SORINT SEC

THREAT HUNTING

LAB

WEEK 24/02/2025 - 28/02/2025

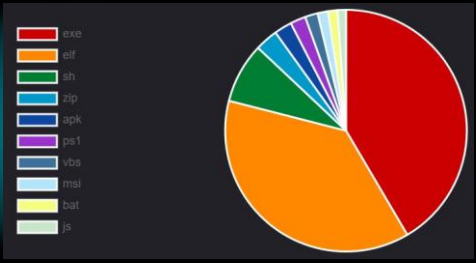
PUBLIC

Index

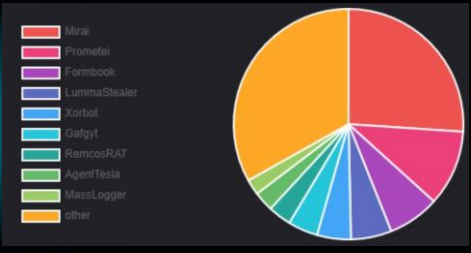
Global Weekly Threat Overview

new malware campaign has been observed targeting edge devices from Cisco, ASUS, QNAP, and Synology to rope them into a botnet named PolarEdge since at least the end of 2023. French cybersecurity company Sekoia said it observed the unknown threat actors deploying a backdoor by leveraging CVE-2023-20118 (CVSS score: 6.5), a critical security flaw impacting Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers that could result in arbitrary command execution on susceptible devices. The vulnerability remains unpatched due to the routers reaching end-of-life status. As workarounds, Cisco recommended in early 2023 that the flaw be mitigated by disabling remote management and blocking access to ports 443 and 60443.

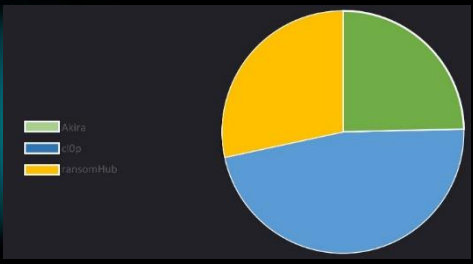
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



More than a year's worth of internal chat logs from a ransomware gang known as Black Basta have been published online in a leak that provides unprecedented visibility into their tactics and internal conflicts among its members. The Russian-language chats on the Matrix messaging platform between September 18, 2023, and September 28, 2024, were initially leaked on February 11, 2025, by an individual who goes by the handle ExploitWhispers, who claimed that they released the data because the group was targeting Russian banks. The identity of the leaker remains a mystery.

Global Weekly Notable One

Exploitation of Remote Services: Lateral Movement

Buffer overflow vulnerabilities are a class of security threats that arise when data exceeds the capacity of a buffer, causing it to spill over into adjacent memory locations. This overflow can lead to unpredictable behavior, including system crashes or, more critically, the execution of malicious code. Buffer overflows are categorized into two main types: stackbased buffer overflows and heap-based buffer overflows.

Heap-based buffer overflows occur when data is written beyond the bounds of a buffer allocated on the heap. The heap is used for dynamic memory allocation, and overflows here can corrupt adjacent memory, potentially allowing attackers to manipulate program behavior or execute malicious code. Heap-based overflows are generally more complex to exploit than stack-based ones, as they require understanding the heap layout and management algorithms of the target system.

Threat Hunting Activity

TACTIC	Lateral Movement
TECHNIQUES	T0866 – Exploitation of Remote Services

Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse. A common goal for post-compromise exploitation of remote services is for initial access into and lateral movement throughout the ICS environment to enable access to targeted systems.

Threat Hunting Activity

The recent disclosure of CVE-2024-12084 has brought attention to a critical vulnerability in Rsync, a widely used open-source utility for efficient file transfer and synchronization between systems. This vulnerability is a heap-based buffer overflow flaw, with a CVSS score of 9.8, indicating a high severity threat. This heap-based buffer overflow vulnerability arises from the improper handling of attacker-controlled checksum lengths (s2length) within the Rsync daemon. In details it occurs when the MAX_DIGEST_LEN value exceeds the fixed SUM_LENGTH of 16 bytes.

In Rsync, checksums are used to verify the integrity of data being transferred. The s2length field is part of the protocol used to communicate these checksums between the client and server. When an attacker manipulates the s2length to exceed the expected bounds, it can cause the Rsync daemon to write out-of-bounds data into the sum2 buffer. This buffer overflow can be exploited to execute arbitrary code on the server, enabling remote code execution.

Threat Hunting Activity

Detection can be made monitoring rsync usage looking for any possible shell spawn by rsync .deamon from auditd logs

```
type=PATH msg=audit(03/03/2025 12:25:30.613:410) : item=0 name=./local/bin/rsync namety
pe=UNKNOWN cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(03/03/2025 12:25:30.617:411) : item=1 name=/usr/bin/rsync inode=461
4876 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none
 cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(03/03/2025 12:25:30.617:411) : item=0 name=/usr/bin/rsync inode=461
4876 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none
 cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(03/03/2025 12:25:30.617:411) : argc=3 a0=rsync a1=sh -c "sh

type=SYSCALL msg=audit(03/03/2025 12:25:30.617:411) : arch=x86_64 syscall=execve succes
s=yes exit=0 a0=0x7fff63022540 a1=0x7f444a350a48 a2=0x55ccb8f52740 a3=0x8 items=3 ppid=
57681 pid=64749 auid=kali uid=root gid=root euid=root suid=root fsuid=root egid=root sg
```

Rsync versions prior of 3.2.7 are vulnerable, a patch is available from updates of the utility.

PUBLIC