
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Sept 05 - 11, 2023

Report Summary:

- **New Threat Detection Added** – 3 (Bumblebee Malware, Red Wolf APT, and AMOS MacOS Stealer)
- **New Threat Protections - 10**
- **New Ransomware Victims Last Week - 87**

Newly Detected Threats Added

1. Bumblebee Malware

The Bumblebee malware, designed for enterprise targeting, spreads via Google Ads and SEO manipulation, masquerading as popular software like Zoom, Cisco AnyConnect, ChatGPT, and Citrix Workspace. Initially discovered in April 2022, it is believed to be Conti's successor to the BazarLoader backdoor, serving as an entry point for network access and ransomware attacks. In September 2022, a new variant surfaced, employing a stealthier attack approach using the PowerSploit framework for reflective DLL injection into memory. A Google Ad campaign, detected by SecureWorks, introduced this malware, leading users to a deceptive Cisco AnyConnect download page. This campaign exposed corporate users to ransomware attacks, with the threat actor deploying various tools for lateral movement, network reconnaissance, and data exfiltration, raising concerns about impending ransomware deployments.

Threat Protected: 02
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Execution T1047 - Persistence T1574.002 - Privilege Escalation T1574.002 - Defence Evasion T1027/1036 - Discovery T1018 – Command-and-Control T1071/T1095

2. Red Wolf APT

Red Wolf, known for corporate espionage since 2018, continues to target commercial organisations in Russia, Canada, Germany, Norway, Ukraine, and the UK. They employ phishing emails to infiltrate their targets and deliver malware through disk images, making detection challenging. Once inside a system, they send compromised data to their command-and-control server and deploy additional malware. Unlike state-sponsored espionage groups, Red Wolf focuses on commercial firms, operating stealthily within compromised IT infrastructures for up to six months. Their ability to evade traditional defences and minimize detection is notable.

Threat Protected: 02
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Execution T1129 - Privilege Escalation T1055 - Defence Evasion T1027/T1055/T1497 - Discovery T1018/T1033/1082 - Command-and-Control T1071/T1095/T1573

3. AMOS MacOS Stealer

A recent campaign was discovered pushing both Windows and Mac malware, particularly an updated version of Atomic Stealer (AMOS) for Mac. AMOS, introduced in April 2023, focuses on stealing crypto assets and can harvest passwords from browsers and Apple's keychain while featuring a file grabber. The developer has actively updated the software, with a new version released in June.

Cybercriminals have been distributing this toolkit primarily through cracked software downloads and by impersonating legitimate websites. They also employ ads on search engines like Google to entice victims.

Threat Protected: 06
Rule Set Type:

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

Class Type: Trojan-activity
Kill Chain: Initial Access T1189/T1566 - Collection T1119 - Credential Access T1555

Known exploited vulnerabilities (Week 2 September 2023):

Vulnerability	Description
CVE-2023-33246	Apache RocketMQ Command Execution Vulnerability

Updated Malware Signatures (Week 2 September 2023)

Threat	Description
Vidar	A stealer designed to collect sensitive data from infected machines. It usually targets Windows-based machines and is spread through email attachments or downloads from compromised websites.
Ramnit	A banking trojan used to steal online banking credentials.
Bifrost	A remote access trojan that enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails.
LokiBot	An information-stealer malware used to gather data from victims' machines such as stored account credentials, banking information and other personal data.
XtremeRAT	A remote access trojan interacts with the infected machine via a remote shell, uploads/downloads files, and records from a webcam/microphone.

New Ransomware Victims Last Week: 87

Red Piranha proactively gathers information about organisations impacted by ransomware attacks through various channels, including the Dark Web. In the past week, our team identified a total of 87 new ransomware victims or updates in a few past victims from 18 distinct industries across 18 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0, a specific ransomware, has affected the largest number of victims (22) updates spread across various countries. Cactus and Ransomed updated 22 & 17 victims, respectively. Below are the victim counts (%) for these ransomware groups and a few others.

Name of Ransomware Group	Percentage of new Victims last week
8Base	4.60 %
Akira	1.15%
AlphV	5.75%
Bianlian	1.15%
BlackByte	3.45%
Cactus	19.54%
Dunghill Leak	1.15%
Everest	3.45%
Incransom	2.30%
Knight	1.15%
LockBit3.0	25.29%
Medusa	2.30%
MoneyMessage	1.15%
Play	6.90%
Qilin	1.15%
Ragnarlocker	2.30%
RaGroup	3.45%
Ransomed	9.20%
Snatch	1.15%
Stormus	1.15%
Trigona	2.30%

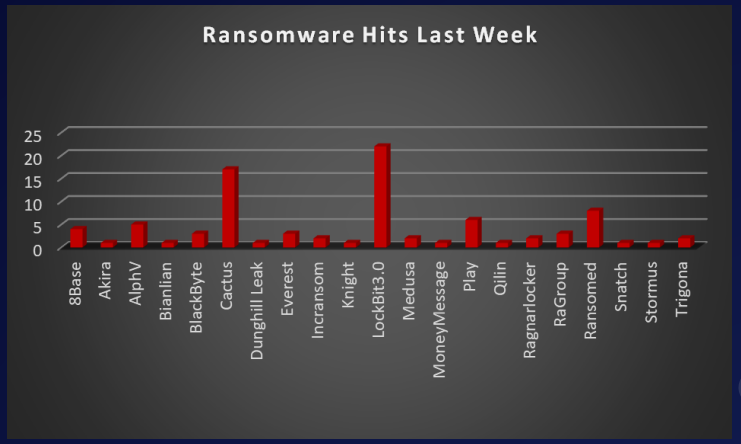

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 18 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 50 victims reported last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Australia	6.90%
Belgium	3.45%
Brazil	3.45%
Canada	3.45%
France	3.45%
Germany	2.30%
India	3.45%
Italy	1.15%
Korea	1.15%
Mexico	1.15%
Singapore	1.15%
South Africa	1.15%
Spain	1.15%
Sweden	1.15%
Turkey	1.15%
UK	5.75%
USA	57.47%
Vietnam	1.15%

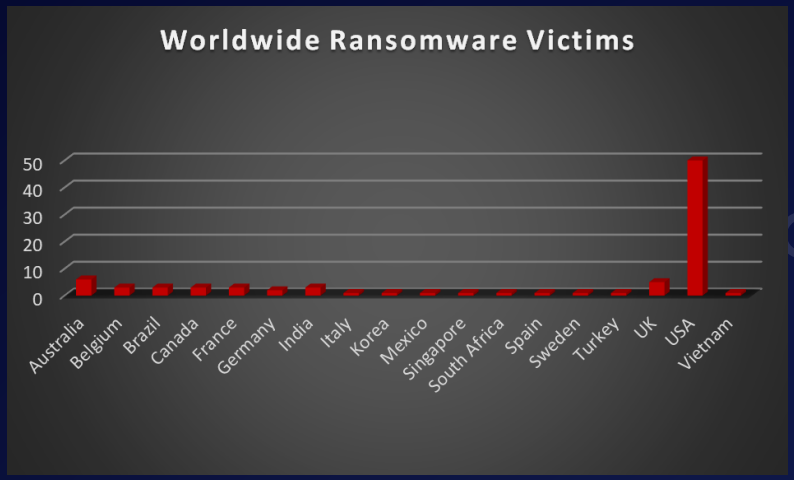

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 18 industries globally. Last week, the Manufacturing and Retail sectors were hit particularly hard, with 16% and 14% of the total ransomware victims belonging to each of those sectors, respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Business Services	12.64%
Construction	8.05%
Consumer Services	3.45%
Education	3.45%
Energy, Utilities & Waste Treatment	2.30%
Finance	4.60%
Healthcare	6.90%
Hospitality	2.30%
Insurance	2.30%
IT	5.75%
Legal Services	3.45%
Manufacturing	16.09%
Media & Internet	2.30%
Metals & Mining	1.15%
Mining & Metals	1.15%
Real Estate	6.90%
Retail	14.94%
Transportation	2.30%

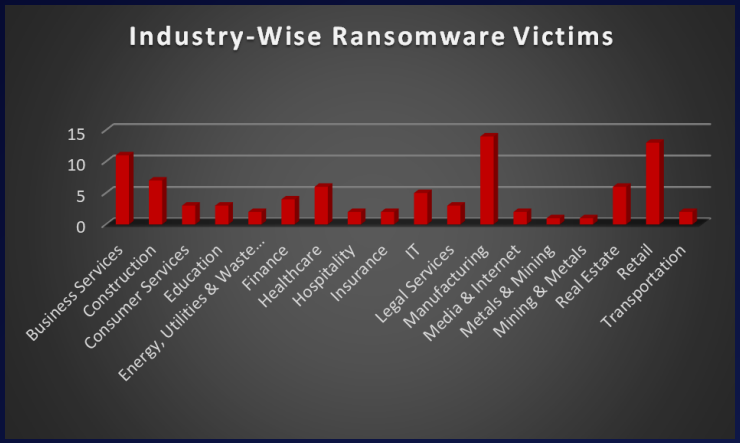

Figure 3: Industry-wise Ransomware Victims