THREAT HUNTING

LAB

Certighost to Domain Takeover:
AD CS chase referrals weaponized for Domain Controller impersonation.

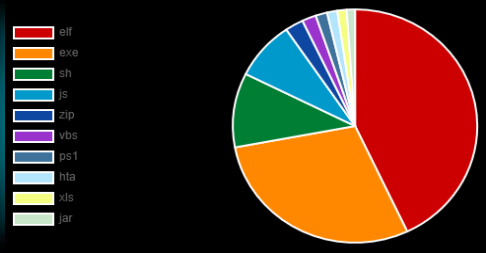
PUBLIC

Index

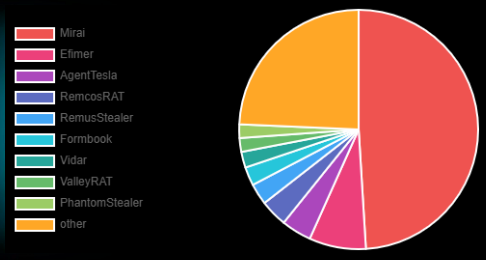
Global Weekly Threat Overview

MedusaHVNC is advertised with a “Mem Exec” feature for running .NET and native payloads in memory alongside AMSI and ETW bypasses, plus a “Browser Recovery” function that extracts saved passwords, cookies, and browsing history from Chrome, Edge, Brave, Firefox, and Telegram.
The operator panel lets a buyer select a target application, launch a hidden desktop session, and adjust frame rate and image quality while watching a live view of the compromised browser, similar to how other Medusa-branded malware families have offered turnkey criminal tooling through affiliate models.

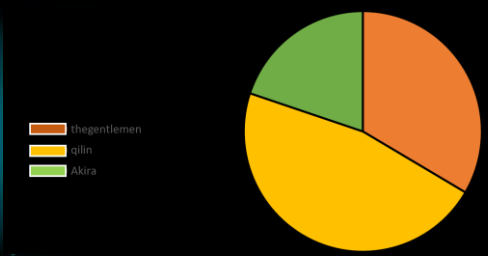
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Cryptocurrency theft is increasingly moving beyond the screen. Criminals are using violence, threats, home invasions, and kidnapping attempts to force victims to unlock wallets or approve transfers while under pressure.
These incidents are known as wrench attacks, a term that describes bypassing strong encryption by targeting the person who controls the keys.
Instead of defeating a wallet’s security, attackers attempt to coerce its owner into giving up access. Analysts at TRM identified a growing pattern of physical attacks against people linked to digital asset wealth, including investors, traders, company leaders, and their relatives.

Global Weekly Notable One

Privilege Escalation: Steal or Forge Authentication Certificates

Certighost (CVE-2026-54121) is an Active Directory Certificate Services (AD CS) vulnerability that allows a low-privileged domain user to impersonate a Domain Controller. The flaw abuses the certificate enrollment “chase” mechanism, where a requester-controlled cdc attribute can redirect the Certification Authority (CA) to attacker-controlled LDAP and LSA services. By supplying forged directory information such as the target Domain Controller's SID, sAMAccountName, and dNSHostName, the attacker can trick the CA into issuing a valid certificate for the Domain Controller.

The issued certificate can then be used with PKINIT to obtain Kerberos credentials and potentially perform DCSync operations, leading to full domain compromise.
Once authenticated as the Domain Controller, the attacker gains access to privileges normally reserved for domain replication partners, allowing the extraction of sensitive directory secrets, including credential material associated with high-privilege accounts such as krbtgt

Threat Hunting Activity

TACTIC

Privilege Escalation

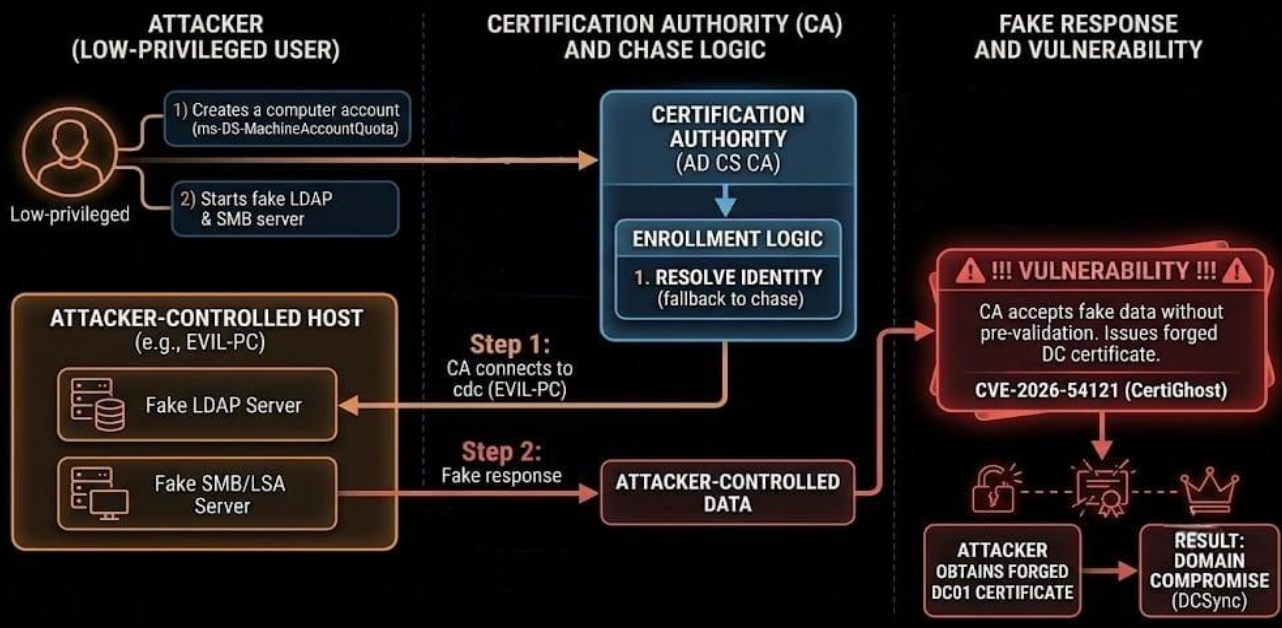
TECHNIQUES

T1649 – Steal or Forge Authentication Certificates

Adversaries may steal or forge certificates used for authentication to access remote systems or resources.
Digital certificates are often used to sign and encrypt messages and/or files. Certificates are also used as authentication material.
For example, Entra ID device certificates and Active Directory Certificate Services (AD CS) certificates bind to an identity and can be used as credentials for domain accounts.

Threat Hunting Activity

The vulnerability exploits a trust boundary failure within the AD CS enrollment chase mechanism. By controlling the cdc referral target and supplying forged LDAP identity attributes such as the target Domain Controller's SID, sAMAccountName, and dNSHostName, an attacker can influence the identity information used by the Certification Authority during certificate issuance. Consequently, the CA may issue a cryptographically valid certificate representing the target Domain Controller instead of the requesting machine account.



Using the issued certificate, the attacker can leverage PKINIT to obtain Kerberos credentials mapped to the Domain Controller account. This grants access to the DC's security context, including directory replication privileges, enabling DCSync attacks against Active Directory. As a result, sensitive credential material, including privileged account secrets and potentially the krbtgt account hash, can be extracted, ultimately leading to full domain compromise.

Threat Hunting Activity

Detection can be on Event ID 4886/4887 looking for suspicious parameters into certificate request.

PUBLIC