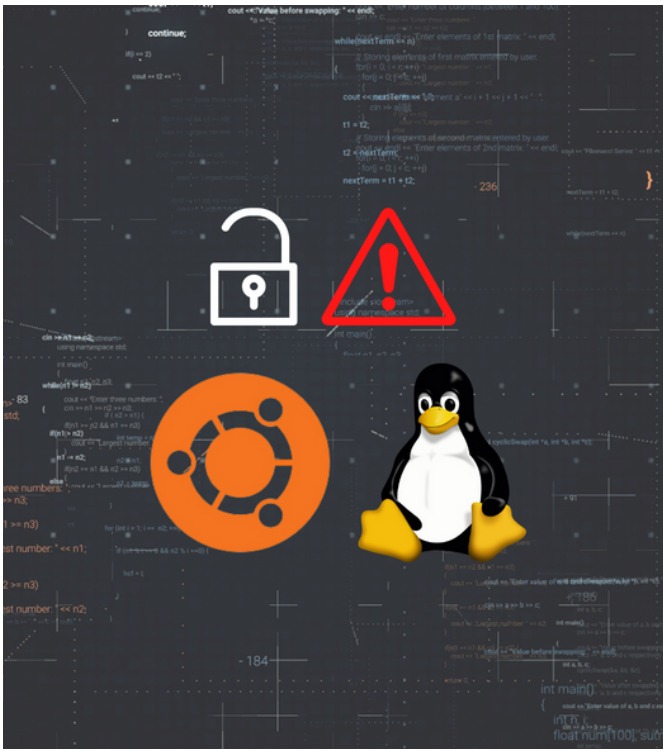
WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

GAMEOVER(LAY): UNVEILING UBUNTU LINUX'S VULNERABILITIES IMPACTING 40% OF CLOUD WORKLOADS

In today's digital world, cybersecurity is vital to protect virtual assets. "GameOver(lay)" in Ubuntu Linux involves two vulnerabilities (CVE-2023-2640 and CVE-2023-32629) discovered by the Wiz security team in OverlayFS. Armoryze's risk-based vulnerability management service enhances security by identifying and prioritizing potential vulnerabilities, safeguarding valuable assets.



GameOver(lay) CVEs:

1. CVE-2023-2640: On Ubuntu kernels with c914c0e27eb0 and "UBUNTU: SAUCE: overlayfs: Skip permission checking for trusted.overlayfs.* xattrs," an unprivileged user can set privileged extended attributes on mounted files without proper security checks.

2. CVE-2023-32629: Local privilege escalation vulnerability in Ubuntu Kernels' overlayfs ovl_copy_up_meta_inode_data skips permission checks when calling ovl_do_setxattr.

A Closer Look at OverlayFS: OverlayFS is a filesystem allowing one filesystem to be placed on top of another without altering the original. It's beneficial for container setups, preserving the base image while enabling easy changes. However, this flexibility attracts hackers, creating a potential entry point for attacks.

GameOver(lay) exploits long-standing vulnerabilities in OverlayFS, allowing attackers to reuse old, well-known tricks. Changes made to the OverlayFS module in Ubuntu in 2018 seemed harmless initially, but subsequent Linux modifications led to unforeseen consequences and the discovery of critical vulnerabilities.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Who is vulnerable?
Vulnerable parties are challenging to identify due to numerous Ubuntu releases. Our research team has pinpointed the impacted versions as follows:

Release	Version	CVE-2023-2640	CVE-2023-32629
Ubuntu 23.04 (Lunar Lobster)			
	6.2.0	✔	✔
Ubuntu 22.10 (Kinetic Kudu)			
	5.19.0	✔	✔
Ubuntu 22.04 LTS (Jammy Jellyfish)			
	5.19.0	✔	✔
	6.2.0	✔	✔
	5.15.0	✗	✗
Ubuntu 20.04 LTS (Focal Fossa)			
	5.15.0	✗	✗
	5.4.0	✗	✔
Ubuntu 18.04 LTS (Bionic Beaver)			
	5.4.0	✗	✔

Vulnerability Detection & Mitigation Strategies:
To protect against these vulnerabilities, take two key steps: establish a user namespace and an OverlayFS mount. This makes remote attacks unlikely as attackers need to execute code on the targeted system.
For safety, Ubuntu users should upgrade to fixed versions of impacted kernels (see the list above).
Alternatively, limit user namespace usage to restricted privilege users to prevent exploitation:

- Use: sudo sysctl -w kernel.unprivileged_userns_clone=0
- For persistent protection after system restart: echo kernel.unprivileged_userns_clone=0 | sudo tee /etc/sysctl.d/99-disable-unpriv-userns.conf

GameOver(lay) reminds us that even the most trusted and widely-used software can be vulnerable, emphasizing the need for continuous monitoring and proactive measures. Upgrading to fixed versions, implementing user namespace restrictions, and leveraging advanced **vulnerability management services** are essential steps in mitigating risks effectively. Schedule a **FREE consultation** today!

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

CISA ALERT: SUBMARINE MALWARE STRIKES BARRACUDA ESG APPLIANCES - WHAT YOU NEED TO KNOW

In response to a recent alert from the Cybersecurity and Infrastructure Security Agency (CISA) regarding the emergence of the dangerous "Submarine" malware, Armoryze, a leading cyber security company, stresses the significance of proactive measures to protect against cyber threats. The malware exploits a new vulnerability **(CVE-2023-2868)** in Barracuda ESG appliances, enabling undetected data-theft attacks.

Armoryze's **Risk-Based Vulnerability Management Service** ensures comprehensive protection against exploits, fortifying organizations' defenses and preventing unauthorized system access..

The Attack Timeline: The attack timeline shows that the exploitation of the vulnerability dates back to October 2022, and the attackers utilized various malware components, including Submarine, Saltwater, SeaSpy, and SeaSide, to gain remote access to the affected systems.

Key Findings:

- The vulnerability was specific to the Barracuda Email Security Gateway (appliance form factor only) versions 5.1.3.001-9.2.0.006.
- The earliest evidence of exploitation dates back to October 2022.
- The attackers used the CVE-2023-2868 vulnerability to gain unauthorized access to a subset of ESG appliances.
- The attackers planted the Saltwater and SeaSpy malware for persistent access and data exfiltration.

Response from Barracuda: Barracuda responded proactively to the attacks, providing replacement devices to affected customers at no charge. However, the attackers introduced a new malware strain, Submarine, to maintain persistent access.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Details about Submarine Malware: Submarine: A sophisticated backdoor operating within the ESG appliance's SQL database. Enables high-level access, stays hidden, manages commands, and exfiltrates sensitive information via MIME attachments.

Details of Malware Components:
1. Saltwater: Stealthy malware posing as Barracuda SMTP server. Allows hackers to control the system, execute commands, and act as a proxy for file transfers.

2. SeaSpy: Hidden malware impersonating Barracuda service. Monitors SMTP traffic, enabling attackers to seize control with a "magic packet."

3. SeaSide: Lua-based malware camouflaged as Barracuda SMTP. Monitors email commands for hidden instructions, establishing a "reverse shell" for unauthorized access.

Advice for Affected Customers:
If you suspect your Barracuda ESG appliance has been compromised, it's essential to discontinue its use and seek assistance from Barracuda support. They recommend obtaining a new ESG virtual or hardware appliance to replace the compromised one.

Security Recommendations:
1. Keep antivirus signatures and engines up-to-date.
2. Maintain the latest operating system patches.
3. Disable File and Printer sharing services, use strong passwords or Active Directory authentication if needed.
4. Restrict user permissions for installing unwanted software; avoid adding users to the local administrators group unnecessarily.
5. Implement a strong password policy with regular changes.
6. Exercise caution with email attachments, even from known senders.
7. Enable personal firewalls on workstations, denying unsolicited connection requests.
8. Disable unnecessary services on workstations and servers.
9. Scan and remove suspicious email attachments, ensuring their true file type matches the extension.
10. Monitor users' web browsing and restrict access to unfavorable content.

Stay Ahead of Cyber Threats with Armoryze! The Submarine malware's exploit of CVE-2023-2868 underscores the need for proactive cybersecurity. Partner with us for **Managed Security services** to safeguard your business. Schedule your **FREE consultation** now and fortify your cybersecurity defenses. Your business's protection is our priority!

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

UNVEILING THE ELUSIVE APT31: CHINA-LINKED HACKERS TARGET AIR-GAPPED SYSTEMS

In today's ever-changing cybersecurity landscape, the activities of one nation-state actor have garnered significant attention from the cybersecurity community. APT31, also known as Bronze Vinewood, Judgement Panda, and Violet Typhoon, is suspected to have ties to China and has orchestrated a series of sophisticated attacks on industrial organizations in Eastern Europe.

Their primary objective: extracting valuable data from air-gapped systems. In this article, we will delve into the tactics employed by APT31, explore their diverse range of implants, and provide valuable insights on how Armoryze MDR can effectively safeguard your organization against these advanced threats.

APT31's Intrusions: A Closer Look

APT31 has demonstrated remarkable versatility, employing a variety of tools categorized into three distinct stages:

1. First-Stage Tools: These clandestine tools are meticulously crafted to enter targeted systems covertly and collect initial data, all while staying undetected.
2. Second-Stage Tools: At the heart of their operation, the second-stage tools are responsible for collecting data and files from even the most isolated systems, disconnected from the internet.
3. Third-Stage Tools: Once the data is acquired, APT31 utilizes third-stage tools to transmit the stolen information to their control center, executing their insidious operation with precision.

Kaspersky has uncovered 15 distinct implants used by APT31, categorized into those establishing remote access, collecting sensitive data, and transmitting pilfered information. Particularly concerning is a modular malware capable of data exfiltration from isolated air-gapped networks.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

Unveiling the APT31 Backdoors:
1. Meatball Backdoor: Among the newly discovered backdoors, Meatball stands out with its extensive remote access capabilities, tailored for both x86 and x64 systems. This versatile backdoor executes a plethora of tasks, including listing processes, devices, and disks, performing file operations, capturing screenshots, utilizing remote shells, and even self-updating. To further its control, Meatball creates a service named "esetcss" or adds itself to the registry key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\esetcss," ensuring automatic execution during OS startup.

2. FourteenHi Backdoor: A formidable malware family identified during the ExCone campaign, FourteenHi targets government entities and industrial organizations alike. Its sophisticated features encompass file manipulation, command execution, reverse shells, and self-erasure, making it a potent weapon in the hands of APT31.

Expanding Horizons: Linux Infiltration: Recent evidence suggests APT31's growing interest in Linux systems, employing the Rekoobe backdoor for attacks on South Korean companies, evading detection through encryption.

Defense Against APT31 with Armoryze MDR:
1. Continuous Monitoring: Armoryze MDR provides 24/7 network monitoring, swiftly identifying any suspicious activity.
2. Advanced Threat Detection: Our state-of-the-art threat detection technologies can pinpoint encrypted payloads, memory injections, and DLL hijacking techniques, ensuring early detection of APT31's presence.
3. Expert Incident Response: In the event of an attack, our seasoned incident response team takes immediate action to mitigate the impact and restore your systems.
4. Cloud Security: Armoryze MDR is equipped to safeguard your cloud infrastructure, thwarting threats like data exfiltration through cloud services.

As APT31 poses multifaceted intrusions on air-gapped systems in Eastern Europe, **Armoryze MDR** is committed to safeguarding organizations from this threat and other advanced adversaries. Their proactive and robust security solutions help protect critical assets, ensure business continuity, and fortify an organization's reputation in the face of ever-evolving cyber threats.

Contact Armoryze MDR today to build a secure and resilient future for your organization.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

UNMASKING THE THREAT: URGENT ADVISORY ON SECOND ZERO-DAY VULNERABILITY IN IVANTI EPMM

In today's rapidly evolving digital landscape, cybersecurity remains a paramount concern for organizations worldwide. In response to recent events, Ivanti, a leading IT software company, has acted swiftly by issuing an urgent **warning** to its customers regarding a second zero-day vulnerability discovered in its widely-used product, Endpoint Manager Mobile (EPMM).

This critical flaw, already exploited in targeted attacks, has sent shockwaves through the cybersecurity community, emphasizing the significance of being vigilant and proactive in defending against potential threats. Safeguarding digital assets and protecting sensitive information are now critical imperatives for businesses.

A New Zero-Day Threat:
On July 24, 2023, Norwegian authorities disclosed that numerous government ministries fell victim to a cyberattack exploiting zero-day vulnerabilities in Ivanti's EPMM.

- **CVE-2023-35078:** An authentication bypass vulnerability in Ivanti EPMM allows unauthorized users to access restricted functionality or resources of the application without proper authentication. This zero-day flaw enables an unauthenticated attacker to access sensitive information and manipulate impacted servers. CVSS 10 (Critical severity).

- **CVE-2023-35081:** Researchers from the cybersecurity firm Mnemonic discovered a high-severity flaw, allowing an authenticated attacker with administrator privileges to remotely write arbitrary files to the server. The CVSS score of 7.2 indicates the severity level as high.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

The Dangers of Remote File Write Vulnerabilities:
Remote File Write (RFW) vulnerabilities pose grave risks to system security. Attackers can exploit these loopholes to create, modify, or delete files on a victim's system from a remote location, potentially leading to data breaches and complete system takeovers.

The Combined Exploitation:
Threat actors combine CVE-2023-35081 and CVE-2023-35078, bypassing admin authentication and ACL restrictions, executing malicious OS commands as the tomcat user. The attacks' sophistication hints at a possible state-sponsored threat, though the attackers' identity remains uncertain.

The Urgent Need for Action:
If you are an Ivanti Endpoint Manager Mobile (EPMM) user, regardless of the version, you are at risk. The impacted versions include 11.4 releases 11.10, 11.9, and 11.8, as well as older releases. The severity of these vulnerabilities has led Ivanti and CISA to issue alerts, urgently advising organizations to apply patches immediately.

To safeguard your systems against the latest zero-day exploits, follow these steps:

1. Update your Ivanti EPMM software to the latest version available.
2. Apply all relevant patches provided by Ivanti as soon as possible.

The attackers are unidentified, but evidence suggests possible state-sponsored actors. With numerous vulnerable internet-exposed systems and PoC code available for CVE-2023-35078, the risk of further exploitation is significant.

As a leading cybersecurity company, Armoryze is dedicated to safeguarding businesses from such threats. We understand the importance of **risk-based vulnerability management** and offer a comprehensive service tailored to your organization's needs. By scheduling a **FREE consultation** with our experts, you can take the first step towards securing your systems against the latest zero-day exploits.

The second zero-day in Ivanti EPMM underscores the evolving cybersecurity landscape. Stay vigilant and proactive. Armoryze can help protect your digital assets. Act now and schedule a FREE consultation to strengthen your defenses against cyber threats.

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

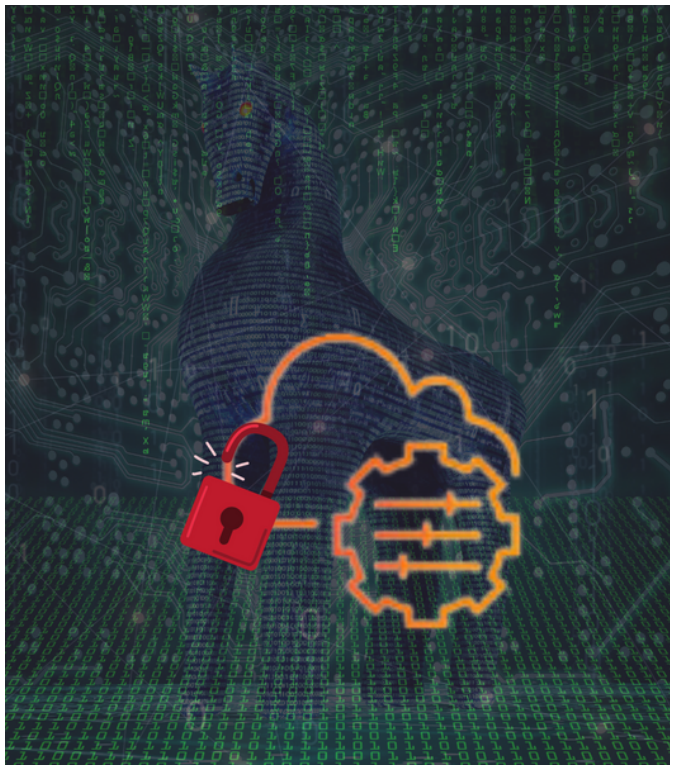
info@armoryze.co.uk +44-0208 427 1131

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

UNVEILING THE NEW THREAT LANDSCAPE: AWS SSM AGENT MISUSE AS A COVERT REMOTE ACCESS TROJAN

In an era where digital transformation is driving businesses to adopt cloud technologies, the security of cloud environments has become a paramount concern. Cyber security researchers at Mitiga have uncovered a disruptive new threat landscape, shaking the foundation of Amazon Web Services (AWS). In a startling revelation, they have exposed how malicious actors can exploit the AWS Systems Manager Agent (SSM Agent) as a Remote Access Trojan (RAT) on both Linux and Windows environments.



This ingenious technique enables attackers to gain covert control over endpoints, evading traditional security measures and laying the groundwork for a range of malicious activities.

A Stealthy Threat Unveiled: The AWS SSM Agent as a RAT:
Our groundbreaking research reveals how threat actors with elevated privilege access on a compromised endpoint can covertly transform the SSM Agent into a silent Remote Access Trojan (RAT). This enables undetected, persistent access, and facilitates various malicious activities on the compromised system.

Key Advantages for Attackers:

1. Camouflaged Legitimacy: The SSM Agent binary is signed by Amazon, deceiving Antivirus (AV) and Endpoint Detection & Response (EDR) solutions into viewing it as approved software, thus evading immediate detection.
2. No Additional Malware Deployment: Attackers can exploit the existing SSM Agent on the target system, eliminating the need to upload and execute new RAT binaries that may trigger security alarms.
3. Command and Control Flexibility: Adversaries can use their malicious AWS account as a Command and Control (C&C) server, making their communication appear genuine and harder to trace.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

4. Minimal Infrastructure Requirements: Attackers can rely solely on the SSM service and agent, reducing the need for elaborate attack infrastructure.
5. Broad Control over Endpoints: Features like "RunCommand" and "StartSession" in the SSM Agent provide attackers with effortless control over compromised endpoints, granting extensive operational authority.

Attacker Techniques:

1. Scenario 1: SSM Agent Hijacking: Attackers register the SSM Agent in "hybrid" mode with a different AWS account, disguising it as a legitimate process to avoid detection.
2. Scenario 2: Running Additional SSM Agent Process: Threat actors launch a second SSM Agent process to communicate with their account, maintaining control over the compromised endpoint without disrupting the original agent's function.
3. Abusing SSM Proxy Feature: By manipulating environment variables, attackers route SSM traffic to their server, evading AWS infrastructure detection while leveraging the SSM Agent.

Detection and Recommendations:
To defend against this emerging threat, organizations are advised to implement several proactive cybersecurity strategies:

1. **AV and EDR Solutions:** Remove SSM Agent binaries from the allow list to enhance detection capabilities and analyze potential malicious activities.
2. Implement Detection Techniques: Monitor instance data changes, track multiple agent processes, and review CloudTrail logs to detect suspicious actions.
3. Restrict Command Receipt: Use the VPC endpoint for Systems Manager to ensure EC2 instances only respond to commands from the original AWS account or organization.
4. **SIEM and SOAR Integration:** Integrate detection techniques into Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms for proactive threat hunting.

The misuse of AWS SSM Agent as a Remote Access Trojan poses a significant threat to cloud-era endpoint security. **Armoryze's MDR service** empowers businesses with 24/7 monitoring and incident response, ensuring resilience against emerging threats.

Embrace security today to stay ahead of evolving cyber threats. **Contact us** to secure your cloud environment.

WEEKLY CYBER SECURITY BRIEFING

Armoryze
Be More Secure

CHECKOUT OUR 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