11
NOV

THREAT INTEL REPORT 2024

CONVERGE
TECHNOLOGY SOLUTIONS

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

Observations for November 2024

Cybersecurity threats to critical infrastructure are escalating, impacting essential services in energy, telecommunications, and water sectors. The interconnected nature of these systems heightens risk, as a compromise in one area can cascade across sectors. This report addresses essential defenses, emphasizing asset management, attack surface reduction, and consistent penetration testing as practical measures to reduce risk in critical infrastructure. Key vulnerabilities, often rooted in basic security gaps such as default credentials and insufficient multi-factor authentication (MFA), require immediate attention to mitigate potential exploitation.

The interconnected structure of critical infrastructure presents broad implications, with disruptions in one sector potentially affecting others, from public health to finance. Many recent attacks, though technologically simple, exploit fundamental vulnerabilities like unpatched systems and default configurations. Addressing these foundational issues is crucial to enhance the resilience of critical infrastructure and reduce the impact of potential cyber incidents.

The recently identified “CRON#TRAP” phishing campaign illustrates a notable advance in threat techniques. This campaign uses an emulated Linux environment within Windows systems to establish hidden, persistent access, evading standard detection methods. The attack, delivered via phishing emails masked as an “OneAmerica Survey,” installs a Tiny Core Linux environment equipped with the Chisel tunneling tool, enabling Command-and-Control (C2) operations while bypassing traditional antivirus defenses. Evidence suggests a targeted focus on North America and Europe, underscoring the need for vigilant detection and response mechanisms.

RETURN

Executive Overview

Cyber Threats to Critical Infrastructure: Understanding the Ripple Effect and Reducing Risks

Audience

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

SUMMARY: Cyberattacks targeting critical infrastructure are increasing, affecting both primary services (such as energy, water, and telecommunications) and interconnected support systems (e.g., ISPs and payment systems). This interconnected structure magnifies risks, as a breach in one sector can trigger a ripple effect, disrupting services in multiple areas. While some attacks demonstrate advanced techniques, many exploits rely on simple weaknesses, such as default credentials, lack of multi-factor authentication (MFA), and reused passwords. This report outlines key areas—asset management, attack surface assessment, and regular penetration testing—that can measurably reduce risk in critical infrastructure.

Tactical guidance >> Cyber Threats to Critical Infrastructure: Understanding the Ripple Effect and Reducing Risks

CRON#TRAP: New Emulated Linux Environment Campaign Bypasses Windows Detection

Audience

- CISO
- Security Managers
- Cybersecurity Professionals
- IT Engineering Teams

SUMMARY: Securonix researchers have identified a sophisticated phishing campaign, codenamed "CRON#TRAP," which leverages an emulated Linux instance to gain unauthorized, persistent access to Windows environments. Delivered via phishing emails masquerading as an "OneAmerica Survey," CRON#TRAP uses the QEMU virtualizer to launch a Tiny Core Linux environment on infected Windows machines. Within this concealed instance, attackers deploy the Chisel tunneling tool, enabling remote Command-and-Control (C2) connections. This tactic bypasses traditional antivirus and security tools, complicating detection and response efforts. Evidence suggests a targeted focus on North America and Europe, but attribution remains unclear.

Tactical guidance >> CRON#TRAP: New Emulated Linux Environment Campaign Bypasses Windows Detection

Audience

- CISO
- Cybersecurity Professionals
- Security Managers

EDR Silencer

SUMMARY: Threat actors are increasingly integrating the open-source tool EDR Silencer into attack campaigns to disable or mute EDR tools and evade detection. EDR Silencer, designed to manipulate the Windows Filtering Platform (WFP), prevents EDRs from sending telemetry data to management consoles, creating blind spots in monitoring and complicating threat detection efforts. This report delves into EDR Silencer's capabilities, its impact on endpoint security strategies, and detection recommendations for defensive teams.

Tactical guidance >> EDR Silencer

Tactical Guidance

Cyber Threats to Critical Infrastructure: Understanding the Ripple Effect and Reducing Risks

Overview & Impact

Disruption in one infrastructure sector

can cascade to others, often due to security gaps

The interconnected nature of critical infrastructure means that disruptions in one sector can quickly impact others. Attacks on core services such as telecommunications or water utilities affect dependent systems across sectors. Often, these incidents exploit fundamental security gaps rather than complex attack methods, emphasizing the need for robust basic defenses.

- **Utility Services and Telecoms:** As utilities increasingly depend on internet and telecom services for operations, disruptions in connectivity or data access can halt customer support, billing, and even essential services.
- **Ripple Effect in Infrastructure:** A past example, the 2021 Colonial Pipeline attack, demonstrated how a cyber incident affecting fuel supply chains had broad economic and public impacts. Today, similar risks exist across other infrastructure sectors.
- **Simple Exploits, Major Disruptions:** Many recent incidents, including the American Water and Free ISP breaches, used low-complexity tactics, such as exploiting default credentials or unpatched systems. These common vulnerabilities show that basic security practices can play a large role in preventing disruptions.

This complex web of dependencies highlights the need for coordinated and proactive cybersecurity strategies across sectors to reduce cascading impacts.

Observations

- **Utility Sector Vulnerabilities:** The recent attack on American Water highlights how utility providers are at risk of operational disruptions even when basic services remain unaffected. Attackers were able to disrupt customer billing and support by targeting core administrative systems.

RETURN

- **Telecom and ISP Attacks:** Incidents involving telecom companies and ISPs reveal how weaknesses in connectivity infrastructure impact a broad range of sectors. Recent breaches in U.S. and European telecoms affected both organizational clients and individual users, showing how failures in one area impact numerous dependent services.
- **Focus on Basic Exploits:** Simple attacks that exploit lack of MFA, reused passwords, or default credentials are commonly used by attackers. These methods bypass more sophisticated defenses, indicating a need for organizations to strengthen fundamental security measures.
- **Need for Proactive Testing:** Lack of regular penetration testing and asset management has left many organizations exposed to low-complexity attacks. Effective asset management and ongoing evaluation of potential vulnerabilities are essential to reducing these risks.

Guidance

Strategic Intelligence

- **Targeting of Interconnected Systems:** Adversaries from countries like China, Russia, and Iran target both primary critical infrastructure (e.g., energy and water) and the secondary systems they rely on. Their approach focuses on exploiting basic vulnerabilities, like credential reuse and insufficient authentication, to establish entry points and maintain long-term access.
- **Increased Need for Cross-Sector Security:** Attackers recognize that disruptions in ISPs, telecoms, or utility services affect all sectors that rely on these providers. This understanding has shifted the focus of cyber threats from direct attacks on individual companies to broader, interconnected infrastructures.
- **Digital Transformation Challenges:** As critical infrastructure sectors integrate digital tools, like APIs and cloud services, they increase their attack surface. Attackers exploit these changes, especially where basic security protocols, such as strong password policies and MFA, are lacking.

Operational Intelligence

- **American Water Incident:** On October 3, American Water disconnected systems in response to unauthorized network activity. Although the water supply remained safe, billing and customer support services were disrupted, demonstrating the operational impacts a cyberattack can have even without direct harm to core services.
- **Telecom Sector Breaches:** Recent attacks on telecom providers in the U.S. and Europe, such as the Salt Typhoon infiltration, have targeted weak credentials and authentication processes, impacting users across sectors that rely on telecom services for secure data and operations.
- **CISA Alerts on Utility Sector Weaknesses:** CISA's recent advisories call attention to simple but effective tactics used against operational technology in utilities, highlighting the need for stronger protection around ICS and OT devices vulnerable to low-effort attacks, such as default credentials and password spraying.

Tactical Intelligence

- **Credential Attacks (e.g., Brute-force, Password Spraying):** Adversaries often rely on brute-force or password spraying attacks, especially where weak password policies and lack of MFA are prevalent.

RETURN

- **Multi-Factor Authentication (MFA) Bombing:** MFA bombing, or sending repeated authentication requests to users, is increasingly used to exploit user fatigue and gain access. Implementing phishing-resistant MFA and number matching can prevent this tactic.
- **Asset Management Gaps:** Many critical organizations lack accurate asset inventories, making it difficult to secure all devices. Attackers exploit these gaps, often targeting outdated or forgotten systems.
- **API and Web Application Attacks:** The digital transformation of utility and telecom sectors has introduced APIs and web applications, which adversaries target to gain unauthorized access and disrupt services.
- **Living-off-the-Land (LotL) Tools:** Threat actors use built-in tools within compromised networks to avoid detection, blending in with normal system activity to remain undetected while maintaining access.

Key Recommendations

To better protect against these attacks, critical infrastructure organizations should prioritize the following:

1. **Asset Management:** Effective asset management helps organizations maintain an up-to-date inventory of all devices and systems, ensuring that critical systems are monitored and secured.
2. **Regular Attack Surface Evaluation and Testing:** Ongoing testing, including penetration testing, allows organizations to detect and address vulnerabilities early, reducing the risk of simple exploits by attackers.
3. **Strong Authentication and MFA Implementation:** By implementing MFA and monitoring for reused or weak passwords, organizations can significantly reduce unauthorized access and mitigate credential-based attacks.

These foundational steps are key to reducing exposure to low-complexity attacks, which are often the entry points for larger disruptions.

Sources

- Reuters - American Water Disconnects Systems Following Cyberattack
- BleepingComputer - Free Confirms Data Breach
- USA Today - Hacking Attacks on Critical Infrastructure More Common
- CISA - Alert on OT and ICS Security in Water Sector
- The Record - Free Telecom Cyberattack
- Cyber Management Alliance - October 2024 Cyber Incidents

CRON#TRAP: New Emulated Linux Environment Campaign Bypasses Windows Detection

Overview & Impact

Emulated Linux on Windows to

establish a covert backdoor

The **CRON#TRAP** campaign is a newly identified phishing attack that leverages an emulated Linux environment to establish a concealed backdoor within Windows systems, creating a stealthy and persistent threat. This attack begins with a phishing email masquerading as an **"OneAmerica Survey"** and contains a large ZIP file (285MB) with a malicious shortcut (.lnk) file. When executed, the shortcut initiates a series of PowerShell commands to extract and deploy a Tiny Core Linux instance within a QEMU virtualization environment, named **"PivotBox."**

This Linux environment comes preloaded with the Chisel tunneling tool, a legitimate utility that enables attackers to establish an encrypted Command-and-Control (C2) connection via WebSockets, effectively bypassing traditional antivirus and security solutions. By deploying this Linux environment on Windows, attackers can operate within a concealed, isolated system, granting them long-term, covert access to execute malicious activities such as data exfiltration, lateral movement, and further payload deployment.

Although specific industries have not been confirmed, early indicators suggest potential targeting in North America and Europe, with limited attribution pointing to North American sources. This campaign underscores a novel evasion technique that abuses legitimate tools, posing significant risks to organizations' security visibility and control over compromised systems.

Observations

- **Initial Infection Vector:** Phishing email with a large (285MB) ZIP file containing a malicious shortcut (.lnk) file disguised as a survey.
- **Execution Chain:** Upon activation, PowerShell commands re-extract ZIP contents, execute a batch script, and initiate a QEMU Linux instance, providing an isolated, concealed environment on the host.
- **Environment Details:**
  - QEMU runs a Tiny Core Linux VM called "**PivotBox,**" renamed to disguise as **"fontdiag.exe."**
  - PivotBox preloaded with Chisel tunneling tool for C2 connections via WebSockets.
- **Persistence Techniques:**
  - Custom aliases and scripts (e.g., get-host-shell and get-host-user) allow attackers to communicate with the host.
  - SSH key generation for re-entry and modified boot scripts ensure persistence across reboots.

RETURN

- **Indicators of Compromise (IoCs):**
  - **C2 IP Address:** 18.208.230[.]174
  - **Phishing URL:** hxxps://forum.hestiacp[.]com/uploads/default/original/2X/9/9aae76309a614c85f880512d8fe7df158fec52cc.png

Guidance

Strategic Intelligence

- **Trend Analysis:**
  - **CRON#TRAP Emulated Environments:** The CRON#TRAP campaign highlights an emerging trend in malware that utilizes emulated Linux environments to bypass conventional security on Windows systems. Attackers increasingly turn to virtualization and legitimate tools like QEMU to conceal malicious activity within isolated environments.
  - **Tool and Technique Evolution:** The use of QEMU and Chisel in CRON#TRAP represents an evolution in evasion tactics, where attackers utilize virtualization to operate undetected. This marks a shift from solely file-based malware to virtualized environments as an attack vector.
- **Implications for Security Frameworks:**
  - **Enhanced Endpoint Security Requirements:** Traditional endpoint protection solutions may struggle to detect emulated environments. This campaign underscores the need for enhanced monitoring of process anomalies, especially those involving virtualized instances on unconventional paths.
  - **Targeting Trends in North America and Europe:** The presence of command-and-control (C2) infrastructure in the U.S. and the phishing campaign's language indicate that North American and European organizations could be primary targets, raising concerns over the potential involvement of state-sponsored actors for cyber espionage.

Operational Intelligence

- **Attack Vectors:**
  - **Initial Access:** CRON#TRAP is distributed via phishing emails containing a large ZIP file and a malicious shortcut (.lnk) file, likely to evade detection by exploiting user curiosity or trust in familiar survey themes.
  - **Execution:** Once opened, the shortcut executes PowerShell commands to unpack and run a QEMU-based emulated Linux environment on the compromised Windows machine, establishing an isolated foothold on the host.
  - **C2 Channel and Remote Access:** Within the emulated Linux environment, a pre-configured Chisel client connects to a hard-coded C2 server, enabling encrypted tunneling for data exfiltration and remote command execution.
- **Detection Challenges:**
  - **Use of Legitimate Tools:** The QEMU and Chisel tools, both legitimate software, complicate detection, as they are unlikely to raise alarms when executed from unconventional locations.

RETURN

- **Emulated Environment Concealment:** Security tools may not recognize or scan processes within the emulated Linux environment, increasing the difficulty of detecting the malware's presence on infected systems.

Tactical Intelligence

- **Mitigation Strategies:**
  - **Endpoint and PowerShell Monitoring:** Enable advanced PowerShell logging and monitor for unusual script execution patterns, particularly for commands that unpack or execute from user profile directories.
  - **Behavioral Detection of QEMU and Virtualization Tools:** Configure endpoint detection and response (EDR) tools to flag any instances of QEMU or similar virtualization software running outside expected directories, such as **%Program Files%**.
  - **Network Traffic Analysis:** Set up alerts for network traffic to the known **C2 IP (18.208.230[.]174)** and other unusual outbound connections from systems using uncommon protocols or port numbers.
  - **Email Security Enhancements:** Improve email filters to detect large ZIP attachments and shortcut files in phishing campaigns, especially those exceeding typical file sizes for attachments.
- **Preventive Measures:**
  - **User Training:** Educate employees to avoid downloading or opening large or unexpected files from unknown sources, as well as to recognize phishing attempts with familiar-sounding yet deceptive branding.
  - **Supply Chain and Insider Threat Monitoring:** Secure endpoints against supply chain compromises and insiders who could introduce emulated environments through local installation or storage devices.
  - **Environment Isolation Policies:** For critical endpoints, implement policies limiting the use of virtualized environments, particularly those that initiate network connections, to prevent unauthorized tunneling and lateral movement.

Threat Hunting Hypotheses

Hidden Linux Backdoor via QEMU Emulation on Windows

- **Hypothesis:** Threat actors are utilizing emulated Linux environments within Windows systems to establish concealed backdoors that bypass traditional detection mechanisms, enabling persistent remote access and covert command-and-control communication.
- **Investigation Approach:**
  - Monitor for unusual process activity linked to QEMU or virtualization software executed from non-standard directories, such as **%HOME%\datax** or other user-profile folders.
  - Analyze PowerShell and script execution logs to identify instances of ZIP extraction and batch file activity that initiate system binaries or executable files outside of normal workflows.
  - Set up alerts on network traffic for consistent or persistent outbound connections to suspicious IPs, such as **18.208.230[.]174**, indicating a potential C2 connection from an emulated Linux instance.

RETURN

- Review endpoint data for unexpected Chisel tunneling activity, including any connections over HTTP or WebSockets to obscure SSH channels that might not align with regular user behavior.

Persistence Through Emulated Environment Configuration

- **Hypothesis:** Attackers are configuring persistent access within emulated environments by manipulating startup scripts and deploying SSH keys to retain access even after system reboots.
- **Investigation Approach:**
  - Monitor startup script modifications in the **%HOME%\datax** or other similar directories, focusing on changes to files like **bootlocal.sh** and other Linux startup configurations.
  - Track SSH key creation and transfers within user profile directories, especially for any public key uploads to external sites, which could indicate persistence mechanisms for remote access.
  - Set alerts for unauthorized SSH connections initiated from the emulated Linux environment that communicate with external IPs or uncommon subnets.

Phishing-Delivered ZIP with Embedded Shortcut Files

- **Hypothesis:** Phishing emails containing large ZIP files and shortcut (.lnk) files are being used to deliver malicious payloads that install emulated Linux environments on Windows endpoints, bypassing traditional AV detection.
- **Investigation Approach:**
  - Audit email traffic for attachments with unusually large ZIP files (e.g., around 285MB) and check if users are accessing or downloading from unknown domains.
  - Examine user execution logs for shortcut (.lnk) files linked to ZIP extraction and subsequent PowerShell commands, especially files mimicking trusted brands or surveys.
  - Implement endpoint alerts for ZIP extraction activity that involves large archive files unpacked in non-standard directories or extracted with embedded executables.

Concealed Command-and-Control Channel through Chisel Tunnel

- **Hypothesis:** Attackers are leveraging the Chisel tunneling tool within the emulated Linux environment to establish encrypted C2 channels, allowing them to evade firewall detection and persistently communicate with compromised systems.
- **Investigation Approach:**
  - Monitor for Chisel executable activities or connections made through uncommon ports or protocols, specifically tunneling over HTTP or WebSocket connections within the emulated Linux system.
  - Analyze network logs for any anomalies that include frequent communication with IP **18.208.230[.]174** or requests to unexpected subdomains associated with public file-sharing services.
  - Set up alerts for encrypted outbound traffic patterns from Linux processes running on Windows endpoints, which might indicate hidden C2 channels.

Sources

- Dark Reading: "Attacker Hides Malicious Activity in Emulated Linux Environment"
- HackRead: "Hackers Deploy CRON#TRAP for Persistent Linux System Backdoors"
- Securonix: "CRON#TRAP Emulated Linux Environments as the Latest Tactic in Malware Staging"
- The Hacker News: "New CRON#TRAP Malware Infects Windows by Emulating Linux to Deploy Backdoor"

RETURN

Blocks EDR telemetry via Windows Filtering Platform, disrupting endpoint monitoring

EDR Silencer

Overview & Impact

EDR Silencer is an advanced evasion tool inspired by MDSec's NightHawk FireBlock. It leverages the WFP on Windows systems to block outbound communications from EDR processes, thus stopping telemetry data from reaching security consoles. By deploying EDR Silencer, adversaries can hinder endpoint monitoring capabilities, making malicious activities, including lateral movement and data exfiltration, significantly harder to detect. This development highlights an urgent need for organizations to strengthen endpoint defenses and implement layered security measures.

Observations

- **Tool Capabilities:** EDR Silencer detects EDR processes and applies WFP filters to block outbound traffic, preventing alerts from reaching security management servers.
- **Tool Integration:** Threat actors are embedding EDR Silencer into broader attack chains to neutralize security monitoring by blocking traffic for multiple EDR tools such as Microsoft Defender, SentinelOne, and Trend Micro Apex One.
- **Detection Challenges:** EDR Silencer's selective blocking capability allows attackers to focus on high-value EDR processes while leaving other network activities undisturbed, reducing the likelihood of detection.
- **EDR Blocking Effectiveness:** Some EDR tools still manage partial reporting due to gaps in the tool's hardcoded executable list, although attackers can expand the list manually to target specific security tools.

Guidance

Strategic Intelligence

- **Trend Analysis:**
  - **EDR Evasion Techniques:** The emergence of EDR Silencer aligns with a broader trend of tools designed to disable or bypass EDR and antivirus solutions. Attackers increasingly rely on techniques that interfere with security tool communications rather than traditional malware signatures.
  - **WFP Exploitation:** The use of the Windows Filtering Platform (WFP) for evading detection highlights a trend towards leveraging system-level filtering frameworks, complicating detection and mitigation for standard security solutions.
- **Implications for Enterprise Security:**
  - **Security Gaps in EDRs:** EDR Silencer's ability to block outbound telemetry presents a serious challenge for organizations reliant on EDRs for real-time threat detection and response.
  - **Increased Exposure to Advanced Threats:** Advanced persistent threats (APTs) and financially motivated attackers are likely to adopt EDR-silencing techniques to improve persistence and stealth, increasing risks for sectors such as finance, healthcare, and critical infrastructure.

RETURN

Operational Intelligence

- **Attack Vectors:**
  - **Initial Access:** EDR Silencer requires administrative access to set WFP filters, indicating that attackers must first gain high privileges through compromised credentials, social engineering, or exploiting unpatched vulnerabilities.
  - **Process Filtering:** The tool dynamically identifies and filters specific EDR processes (e.g., Microsoft Defender, SentinelOne) using hardcoded executable paths, enabling attackers to selectively block outbound network communications.
- **Detection Challenges:**
  - **Hidden Network Modifications:** Standard network monitoring tools may fail to detect EDR Silencer's filtering activities since the WFP operates at the OS kernel level, making it challenging to identify malicious modifications.
  - **Log Availability:** Many environments lack the necessary logging (e.g., Event IDs 5448, 5157) to identify unauthorized WFP changes, reducing visibility into EDR Silencer's actions.

Tactical Intelligence

- **Mitigation Strategies:**
  - **Enhanced Network Monitoring:** Deploy monitoring solutions that can detect suspicious WFP filter additions and modifications, especially those affecting known EDR processes.
  - **WFP-Specific Logging:** Enable and monitor specific Event IDs (e.g., 5448 for "Filtering Platform Policy Change" and 5157 for "Filtering Platform Connection") to track any abnormal changes in network filtering policies.
  - **Access Control and Privilege Management:** Strengthen access controls to limit administrative privileges. Employ least privilege policies and regularly audit access to ensure only authorized users can make changes to WFP settings.
  - **Anomaly Detection for EDR Processes:** Implement behavioral monitoring to identify unusual patterns in EDR process activity, such as unexpected process blocking or terminations, which may indicate tampering.
- **Preventive Measures:**
  - **Regular Audits of WFP Configurations:** Conduct periodic audits of WFP filters and policies to ensure no unauthorized filters are in place.
  - **Endpoint Hardening:** Apply updates and security patches to EDR solutions to address any potential vulnerabilities that attackers could exploit.
  - **Incident Response Training:** Train security teams to recognize and respond to the signs of WFP-based attacks, ensuring they can quickly mitigate any suspicious network filtering activity.

RETURN

Threat Hunting Hypotheses

Malicious Network Filtering Using WFP to Evade EDR Detection

- **Hypothesis:** Threat actors may leverage EDR Silencer to apply WFP filters that selectively block communications from EDR agents, preventing alerts from reaching the management console and hiding malicious activities.
- **Investigation Approach:**
  - **Monitor WFP Events:** Continuously monitor WFP-related Event IDs, particularly those indicating changes to filtering policies or blocked connections related to EDR processes.
  - **Cross-Reference with Process Logs:** Correlate WFP filter changes with EDR process activity to detect patterns indicating unauthorized filtering of EDR processes.
  - **Real-Time Alerts for WFP Modifications:** Set up alerts for unusual WFP modifications, especially when applied to processes linked to EDRs.

Indicators of EDR Process Blocking

- **Hypothesis:** Attackers using EDR Silencer may deliberately block high-priority EDR processes to disrupt telemetry and evade detection.
- **Investigation Approach:**
  - **Behavioral Analysis:** Analyze EDR processes for unexpected terminations or blocked network communications, flagging any patterns consistent with EDR Silencer activity.
  - **EDR-Specific Log Review:** Review logs from impacted EDR solutions for signs of tampering or network connection failures that may correlate with malicious WFP filters.

Sources

- Security Artwork: "EDR Silencer v2"
- The Hacker News: "Hackers Abuse EDR Silencer Tool"
- Bleeping Computer: "EDR Silencer Red Team Tool Used in Attacks"

RETURN

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

convergetp.com/cybersecurity