Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Apr 02 - 08, 2024

Report Summary:

- **New Threat Detection Added** – 3 (WarzoneRAT, Xehook Stealer and Lumma Stealer)
- **New IDPS Rules Created - 55**

Newly Detected Threats Added

1. WarzoneRAT

In February, the FBI shut down the WarzoneRAT malware operation and arrested two people involved. Recently, researchers found malware spread via tax-themed spam emails, using WarzoneRAT as the final attack. One method involves an attachment with a LNK file that triggers a chain of downloads leading to malicious activity. Another method uses an executable file to load the WarzoneRAT DLL module. Once activated, WarzoneRAT connects to a Command-and-Control server to carry out harmful actions on the victim's computer.

Rules Created: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity
Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Spear phishing Attachment
Execution	T1059.003 T1059.005	Command and Scripting Interpreter: Windows Command Shell Command and Scripting Interpreter: Visual Basic
Persistence	T1053.001	Registry Run Keys / Startup Folder
Defence Evasion	T1036 T1027	Masquerading Obfuscated Files or Information
Discovery	T1057	Process Discovery
Collection	T1114	Email Collection
C&C	T1071	Application Layer Protocol

2. Xehook Stealer

Discovered in January 2024, Xehook Stealer is a malware designed for Windows computers using .NET. It can collect data from Chromium and Gecko browsers, supporting over 110 cryptocurrencies and 2FA extensions. The Stealer also has tools for creating custom traffic bots and recovering Google cookies. Its evolution traces back to the free MaaS Cinoshi Project, leading to Agniane Stealer and finally, Xehook Stealer, possibly indicating rebranding and improvements. Xehook Stealer spreads mainly through SmokeLoader binaries, showing active distribution efforts. It shares code similarities with Agniane Stealer and communicates with the same control server, suggesting a close connection. Similar web panel designs across Cinoshi, Agniane, and Xehook Stealer indicate ongoing development.

Rules Created: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Defence Evasion	T1027 T027.002	Obfuscated Files or Information Software Packing
Credential Access	T1003	OS Credential Dumping
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Collection	T1005 T1560	Data from Local System Archive Collected Data
Command-and-Control	T1071	Application Layer Protocol

3. Lumma Stealer

Lumma is a piece of malicious software categorised as a stealer. Malware within this category is designed to steal sensitive data. These programs are capable of exfiltrating data from infected systems and the applications installed onto them. Lumma's behaviour is like that of the Mars, Arkei, and Vidar stealers. Stealer-type malware can exfiltrate both device/system and personal data. The latter entails downloading various files (e.g., databases, images, documents, videos, etc.) from the compromised system. Typically, these malicious programs can extract information from browsers, which could include browsing and search engine data, autofills, usernames/passwords, personally identifiable details, credit card numbers, and so forth. Stealers often target various accounts like emails, social media, social networking, messengers, gaming-related software, online banking, e-commerce, cryptocurrency wallets, FTPs, password managers, authentication software, VPNs, and many others.

Rules Created: 10
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1129	Shared Modules
Defence Evasion	T1027	Obfuscated Files or Information
	T1140	Deobfuscate/Decode Files or Information
	T1222	File and Directory Permissions Modification
Discovery	T1057	Process Discovery
	T1083	File and Directory Discovery
Impact	T1496	Resource Hijacking

Known exploited vulnerabilities (Week 1 April 2024):

Vulnerability	CVSS	Description
CVE-2024-29748	On-going analysis	Android Pixel Privilege Escalation Vulnerability
CVE-2024-29745	On-going analysis	Android Pixel Information Disclosure Vulnerability

Updated Malware Signatures (Week 1 April 2024)

Threat	Description
Cerber	Another type of ransomware but instead of the usual ransom text files, it plays audio on the victim's infected machine.
Remcos	Remcos functions as a remote access trojan (RAT), granting unauthorised individuals the ability to issue commands on the compromised host, record keystrokes, engage with the host's webcam, and take snapshots. Typically, this malicious software is distributed through Microsoft Office documents containing macros, which are often attached to malicious emails.
Gh0stRAT	Gh0stRAT is a widely recognised group of remote access trojans strategically crafted to grant an assailant full authority over a compromised system. Its functionalities encompass monitoring keystrokes, capturing video via the webcam, and deploying subsequent malware. The source code of Gh0stRAT has been openly accessible on the internet for an extended period, substantially reducing the hurdle for malicious actors to adapt and employ the code in fresh attack endeavours.
MacStealer	A remote access trojan enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.

Ransomware Report

The Red Piranha Team actively collects information on organisations globally affected by ransomware attacks from various sources, including the Dark Web. In the past week alone, our team uncovered new ransomware victims and updates on previous victims across 16 different industries spanning 18 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Hunters International ransomware group stands out as the most prolific, having updated a significant number of victims (13%) each distributed across multiple countries. In comparison, Cactus and INC Ransom ransomware groups updated 10% of victims each, in the past week. The following list provides the victim counts in percentages for these ransomware groups and a selection of others.

Name of Ransomware Group	Percentage of new Victims last week
8Base	7.69%
Akira	4.62%
Bianlian	1.54%
Black Suit	6.15%
Blackbasta	4.62%
Cactus	10.77%
Ciphbit	1.54%
Everest	3.08%
Hunters	13.85%
INC Ransom	10.77%
Killsec	1.54%
Lockbit3	6.15%
Malek Team	1.54%
Play	6.15%
Qilin	6.15%
RA Group	6.15%
Ransomhub	4.62%
Rhysida	1.54%
Trigona	1.54%

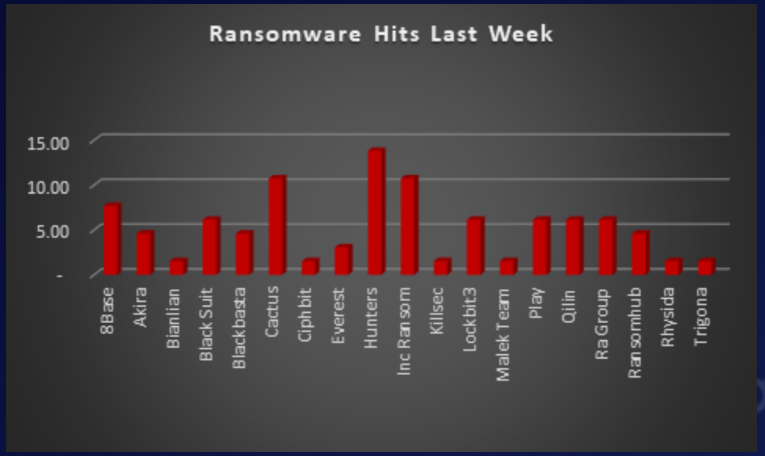

Figure 1: Ransomware Group Hits Last Week

Hunters International Ransomware Group

Hunters International, a Ransomware-as-a-Service (RaaS) entity, surfaced in Q3 of 2023, showing resemblances to the notorious Hive ransomware strain. The analysis revealed a significant overlap of approximately 60% between Hunters International and Hive ransomware version 61. This suggests a potential connection to the disrupted Hive cartel. Despite reports linking them, Hunters International has denied any affiliation with Hive.

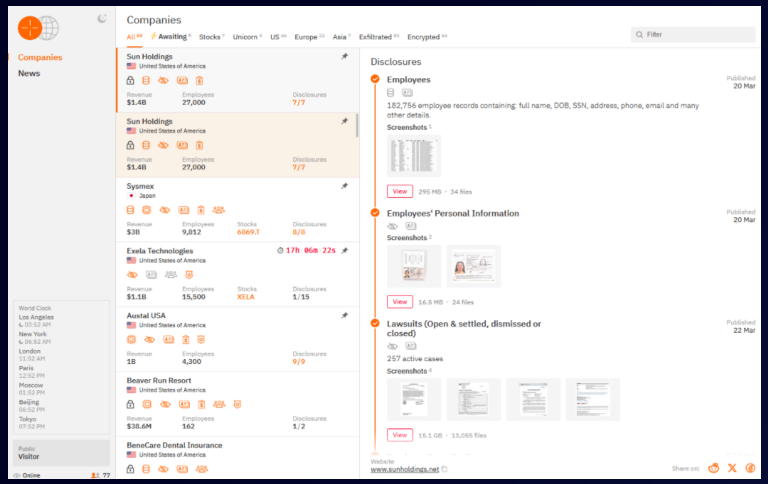

Figure 2: Leak Site of Hunters International Ransomware

Hunters International primarily targets Windows and Linux environments. Here's a breakdown of their attack methods:

Data Exfiltration: Similar to its predecessor, Hunters International prioritises exfiltrating sensitive data before encryption. This stolen information becomes leverage for double extortion tactics.

Encryption: The ransomware encrypts the victim's data, hindering access and demanding a ransom payment for decryption. The specific encryption algorithm used by Hunters is not definitively known in publicly available reports.

Victim Targeting: Hunters International appears to target a broad range of industries, including healthcare, as evidenced by an attack on a plastic surgery clinic where patient data was stolen.

Intelligence indicates that Hunters International primarily aims to exfiltrate data and extort victims with ransom demands. Notably, they targeted a US plastic surgery clinic, compromising data of around 248,000 files, including patient information. The ransomware appends ".LOCKED" to encrypted files and leaves "Contact Us.txt" instructions for victims to initiate negotiations on the dark web. Although the goal is to encrypt files, it will skip the following:

Files in folders with these substrings in their names: $Recycle bin, $windows.~bt, $windows.~ws, all users, appdata, boot, config.msi, default, Google, Intel, Mozilla, MSOcache, perflogs, system volume information, tor browser, internet explorer, windows, windows.old, windows nt.

Files named: autorun.inf, bootfont.bin, boot.ini, bootsect.bak, desktop.ini, iconcache.db, ntldr, ntuser.dat, ntuser.dat.log, ntuser.ini.log, thumbs.db

Files with the following extensions: 386, adv, ani, bat, bin, cab, cmd, com, cpl, cur, deskthemepack, diagcab, diagcfg, diagpkg, dll, drv, exe, hlp, hta, icl, icns, ico, ics, idx, key, ldf, lnk, lock, mod, mpa, msc, msi, msp, msstyles, msu, nls, nomedia, ocx, pdb, prf, ps1, rom, rtp, scr, shs, spl, sys, theme, themepack, wpx

```
To contact us follow the instructions:

1) Install and run â  Tor Browserâ   from https://www.torproject.org/download/
2) Go to https://hunters33mmcwww7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.onion/
or https://hunters33dootzzwybhxyh6xnmumopeoza6u4hkontdqu7awnhmix7ad.onion/
3) Log in using the credentials: [snip]

---
Don't waste time. Inform your CEO about the incident ASAP. Show Data Leak Site:
https://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/
or https://hunters55atbdusuladzv7vzv6a423bkh6ksl2uftwrxyuarbzlfh7yd.onion/
```

Figure 3: Ransom Note of the Hunters International Ransomware

Hunters International remains a relatively new threat actor, but their connection to Hive and their aggressive tactics warrant close attention. By prioritising data security, staying informed about evolving threats, and implementing strong cybersecurity measures, organisations can minimise the risk of falling victim to Hunters International.

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1047	Windows Management Instrumentation
Defence Evasion	T1497.003 T1622	Virtualization/Sandbox Evasion: Time Based Evasion6 Debugger Evasion
Discovery	T1057 T1082 T1083 T1135	Process Discovery System Information Discovery File and Directory Discovery Network Share Discovery
Impact	T1486 T1489 T1490	Data Encrypted for Impact Service Stop Inhibit System Recovery1

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onio hxxp://hunters33mmcwww7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.onion hxxp://hunters55atbdusuladzv7vzv6a423bkh6ksl2uftwrxyuarbzlfh7yd.onion	URLs	Onion Leak Site
hxxp://huntersinternational.org	URL	Leak Site
c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e	File Hash (SHA256)	Executable
.LOCKED	File Extension	Encrypted Files
.Contact Us.txt	Files Extension	Ransomware Note

In a comprehensive analysis of ransomware victims across 19 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 53% victim updates in the past week. The following list provides a breakdown of the number and percentage of new ransomware victims per country, underscoring the persistent and concerning prevalence of ransomware attacks, with the USA particularly susceptible to these cybersecurity threats.

Industry	Victims Count (%)
Argentina	1.54%
Austria	1.54%
Brazil	1.54%
Canada	6.15%
Ecuador	1.54%
Germany	4.62%
India	3.08%
Italy	3.08%
Japan	3.08%
Poland	1.54%
Seychelles	1.54%
Singapore	1.54%
South Korea	1.54%
Spain	4.62%
Switzerland	1.54%
UAE	1.54%
UK	6.15%
USA	53.85%

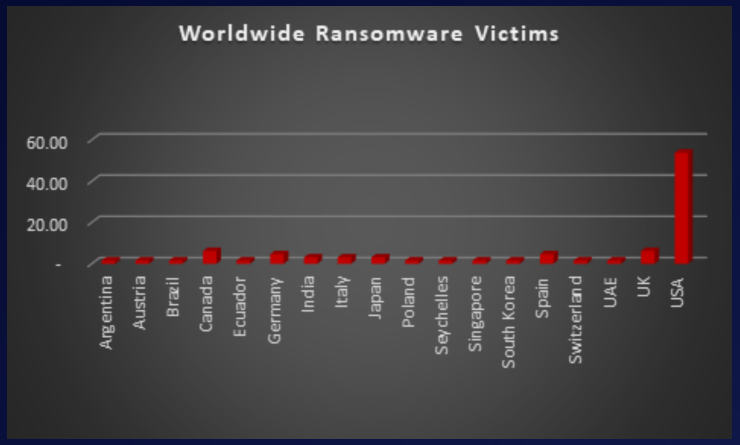

Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 16 different industries worldwide. Notably, the Manufacturing industry bore the brunt of the attacks in the past week, accounting for 27% of victims. The table below delineates the most recent ransomware victims, organised by industry, shedding light on the sectors grappling with the significant impact of these cyber threats.

Industry	Victims Count (%)
Business Services	6.15%
Cities, Towns & Municipalities	1.54%
Construction	12.31%
Consumer Services	3.08%
Finance	1.54%
Government	1.54%
Healthcare	4.62%
Hospitality	4.62%
Insurance	3.08%
IT	4.62%
Legal Services	1.54%
Manufacturing	27.69%
Real Estate	4.62%
Retail	12.31%
Telecom	6.15%
Transportation	4.62%

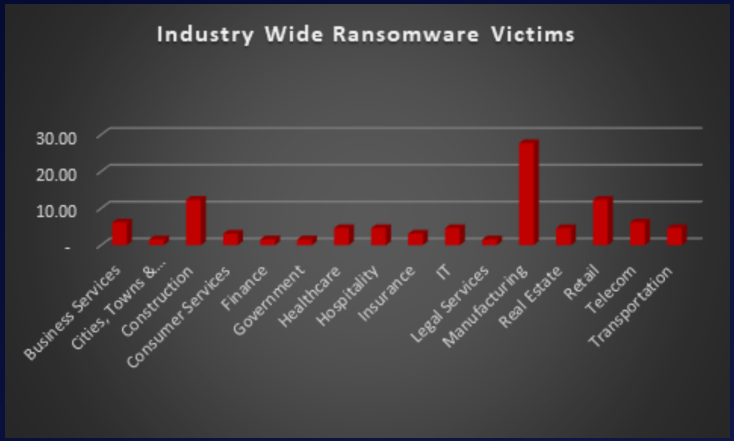

Figure 5: Industry-wise Ransomware Victims