CONVERGE
TECHNOLOGY SOLUTIONS

THREAT INTEL REPORT 2025

Prepared by: Converge Cybersecurity Practice
convergetp.com/cybersecurity | 800.747.8585

April

Observations for April 2025

In 2025, organizations are facing a mounting security challenge driven by the unchecked spread of secrets across code repositories, containers, and collaboration platforms. A **5% year-over-year increase in exposed credentials–totaling over 23 million**–underscores a breakdown in secrets hygiene and access governance. Developers continue to hardcode credentials in Docker layers and leak sensitive tokens through platforms like Slack and Jira, often bypassing protective tools due to misconfiguration, token overprivileging, and poor rotation practices. These exposures, particularly from non-human identities (NHIs), create persistent vulnerabilities that are difficult to monitor and control, significantly expanding the enterprise attack surface.

Compounding the issue is the rapid integration of generative AI tools such as GitHub Copilot and low-code platforms. While these technologies boost productivity, they have also contributed to a **40% increase in secret leakage incidents**. Many AI-generated repositories–despite using secrets managers–still leak credentials due to human oversight and lax enforcement. This confluence of AI-driven development, decentralized collaboration, and fragmented secrets management leaves organizations increasingly exposed to unauthorized access, lateral movement, and long-term compromise.

Meanwhile, threat actors tied to the Democratic People's Republic of Korea (DPRK) are actively exploiting remote work trends to gain insider-level access to Western organizations. By posing as freelance IT professionals, DPRK operatives are bypassing identity verification systems and embedding themselves within sensitive environments without using malware or zero-day exploits. These workers have been involved in extortion, proprietary data theft, and operational support for sanctioned regimes, all while operating under legitimate credentials and within unmanaged device scenarios. The breadth of their infiltration–particularly across finance, tech, and defense sectors–has escalated the insider threat landscape from an HR issue to a matter of national security.

Adding to the threat landscape, the China-linked group Earth Alux is expanding its global reach with highly modular malware campaigns. Using tools like VARGEIT and RAILSETTER, the group deploys stealthy, multi-stage operations that combine DLL sideloading, fileless execution, and abuse of legitimate APIs like Microsoft Graph for covert communications. Initially active in APAC, Earth Alux has extended its campaigns into Latin America, targeting key sectors such as government, telecommunications, and logistics. Their ability to operate undetected over long durations, pivoting through benign processes and exploiting cloud infrastructure, positions them as a significant threat to both regional stability and multinational organizations.

RETURN

Executive Overview

Audience
- C-Suite Executives
- CISO
- IT Managers
- Risk Management Professionals
- Cybersecurity Professionals and Analysts
- Developers
- Project Managers
- Business Organizations

AI ADOPTION AND SECRET SPRAWL - GROWING ORGANIZATIONAL RISK FROM GPT USAGE

In 2025, secrets sprawl has become a critical vulnerability for modern organizations, exacerbated by rapid adoption of GenAI tools like GitHub Copilot, ChatGPT, and low-code platforms. GitGuardian's latest report reveals a 25% increase in leaked secrets, with over 23.7 million new exposures in 2024 and more than 101,000 valid secrets discovered in Docker Hub alone. Generic secrets now represent 58% of all leaks, and tools meant to protect secrets—like GitHub Push Protection and secrets managers—are proving insufficient due to inconsistent usage and excessive token permissions.

The convergence of generative AI, fragmented secrets management practices, and poor credential hygiene among developers and infrastructure teams is expanding the enterprise attack surface. With NHIs (Non-Human Identities) vastly outnumbering users in cloud environments and remaining valid long after exposure, attackers are increasingly able to gain initial access and persist undetected.

READ MORE: TACTICAL GUIDANCE

Audience
- CISO
- Security Managers
- Cybersecurity Professionals
- Human Resources Professionals
- Third-Party Risk Managers
- Government & Defense Sector Leaders

EXTERNALIZED INSIDER ACCESS: DPRK IT WORKERS EXPLOITING REMOTE WORK TO INFILTRATE GLOBAL ENTERPRISES

Nation-state threat actors from the Democratic People's Republic of Korea (DPRK) continue to infiltrate global organizations by posing as freelance or remote IT workers. This tactic, known as the DPRK IT Worker Threat, enables external operatives to obtain insider access to corporate systems and data without deploying malware or traditional intrusion techniques. These actors utilize stolen or falsified identities, manipulate onboarding processes, exploit bring-your-own-device (BYOD) policies, and employ facilitators to launder devices and payments. Once inside, DPRK IT workers have executed extortion campaigns, exfiltrated proprietary code, and supported broader state objectives, including revenue generation for sanctioned military programs.

READ MORE: TACTICAL GUIDANCE

RETURN

Audience

- C-Suite
- CISO
- Security Managers
- Cybersecurity Professionals

EARTH ALUX

A newly observed cyber espionage campaign attributed to the China-linked APT group Earth Alux demonstrates significant advancements in threat capabilities. Active since at least mid-2023, the group has expanded operations from Asia-Pacific (APAC) to Latin America, targeting key sectors such as government, technology, logistics, telecommunications, and retail.

Earth Alux's operations revolve around its modular and multi-stage backdoor VARGEIT, supported by tools like COBEACON, RAILLOAD, and RAILSETTER. These tools enable stealthy initial access, persistent control, and covert data exfiltration, using advanced evasion techniques such as DLL sideloading, timestomping, and the abuse of Microsoft Outlook's Graph API for command-and-control (C2) communications.

READ MORE: TACTICAL GUIDANCE

RETURN

Tactical Guidance

AI ADOPTION AND SECRET SPRAWL - GROWING ORGANIZATIONAL RISK FROM GPT USAGE

OVERVIEW

Secrets sprawl continues to accelerate in 2025, posing a mounting risk to enterprise security and cloud infrastructure. With over 23 million new secrets exposed on GitHub in 2024 alone—a 25% year-over-year increase—and AI tools like Copilot contributing to a 40% rise in leakage incidence, organizations face unprecedented challenges in safeguarding credentials across source code, containers, and collaboration platforms.

IMPACT

- Cloud and Container Risk Amplification
- Hardcoded credentials in Docker layers, especially ENV and RUN instructions, are enabling persistent access to cloud services like AWS, GCP, and GitHub.
- Over 101,000 valid secrets were discovered in Docker images, many tied to production environments and Fortune 500 companies.
- AI-Driven Sprawl Expansion
- GitHub Copilot and other LLM coding assistants have increased secrets leakage rates by 40%, with 6.4% of Copilot-enabled repos leaking at least one secret.
- Even repositories using secrets managers (e.g., HashiCorp, AWS, Azure Key Vault) had a 5.1% leak rate, proving secure tools are not effective without proper enforcement.
- Secrets Mismanagement and Long-Term Exposure
- Generic secrets now dominate leak volumes and are harder to detect, bypassing automated protection like GitHub Push Protection.
- 74.4% of secrets in private repos are generic, with developers treating private code as inherently safe—a flawed assumption.
- Many secrets remain valid months after detection, especially among NHIs, due to poor rotation, lack of automation, and weak governance.
- Supply Chain and Collaboration Platform Vulnerability
- Secrets are increasingly found in Slack, Jira, and Confluence, often classified as critical (38% in collaboration tools vs. 31% in SCMs).
- Real-time messaging, ticket-based troubleshooting, and documentation are new frontiers of uncontrolled credential sharing.
- Overprivileged Tokens Amplify Blast Radius
- GitHub and GitLab tokens retain excessive privileges—95-99% grant full or write access.
- Combined with leaked tokens, this enables widespread lateral movement, privilege escalation, and persistent backdoor access.

OBSERVATIONS

- GitHub Push Protection mitigated some specific credential leaks (e.g., sk- or ghu_ prefixed keys), but did not address the growing volume of generic secrets.
- AI-generated code frequently embeds insecure practices such as hardcoded credentials or weak authentication.

- “Zombie leaks”—secrets deleted from repositories without revocation—persist in public archives or mirrors.
- Collaboration platforms are emerging as high-risk exposure vectors for credentials due to lack of built-in scanning or structured security controls.
- Secrets exposure was most prevalent in industries including IT (65.9%), Education (20.1%), and Finance (1%), though no sector remains unaffected.

GUIDANCE

Strategic Intelligence

- **Reframe AI as a Core Risk Vector**
    - Treat GenAI platforms like ChatGPT and Copilot as part of the organization’s attack surface, regardless of official adoption.
    - Include AI usage in enterprise risk assessments and internal security audits.
- **Establish Governance for AI Tool Usage**
    - Implement clear AI usage policies covering acceptable data inputs, prompt content, and prohibited data types (e.g., PII, credentials).
    - Require departmental approval and security vetting for integration of GenAI into operational workflows.
- **Address Regulatory and Compliance Exposure**
    - Evaluate how usage of free-tier GenAI tools may conflict with data residency, privacy, and industry compliance requirements.
    - Collaborate with legal and privacy teams to create safeguards against unintentional violations (e.g., GDPR, HIPAA, CCPA).

Operational Intelligence

- **Threat Vectors**
    - **Secret Exposure in Prompts:** Employees unknowingly submit sensitive data (API keys, customer info, internal configs) in GenAI prompts.
    - **Insecure Code Suggestions:** Developers use AI-generated code that includes hardcoded credentials or unsafe logic.
    - **Zombie Leaks via GitHub:** Secrets deleted from repositories without revocation remain accessible, creating persistent backdoor risks.
- **Detection & Monitoring Gaps**
    - **Lack of Prompt Visibility:** Consumer AI tools do not offer enterprise-grade logging or auditing of user interactions.
    - **Unmanaged Device Usage:** AI tools accessed on personal accounts bypass corporate controls and increase data leakage potential.
    - **Insufficient AI-Specific DLP:** Traditional data loss prevention tools often miss AI interaction channels like web-based chat, IDE plugins, and CLI-based AI interfaces.
- **Security Enhancements for Organizations**
    - **Deploy AI-Native DLP Solutions:** Use tools like Nightfall or SpectralOps to monitor and restrict sensitive data flow to GenAI platforms.
    - **Prompt Filtering Controls:** Integrate browser extensions or endpoint controls that prevent copying secrets into AI prompt boxes.
    - **Centralize Secrets Management:** Require use of secret vaults (e.g., HashiCorp Vault, Akeyless) to eliminate developer reliance on copy-paste workflows.

RETURN

Tactical Intelligence

- **Mitigation Strategies**
  - **Restrict Personal GenAI Access:** Block free-tier ChatGPT and Copilot access via proxy or DNS to reduce unmonitored data sharing.
  - **AI-Aware Access Policies:** Limit GenAI tool access based on job role, device trust level, and data classification zones.
  - **Automated Secrets Scanning:** Continuously scan GitHub, PyPI, and internal repos for exposed secrets using automated tools.
  - **AI Code Review Pipelines:** Implement secure coding pipelines that detect AI-generated code and validate for embedded secrets or poor security practices.
- **Preventive Measures**
  - **Employee Education on AI Bias and Risk:** Train users to validate GenAI outputs and avoid entering confidential data into prompts.
  - **Session Logging and Monitoring:** Ensure that interactions with GenAI tools are logged and reviewed for high-risk data use.
  - **Periodic GenAI Usage Audits:** Conduct regular audits of who is using AI tools, for what purpose, and from which devices.
  - **Cross-Department Risk Collaboration:** Include HR, Legal, DevOps, and Security in AI risk management to align policy with real-world usage.

THREAT HUNTING HYPOTHESES

Sensitive Data Exposure via Free-Tier ChatGPT

Hypothesis: Employees are unintentionally submitting confidential data to ChatGPT, where it may be retained or re-generated by the model.

Investigation Steps:

- Analyze network traffic for prompt submissions containing high-entropy strings (API keys, tokens).
- Correlate known sensitive file access with AI-related browser sessions.
- Detect repeated use of “ChatGPT” or related domains via clipboard monitoring.

Zombie Secrets Persisting in Public Repositories

Hypothesis: Developers delete repositories to hide leaks instead of revoking keys, creating “zombie leaks” accessible to threat actors.

Investigation Steps:

- Monitor GitHub activity for deleted repos containing past valid secrets.
- Cross-reference revoked secrets with access logs to confirm effective decommissioning.
- Use HasMySecretLeaked to validate whether secrets appear in public repositories.

Exploitation of AI Outputs for Credential Harvesting

Hypothesis: Threat actors are crafting AI prompts to generate credentials or exploit AI training data that contains leaked secrets.

Investigation Steps:

- Test known AI interfaces with obfuscated prompts to elicit credential patterns.
- Analyze AI outputs for synthetic secrets matching AWS, Google, or Azure formats.
- Track attacker toolkits that leverage AI-generated code as entry vectors.

Sources

- **GitGuardian:** State of Secrets Sprawl Report 2025
- **DarkReading:** ChatGPT Prompt Risks and Employee Usage
- **Nightfall:** DLP for a ChatGPT World
- **SpectralOps:** Secrets Sprawl in DevOps
- **Akeyless:** Secrets Management Glossary

Externalized Insider Access: DPRK IT Workers Exploiting Remote Work to Infiltrate Global Enterprises

OVERVIEW

DPRK IT workers are transforming the insider threat model by gaining legitimate access to global organizations through deception. Rather than exploiting employees with personal issues, DPRK operatives impersonate trusted professionals, infiltrate sensitive environments, and act with the intent of long-term exploitation. These actors are not just contractors, they are covert assets of a nation-state. Their expanding global operations, technical fluency, and ability to evade vetting processes have made them a persistent and strategic security risk.

IMPACT

- **Global Brand Infiltration:** Organizations across Europe and the U.S.—including those in defense, tech, and finance—have unknowingly onboarded DPRK operatives posing as remote IT workers.
- **Credentialed Access for Espionage:** These workers use valid credentials to steal sensitive data, plant backdoors, or threaten extortion upon dismissal.
- **Bypassed Identity Verification:** Facilitators and falsified documents enable DPRK operatives to defeat onboarding and KYC controls at scale.

- **Unmonitored Environments:** BYOD and remote access policies give these actors pathways to operate without detection, particularly in unmanaged device scenarios.
- **Revenue Generation for Sanctioned Regimes:** Proceeds from these schemes directly fund DPRK military and weapons development, escalating the geopolitical stakes.

OBSERVATIONS

- **Identity Fraud at Scale:** Operatives adopt false nationalities (e.g., Italian, Singaporean, Ukrainian, American) and deploy fabricated personas, sometimes reinforcing one another's credibility in job applications.
- **Exploitation of Remote Work Platforms:** Targets include Upwork, Freelancer, and Telegram-based job boards. Authentication is often circumvented using false references and document forgeries.
- **Technical Expertise:** Identified projects include advanced blockchain apps, CMS builds, AI platforms, and Solana smart contracts. These workers mimic legitimate developers, blending into engineering teams.
- **Use of Facilitators:** Individuals and entities in the US and UK are helping DPRK operatives defeat KYC checks, launder equipment (e.g., corporate laptops rerouted to London), and acquire fraudulent documentation.
- **BYOD Weak Points:** Workers exploit virtualized access environments where traditional endpoint detection is disabled or reduced.
- **Extortion Post-Termination:** Dismissed operatives have demanded ransom, threatening to release proprietary data or share it with competitors.

GUIDANCE

Strategic Intelligence

- **Reframe Insider Threat Definitions**
  - Treat remote contractors and third-party developers as high-risk access points.
  - Consider nation-state operatives as potential insiders, not just external hackers.
- **Evolve Background Vetting Standards**
  - Require enhanced identity verification processes for remote roles, such as video-based ID confirmation and biometric matching.
  - Mandate secure documentation from trusted entities and use E-Verify or equivalent systems.
- **Global Sanctions Compliance**
  - Partner with legal and compliance teams to ensure that hiring practices do not violate sanctions regulations.
  - Monitor for red flags including document mismatches, foreign payment channels, or repeated onboarding failures.

Operational Intelligence

- **Threat Vectors**
  - **Initial Access:** DPRK IT workers gain entry by posing as legitimate job applicants using fake personas, forged documentation, and stolen identities.
  - **Insider-Level Privilege:** Once hired, they receive internal access to code repositories, sensitive project data, and production environments.
  - **Persistence & Espionage:** They operate undetected within BYOD and remote-access environments, exfiltrating data or planting backdoors.

- **Detection & Monitoring Gaps**
  - **Identity Verification Weaknesses:** Remote hiring pipelines often lack rigorous vetting, allowing fabricated identities to pass undetected.
  - **BYOD Blind Spots:** Personal devices used for virtual desktop access often lack endpoint detection and response (EDR) tools.
  - **Facilitator Involvement:** Devices shipped to legitimate addresses are re-routed overseas, defeating geo-based security controls.

- **Security Enhancements for Organizations**
  - **Contractor Risk Assessments:** Apply the same scrutiny to third-party developers and freelancers as full-time employees.
  - **Continuous Access Review:** Periodically audit contractor access privileges and monitor for anomalous behavior or unauthorized tool usage.
  - **Enhanced Remote Identity Checks:** Require real-time video ID verification during onboarding and corroborate documentation using independent channels.

Tactical Intelligence

- **Mitigation Strategies**
  - **Endpoint Monitoring in Virtual Environments:** Ensure virtual desktop infrastructure (VDI) and BYOD endpoints are integrated with EDR/XDR tools.
  - **Geolocation & Device Fingerprinting:** Use IP analytics, device fingerprinting, and behavioral baselines to flag anomalies in access patterns.
  - **Contractor Segmentation:** Isolate contractor environments from core infrastructure and enforce role-based access restrictions.
  - **Source Code Integrity Checks:** Implement automated code review tools to detect injected backdoors or unauthorized changes.

- **Preventive Measures**
  - **Multi-Layered Background Checks:** Cross-reference employment, education, and identity information via trusted third-party services.
  - **Crypto Transaction Monitoring:** Flag payments made to developers via cryptocurrency or suspicious payment channels.
  - **Freelancer Platform Screening:** Monitor for overlapping applicant personas across platforms like Upwork and Freelancer.
  - **Sanctions Compliance Validation:** Integrate sanctions screening to ensure no affiliations with DPRK or other high-risk entities.

THREAT HUNTING HYPOTHESES

Embedded Nation-State Personas in Freelance Marketplaces

Hypothesis: DPRK actors are posing as remote IT freelancers across platforms like Upwork and Freelancer, using falsified nationalities and documents.

Investigation Steps:

- Aggregate freelancer hiring data and IP metadata
- Identify clusters of applicants with overlapping references, portfolios, or payment addresses
- Correlate with known DPRK-linked wallets and job site accounts

Post-Termination Extortion from Former Contractors

Hypothesis: Recently terminated contractors may attempt extortion using proprietary data they exfiltrated during employment.

Investigation Steps:

- Search for out-of-band communications from former accounts
- Monitor leak sites and dark web forums for leaked internal code, credentials, or product plans
- Cross-check previous contractor access logs with data access anomalies

Use of BYOD Virtual Environments to Evade Detection

Hypothesis: DPRK IT operatives are leveraging BYOD remote access setups to avoid device-level monitoring and enable data exfiltration.

Investigation Steps:

- Identify endpoints accessing sensitive assets without full logging or EDR coverage
- Compare internal BYOD access patterns with those from issued corporate laptops
- Use behavior analytics to flag anomalous command-line or file transfer activity

Coordinated Facilitator Activity in Identity Laundering

Hypothesis: A network of facilitators is helping DPRK IT workers bypass identity verification and acquire Western hardware.

Investigation Steps:

- Trace mismatches between declared job locations and device activation geolocation
- Monitor for reused references, shared contact numbers, or addresses linked to known cases
- Inquire into suspicious document patterns or formatting anomalies in job applications

Sources

- **Google Threat Intel Group:** DPRK IT Workers Expanding Scope and Scale
- **SecureWorld:** Unmasking North Korea's Covert IT Army
- **Bleeping computer:** North Korean IT Worker Army Expands Operations in Europe
- **NYDFS: Cybersecurity Advisory:** Remote Workers and DPRK Risk
- **Hppy:** HR Background Checks and Insider Risk
- **Alston Privacy: Combatting the New Insider Threat:** North Korean IT Workers
- **PurpleSec:** Preventing Insider Threats in Hybrid Workforces

EARTH ALUX

OVERVIEW

Earth Alux, a China-linked APT group, is redefining modern cyberespionage through the use of modular malware and multi-stage attack chains that embed deeply into organizational systems. Their operations span from initial access via web shells to advanced persistence using customized backdoors like VARGEIT. These campaigns reflect a persistent, stealthy threat aimed at intelligence collection, operational disruption, and strategic data theft across the APAC and LATAM regions.

IMPACTS

- **Multistage Espionage Campaigns:** Earth Alux infiltrates organizations using layered malware and stealthy persistence mechanisms to collect and exfiltrate sensitive data over extended periods.
- **Sectoral Disruption:** Attacks have targeted government, telecom, logistics, technology, and retail industries, disrupting essential services and risking critical supply chains.
- **Cloud and API Abuse:** Use of legitimate platforms such as Microsoft Outlook's Graph API for covert command-and-control enables long-term evasion.
- **Fileless Execution:** Payloads run via benign processes like mspaint.exe and conhost.exe, bypassing traditional antivirus tools and complicating forensic investigations.
- **Regional Escalation:** Activity originally confined to APAC now includes Latin America, signaling geopolitical expansion and increased global reach.

OBSERVATIONS

- **Initial Access via Exploited Services:** Earth Alux exploits vulnerable, internet-facing services to deploy web shells such as GODZILLA, enabling stealthy first-stage access.
- **VARGEIT Backdoor Modularity:** Used in all stages of attack, VARGEIT allows command execution, reconnaissance, and covert tool deployment via process injection.
- **Injection into System Utilities:** Fileless attacks utilize mspaint.exe to host backdoor commands and exfiltration tools, eliminating disk artifacts.
- **Command & Control via Outlook API:** Communications pass through Outlook draft folders using the Graph API, avoiding detection by standard network filters.
- **Advanced Evasion Techniques:** Tactics include DLL sideloading, timestomping, encrypted payloads, and anti-hooking methods in MASQLOADER.
- **Exfiltration via Cloud Buckets:** Stolen data is compressed and sent to attacker-controlled cloud storage, reused across multiple intrusions.
- **Malware Testing with Chinese Tools:** Open-source tools like ZeroEye and VirTest are employed to evade detection and simulate clean payloads.

GUIDANCE

Strategic Intelligence

- Reassess Cloud and API Trust Models
- Monitor use of Outlook APIs and other cloud-native services for potential covert communications.
- Restrict access to Graph API operations not required for business operations.
- Evolve Threat Attribution Readiness
- Incorporate geopolitical intelligence into threat modeling–track Chinese-speaking communities and toolsets (e.g., ZeroEye).
- Flag unusual sideloading behaviors or persistent access tactics aligned with PRC-linked TTPs.
- Defense in Depth for Multistage Malware
- Harden endpoints and servers with memory monitoring, script control, and process behavior baselining.
- Deploy deception technology to trap and study lateral movement behavior of stealth actors.

Operational Intelligence

- **Threat Vectors**
  - **Initial Access:** Web shell implantation via vulnerable public-facing services.
  - **Persistence:** Scheduled tasks and timestomping enabled by RAILSETTER.
  - **Command Execution:** Code injected via VARGEIT into system binaries like mspaint.exe.
  - **Exfiltration:** Cloud storage buckets act as repeat-use destinations for compressed reconnaissance data.
- **Detection & Monitoring Gaps**
  - **API Misuse:** Outlook's Graph API allows command exchange undetected by perimeter tools.
  - **Process Injection Evasion:** Tool execution through trusted binaries bypasses traditional antivirus heuristics.
  - **Lack of Application Whitelisting:** Systems often allow execution of QEMU, CDB, and regsvr32-based payloads without inspection.
- **Security Enhancements for Organizations**
  - **Monitor Draft Folder Anomalies:** Detect and alert on API write patterns involving unusual Outlook folders.
  - **Control Use of LOLBins:** Block use or closely monitor binaries like cdb.exe, regsvr32.exe, and rundll32.exe.
  - **Endpoint Protection Uplift:** Mandate advanced behavioral EDR/XDR coverage for endpoints accessing sensitive services.

Tactical Intelligence

- **Mitigation Strategies**
  - **Script Logging & Monitoring:** Enable full PowerShell, WMI, and command-line logging; flag odd usage paths.
  - **Memory and Injection Monitoring:** Detect anomalous code execution within mspaint.exe or conhost.exe.
  - **Scheduled Task Auditing:** Identify timestomped tasks that launch renamed system binaries or unauthorized DLLs.
- **Preventive Measures**
  - **Hardening of Email and API Access:** Implement granular access controls to cloud APIs such as Microsoft Graph.

- **Service Isolation & Network Segmentation:** Isolate legacy servers and ensure external-facing services are segmented.
- **Restrict DLL Sideloading Opportunities:** Lock down directories and tighten permissions to prevent drop-and-load behavior.

THREAT HUNTING HYPOTHESES

Covert C2 via Outlook Graph API

Hypothesis: Earth Alux is leveraging Outlook's Graph API to send and receive encrypted command traffic via the drafts folder

Investigation Steps:

- Monitor for repeated creation and deletion of drafts across accounts.
- Detect API calls with base64 content posted to drafts.
- Alert on GUID usage for storing auth tokens in registry entries.

Stealth Execution Through MSPaint

Hypothesis: VARGEIT injects secondary payloads into benign system processes like mspaint.exe to conduct fileless operations.

Investigation Steps:

- Search for mspaint.exe instances with unusual command-line arguments or extended runtime.
- Correlate with concurrent network activity to known C2 endpoints.
- Scan memory for injected shellcode in system utilities.

Timestomped Persistence with RAILSETTER

Hypothesis: RAILSETTER is used to hide RAILLOAD-based persistence through scheduled tasks and timestamp manipulation.

Investigation Steps:

- Identify new scheduled tasks with timestamps incongruent with installation logs.
- Look for renamed binaries in non-standard directories matching known sideloaded DLLs.
- Cross-reference with DLLs matching cloned export tables (CloneExportTable artifacts).

Tool Testing Using Chinese Open-Source Malware Kits

Hypothesis: Earth Alux performs malware stealth tests using ZeroEye and VirTest before payload deployment.

Investigation Steps:

- Scan for binaries with signatures matching ZeroEye/CloneExportTable routines.
- Search logs for execution of these tools in staging or dev environments
- Analyze portable executables (PEs) for overwritten export tables.

Sources

- **Trend Micro:** The Espionage Toolkit of Earth Alux
- **The Hacker News:** China-Linked Earth Alux Uses VARGEIT Backdoor
- Earth Alux Exposed Targeting Critical Infrastructure
- Earth Alux Indicators of Compromise

UNLOCK CRITICAL INSIGHTS

Download the full Converge Red Team Report: 2024 Penetration Testing Findings & 2025 Strategies now and gain the critical insights needed to stay ahead of attackers. Together, we can create a safer digital world.

FREE REPORT

Download Your Copy

RETURN

CONVERGE
TECHNOLOGY SOLUTIONS

Contact the Converge Threat Intel Group at cybersecurity@convergetp.com

convergetp.com/cybersecurity