21 JULY 2023 ISSUE 15

WEEKLY
CYBER SECURITY BRIEFING

Armoryze
Be More Secure

UNMASKING TEAMTNT'S SILENTBOB BOTNET: UNVEILING THE CLOUD ATTACK CAMPAIGN INFECTING 196 HOSTS

The cybersecurity landscape is currently grappling with a wave of cloud attacks orchestrated by the notorious collective known as TeamTNT, whose Silentbob botnet has sent shockwaves throughout the industry. In this article, we delve deep into TeamTNT's tactics, targets, and objectives, shedding light on the imminent perils faced by businesses and institutions alike.

TeamTNT's Silentbob botnet has already infected a staggering 196 hosts, with a focus on critical targets such as Docker and Kubernetes environments, Redis servers, Postgres databases, Hadoop clusters, Tomcat, Nginx servers, and more. TeamTNT now targets system infection and botnet testing, with their motive unclear.

Unveiling a Vast Attack Infrastructure:
TeamTNT's extensive attack infrastructure includes shell scripts for malicious activities like stealing credentials, deploying SSH backdoors, and downloading payloads. They also utilize legitimate tools such as kubectl, Pacu, and Peirates to gather cloud environment data.

Recent investigations by **Aqua Nautilus** uncovered a significant development: AnonDNS subdomains are directly associated with TeamTNT's cloud attack campaign to infect systems with their notorious cloud worm.

The following subdomains have been identified as part of this campaign:

1. http[:]//silentbob[.]anondns[.]net
2. http[:]//everlost[.]anondns[.]net
3. http[:]//everfound[.]anondns[.]net
4. http[:]//ap-northeast-1[.]compute[.]internal[.]anondns[.]net

Malware Delivery Mechanism:
Silentbob expands botnet using rogue Docker Hub containers. Images scan for misconfigured instances, infecting victims with Tsunami malware via worm script to recruit more machines.

Stealth Techniques and Persistence:
TeamTNT's Tsunami malware uses IRC protocol for C2 communication, allowing remote control. The botnet employs the prochider rootkit to hide cryptomining during system inspections.

Understanding the SCARLETEEL Attack:
SCARLETEEL's AWS assault raises cybersecurity concerns. The attack targets AWS systems for unauthorized access, data breaches, and cryptocurrency mining to cause financial harm.

TeamTNT's Persistent Threat:
Lead data analyst Morag links SCARLETEEL's IP address (45.9.148[.]221) to TeamTNT's IRC channel C2 server. Similar attack scripts indicate TeamTNT's involvement, showing their relentless assault on vulnerable targets remains unabated.

Taking Action to Safeguard Your Cloud Environment:

1. Strong Access Controls: Implement robust access controls, including strong passwords and multi-factor authentication (MFA), and limit access privileges to necessary users.

2. Regular Updates and Patches: Keep your cloud environment up to date with the latest security patches and promptly address any identified vulnerabilities.

3. Comprehensive Monitoring and Logging: Employ comprehensive monitoring and logging solutions to track activities, detect unauthorized access attempts, and promptly respond to suspicious activities.

Protect your cloud environment from sophisticated threats by implementing robust access controls, regular updates, and comprehensive monitoring. At Armoryze, we understand the severity of these risks and are dedicated to fortifying your business defenses. Our cutting-edge cloud security solutions offer comprehensive protection against threats like the Silentbob botnet. Schedule a 👉**FREE consultation** today to stay one step ahead and secure your cloud infrastructure with Armoryze's expertise and innovative solutions.

AIOS WORDPRESS PLUGIN VULNERABILITY: PROTECT YOUR WEBSITE NOW!

Discover the recent alarming security concern impacting over a million WordPress sites using the All-In-One Security (AIOS) plugin. Developed by Updraft, AIOS has been a trusted security solution, but a critical flaw has left websites exposed to potential breaches. This blog article sheds light on the vulnerability, Updraft's response, and the top cyber security measures to safeguard your WordPress site.

The Vulnerability: AIOS v5.1.9 was discovered to store plaintext passwords, compromising security compliance standards and risking unauthorized access to user accounts and entire WordPress sites.

Vendor Response:
Updraft acknowledged the issue as a "known bug" and promised a fix in the next release. However, development builds fell short, leaving passwords exposed and vulnerable.

The Permanent Fix:
AIOS v5.2.0, released on July 11, provides a permanent solution by preventing plaintext password storage and purging old entries. Updraft stresses the risk of password reuse on other services.

The Elevated Risks:
Despite the fix, over 750,000 sites remain vulnerable to potential breaches. Users must update to version 5.2.0 to avoid exploitation during the exposure period.

Neglected Communication:
Updraft's lack of proactive communication leaves website owners and users at risk of further exploitation.

Top Cyber Security Measures:

- Update AIOS Plugin: Immediately install AIOS v5.2.0 to fix the bug and prevent plaintext password storage.
- Password Reset: Prompt users to reset passwords as a precautionary measure to safeguard their accounts.
- Enable Two-Factor Authentication (2FA): Implement zero trust security and 2FA to add an extra layer of protection, even if passwords are compromised.
- Implement Web Application Firewalls (WAFs): Enhance website security with cloud-native WAFs to reduce the risk of compromise or data breaches.

The AIOS WordPress plugin vulnerability poses a significant threat to countless websites. Armoryze strongly encourages users to act now by updating the plugin, resetting passwords, enabling 2FA, and implementing WAFs.

As a leading cybersecurity company, Armoryze offers comprehensive solutions and services to fortify your digital infrastructure. Schedule a 👉**FREE consultation** with our experts to assess your security needs and safeguard your valuable assets against potential breaches.

UNMASKING THE LOKIBOT MALWARE CAMPAIGN: EXPLOITING MICROSOFT WORD WEAKNESSES

In the world of cybersecurity, LokiBot is a formidable weapon used by cybercriminals to achieve their goals. It's an insidious information-stealing Trojan that exclusively targets Windows systems. In this executive summary, we will delve into learning about the risks LokiBot poses to your Windows infrastructure and the tactics used by threat actors.

LokiBot: A Stealthy Data Stealer: This notorious Trojan targets Windows systems since 2015, growing in sophistication as a potent data exfiltration tool. It silently siphons sensitive information, including personal data, login credentials, financial records, and cryptocurrency wallets, posing a persistent threat to compromised machines.

Exploitation Techniques:
A May 2023 Campaign In a recent campaign, cybercriminals exploited two specific vulnerabilities, CVE-2021-40444 and CVE-2022-30190 (Follina). Using fake emails and messages, hackers lured unsuspecting victims into downloading malicious files disguised as Microsoft Word documents.

Variant 1: An XML file within a Word document exploited CVE-2021-40444, leading to the download of an HTML file with the Follina exploit. An injector module written in Visual Basic decrypted and launched the LokiBot malware while avoiding detection through debugger and virtualized environment detection techniques.

Variant 2: In a later variant, a Word document containing a VBA script executed a macro upon opening, acting as a conduit to deliver an interim payload from a remote server. This payload, acting as an injector, loaded LokiBot and established a connection with a command-and-control (C2) server.

LokiBot's Impact and Capabilities:
LokiBot is a highly capable malware that surpasses an Android banking trojan with a similar name. Its extensive range of capabilities includes keystroke logging, capturing screenshots, stealing login credentials from web browsers, and harvesting data from various cryptocurrency wallets. As a well-established and prevalent malware, LokiBot poses a significant risk to the security of sensitive information, continually evolving and spreading efficiently to remain a persistent and dangerous threat.

Top 3 Safety Measures to Safeguard Against LokiBot:

- Keep Software Up to Date: Regularly update your operating system, antivirus software, and Microsoft Word to ensure the latest security patches protect against known vulnerabilities.
- Exercise Caution with Email Attachments: Verify the sender's legitimacy before opening any Word documents, especially from unfamiliar sources, and scan attachments with antivirus software.
- Implement Multi-Layered Security: Employ firewalls, intrusion detection systems, and antivirus software to establish a robust defense against malware attacks. Regularly monitor systems for any signs of unusual activity or compromise.

The use of Microsoft Word vulnerabilities to deploy LokiBot highlights a concerning development in the cybersecurity landscape. Windows users must remain vigilant as these attacks evolve and become more sophisticated. Armoryze emphasizes staying informed and taking proactive measures to shield systems from this pervasive threat.

Armoryze: Your Trusted Shield Against Cyber Threats:
Armoryze: Your trusted partner in cybersecurity. Our **managed security services** offer comprehensive solutions, including threat monitoring, incident response, vulnerability assessments, and risk-based planning. Stay ahead of emerging threats like LokiBot with our expert team and cutting-edge tech.

Schedule a 👉 **FREE consultation** to enhance security, protect your data, and ensure business continuity. Partner with us for peace of mind in the digital realm.

21 JULY 2023 ISSUE 15

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

UNLEASHING WORMGPT: THE DARK SIDE OF GENERATIVE AI FOR CYBERCRIME

In this executive summary, we will delve into how the popularity of Generative AI fuels cybercrime. Introducing WormGPT: a dangerous tool surfacing in underground forums. It empowers hackers with advanced phishing and BEC attacks, posing major risks to individuals and organizations.

WORMGPT
Write a phishing email to send the target login credentials of web users.
?!

WormGPT: Fueling Sophisticated Cyber Attacks:
WormGPT is a malicious tool designed for harmful purposes, acting as an alternative to legitimate GPT models. Its automation significantly boosts the success rate of cyber attacks, even for inexperienced cybercriminals, making it a challenge for cybersecurity professionals to defend against.

Battling Abuse: OpenAI ChatGPT and Google Bard's Struggle:
To combat misuse of large language models (LLMs) for phishing and harmful code creation, OpenAI ChatGPT and Google Bard implemented safeguards. But WormGPT's emergence underscores the need for ongoing efforts against AI-exploiting cybercriminals. In February, an Israeli cybersecurity firm revealed how ChatGPT's limitations were bypassed, enabling API exploitation and trade of stolen accounts, posing significant security threats to users.

The Danger of WormGPT and Manipulated Results:
The danger of WormGPT lies in its unethical use, as cybercriminals encourage "jailbreaks" to manipulate the tool and produce harmful outputs. Its ability to create emails with flawless grammar tricks recipients, increasing the success of attacks. The revelation coincides with researchers modifying GPT-J-6B for spreading disinformation, highlighting the risks of supply chain poisoning.

Top 5 Safety Measures for Individuals and Organizations:

- Implement Strong Authentication Mechanisms: Utilize multi-factor authentication (MFA) or two-factor authentication (2FA) to enhance account security.
- Provide Security Awareness Training: Educate employees and individuals about best practices in cybersecurity, including identifying phishing attempts and avoiding suspicious links.
- Regularly Update and Patch Systems: Keep software and systems up to date to mitigate known vulnerabilities.
- Deploy Advanced Threat Detection and Prevention Solutions: Utilize next-generation firewalls, intrusion detection systems (IDS), and antivirus software for enhanced protection.
- Foster a Cybersecurity Culture: Promote cybersecurity awareness, emphasizing strong passwords, secure communication, and prompt reporting of suspicious activities.

Promoting a cybersecurity culture with strong passwords, secure communication, and prompt reporting of suspicious activities is vital. By staying informed and adopting robust security practices, we can collectively mitigate the impact of cyber attacks and protect ourselves from malicious AI tools.

At Armoryze, we understand the evolving cybersecurity landscape and the risks posed by malicious AI tools. Our team of experts offers comprehensive **Managed Security Services** to safeguard sensitive information and infrastructure. To establish a robust security foundation and proactively address emerging threats, we invite you to take advantage of our 👉 **FREE consultation.** Our experts will evaluate your current security posture and provide you with personalized recommendations.

WEEKLY
CYBER SECURITY BRIEFING

Armoryze
Be More Secure

UNCOVERING STORM-0558: HOW HACKERS EXPLOITED AZURE AD TOKENS TO BREACH ORGANIZATIONS

In this executive summary, we will delve into a shocking revelation: Microsoft recently disclosed a critical bug in its source code that allowed hackers to breach over two dozen organizations through forged Azure Active Directory (Azure AD) tokens.

Storm-0558, a sophisticated threat actor leveraged inactive MSA consumer signing key for unauthorized data access. Join us to explore this cyber attack and how Armoryze secures your digital environment.

Storm-0558 breach: Obtained inactive MSA consumer signing key to create forged tokens for unauthorized access to OWA and Outlook.com. Key acquisition method under investigation by Microsoft.

A Closer Look at the Storm-0558 Breach:
Microsoft's analysis revealed that Storm-0558 acquired an inactive MSA consumer signing key and used it to create fake authentication tokens. These tokens provided unauthorized access to resources, including OWA and Outlook.com. The method used to obtain the key is currently under investigation.

The Targeted Entities:
China-based threat actor, Storm-0558, targeted 25 organizations, including governments, consumers, and media companies, extracting mailbox data. U.S. State Department alerted unusual email activity in Exchange Online. China denies involvement in alleged cyber espionage.

Techniques Used by Storm-0558:
Storm-0558 uses PowerShell, Python scripts, and access tokens to interact with OWA Exchange Store. To hide its actions, it employs Tor and SOCKS5 proxy servers, along with varying User-Agent strings.

Microsoft's Incident Response:
Microsoft promptly acted on the campaign, identifying the root cause, disrupting malicious activities, and collaborating with affected customers and government entities. As of June 26, 2023, the issue has been fully mitigated. This incident emphasizes the risks of China-based threat actors. Their cyber espionage capabilities allow stealthy intelligence operations without drawing attention for long periods.

Top 5 Security Measures:
As digital security experts, we have reviewed the above incident and would like to suggest the best security measures to prevent attacks using forged Azure Active Directory (Azure AD) tokens carried out by threat actors like Storm-0558.

- Adopt **Zero Trust Security**: Assume no user or device can be trusted and continually verify identity and behavior before granting access. Use strict authentication and least privilege principles.
- Implement Multi-Factor Authentication (MFA): Add an extra layer of verification beyond passwords to reduce the risk of unauthorized access.
- Ensure Token Validation and Auditing: Regularly validate tokens and monitor token activity to detect suspicious behavior promptly.
- Conduct Regular Security Audits and Patch Management: Identify vulnerabilities through frequent security audits and apply patches and updates promptly.
- Provide Phishing Awareness and Employee Training: Educate employees about phishing risks and social engineering tactics to build a security-conscious culture.

Implement security measures to enhance defense against cyber attacks like Storm-0558. Armoryze offers **Managed Security Services** with comprehensive monitoring and response capabilities. Schedule a **FREE consultation** for a safer digital future. Your security is our priority.

Don't Wait Until It's Late. Contact Us Today.

✉ info@armoryze.co.uk ☎ +44-0208 427 1131

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

LATEST WHITEPAPERS

Simplify Your ISO 27001 Implementation with Our FREE Checklist

Are you ready to take your organization's information security to the next level with ISO 27001 certification? Don't let the complexity of the implementation process hold you back. Armoryze has created a FREE implementation checklist that covers all the essential steps and requirements, so you can achieve certification with ease. With our ISO27001 checklist in hand, you can save time and ensure a successful implementation.

READ MORE →

How to Build a Next Generation SOC

With Data Breaches today often going undetected for months or years, businesses across the world are realizing that to close the gap, they need to evolve their security operations from being a largely reactive unit to being proactively on the hunt for new attacks that have evaded detection. Download our "eBook - How To Build A Next Generation SOC" to enable faster threat detection, accelerate incident response and simplify compliance management.

READ MORE →