SORINT.SEC

THREAT HUNTING

LAB

ClickFix's Second Door:
SocGholish-Inspired Proxy-Based Intrusion Chains

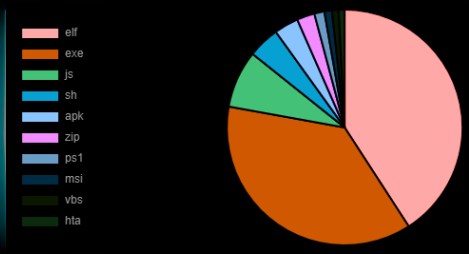
PUBLIC

Index

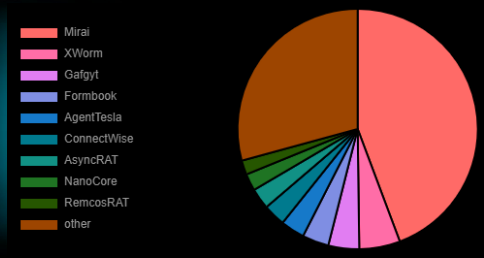
Global Weekly Threat Overview

A new denial-of-service (DoS) attack dubbed HTTP/2 Bomb can be launched from a single machine to take down web servers within seconds. The technique works on default HTTP/2 configurations of major web servers, including NGINX, Apache HTTP Server, Microsoft IIS, Envoy, and Cloudflare Pingora. HTTP/2 Bomb combines two previously known HTTP/2 DoS methods: the HPACK compression amplification and Slowloris-style resource retention via HTTP/2 flow-control stalling. When combined, a single client on a 100 Mbps connection can exhaust tens of gigabytes of RAM within seconds, forcing the server to allocate it and then preventing its release.

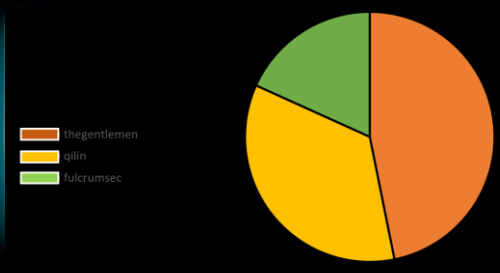
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



A Chinese-speaking cybercrime group has expanded its targeting to the European space, deploying previously undocumented malware and the Atlas backdoor. Tracked as TA4922, the threat actor is associated with financially motivated attacks aimed at breaching target networks for fraud, data theft, and the sale of access. TA4922 has previously targeted organizations in East Asia, but recent campaigns have focused on entities in Germany, Italy, the United Kingdom, and South Africa. Researchers note that TA4922 shares overlaps with activity previously reported as ‘Silver Fox’ and ‘Void Arachne. However, the activity cluster is tracked separately as it is more consistent with cybercrime than espionage. Since March, TA4922’s activity has increased sharply, and since April, it has shown unprecedented operational diversity and high tempo.

Global Weekly Notable One

Command and Control: Proxy

The ClickFix campaign has undergone a significant transformation, evolving from a one-time social engineering trick into a sophisticated, multi-layered intrusion system that closely mirrors the operational patterns of SocGholish. This shift marks its maturation from a simple launch point for payloads into a modular post-exploitation platform that security researchers now view as a serious pre-ransomware delivery system.

This evolution was highlighted in the last months when was discovered the campaign pairing its traditional tactics with PySoxy, an open-source Python-based SOCKS5 proxy that is approximately a decade old. By utilizing this tool, the threat actors demonstrate a "bring-your-own-interpreter" strategy, using available scripting runtimes to stage proxy capabilities without needing traditional, easily detectable malware.

Threat Hunting Activity

TACTIC Command & Control

TECHNIQUES T1090 – Proxy

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic.

Threat Hunting Activity

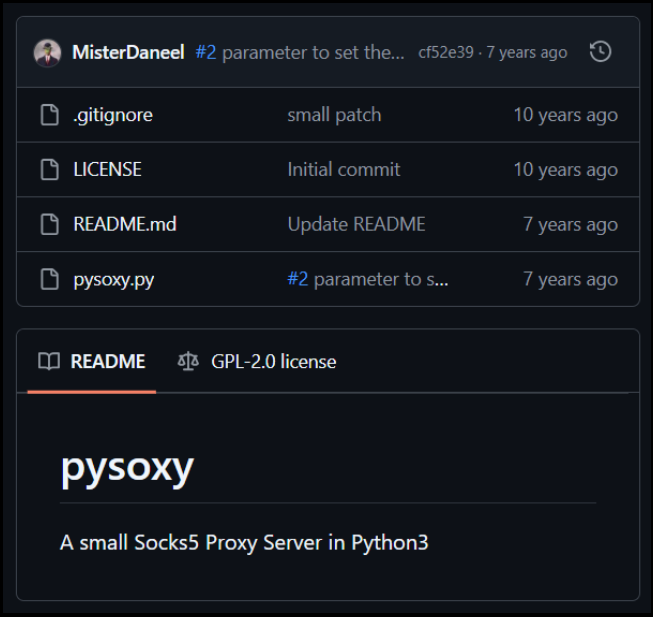
Beginning with a social engineering lure tricking users into executing PowerShell, this chain establishes persistence via scheduled tasks in the ProgramData directory and a polling RAT before progressing through domain reconnaissance; however, the sophisticated new addition is the deployment of PySoxy, a Python-based proxy that creates a redundant, encrypted secondary access path to ensure durability even if primary command-and-control channels are blocked.

Infection chain

Attackers do not drop PySoxy immediately; they deploy it only after conducting extensive domain reconnaissance to map the environment and verify that the host can communicate with their staging infrastructure. This deliberate sequence ensures the tool is used to solidify a highly reliable, long-term access point.

Threat Hunting Activity

The combination of ClickFix traditional tactics and PySoxy creates a durable access chain, allowing attackers to maintain a persistent foothold even if their primary outbound connections are interrupted by security controls. After initial enumeration, once the environment is understood and a path to staging infrastructure is verified, the attacker introduces PySoxy, to establish the secondary encrypted access path.



PySoxy public github repository

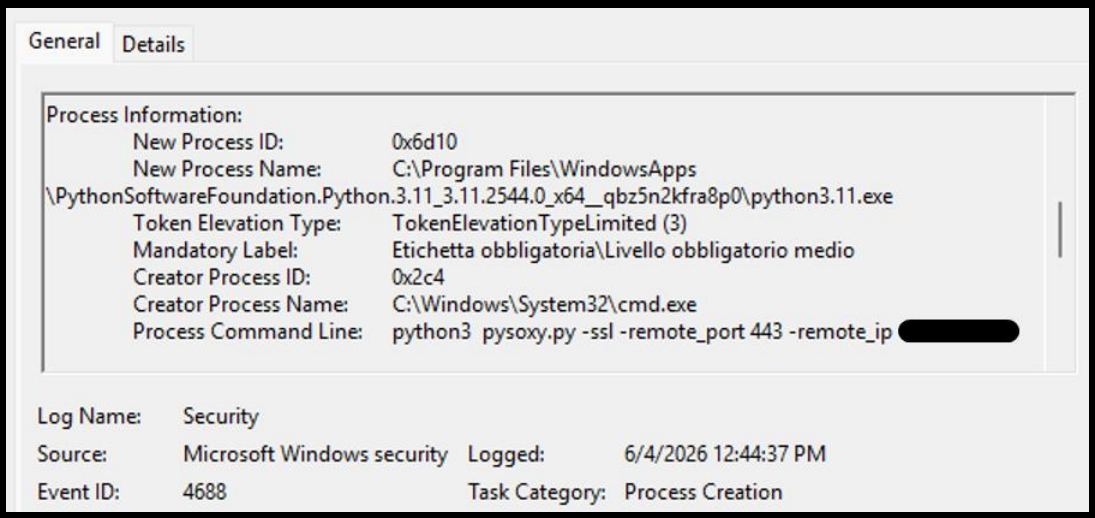
The use of PySoxy highlights a "bring-your-own-interpreter" (BYOI) strategy, where attackers leverage standard scripting runtimes like Python to bypass signature-based detection and create redundant backdoors into the environment. This secondary proxy channel often uses entirely different infrastructure and traffic patterns than the initial PowerShell-based RAT, ensuring the attacker maintains access even if the primary connection is severed. To detect these resilient chains, analysts are advised to move beyond monitoring for known malware signatures and instead hunt for specific behavioral indicators, such as python.exe execution from non-standard directories using proxy-related arguments.

```
:>python.exe [{filename}.pyc/{filename}.py] -ssl -remote_port {port} -remote_ip {ip}
```

PySoxy execution example

Threat Hunting Activity

This depth of post-exploitation suggests that ransomware affiliates may now view ClickFix as a primary initial-access source, functionally equivalent to established loaders or initial access broker purchases. Hunting for the PySoxy proxying stage involves looking for python.exe execution that originates from unexpected paths or runs compiled Python bytecode (.pyc files) instead of standard scripts. Specific high-value command-line arguments to monitor include -ssl, -remote_ip, and -remote_port, which indicate the establishment of an encrypted SOCKS5 proxy tunnel to external attacker infrastructure.



EID 4688

PUBLIC