Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 24 - 30, 2023

Report Summary:

- **New Threat Detection Added** – 4 (RogueRaticate, GoLang Easy Stealer, DarkCrystal RAT and NetDooka Malware)
- **New Threat Protections - 13**
- **New Ransomware Victims Last Week - 89**

Newly Detected Threats Added

1. RogueRaticate

A new emerging threat has surfaced within the realm of "fake updates". This recently unveiled campaign, dubbed FakeSG, leverages compromised WordPress websites to present a tailored landing page mirroring the user's browser. Malicious actors behind this scheme disseminate the NetSupport RAT through either a zipped download or an Internet shortcut. Its main goal is to install fake updates on users' browsers to steal saved credentials.

Threat Protected: 07
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: Initial Access T1189 - Credential Access T1555

2. GoLang Easy Stealer

This stealer is available for purchase on underground markets which offers a range of capabilities that targets cryptocurrency wallets and passwords. The GoLang Easy Stealer seems to have connections to several recent infection chains, including potential links to Wasabi Seed, a component utilised in a recent campaign called "Screentime". It advertises to collect passwords, cookies, autofill history, and banking information for browsers; 50+ crypto wallets, it works in-memory and supports PE and DLL formats.

Threat Protected: 02
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: Execution T1059 - Credential Access T1555 - Collection T1005

3. DarkCrystal RAT

Ukraine's government Computer Emergency Response Team, CERT-UA, has received concerning reports regarding the distribution of suspicious emails. These emails, originating from addresses within the gov.ua domain, appear to be compromised. The subject line reads Free primary legal assistance, and they include an RAR attachment Algorithm of actions of family members of a missing military serviceman. Within this RAR archive lies a document ostensibly addressing legal aid issues. However, when the document is opened and its macro activated, a PowerShell command triggers the download and execution of the .NET loader. This loader, in turn, fetches and deploys the DarkCrystal RAT malware. The choice of email recipients and the DarkCrystal RAT's control domain suggest that the attack is aimed at Ukrainian telecommunications operators and providers.

Threat Protected: 02
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: Execution T1059/T1064/T1203 - Persistence T1137 - Privilege Escalation T1055 - Defence Evasion T1027.002/T1036/T1497 - Discovery T1010/T1018 - Collection T1005 - Command-and-Control T1071/T1105

4. NetDooka Malware

Researchers recently encountered a highly sophisticated malware framework dubbed NetDooka, named after its components. This framework is distributed through a pay-per-install (PPI) service and comprises a loader, dropper, protection driver, and a full-featured remote access trojan (RAT) with its own communication protocol. The analysis revealed that NetDooka spreads via the PrivateLoader malware, initiating the entire infection chain. PrivateLoader serves as a downloader, responsible for installing various malware components as part of the PPI service. The specific payloads installed can vary depending on the malware version, with known families like SmokeLoader, RedLine, and Anubis distributed via PPI services. The inclusion of a malicious driver expands the attack surface, enabling attackers to employ various tactics, including process and file protection, antivirus evasion, and concealing malware and network communications. With the RAT payload, malicious actors can steal critical information, gain remote control, and create botnet networks. NetDooka serves as an entry point for additional malware.

Threat Protected: 02
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: Persistence T1546 - Privilege Escalation T1055 - Defence Evasion T1036/T1055/T1497 - Discovery T1010/T1012 - Collection T1113 - Command-and-Control T1071

Known exploited vulnerabilities (Week 4 October 2023):

Vulnerability	Description
CVE-2023-20273	Cisco IOS XE Web UI Command Injection Vulnerability
CVE-2023-5631	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability

Updated Malware Signatures (Week 4 October 2023)

Threat	Description
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
Agent Tesla	AgentTesla is a remote access trojan designed to log keystrokes and make efforts to pilfer sensitive data from web browsers and other installed software applications.
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
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.
HawkEye	A trojan and keylogger used to steal various account credentials.
DarkKomet	A remote access trojan that can take full control over an infected machine.

New Ransomware Victims Last Week: 89

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 89 new ransomware victims or updates in few past victims from 20 distinct industries across 16 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

NoEscape, a specific ransomware, has affected the largest number of victims (31) updates spread across various countries. LockBit3.0 and 8Base ransomware groups updated 13 & 11 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
3Am	2.25%
8Base	12.36%
Abyss-Data	1.12%
Akira	2.25%
Alphv	7.87%
Blackbasta	4.49%
Cuba	1.12%
Donutleaks	1.12%
Hunters	1.12%
Inc Ransom	1.1% 2
Lockbit3	14.61%
Lorenz	1.12%
Mallox	1.12%
Medusa	4.49%
Monti	1.12%
NoEscape	34.83%
Qilin	2.25%
Ransomhouse	1.12%
Ransomware Blog	2.25%
Snatch	2.25%

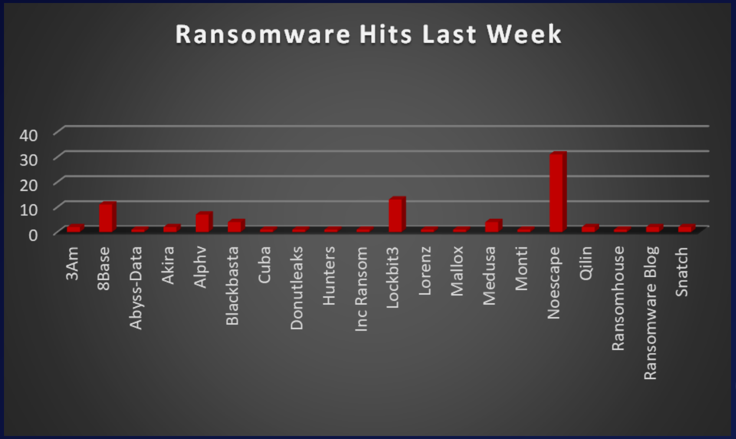

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 16 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 47 victims updates last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Australia	2.25%
Belgium	1.12 %
Canada	7.87%
Chile	1.12%
China	1.12%
Czech Republic	1.12%
France	4.49%
Germany	2.25%
India	1.12%
Italy	2.25%
Mexico	1.12%
South Korea	1.12%
Spain	4.49%
UAE	2.25%
UK	13.48%
USA	52.81%

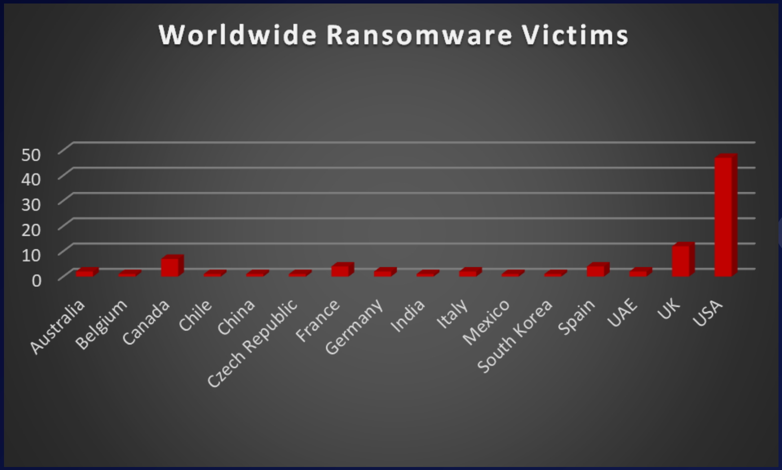

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 20 industries globally. Last week, the Manufacturing and Retail sectors were hit particularly hard, with 19% 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	7.87%
Cities, Towns & Municipalities	2.25%
Construction	10.11%
Consumer Services	4.49%
Education	6.74%
Energy, Utilities & Waste Treatment	1.12%
Finance	2.25%
Government	2.25%
Healthcare	5.62%
Hospitality	1.12%
Insurance	2.25%
IT	1.12%
Legal Services	3.37%
Manufacturing	19.10%
Media & Internet	2.25%
Organisations	3.37%
Real Estate	4.49%
Retail	14.61%
Telecom	1.12%
Transportation	4.49%

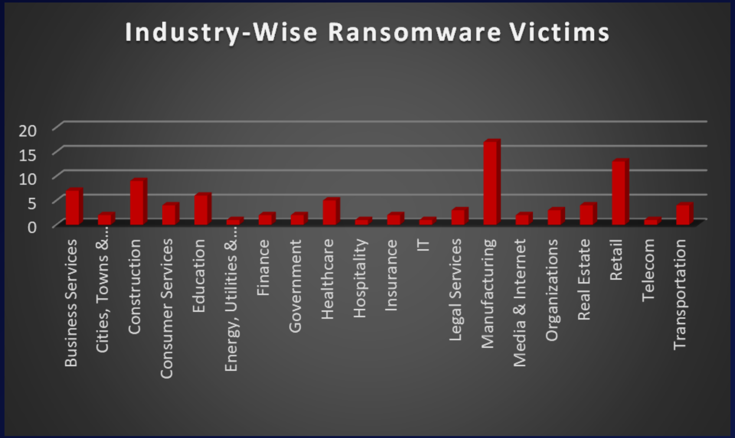

Figure 3: Industry-wise Ransomware Victims