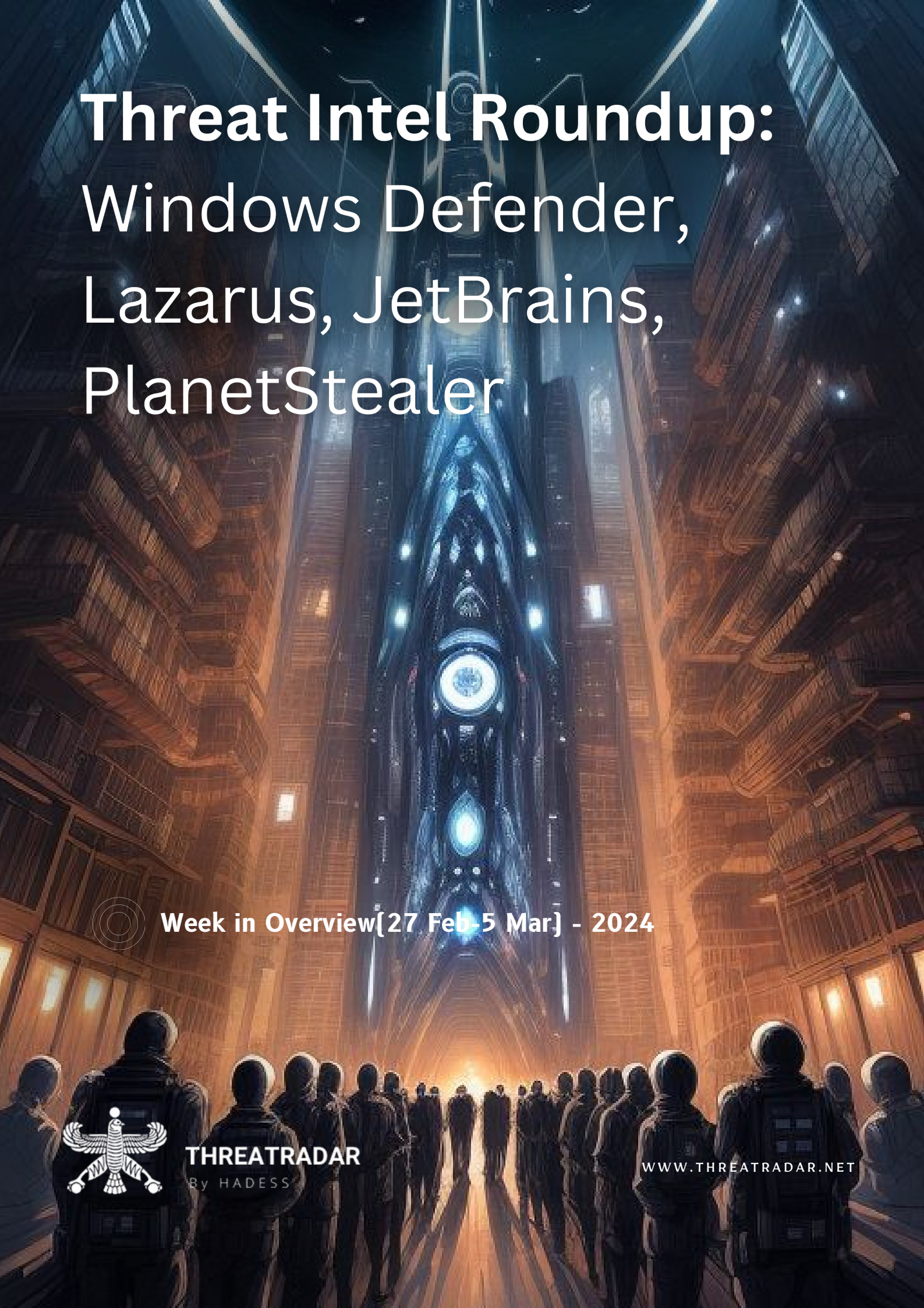


Threat Intel Roundup: Windows Defender, Lazarus, JetBrains, PlanetStealer

Week in Overview{27 Feb-5 Mar} - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **Analysis and Evasion of Windows Defender Detection for Shellcode Loaders:**
   - Focus: Evaluation of techniques for evading Windows Defender detection in shellcode loaders.
   - Methodology: Retrospective analysis of older evasion techniques and their effectiveness against modern antivirus solutions.
   - Findings: Mixed results in replicating traditional evasion techniques, highlighting the challenge of evolving antivirus technologies.
2. **Zero-Day Exploitation of Windows AppLocker Driver (CVE-2024-21338) by Lazarus Group:**
   - Focus: Disclosure of a zero-day vulnerability (CVE-2024-21338) exploited by the Lazarus Group in the Windows AppLocker driver.
   - Impact: Allows elevated privileges and bypass of application whitelisting controls, posing significant risks to affected systems.
3. **Ongoing Phishing Campaign Exploiting Telegram Bot and Cloudflare Workers:**
   - Focus: Identification of a phishing campaign utilizing Telegram bots and Cloudflare Workers to steal credentials.
   - Techniques: Crafting phishing pages, exfiltrating data via Telegram, and hosting on Cloudflare Workers.
   - Recommendations: Vigilance in verifying URL legitimacy and proactive steps to safeguard against phishing attempts.

4. **Critical Vulnerability in Linksys E2000 Router (CVE-2024-27497):**
   - Focus: Disclosure of a critical vulnerability (CVE-2024-27497) in the Linksys E2000 router firmware.
   - Impact: Allows unauthorized access and potential data theft or compromise of connected devices.
   - Mitigation: Prompt application of security patches and updates to mitigate the risk of exploitation.
5. **Vulnerabilities in JetBrains TeamCity CI/CD Server:**
   - Focus: Identification of vulnerabilities affecting JetBrains TeamCity CI/CD server.
   - Impact: Allows for potential unauthorized access or system compromise.
   - Remediation: Urgent upgrading to patched versions recommended to address identified vulnerabilities.
6. **New #PlanetStealer Malware Threat:**
   - Focus: Discovery of a new malware threat named #PlanetStealer, written in Golang.
   - Characteristics: UPX-packed, XOR string encryption, communication with C2 server, exfiltration of data.
   - Recommendations: Implement robust endpoint protection and network monitoring to detect and prevent infection.

Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- Analysis and Evasion of Windows Defender Detection for Shellcode Loaders
- Zero-Day Exploitation of Windows AppLocker Driver (CVE-2024-21338) by Lazarus Group
- Ongoing Phishing Campaign Exploiting Telegram Bot and Cloudflare Workers
- Critical Vulnerability in Linksys E2000 Router (CVE-2024-27497)
- Vulnerabilities in JetBrains TeamCity CI/CD Server
- New #PlanetStealer Malware Threat

🚨 Vulnerability of the Week

TeamCity CVE-2024-27198

In February 2024, Rapid7's vulnerability research team discovered two critical vulnerabilities affecting JetBrains TeamCity CI/CD server. These vulnerabilities, identified as CVE-2024-27198 and CVE-2024-27199, pose significant security risks to organizations utilizing TeamCity for their continuous integration and delivery processes.

Vulnerability Details:

1. **CVE-2024-27198 (CVSS 9.8 - Critical):** This vulnerability is an authentication bypass issue within the web component of TeamCity, stemming from an alternative path flaw (CWE-288). It permits a remote unauthenticated attacker to completely compromise a vulnerable TeamCity server, potentially leading to unauthenticated remote code execution (RCE) and full control over projects, builds, agents, and artifacts.
2. **CVE-2024-27199 (CVSS 7.3 - High):** The second vulnerability is also an authentication bypass flaw in the web component of TeamCity, resulting from a path traversal issue (CWE-22). Although not as severe as CVE-2024-27198, it allows for limited information disclosure and system modification. An unauthenticated attacker could replace the HTTPS certificate on a vulnerable TeamCity server with a malicious certificate, potentially facilitating further attacks.

Impact: Exploitation of these vulnerabilities could lead to severe consequences, including unauthorized access to sensitive information, manipulation of system configurations, and even the execution of arbitrary code on affected servers. Additionally, compromised TeamCity servers could serve as entry points for supply chain attacks, jeopardizing the integrity of software development pipelines.

Remediation: JetBrains responded promptly to these vulnerabilities by releasing TeamCity 2023.11.4 on March 3, 2024, which addresses both CVE-2024-27198 and CVE-2024-27199. Rapid7 strongly advises all TeamCity users to upgrade to the latest patched version immediately, regardless of their regular patch cycle. Failure to do so could leave systems vulnerable to exploitation.
For detailed instructions on upgrading to the patched version, please refer to the JetBrains release blog. Additionally, Rapid7 has provided sample indicators of compromise (IOCs) to assist in identifying potentially compromised systems.

https://twitter.com/stephenfewer/status/1764733774279872699

😰 Malware or Ransomware

https://twitter.com/RussianPanda9xx/status/1764855507137749439

A new variant of the #PlanetStealer malware has been identified, this time written in Golang. It employs sophisticated techniques to infiltrate systems and exfiltrate sensitive data, posing a significant security threat to organizations and individuals alike.

Key Characteristics:

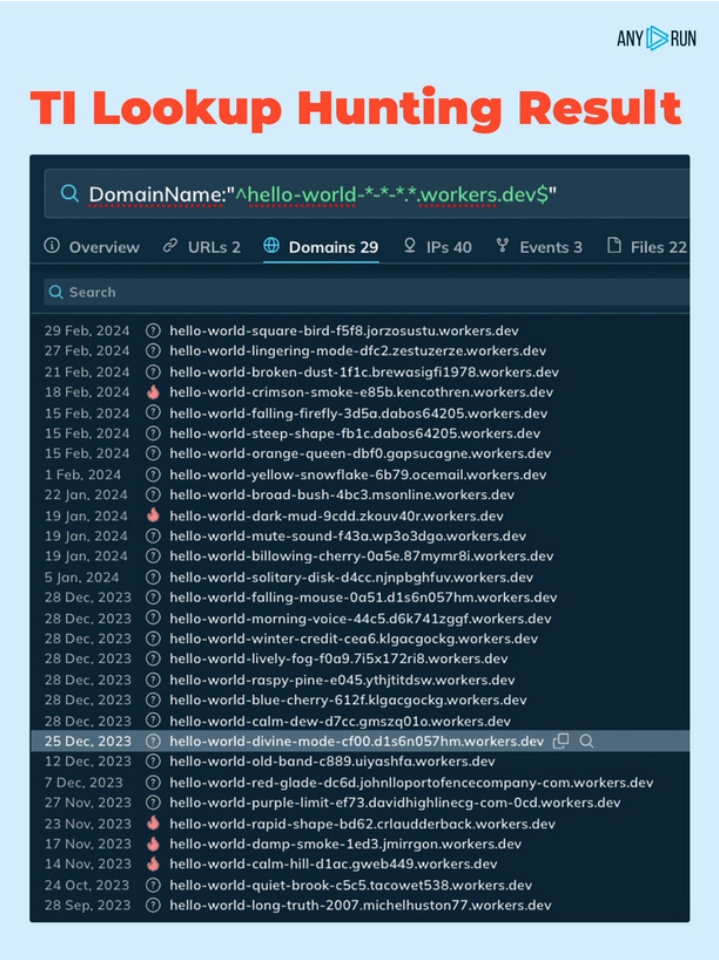
- **Packaging and Encryption:** The malware is UPX-packed and utilizes simple XOR string encryption, likely to evade detection and analysis.
- **Command and Control (C2) Communication:** Upon successful infiltration, the malware establishes communication with a C2 server located at 193.178.170[.]30. It sends exfiltrated data via POST requests to specific endpoints:
  - **/submit/info**: Sends initial information, including bot ID, builder ID, and user information.
  - **/submit/file**: Transmits a ZIP archive containing collected data.

- **Indicators of Compromise (IOCs):**
  - File creations under the %TEMP% folder, such as:
    - **Cookies\chrome-default.txt**
    - **system.txt**
    - SQLite files (e.g., **qEyjW2Mb.dat**)

for the sandbox analysis:

- https://app.any.run/tasks/b47a121d-02c7-4ceb-9a18-198201d0b9dc/#
- https://app.any.run/tasks/a55c931e-99d7-4b32-8672-2b5733ae3dd4/

Art of Detection



https://twitter.com/anyrun_app/status/1764640774787047838

An ongoing phishing campaign has been identified, leveraging Telegram bots and pages hosted on Cloudflare Workers to steal credentials from unsuspecting victims. The attackers craft sophisticated phishing pages using various elements to mimic legitimate login interfaces and lure users into disclosing sensitive information.

Phishing Pages: The phishing pages are crafted using https://www.html-code-generator[.]com and contain the following components:

- Base64 background images
- Design elements from Microsoft resources
- JavaScript code for functionality
- Communication with a Telegram bot
- A redirect to a legitimate-looking website, such as outlook[.]com

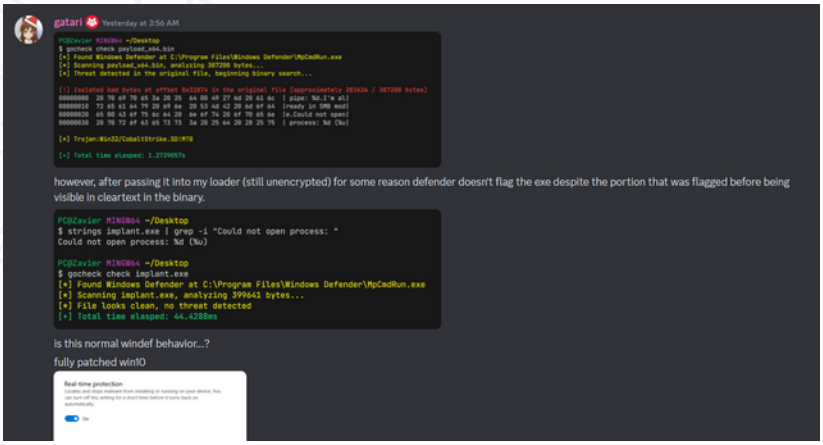
Cloudflare Workers Hosting: The attackers utilize https://workers.cloudflare.com to host these phishing pages, adding malicious content and additional functionality to enhance their effectiveness.

Telegram Exfiltration: Stolen credentials are exfiltrated via a Telegram bot using HTTP GET sendMessage requests. The stolen data, including email addresses, passwords, and IP addresses, is sent to the bot in a predefined template format.

Identifying the Threat: To identify malicious domains associated with this campaign, a regex pattern has been provided for creating hunting rules. Additionally, Threat Intelligence (TI) lookup queries can be performed to identify related domains.

THREATRADAR
By HADESS

TTP Analysis



Antivirus evasion, particularly in the context of Windows Defender, remains a critical concern for cybersecurity professionals. In this report, we explore the evolution of techniques used to evade Windows Defender detection, focusing on shellcode loaders. We revisit classic methodologies and analyze their effectiveness against modern antivirus solutions.

Background: Antivirus evasion has become a prominent topic within the cybersecurity community, with numerous articles and discussions dedicated to bypassing security measures. However, the efficacy of these techniques can diminish over time due to advancements in malware detection and prevention capabilities.

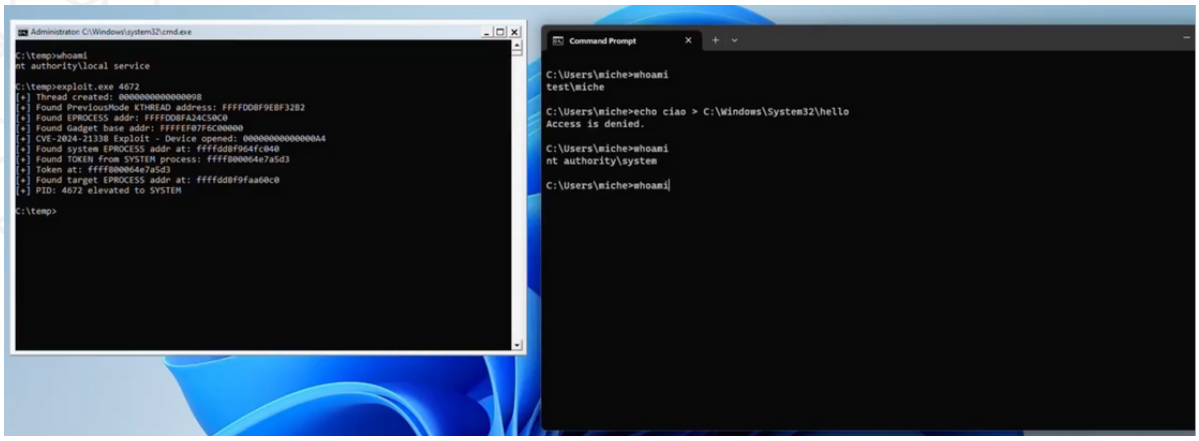
Methodology: Our analysis begins with a retrospective examination of older techniques, notably those outlined in a classic blog post discussing AV Bypass with Metasploit Templates and Custom Binaries. We attempt to replicate the steps outlined in the original post to assess their effectiveness against contemporary antivirus solutions.

Findings: Despite initial optimism, our attempts to evade Windows Defender detection using traditional shellcode loaders yielded mixed results. While some evasion techniques demonstrated marginal success, others were ineffective against modern antivirus signatures.

Challenges: The rapid evolution of antivirus technologies presents a significant challenge for malware developers and red team operators. Techniques that were once successful may now be detected by advanced heuristics and signature-based detection algorithms.

https://twitter.com/gatariee/status/1764406324803293557

1Day



https://twitter.com/s1ckb017/status/1764703383875723438
https://twitter.com/blackorbird/status/1763112467654414386

The Lazarus Group, a highly sophisticated threat actor known for its association with nation-state activities, has exploited a zero-day vulnerability in the Windows AppLocker driver (appid.sys). This flaw, identified as CVE-2024-21338, grants the attacker kernel-level access, allowing them to bypass security controls and disable security tools. The exploitation of this vulnerability poses significant risks to affected systems, potentially leading to unauthorized access, data theft, and system compromise.

Technical Details: The zero-day vulnerability in the Windows AppLocker driver (appid.sys) enables the Lazarus Group to gain elevated privileges, from administrative to kernel level, within the Windows operating system. By exploiting this flaw, attackers can bypass application whitelisting controls enforced by AppLocker and disable security tools, effectively undermining the system's security posture.

Threat Actor: The Lazarus Group is a well-known threat actor with a history of conducting sophisticated cyber espionage and financially motivated attacks. This group has been associated with various high-profile cyber incidents, including the infamous WannaCry ransomware attack and the theft of funds from financial institutions.

Attack Vector: The exploitation of CVE-2024-21338 likely involves the delivery of a malicious payload through targeted phishing emails, watering hole attacks, or the exploitation of other vulnerabilities to gain initial access to the target system. Once inside the system, the attacker leverages the zero-day vulnerability to escalate privileges and execute further malicious activities.

🌶️ Trending Exploit

https://securityonline.info/cve-2024-27497-replace-your-linksys-e2000-router-now/
https://twitter.com/HunterMapping/status/1764845663668539681

A critical security vulnerability, identified as CVE-2024-27497, has been discovered in the Linksys E2000 router firmware version Ver.1.0.06 build 1. This flaw poses a severe risk to network security, allowing attackers to bypass authentication mechanisms and gain unauthorized access to the router's administration interface, potentially leading to data theft, device compromise, and further malicious activity.

Vulnerability Details: The vulnerability resides within the position.js file of the router firmware, mishandling the session_key data used to secure user sessions. Exploiting this flaw, attackers can craftily retrieve active session keys, effectively bypassing the login process without requiring legitimate credentials.

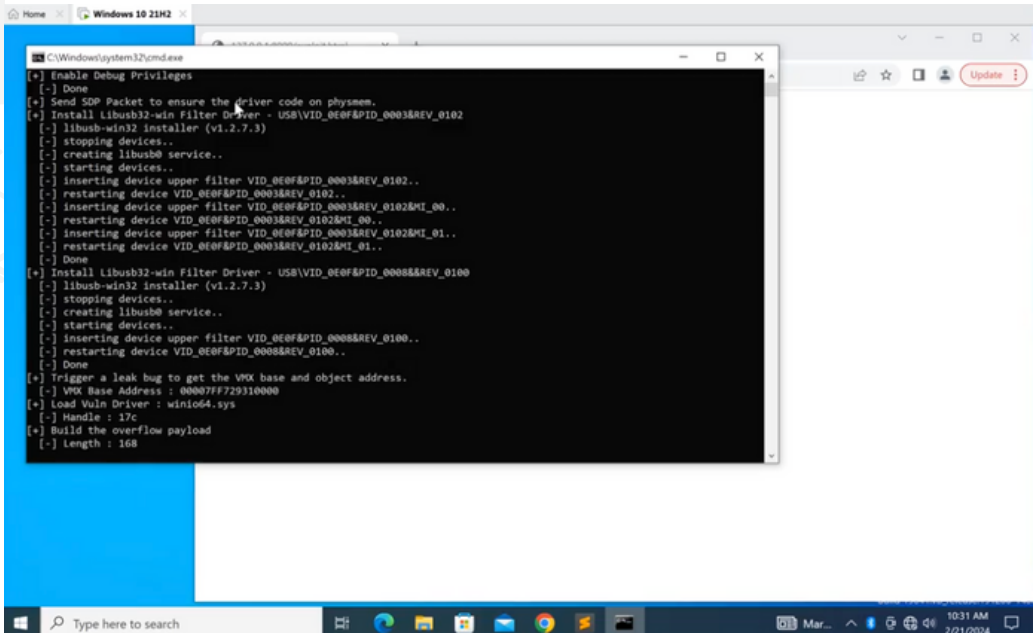
Attack Scenario:

1. The attacker waits for an administrator to log into the router's web management interface, generating a valid session ID string.
2. The attacker then sends a specially crafted GET request to leak the session ID from /position.js or related files.
3. With the acquired session ID, the attacker gains unauthorized access to the router's admin interface, enabling configuration alterations, network monitoring, and deployment of further malicious activities.

Impact:

- Unauthorized access to router administration interface
- Potential data theft and compromise of connected devices
- Ability to manipulate network configurations and deploy malicious activities

The Topic of the Week



https://twitter.com/theori_io/status/1764544922005430576

The featured article explores the security risks associated with using virtual machines (VMs) for browsing potentially dangerous links and examines the vulnerabilities inherent in running the Chrome browser within a VM environment.

Key Points:

1. **Virtual Machine Usage:** Many users rely on VMs to browse potentially risky or malicious websites safely, isolating their main operating system from potential threats.
2. **Chrome Browser Vulnerabilities:** Despite the perceived security of using VMs, the article highlights six unique Common Vulnerabilities and Exposures (CVEs) from 2023 that pose significant risks when using the Chrome browser within a VM environment:
   - Chrome Renderer Remote Code Execution (RCE) (CVE-2023-3079)
   - Chrome Sandbox Escape (CVE-2023-21674)
   - Local Privilege Escalation (LPE) in guest OS (CVE-2023-29360)
   - VMware Information Leak (CVE-2023-34044)
   - VMware Escape (CVE-2023-20869)
   - Local Privilege Escalation (LPE) in host OS (CVE-2023-36802)

3. **Chained Vulnerabilities:** The article underscores the potential for attackers to chain these CVEs together, exploiting vulnerabilities in both the Chrome browser and the underlying VM infrastructure to achieve various levels of compromise, including remote code execution and privilege escalation.
4. **Security Implications:** The presence of these vulnerabilities highlights the importance of adopting a multi-layered security approach when using VMs for browsing unsafe content. While VMs offer isolation, they are not impervious to security risks, particularly when running vulnerable software such as web browsers.

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Threat Radar
WWW.THREATRADAR.NET

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.