THREAT HUNTING

LAB

WEEK 30/12/2024 - 03/01/2025

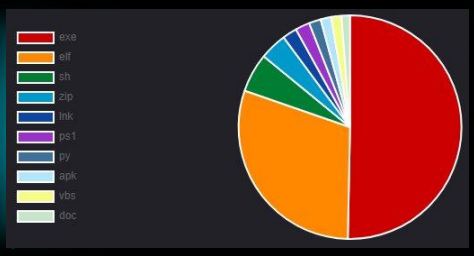
PUBLIC

Index

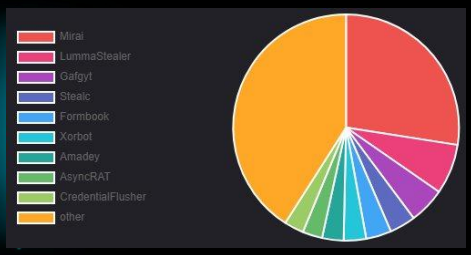
Global Weekly Threat Overview

A high-severity security flaw has been disclosed in ProjectDiscovery's Nuclei that could allow attackers to bypass signature checks and potentially execute malicious code. Tracked as CVE-2024-43405, it carries a CVSS score of 7.4 and it impacts all versions of Nuclei later than 3.0.0. The vulnerability stems from a discrepancy between how the signature verification process and the YAML parser handle newline characters, combined with the way multiple signatures are processed. This allows an attacker to inject malicious content into a template while maintaining a valid signature for the benign part of the template.

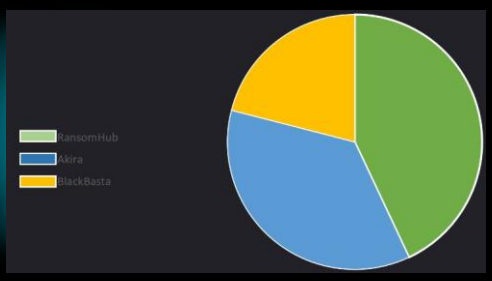
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



A proof-of-concept exploit has been released for a now-patched security flaw impacting Windows LDAP that could trigger a DoS condition. The out-of-bounds reads vulnerability is tracked as CVE-2024-49113 (CVSS score: 7.5). It was addressed by Microsoft as part of Patch Tuesday updates for December 2024, alongside CVE-2024-49112 (CVSS score: 9.8), a critical integer overflow flaw in the same component that could result in remote code execution. The PoC devised by SafeBreach Labs, codenamed LDAPNightmare, is designed to crash any unpatched Windows Server with no prerequisites except that the DNS server of the victim DC has Internet connectivity.

Global Weekly Notable One

Use Alternate Authentication Material: Defense Evasion

In the rapidly evolving landscape of cybersecurity, the integrity of application access tokens has become a critical concern for organizations worldwide. These tokens serve as digital keys, allowing applications to authenticate users without the need for constant password verification. However, their convenience also creates significant vulnerabilities that malicious actors can exploit. Attackers have increasingly demonstrated their ability to craft or abuse these tokens, effectively bypassing security measures meant to protect sensitive information.

A recent breakthrough in this area was presented at Blackhat EU 2024, where researchers unveiled a new technique by TEMP43487580. This method highlights how attackers can manipulate token validation processes to circumvent conditional access policies, which are designed to restrict access based on specific criteria such as user location or device security status. By exploiting weaknesses in token management and validation, attackers can gain unauthorized access to resources that should be protected.

The new technique specifically demonstrates the potential for adversaries to alter or forge access tokens, allowing them to impersonate legitimate users and bypass established security protocols. This manipulation can occur through various means, including token theft and impersonation, where attackers duplicate an existing token from a legitimate user's session. Once they have a valid token, they can leverage it to escalate privileges or gain access to sensitive data without triggering security alerts.

Global Weekly Notable One

Use Alternate Authentication Material: Defense Evasion

The newly released tool TokenSmith by JumpsecLabs, designed for offensive engagements, it facilitates the generation of Entra ID access and refresh tokens while incorporating features that allow for bypassing Intune compliant device conditional access. This tool enables users to authenticate from noncompliant devices, effectively undermining established security protocols.

TokenSmith not only streamlines the process of token creation but also provides insights into the underlying mechanics of token validation, making it a valuable resource for penetration testers and security researchers alike. By demonstrating how easily these tokens can be manipulated, TokenSmith emphasizes the urgent need for organizations to reassess their security measures surrounding token management.

Threat Hunting Activity

SORINTSEC

TACTIC

Defense Evasion

TECHNIQUES

T1550 – Use Alternate Authentication Material

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls. Authentication processes generally require a valid identity along with one or more authentication factors. Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process.

Threat Hunting Activity

TokenSmith tool guides during all the phases of the code crafting. With the flag “—intune-bypass” it will provide instructions to perform via browser


```
[1] To get your Entra ID tokens while bypassing Compliant Device Requirement, login on a browser
 (chromium-based recommended) with this URL:
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=9ba1a5c7-f17a-4de9-a1f1
-6178c8d51223&redirect_uri=ms-appx-web%3A%2F%2FMicrosoft.AAD.BrokerPlugin%2FS-1-15-2-2666988183-
1750391847-2906264630-3525785777-2857982319-3063633125-1907478113&response_type=code&scope=openi
d+offline_access+https%3A%2F%2Fgraph.microsoft.com%2F.default

[2] After authentication has completed, the page would either show:

  [a] 'Are you trying to sign in to Microsoft Intune Company Portal?'. Click [Continue] and then
 press <Ctrl+Shift+J> to open DevTools.
  [b] Or, there're dots [.....] looping. Press <Ctrl+Shift+J> to open DevTools.

[3] On the Console Tab, locate the 'Failed to launch ms-appx-web://' error message, Right click
and copy link address. The URL should look like ms-appx-web://Microsoft.AAD.BrokerPlugin/ ...

[4] Paste URL here and Press <RETURN>
>
```

Threat Hunting Activity

After a few steps via browser DevTools Console a valid token is provided

```
[4] Paste URL here and Press <RETURN>
>ms-appx-web://microsoft.aad.brokerplugin/S-1-15-2-2666988183-1750391847-2906264630-3525785
777-2857982319-3063633125-1907478113?code=1.AUEBe6mZqbzPUkCglYFUh6CA8celoZt68elNofFheMjVEiM
[redacted]

[+] SUCCESSFULLY REDEEMED TOKENS!

[+] Access Token:
============================
evJ0eXAiOiJKV1QiLCJub25iZSI6IlZ[redacted]
```

The generated token provide a valid session which can be imported into a postexploitation tool like GraphRunner or ROADtools to enumerate the tenant.

Threat Hunting Activity

Dection can be done looking for events about ApplicationId “9ba1a5c7-f17a4de9-a1f1-6178c8d51223” (Microsoft Intune Company Portal)

Timestamp	AccountUpn	Application	ApplicationId	ErrorCode	CAP_result	IsCompliant	IsManaged
3 gen 2025 11:47:15	[redacted]	Microsoft Intune Compa...	9ba1a5c7-f17a-4de9-a1...	0	notApplied	0	1
3 gen 2025 11:47:15	[redacted]	Microsoft Intune Compa...	9ba1a5c7-f17a-4de9-a1...	0	notApplied	0	1
3 gen 2025 11:45:45	[redacted]	Microsoft Intune Compa...	9ba1a5c7-f17a-4de9-a1...	0	notApplied	0	1
3 gen 2025 11:45:45	[redacted]	Microsoft Intune Compa...	9ba1a5c7-f17a-4de9-a1...	0	notApplied	0	1

PUBLIC