THREAT HUNTING

LAB

WEEK 13/01/2025 - 17/01/2025

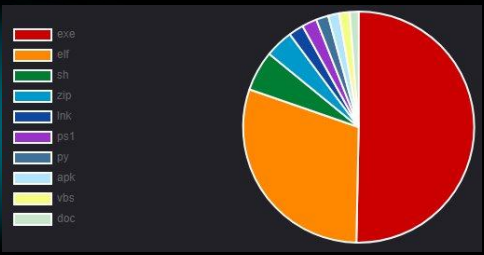
PUBLIC

Index

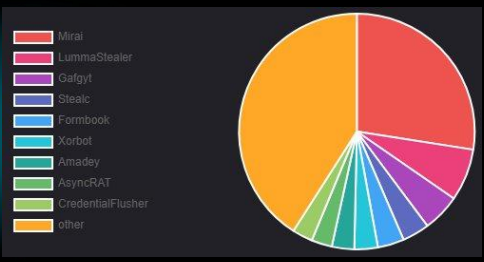
Global Weekly Threat Overview

Cybersecurity researchers are calling attention to a series of cyber attacks that have targeted Chinese-speaking regions like Hong Kong, Taiwan, and Mainland China with a known malware called ValleyRAT. The attacks leverage a multi-stage loader dubbed PNGPlug to deliver the ValleyRAT payload. The infection chain commences with a phishing page that's designed to encourage victims to download a malicious MSI package disguised as legitimate software.
Once executed, the installer deploys a benign application to avoid arousing suspicion, while also stealthily extracting an encrypted archive containing the payload.

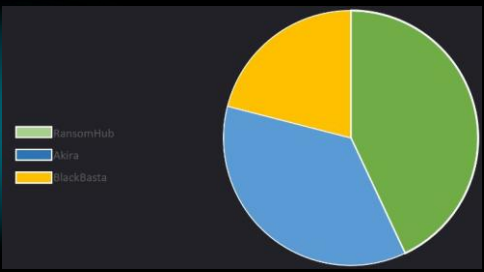
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Cybersecurity researchers have disclosed three security flaws in Planet Technology's WGS-804HPT industrial switches that could be chained to achieve pre-authentication remote code execution on susceptible devices. The vulnerabilities are rooted in the dispatcher.cgi interface used to provide a web service. The list of flaws is CVE-2024-52558 (CVSS score: 5.3), CVE-2024-52320 (CVSS score: 9.8), CVE-2024-48871 (CVSS score: 9.8). Successful exploitation of the flaws could permit an attacker to hijack the execution flow by embedding a shellcode in the HTTP request and gain the ability to execute operating system commands.

Global Weekly Notable One

Account Discovery: Discovery

Domain enumeration represents a critical initial phase of reconnaissance for malicious actors. The Lightweight Directory Access Protocol (LDAP) has emerged as a powerful yet vulnerable mechanism for extracting comprehensive information about organizational networks, providing unprecedented insights into an organization's digital infrastructure. Active Directory serves as a treasure trove of sensitive organizational data, containing exhaustive details about users, groups, devices, and network configurations. Traditionally, attackers have leveraged LDAP to perform detailed network mapping, extracting critical information that can be used to identify potential attack vectors and privileged access pathways.

The conventional LDAP enumeration methods have long been monitored by defensive security tools, prompting the development of more sophisticated reconnaissance techniques. An innovative approach designed to bypass traditional LDAP monitoring mechanisms is via the Active Directory Web Services (ADWS) protocol.
ADWS represents a unique communication channel that wraps LDAP queries within SOAP messages, effectively circumventing standard network monitoring tools. By routing queries through a NetTCPBinding communication channel, ADWS allows attackers to extract identical information as LDAP, but with significantly reduced detection risks.

Global Weekly Notable One

Account Discovery: Discovery

SOAPHound emerges as a cutting-edge tool specifically engineered to exploit the ADWS protocol's capabilities. Developed as a .NET data collector, it offers several key advantages. Stealthy Reconnaissance as it avoids direct LDAP traffic detection, Comprehensive Data Extraction as it Retrieves detailed Active Directory information, Flexible Collection Methods as it supports multiple enumeration approaches including BloodHound data dumping, certificate service exploration, and DNS data collection.

The tool's effectiveness stems from its unique approach of first retrieving all Active Directory objects and then processing them systematically.
This method minimizes the number of LDAP queries, reducing the likelihood of triggering security monitoring systems.

Threat Hunting Activity

TACTIC

Discovery

TECHNIQUES

T1087 – Account Discovery

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

When using SOAPHound different flag are available to make the tool more precise and stealth

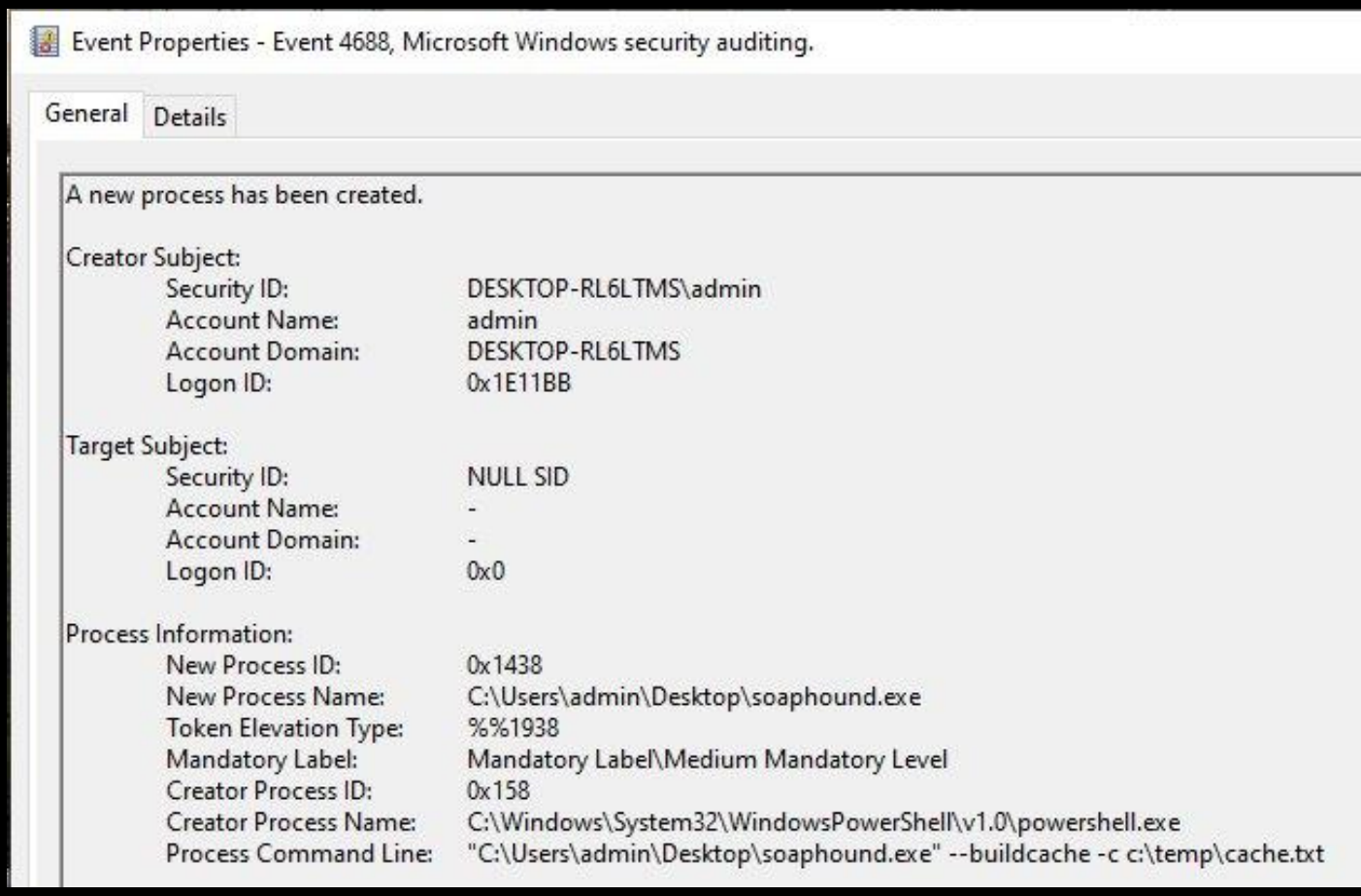
```
Connection and authentication options:
  --user                    Username to use for ADWS Connection. Format: domain\user or user@domain
  --password                Password to use for ADWS Connection
  --domain                  Specify domain for enumeration
  --dc                      Domain Controller to connect to

Supported collection methods:
  --buildcache              (Default: false) Only build cache and not perform further actions
  --dnsdump                 (Default: false) Dump AD Integrated DNS data
  --certdump                (Default: false) Dump AD Certificate Services data
  --bhdump                  (Default: false) Dump BH data

Output options:
  -o, --outputdirectory     Folder to output files to (full path needed)
  -c, --cachefilename       Filename for the cache file (full path needed)

Splitting options:
  -a, --autosplit           (Default: false) Enable AutoSplit mode: automatically split object retrieval
  -t, --threshold           (Default: 0) AutoSplit mode: Define split threshold based on number of objec

Miscellaneous options:
  --nolaps                  (Default: false) Do not request LAPS related information
  --showstats               Show stats of local cache file
  --logfile                 Create log file
  --help                    Display this help screen.
```

One of the following collection methods must be specified

- `--buildcache` : Only build cache and not perform further actions
- `--bhdump` : Dump BloodHound data
- `--certdump` : Dump AD Certificate Services (ADCS) data
- `--dnsdump` : Dump AD Integrated DNS data

Threat Hunting Activity

Detection can be made auditing the process creation looking for toll execution.



THREAT HUNTING

SORINT.SEC

PUBLIC