TITLE: THREAT HUNT | DESKTOP- [redacted]

CASE ID [redacted]

CaseID : [redacted]

Created By : [redacted]

Subject : **Threat Hunt |** [redacted]

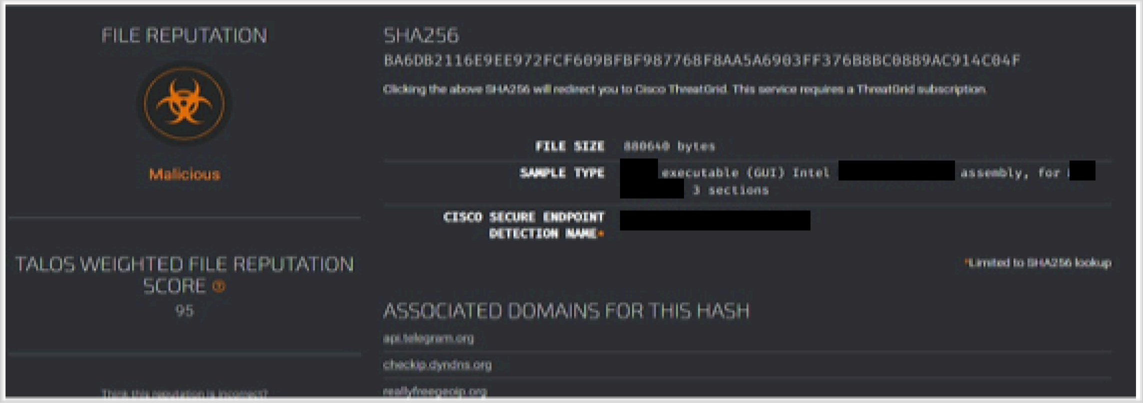
Category	Sub Category	Severity	Status
Malware Infection	Virus	Critical	Opened

Analysis Summary

On April 3, 2025, at 10:25:58, suspicious activity was detected on the host [redacted], where a chain of processes starting from [redacted] led to the execution of a suspicious binary named ba6db2116e9ee972fcf609bfbf987768f8aa5a6903ff376b8bc0889ac914c04f[redacted] This executable was launched twice after being extracted using WinRAR.exe, which was itself spawned by chrome[.]exe an unusual and suspicious process path indicating that a malicious file was downloaded and executed via the browser. DNS analysis revealed outbound connections to checkip[.]dyndns.org and reallyfreegeoip[.]org, both commonly used by malware for external IP and geolocation discovery. Additionally, a connection to api.telegram[.]org was observed, a known tactic used by threat actors to establish command-and-control (C2) communication via Telegram bots. File reputation analysis confirms the hash is malicious. VirusTotal reports that 51 out of 71 antivirus vendors flagged this file, identifying it as a variant of Trojan.MSIL.Jalapeno, associated with the Agent Tesla malware family. Cisco Talos Intelligence assigns the file a 95/100 malicious score and ties it to the same suspicious domains. The file exhibits spreader, persistence, and information-stealing behavior, confirming its use as a remote access trojan (RAT).

Groups	Contributors
SOC	[redacted]

Evidence



FILE REPUTATION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE
95

Think this reputation is incorrect?

SHA256
BA6DB2116E9EE972FCF609BFBF987768F8AA5A6903FF376B8BC0889AC914C04F

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

```
                FILE SIZE  880640 bytes
              SAMPLE TYPE  [redacted] executable (GUI) Intel [redacted] assembly, for [redacted]
                           [redacted] 3 sections
  CISCO SECURE ENDPOINT    [redacted]
          DETECTION NAME*
```

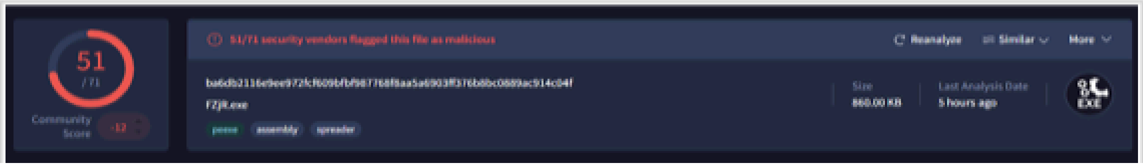
*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

api.telegram.org

checkip.dyndns.org

reallyfreegeoip.org



51
/ 71
Community Score -12

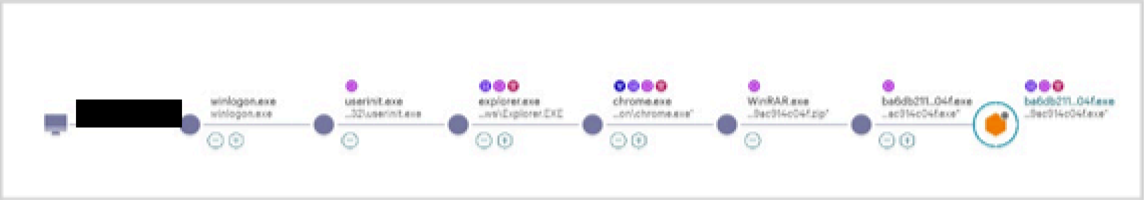
51/71 security vendors flagged this file as malicious

ba6db2116e9ee972fcf609bfbf987768f8aa5a6903ff376b8bc0889ac914c04f
FZjR.exe

peexe assembly spreader

Size
860.00 KB

Last Analysis Date
5 hours ago



Remediation

1. Contain the host immediately.
2. Block [redacted] and [redacted].
3. Delete the malicious .exe from the Temp RAR folder and remove the associated archive.

Comments

No Comments