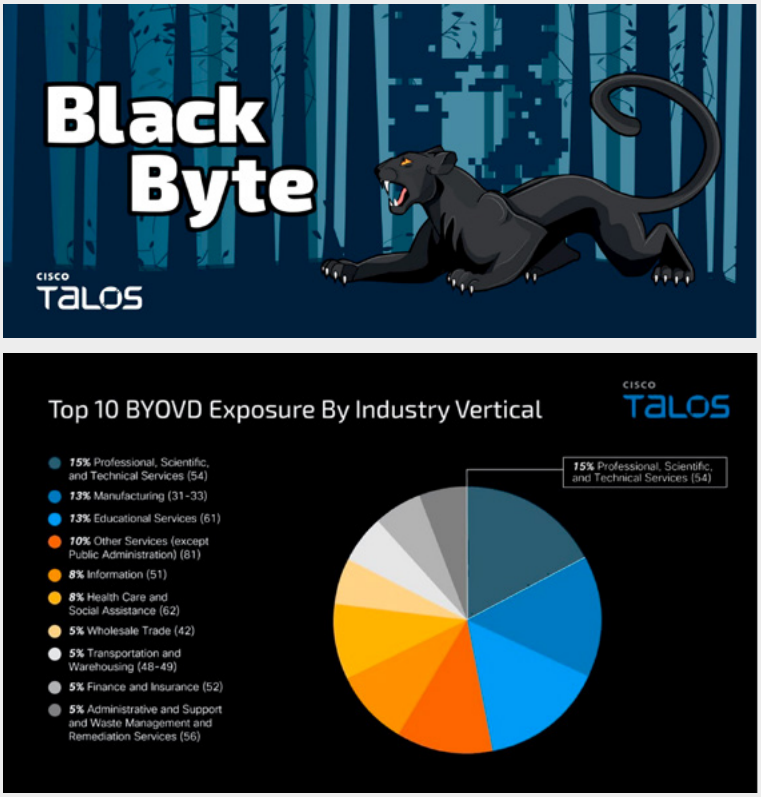


Figure 1: Top 10 BYOVD exposure by industry vertical

Detection

Initial Access

- BlackByte's initial access gained using valid credentials through VPN, possibly obtained via brute-force attacks.
- Use of a victim's authorized remote access mechanism rather than deploying commercial tools like AnyDesk.
- Exploitation of public-facing vulnerabilities, including the new CVE-2024-37085 in VMware ESXi.

Reconnaissance and Enumeration

- Compromising Domain Admin accounts and joining VMware ESXi hosts to the Active Directory domain.
- Use of NTLM for authentication and lateral movement, often indicating pass-the-hash attacks.
- Execution of suspicious files (e.g., "atieclxx.exe") from non-standard directories to disguise malware.
- Tampering with security tools, uninstalling EDR, and modifying system configurations.

Indicators of Compromise (IOCs)

- File extension “blackbytent_h” appended to encrypted files.
- Deployment of four vulnerable drivers (e.g., RtCore64.sys, DBUtil_2_3.sys) for BYOVD (Bring Your Own Vulnerable Driver) attacks.
- High volumes of NTLM authentication and SMB connections just before file encryption.

RtCore64.sys – 01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd
DBUtil_2_3.sys – 0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5
zamguard64.sys – 543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91
gdrv.sys – 31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427

Prevention

Entry Points

- Secure VPN access with multi-factor authentication (MFA) and strong password policies.
- Regularly audit and patch public-facing applications and services, especially VMware ESXi hosts.
- Monitor for unusual activity in privileged groups and unexpected configuration changes.

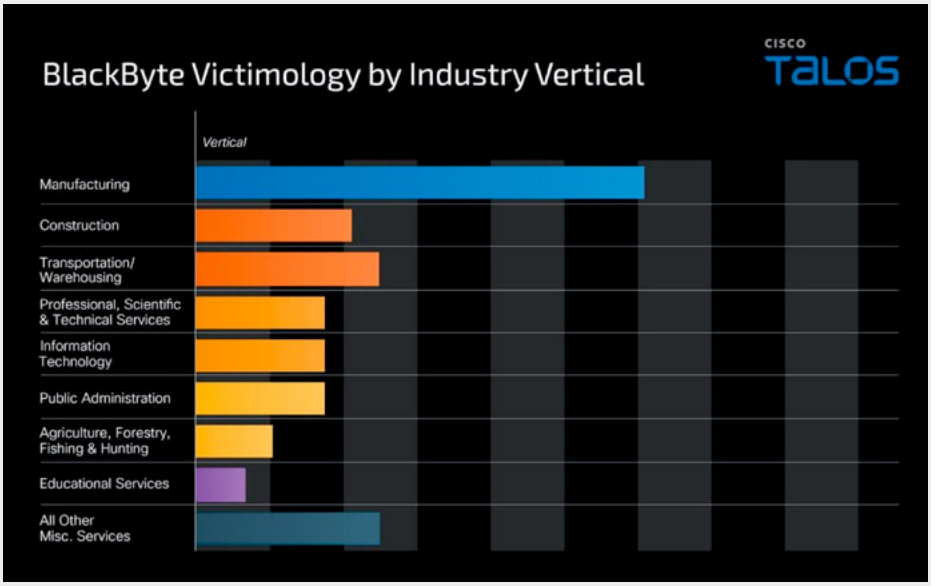


Figure 2: BlackByte victimology by industry vertical

Security Measures

- **Multi-Factor Authentication (MFA):** Implement MFA for all remote access and cloud connections, prioritizing secure methods like verified push notifications.
- **VPN Configuration Audit:** Ensure legacy VPN policies are removed, restrict VPN access to essential segments, and deny non-compliant authentication attempts.
- **NTLM and SMB Hardening:** Limit or disable NTLM, enforce Kerberos, disable SMBv1, and implement SMB signing and encryption.

Monitoring and Detection

- Deploy and protect EDR clients across the environment, ensuring administrator-level protections are in place to prevent tampering.
- Set up alerts for unauthorized configuration changes, including modifications to Windows Defender policies and Group Policy Objects.

Remediation

Containment

- Conduct an enterprise-wide password reset to invalidate compromised credentials, including rolling critical Kerberos tickets.
- Isolate affected systems and remove vulnerable drivers and malware binaries from the environment.

Post-Exploitation Tools

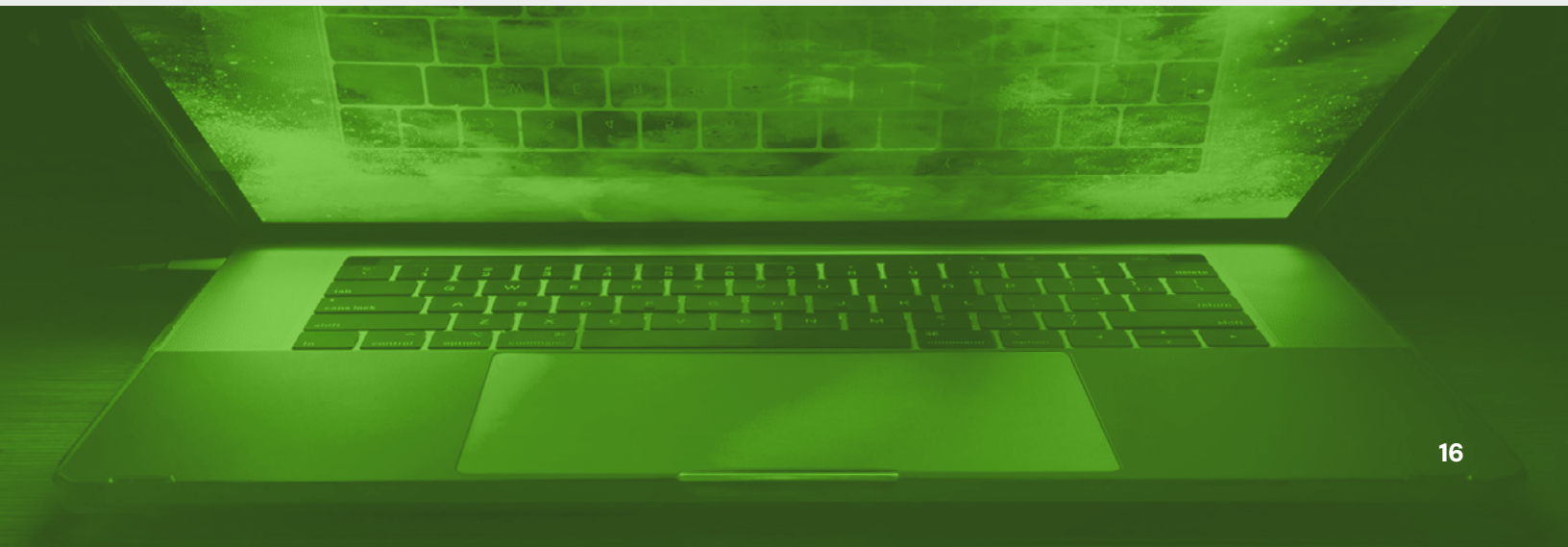
- BlackByte employs the use of its custom data exfiltration tool, ExByte, which may be disguised as legitimate files (e.g., "atieclxx.exe").
- The ransomware binary operates from non-standard directories and attempts to delete itself post-execution to evade detection.

Recovery

- **Incident Response:** Engage in thorough forensic analysis to identify all compromised accounts and systems.
- **Patch Management:** Ensure that all systems, especially critical VMware ESXi hosts, are fully patched against known vulnerabilities.
- **User Education:** Train users on the importance of strong passwords and the risks associated with phishing and brute-force attacks.

Implications for Defenders

BlackByte's evolving tactics, such as the shift from using commercial remote administration tools to exploiting newly disclosed vulnerabilities, highlight the group's adaptability. The increased complexity of their ransomware, including its self-propagating capabilities and use of advanced programming languages, poses significant challenges for defenders. Organizations must stay ahead by implementing robust security controls, conducting regular audits, and preparing for rapid incident response to contain and mitigate the impact of such attacks.



In-Depth Analysis of Bling Libra's AWS Compromise Tactics Using S3 Browser and WinSCP

Executive Summary

In a recent incident response engagement by Unit 42, the threat actor group Bling Libra, known for their ShinyHunters ransomware, has shifted from their traditional data sale model to extortion. This report examines their tactics, particularly focusing on how they leveraged compromised credentials to access and manipulate AWS environments. The attack demonstrates how Bling Libra uses tools like S3 Browser and WinSCP for reconnaissance and data manipulation, emphasizing the importance of robust cloud security practices.

Detection

- **Initial Access:** Bling Libra obtained AWS credentials from a sensitive file exposed online. The credentials, though limited to S3 actions, allowed access to various bucket configurations and data.
- **Discovery:** The threat actors used API calls to explore AWS S3 resources. Key API calls included `ListBuckets`, `GetBucketLocation`, and `GetBucketObjectLockConfiguration`. Activities were logged by AWS CloudTrail, which tracked the interactions and access attempts.
- **Data Access and Impact:** After gaining access, the attackers waited to delete selected S3 buckets. The absence of detailed logging made it challenging to trace the exact data exfiltrated. They also created new S3 buckets as a mockery of the organization's defenses.

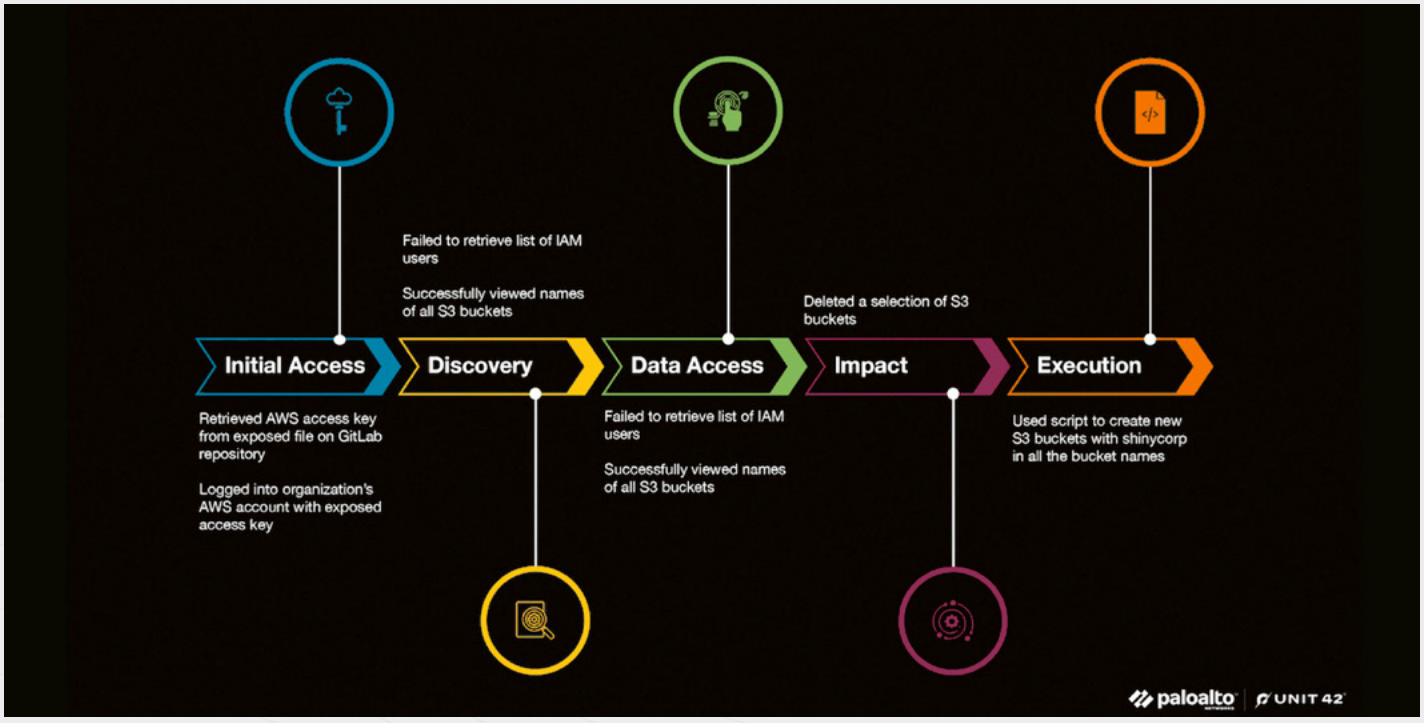


Figure 1. The MITRE timeline details the attack path taken by the threat actor.

Indicators of Compromise (IOCs)

Threat actor email address
shinycorp@tutonota[.]com

User Agents (X stands for varying version numbers)
S3 Browser/X.X.X (https://s3browser.com)
WinSCP/X.X.X neon/X.X.X
aws-cli/X.X.X Python/X.X.X Linux/X.X.X-aws botocore/X.X.X
aws-cli/X.X.X md/Botocore#X.X.X ua/X.X os/linux#X.X.X-aws md/arch#x86_64 lang/python#X.X.X md/pyimpl#CPython cfg/retry-mode#legacy botocore/X.X.X
aws-cli/X.X.X md/Botocore#X.X.X md/awscrt#X.X.X ua/2.0 os/linux#X.X.X md/arch#x86_64 lang/python#X.X.X md/pyimpl#CPython cfg/retry-mode#legacy botocore/X.X.X

Prevention

- **Credential Management:** Ensure that AWS credentials follow the principle of least privilege to limit the potential impact of a breach. Regularly review and update permissions.
- **Logging and Monitoring:** Enable detailed logging for all AWS S3 activities, including data events, using CloudTrail. Implement AWS GuardDuty and AWS Security Hub for real-time threat detection and analysis.
- **Access Controls:** Use IAM Access Analyzer to evaluate and manage access risks. Implement AWS Service Control Policies and permission boundaries to enforce strict access controls within AWS Organizations.

Remediation

- **Incident Response:** If compromised, promptly review CloudTrail logs to identify unauthorized access and actions. Use IAM Access Analyzer to audit permissions and adjust them as needed.
- **Security Enhancements:** Apply MFA to critical actions like deleting buckets. Consider replicating important data across regions or accounts to enhance availability and resilience.
- **Ongoing Monitoring:** Continuously audit access controls, encryption settings, and network configurations. Leverage AWS Config for compliance and AWS Security Hub for a comprehensive security posture assessment.

S3 Browser and WinSCP Analysis

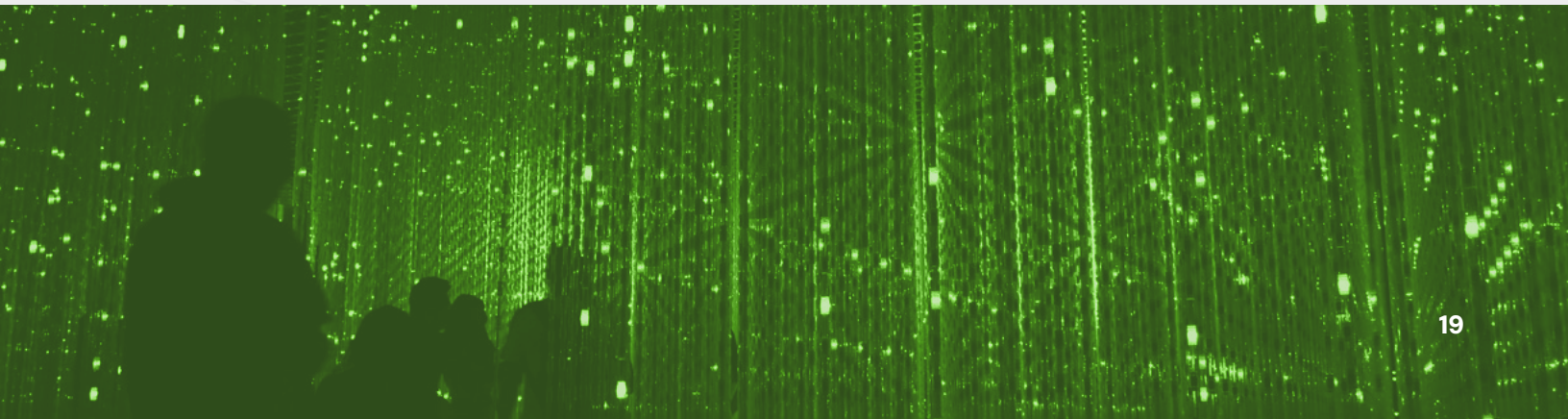
- **S3 Browser:** Generates numerous API calls based on user interactions. Key calls include `ListBuckets`, `ListObjects`, `GetBucketLocation`, `HeadObject`, and others related to object management and permissions.
- **WinSCP:** Although versatile for file transfers, it generates fewer API calls compared to S3 Browser. Significant calls include `ListBuckets`, `GetObjectAcl`, and object manipulation calls.

EVENTTIME	EVENTSOURCE	EVENTNAME	USERAGENT	RESOURCES
May 12th 2024 08:20:38	s3.amazonaws.com	ListBuckets	[S3 Browser/11.6.7 (https://s3browser.com)]	
May 12th 2024 08:20:38	cloudfront.amazonaws.com	ListDistributions	S3 Browser/11.6.7 (https://s3browser.com)	
May 12th 2024 08:20:38	s3.amazonaws.com	GetBucketLocation	[S3 Browser/11.6.7 (https://s3browser.com)]	[{"ARN": "arn:aws:s3:::aa-test-1111", "accountId": "[redacted]", "type": "AWS::S3::Bucket"}] Show more
May 12th 2024 08:20:22	s3.amazonaws.com	GetBucketObjectLockConfiguration	[S3 Browser/11.6.7 (https://s3browser.com)]	[{"ARN": "arn:aws:s3:::aa-test-1111", "accountId": "[redacted]", "type": "AWS::S3::Bucket"}] Show more

Figure 2. API calls for first connection to S3 service using S3 Browser.

Conclusion

The Bling Libra attack underscores the necessity of implementing stringent cloud security measures. Proper credential management, comprehensive logging, and continuous monitoring are crucial in safeguarding AWS environments from similar threats. By understanding and anticipating threat actor tactics, organizations can better prepare and defend against potential cloud-based attacks.



Operation DevilTiger: Unmasking the APT-Q-12 Cyber Espionage Campaign and its Advanced Techniques

Executive Summary

The QiAnXin Threat Intelligence Center has disclosed details of a sophisticated cyber espionage campaign dubbed "Operation DevilTiger," led by the APT-Q-12 group, also known as "Pseudo Hunter." This group, rooted in Northeast Asia, has been actively targeting entities across China, North Korea, Japan, South Korea, and other East Asian countries. The campaign uses zero-day vulnerabilities and advanced techniques to infiltrate high-value targets, indicating deep ties to the infamous Darkhotel group first documented in 2017. APT-Q-12's attacks are part of a broader geopolitical strategy, focusing on intelligence related to semiconductor competition and regional political dynamics.

Operation DevilTiger and APT-Q-12

APT-Q-12, also referred to as Pseudo Hunter, has been traced back to the Darkhotel group. Over the years, APT-Q-12 and other subsets, such as APT-Q-11 (ShadowTiger) and APT-Q-14 (ClickOnce), have evolved their methods, becoming a formidable force in cyber espionage. These groups share infrastructure and overlapping techniques, signaling a common origin from Darkhotel's earlier operations.

Key Tactics Used

- **Zero-Day Vulnerabilities:** APT-Q-12 exploits undisclosed vulnerabilities in widely used email clients and office software.
- **Probes and Exploits:** The group uses complex probes to detect vulnerabilities, tailoring their zero-day attacks based on specific software platforms.
- **Command and Control (C2) Techniques:** APT-Q-12 embeds C2 probe links in legitimate-looking emails to gather intelligence on the victim's environment, facilitating precise attacks.
- **Plugins for Data Exfiltration:** The group employs browser steganography and keylogger plugins to steal sensitive information, encrypting the data before exfiltration.

Indicators of Compromise (IOCs)

IPv4 Port Combinations
82.118.27.129:80

Domains
web-oauth.com

URLs
https://bitbucket.org/noelvisor/burdennetted/downloads/
https://bitbucket.org/noelvisor/burdennetted/downloads/OAQDDI32.bmp

MD5 Hashes
59cd91c8ee6b9519c0da27d37a8a1b31
71094ef9f2cf685e6c7d11fe310e5efb

Detection

- **Email Probes:** Malicious probe emails that imitate advertisements or subscription messages to gather information about victims' software usage.
- **C2 Probes:** Embedded links that assess whether the target uses specific email clients and office products, such as Foxmail or Microsoft Word.
- **Plugins:** Steganography and keylogger plugins deployed post-exploitation to gather data stealthily.

Prevention

- **Zero-Day Patching:** Ensure timely patching of software vulnerabilities by implementing automatic updates wherever possible.
- **Email Security Solutions:** Use advanced email filtering techniques to detect suspicious probes disguised as legitimate emails.
- **Endpoint Detection and Response (EDR):** Deploy robust EDR solutions that can detect and block malicious activities at the endpoint level.

Remediation

- **Incident Response:** Establish a strong incident response plan to address and mitigate the damage caused by APT-Q-12 intrusions.
- **Forensic Analysis:** Perform forensic analysis to detect the presence of steganography and keylogging plugins in compromised systems.
- **Threat Intelligence Sharing:** Collaborate with threat intelligence providers to stay updated on evolving tactics used by APT-Q-12 and similar APT groups.

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
Windows Telephony Server Elevation of Privilege Vulnerability CVE-2024-26230	Vulnerability allows attackers to gain SYSTEM privileges on affected systems through a use-after-free vulnerability in the telephony service. The Windows Telephony Service is an RPC-based service that, while not running by default, can be activated by invoking the StartServiceW API with standard user privileges. The vulnerability arises in the way this service handles objects with the magic value "GOLD," a unique identifier used within the service's global handle table.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26230
Kibana arbitrary code execution Vulnerability CVE-2024-37288	Vulnerability allows Attackers to exploit this flaw by crafting malicious YAML payloads, leading to remote code execution. Users who have configured an Amazon Bedrock connector within Elastic Security's built-in AI tools are particularly vulnerable	https://discuss.elastic.co/t/kibana-8-15-1-security-update-esa-2024-27-esa-2024-28/366119
HAProxy 2.9.x before 2.9.10, 3.0.x before 3.0.4, and 3.1.x denial of service Vulnerability CVE-2024-45506	Under certain conditions, it can cause an endless loop, leading to a system crash and a remote denial-of-service (DoS) attack. This flaw impacts several HAProxy products, including Enterprise, ALOHA, and Kubernetes Ingress Controllers.	HAProxy Vulnerability CVE-2024-45506 Under Active Exploit: Urgent Patching Required (securityonline.info)
Gunicorn versions prior to 22.0 authentication bypass vulnerability CVE-2024-7923	It allows unauthorized users to gain administrative access, potentially leading to a complete system compromise. The vulnerability emerges when Pulpcore (version 3.0+) is deployed with Gunicorn versions prior to 22.0. The issue lies in how Apache's mod_proxy handles HTTP headers, specifically related to the restrictions on underscores in headers. Apache mod_proxy fails to correctly unset or filter out malformed HTTP headers, leaving room for attackers to inject malicious headers that trick the system into granting unauthorized access.	Red Hat Issues Critical Patch for Pulpcore Authentication Bypass Flaw (CVE-2024-7923) (securityonline.info)
Veeam Backup and Replication 12.x < 12.2.0.334 Multiple Vulnerabilities (September 2024) (KB4649) CVE-2024-40711	Vulnerability allows unauthenticated attackers to execute code remotely, granting them full control over the affected system. These vulnerabilities impact various aspects of Veeam Backup & Replication.	Veeam Backup & Replication Faces RCE Flaw– CVE-2024-40711 (CVSS 9.8) Allows Full System Takeover (securityonline.info)
VMware vCenter Server updates address heap-overflow and privilege escalation vulnerability CVE-2024-38812, CVE-2024-38813	Vulnerability allows a malicious actor with network access to vCenter Server to trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution," the virtualization services provider saidin a bulletin	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968
Ivanti Cloud Services Appliance OS Command Injection Vulnerability CVE-2024-8190	Vulnerability allows a remote authenticated attacker to obtain remote code execution," Ivanti noted in an advisory released earlier this week. "The attacker must have admin level privileges to exploit this vulnerability."	https://thehackernews.com/2024/09/ivanti-warns-of-active-exploitation-of.html
Azure Stack Hub Elevation of Privilege Vulnerability CVE-2024-38220	Vulnerability allows the attacker to gain the ability to interact with other tenant's applications and content. An attacker who successfully exploited this vulnerability could gain unauthorized access to system resources, potentially allowing them to perform actions with the same privileges as the compromised process. This would lead to further system compromise and unauthorized actions within the network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38220
Adobe ColdFusion < 2021.x < 2021u16 / 2023.x < 2023u10 Vulnerability (APSB24-71) CVE-2024-41874	Vulnerability allows attacker to exploit it by providing crafted input to the application, which when deserialized, leads to execution of malicious code. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/coldfusion/apsb24-71.html
Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability CVE-2024-38225	It allows attackers to edit the local configuration file to contain malicious code, then send the request to the server to exploit this vulnerability after that attacker would gain administrator privileges	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38225
SonicWall SonicOS Improper Access Control Vulnerability CVE-2024-40766	Vulnerability allows to gain unauthorized access to sensitive information or even execute arbitrary code on the affected device. In certain scenarios, the vulnerability could also cause the firewall to crash, disrupting network connectivity and leaving organizations vulnerable to further attacks.	https://securityonline.info/sonicwall-issues-urgent-patch-for-critical-firewall-vulnerability-cve-2024-40766/?&web_view=true

Security Bulletin

Online Stores Hacked in New Campaign: Whenever you shop online and enter your payment details, you could be at risk of being a victim of fraud. Digital skimmers are snippets of code injected into online stores that can steal your credit card number, expiration date and CVV/CVC as you type it in, as per the research by Malwarebytes. Each online store is injected with one seemingly harmless line of code, a simple script tag loading content from a remote website. Interestingly, across different hacked websites we noticed the same naming pattern: {domain}.{shop|online)/img/. This loader contains a simple function that will retrieve information from the site it is being called from. Digital skimmers are often impossible to recognize due to how they blend into a website. Unless you are inspecting network traffic or debugging the checkout page with Developer Tools, you simply can't be sure that a store has not been compromised.

New RAMBO Attack Steals Data Using RAM in Air-Gapped Computers: A novel side-channel attack dubbed "RAMBO" (Radiation of Air-gapped Memory Bus for Offense) generates electromagnetic radiation from a device's RAM to send data from air-gapped computers. Air-gapped systems, typically used in mission-critical environments with exceptionally high-security requirements, such as governments, weapon systems, and nuclear power stations, are isolated from the public internet and other networks to prevent malware infections and data theft.

Rising Cost of Insecure APIs and Bot Attacks: Annual financial losses between $94 billion to $186 billion define the increased adoption of Insecure API combined with AI-powered BOT Attacks. Larger companies manage hundreds of API endpoints in production and the endpoints in their complex API ecosystems each represent a potential entry point for an attacker.

Reference Links

1. https://www.helpnetsecurity.com/2024/09/06/organizations-experienced-ransomware-attack/?web_view=true
2. https://www.helpnetsecurity.com/2024/08/30/cyber-threat-intelligence-report-key-threats/?web_view=true
3. https://www.helpnetsecurity.com/2024/08/30/forescout-2024h1-threat-review/?web_view=true
4. https://www.cybersecuritydive.com/news/cyber-insurance-government-900b/726305/?&web_view=true
5. https://cybersecuritynews.com/gcp-rce-flaw/#google_vignette
6. https://unit42.paloaltonetworks.com/shinyhunters-ransomware-extortion/
7. https://1275-ru.translate.goog/ioc/3902/pseudo-hunter-apt-q-12-apt-iocs/?_x_tr_sl=ru&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc
8. https://securityonline.info/operation-deviltiger-apt-q-12s-shadowy-tactics-and-zero-day-exploits-unveiled/?&web_view=true
9. https://ransomwatch.telemetry.ltd/#/stats
10. https://www.trendmicro.com/en_us/research/24/h/earth-baku-latest-campaign.html?&web_view=true
11. https://blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/?&web_view=true
12. https://foresiet.com/blog/the-rising-cost-of-insecure-apis-and-bot-attacks-global-firms-face-186-billion-in-losses

About SDG

SDG is a global cybersecurity, identity governance, GRC, risk consulting and advisory firm. SDG's SaaS platform TruOps in combination with its services deliver a comprehensive range of identity, cybersecurity, risk, compliance, and cloud security solutions that enable organizations to identify and mitigate cyber risk, protect cyber assets, and manage their business securely.

To learn how SDG can help ensure the security and compliance of your technology and data infrastructure visit **www.sdgc.com** and **www.truops.com**.

SDG

- 75 North Water Street, Norwalk, CT 06854
- 203.866.8886
- sdgc.com