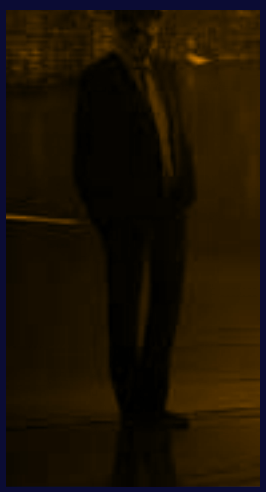
04
APR

THREAT INTEL REPORT 2024



CONVERGE
TECHNOLOGY SOLUTIONS

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

Observations for April 2024

In our latest threat intelligence report, the Sekoia Detection & Research team delves into the unsettling reality of the Tycoon 2FA Phishing-as-a-Service (PhaaS) platform, a sophisticated tool wreaking havoc in the cybersecurity realm. Targeting Microsoft 365 users with adversary-in-the-middle (AiTM) phishing tactics, Tycoon 2FA has already stamped its footprint, with over 1,100 associated domain names discovered. What's more alarming is its adeptness at bypassing multifactor authentication (MFA), making it a favored choice among cyber criminals seeking unauthorized access. As organizations navigate the evolving threat landscape, this report underscores the imperative for robust cybersecurity measures to combat such insidious attacks.

Meanwhile, the discovery of a cunning backdoor nestled within XZ Utils, a vital component of Linux distributions, raises grave concerns about potential supply chain attacks. Crafted by Jia Tan under the guise of a maintainer, this backdoor could have paved the way for remote execution of arbitrary code, particularly targeting systems with exposed SSH. Tan's strategic infiltration of the open-source contribution processes is a chilling reminder of the vulnerabilities inherent in collaborative software development. With the potential for widespread unauthorized access looming, this incident emphasizes the critical need for stringent oversight in managing open-source project contributions and permissions.

In addition to these threats, a novel Loop denial-of-service (DoS) attack exploiting vulnerabilities in the User Datagram Protocol (UDP) has emerged, posing a significant risk to approximately 300,000 hosts. This attack's simplicity and difficulty in halting it once initiated underscores its disruptive potential across crucial internet protocols like DNS, NTP, and TFTP. As organizations grapple with mitigating these diverse threats, our report serves as a beacon for security professionals, offering invaluable insights into the evolving threat landscape and the urgent need for proactive defense strategies.

The following comprehensive analysis highlights the overarching importance of a holistic approach to cybersecurity. These distinct challenges collectively underscore the dynamic and evolving nature of cyber threats. By understanding and addressing these threats in tandem, organizations can better fortify their defenses against the multifaceted risks posed by malicious actors. This integrated approach emphasizes the critical need for continuous monitoring, proactive threat intelligence, and collaborative efforts across industries to stay ahead of emerging cybersecurity challenges.

RETURN

Executive Overview

PhaaS: Tycoon 2FA phishing kit

Audience

- Cybersecurity professionals and analysts
- C-suite executives of affected and potentially vulnerable companies
- IT and network administrators
- Email and web hosting service providers
- Digital marketing and ad operations teams
- Legal and compliance officers

Summary

The Sekoia Threat Detection & Research team uncovered significant details about the Tycoon 2FA Phishing-as-a-Service (PhaaS) platform, revealing its widespread usage in AiTM phishing attacks.

This analysis offers insights into Tycoon 2FA's operations, technical mechanisms, and impact on organizations, highlighting the evolving threat landscape and the necessity for robust cybersecurity measures.

Go to tactical guidance >>

Audience

- C-suite executives
- Cybersecurity professionals
- Data privacy officers
- Compliance and regulatory personnel
- Software developers and engineers
- IT management and operations teams

XZ Utils backdoor uncovers intricacies and implications for Linux systems

Summary

The discovery of a sophisticated backdoor in XZ Utils, a crucial data compression utility within Linux distributions, unveiled a potential catastrophic supply chain attack. This backdoor, intricately placed by ostensible maintainer Jia Tan after a long-drawn campaign of social engineering and credibility establishment, could have allowed remote attackers to execute arbitrary code on affected machines, particularly targeting systems with SSH exposed to the internet.

The uncovering of this backdoor by Andres Freund, stemming from an investigation into performance anomalies, has possibly averted a significant security disaster within the Linux ecosystem.

Go to tactical guidance >>

Audience

- C-suite executives
- IT and cybersecurity teams
- Data protection officers
- Compliance and risk management professionals
- Incident response and threat intelligence analysts
- End users affected by the breach

Innovative Loop DoS attack exploits UDP protocol vulnerabilities, threatening vast network infrastructure

Summary

A novel Loop denial-of-service (DoS) attack, exploiting vulnerabilities in the User Datagram Protocol (UDP), has emerged and poses a significant risk to approximately 300,000 hosts. This attack induces a perpetual communication loop between paired network services leading to an unmanageable surge in traffic and service disruption.

Researchers at the CISPA Helmholtz Center for Information Security identified this vulnerability, currently tracked as CVE-2024-2169, affecting a range of crucial internet protocols, including DNS, NTP, and TFTP.

Go to tactical guidance >>

Tactical Guidance | Emerging Threats

Significant 2FA Bypass

Associated With Over 1,100 Domains

PhaaS: Tycoon 2FA phishing kit

Overview & Impact

Tycoon 2FA, identified by Sekoia in August 2023, employs sophisticated Adversary-in-The-Middle (AiTM) phishing tactics to bypass multifactor authentication and predominantly targets Microsoft 365 users. With over 1,100 associated domain names discovered, Tycoon 2FA's significant footprint underscores its effectiveness in harvesting session cookies and facilitating unauthorized access.

Observations

- **Attack vector:** Utilizing phishing emails with malicious links or QR codes, Tycoon 2FA deceives users into compromising their credentials and MFA responses.
- **Credential and session hijacking:** By capturing session cookies post-MFA authentication, attackers gain unauthorized access, demonstrating the kit's capability to subvert even MFA-protected accounts.
- **Rising popularity:** The accessibility and effectiveness of Tycoon 2FA in bypassing MFA make it a favored tool among cyber criminals, indicating a growing trend towards more sophisticated phishing attacks.

Guidance

Strategic Intelligence

- **Awareness and training:** Intensify training programs to educate users on the sophistication of phishing threats and the critical need for vigilance.
- **Collaborative defense:** Promote industry collaboration and threat intelligence sharing to bolster collective defenses against evolving phishing kits.

Operational Intelligence

- **Implement FIDO2 MFA:** Transition to *FIDO2-based* hardware authentication solutions to fortify defenses against phishing attempts that exploit weaker MFA forms.
- **Enhanced monitoring:** Deploy sophisticated monitoring systems to identify unusual access patterns or authentication anomalies indicative of phishing attempts.

Tactical Intelligence

- **Deploy phishing detection tools:** Utilize advanced detection solutions to identify and neutralize phishing attempts, focusing on the specific tactics employed by Tycoon 2FA.

RETURN

- **User vigilance training:** Empower users to critically assess authentication requests, email links, and QR codes, encouraging proactive reporting of suspicious activities.
- **Incorporate IoCs in defense mechanisms:** Utilize identified indicators of compromise (IoCs) associated with Tycoon 2FA to enhance detection and response strategies. Monitor network traffic for connections to known malicious domains and scrutinize login sessions for signs of AiTM interference.

Tactical Intelligence - Threat Hunting Hypotheses

- **Hypothesis:** Unauthorized session activity

  Given Tycoon 2FA's ability to steal session cookies, there may be unauthorized activities within user sessions that bypass MFA. Security teams should hunt for anomalies in session durations, locations, and activities that don't align with typical user patterns.
- **Hypothesis:** Anomalous authentication requests

  If Tycoon 2FA is present, there might be an increase in failed authentication attempts or unusual MFA prompts. Monitoring for such anomalies could reveal indicators of the phishing kit's activities.
- **Hypothesis:** Suspicious network traffic

  Tycoon 2FA's communication with C2 servers may generate detectable network traffic patterns. Analyzing outbound traffic for connections to known Tycoon 2FA-associated domains or IP addresses can help identify potential compromises.
- **Hypothesis:** JavaScript and HTML anomalies

  Considering Tycoon 2FA's use of malicious JavaScript and HTML, any unusual or obfuscated scripts running on company websites, particularly authentication pages, should be scrutinized for signs of the phishing kit.

Sources

- *New Tycoon 2FA Phishing Kit Raises Cybersecurity Concerns*
- *Hackers Are Using This New Phishing Technique to Steal Gmail and Microsoft 365 Accounts*
- *New Tycoon 2FA Phishing Kit Raises Cybersecurity Concerns*

Malicious Backdoor Code

Hidden in Build Process Targeting Linux Systems

XZ Utils backdoor incident uncovers intricacies, implications for Linux systems

Overview & Impact

Jia Tan's insertion of the backdoor into the XZ Utils repository showcases a strategic manipulation of open-source contribution processes. By using social engineering tactics, including creating fake accounts to exert pressure on the existing maintainer, Tan gradually gained trust and elevated privileges within the project.

RETURN

This long-term campaign culminated in Tan obtaining release manager rights, allowing the introduction of malicious code into the XZ Utils' release tarballs while avoiding direct inclusion in the public Git repository. This method ensured the backdoor remained hidden during the build process, highlighting a significant vulnerability in open-source software distribution.

The backdoor's impact is profound, as it targets a utility intrinsic to Linux systems, potentially enabling widespread unauthorized access and control over affected systems. The backdoor's design to only activate under specific conditions further indicates a targeted approach, aiming to compromise systems with significant strategic value.

Observations

- **Methodical infiltration:** Tan's approach to gaining repository access and trust over an extended period underlines the need for stringent oversight in open-source project contributions and permissions.
- **Stealthy code introduction:** The exclusion of the backdoor code from the public repository and its inclusion only in the release tarballs demonstrate a sophisticated strategy to evade detection.
- **Selective activation:** The backdoor's design to trigger under specific conditions suggests a targeted attack aimed at maximizing impact while minimizing detection.

Guidance

Strategic Intelligence

- **Vetting contributors:** If supporting an open-source project, implement rigorous background checks and monitoring for all contributors, especially those seeking elevated privileges.
- **Access control:** Enforce strict controls on who can commit and manage releases within repositories to prevent unauthorized insertions.
- **Community engagement:** Encourage active participation and oversight from the broader community to spot anomalies in contributions and maintainer activities.

Operational Intelligence

- **Code integrity checks:** Establish routine checks to compare repository code against release binaries to detect discrepancies.
- **Audit trails:** Maintain detailed logs of all changes, including contributor activities and file modifications, to trace any unauthorized insertions.
- **Incident response:** Develop a swift incident response plan to mitigate the impact of any detected backdoors or unauthorized code modifications.

RETURN

Tactical Intelligence

- **Version validation:** Regularly verify the integrity and authenticity of the XZ Utils versions that are used within the organization.
- **Anomaly detection:** Employ monitoring tools to detect unusual behavior in systems that could indicate backdoor activation.
- **Patch management:** Ensure timely application of patches and updates, particularly relating to security vulnerabilities or integrity issues.

Tactical Intelligence - Threat Hunting Hypotheses

- **Hypothesis:** Unauthorized code changes in open-source repositories

  Given the sophisticated backdoor in XZ Utils, there's a risk that similar unauthorized code changes could be present in other open-source software used within the environment. Security teams should scrutinize recent commits for anomalies such as unexpected contributors, substantial code modifications, or unusual commit times.

- **Hypothesis:** Anomalous build and release activities

  If a backdoor similar to the one in XZ Utils is present, there might be discrepancies in the open-source components' build and release processes. Monitoring for unauthorized modifications, unexpected artifacts, or alterations in the build process could reveal signs of tampering.

- **Hypothesis:** Unusual system or network behaviors

  The exploitation of a backdoor like that in XZ Utils may result in abnormal system or network behavior. Investigating unexpected network traffic, unusual system process activities, or system performance deviations can help detect the presence of a backdoor.

- **Hypothesis:** File integrity anomalies

  Considering the backdoor mechanism found in XZ Utils involved the introduction of obfuscated objects and scripts, any unexpected changes or access patterns in system files, particularly those associated with open-source software, should be closely monitored for signs of similar backdoor implementations.

Sources

- *Critical Linux Backdoor in XZ Utils Discovered: What to Know*
- *Malicious Code in XZ Utils for Linux Allows Remote Code Execution*
- *What We Know About the XZ Utils Backdoor That Almost Infected the World*

Server Loop Initiation

Poses Risk to 300,000 Internet Hosts

Innovative Loop DoS attack exploits UDP protocol vulnerabilities, threatening vast network infrastructure

Overview & Impact

The Loop DoS attack capitalizes on the connectionless nature of UDP, which lacks source IP address validation, allowing for IP spoofing. Attackers can initiate a loop between two servers, causing them to exhaust resources by continuously responding to each other's error messages. This loop generates substantial network traffic, impairing the involved systems or networks. The attack's simplicity and the difficulty in halting it once initiated are particularly concerning. The affected protocols are fundamental to internet operation, emphasizing the attack's potential to disrupt significant portions of network infrastructure globally.

Observations

- Approximately 300,000 internet hosts are susceptible to the Loop DoS attack.
- Affected protocols include DNS, NTP, and TFTP, along with legacy protocols like Echo and CHARGEN.
- The attack leverages IP spoofing, making it challenging to trace and stop.
- The vulnerability has widespread implications due to the essential nature of the affected services.

Guidance

Strategic Intelligence

- **Policy enforcement:** Strengthen policies around UDP service exposure and IP spoofing mitigation to enhance network resilience against Loop DoS threats.
- **Industry collaboration:** Foster partnerships and intelligence-sharing within the cybersecurity community to stay informed about emerging UDP vulnerabilities and countermeasures.
- **Risk assessment:** Conduct comprehensive risk evaluations focusing on UDP-based services to prioritize security enhancements and resource allocation.

Operational Intelligence

- **Vulnerability management:** Rigorously monitor and patch identified vulnerabilities in UDP-based services, particularly those implicated in the Loop DoS attack vector.
- **Traffic analysis:** Implement advanced network monitoring tools to detect and analyze anomalous UDP traffic patterns that could signify a Loop DoS attack.
- **Incident response planning:** Develop and refine incident response

RETURN

protocols to quickly and effectively address potential Loop DoS incidents to minimize their impact.

Tactical Intelligence

- **Anomaly detection:** Deploy network anomaly detection systems to identify and alert on unusual communication loops or surges in UDP traffic.
- **Configuration controls:** Apply strict configuration management to UDP services, ensuring they are hardened against exploitation and unauthorized interactions.
- **Active monitoring:** Establish proactive monitoring for the specific behavioral signatures of a Loop DoS attack, enabling swift detection and mitigation to prevent service disruption.

Tactical Intelligence - Threat Hunting Hypotheses

- **Hypothesis:** Unexpected UDP traffic patterns

  Given the nature of the Loop DoS attack exploiting UDP protocols, an unusual increase in UDP traffic, especially with repetitive patterns between specific hosts, could indicate an ongoing or attempted Loop DoS attack. Monitoring for spikes or anomalies in UDP traffic can help identify potential exploitation attempts.
- **Hypothesis:** Anomalous inter-server communication

  If a Loop DoS attack is active within the network, there may be observable, continuous, and reciprocal communication between two or more servers that do not align with normal operational patterns. Identifying such persistent and cyclical traffic between servers could signal the presence of a Loop DoS attack.
- **Hypothesis:** Resource exhaustion without a corresponding increase in legitimate traffic

  A successful Loop DoS attack can lead to resource exhaustion on the affected servers. A noticeable degradation in server performance or availability without a corresponding increase in user-driven traffic could suggest a Loop DoS attack is exploiting the servers.
- **Hypothesis:** Presence of vulnerable services

  With the known vulnerabilities in specific UDP-based services like DNS, NTP, and TFTP, the presence and public exposure of these services could elevate the risk of a Loop DoS attack. Investigating the existence and accessibility of these services can help assess the potential threat landscape and prioritize protective measures.

Sources

- *Loop DoS: Datagram Application-Layer Denial-of-Service Attacks*
- *300,000 Servers, Devices at Risk From 'Loop' DoS Attack Technique*
- *New Loop DoS Attack May Impact Up to 300,000 Online Systems*

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

convergetp.com/cybersecurity