Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 12 - 18, 2023

Report Summary:

- **New Threat Detection Added** – 3 (KandyKorn Malware, DarkGate Malware and ClearFake)
- **New Threat Protections - 11**
- **New Ransomware Victims Last Week - 100**

Newly Detected Threats Added

1. KandyKorn Malware

A new macOS malware called KandyKorn, designed to target cryptocurrency engineers has been detected in the wild. KandyKorn employs sophisticated techniques, including social engineering tactics and a malicious payload hidden in a decoy document. The malware aims to compromise the security of cryptocurrency wallets and steal sensitive information. Researchers emphasize the importance of user awareness and caution against clicking on unfamiliar links or downloading suspicious files. This has become a warning to the crypto community and need for robust security measures.

Threat Protected: 05
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: Discovery T1082 - Command-and-Control T1071/T1095/T1573

2. DarkGate Malware

The new DarkGate is a threat that uses various tricks to spread. It can show up through harmful ads, fake search results, and spam emails. DarkGate is good at hiding from security tools. It's like a ninja on your computer – it hides in the Task Manager and starts up secretly. It can take control of your computer, do things with your files, and even give itself special powers. This means it can cause more problems, like letting in other harmful stuff, such as viruses or programs that demand money. DarkGate is like a spy tool which can steal your internet history, saved passwords, and even record what you type on your keyboard.

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 T1129 - Privilege Escalation T1055 - Defence Evasion T1027/ T1497 - Discovery 1082 - Command-and-Control T1095/T1573

3. Clearfake

Multiple malicious fake update campaigns are active impacting numerous compromised websites. This is a campaign called ClearFake which was observed to have started around July 19th, 2023. A PublicWWW search for the injection base64 reveals at least 434 infected sites.

The name "ClearFake" is coined due to the prevalent use of unobfuscated Javascript, with only three instances of base64. When users access a compromised ClearFake website, the page initially loads normally before a takeover occurs, prompting a Chrome update. Once a user has downloaded the fake chrome update, it installs the 'Amadey Stealer' malware. This malware is designed to gather important and sensitive information from the victim machine.

Threat Protected: 04
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

Known exploited vulnerabilities (Week 2 December 2023):

Vulnerability	Description
CVE-2023-6448	Unitronics Vision PLC and HMI Insecure Default Password Vulnerability

Updated Malware Signatures (Week 2 December 2023)

Threat	Description
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.
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
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.
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.
CoinMiner	This malicious software installs and runs cryptocurrency mining applications.

New Ransomware Victims Last Week: 100

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 100 new ransomware victims or updates in the few past victims from 19 distinct industries across 26 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0 ransomware group has affected the largest number of 23 victims' updates spread across various countries. Dragonforce and Siegedsec ransomware groups updated 17 and 13 new 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%
8Base	9%
Akira	7%
Alphv	1%
Bianlian	4%
Blackbasta	4%
Cactus	2%
Daixin	1%
Dragonforce	17%
Hunters	2%
Inc Ransom	1%
Knight	1%
Lockbit3	23%
Lorenz	1%
Medusa	2%
Meow	2%
Play	1%
Ransomhouse	1%
Raznatovic	2%
Rhysida	4%
Siegedsec	13%

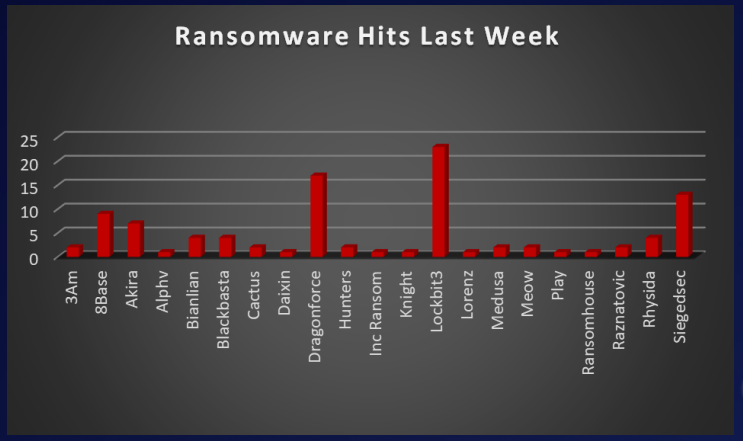

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 26 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 55 victims updates last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Argentina	3%
Australia	4%
Belgium	3%
Brazil	2%
Canada	1%
China	3%
Denmark	1%
Germany	1%
India	1%
Israel	2%
Italy	1%
Japan	1%
Kenya	1%
Mexico	2%
Netherlands	2%
Peru	1%
Poland	1%
Qatar	2%
Singapore	2%
Slovenia	1%
South Africa	1%
Spain	1%
Sweden	1%
Switzerland	1%
UK	6%
USA	55%

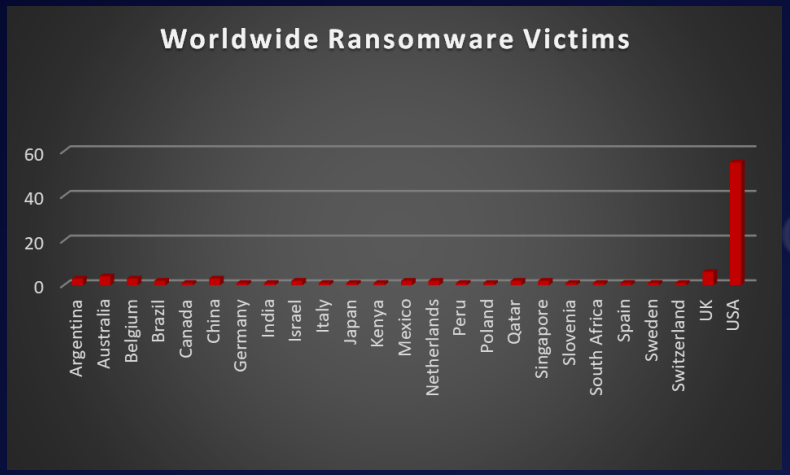

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 19% and 15% 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	15%
Construction	6%
Consumer Services	2%
Education	5%
Energy, Utilities & Waste Treatment	4%
Finance	5%
Government	4%
Healthcare	10%
Hospitality	5%
IT	4%
Legal Services	2%
Manufacturing	19%
Media & Internet	2%
Metals & Mining	1%
Organisations	2%
Real Estate	2%
Retail	6%
Telecom	2%
Transportation	4%

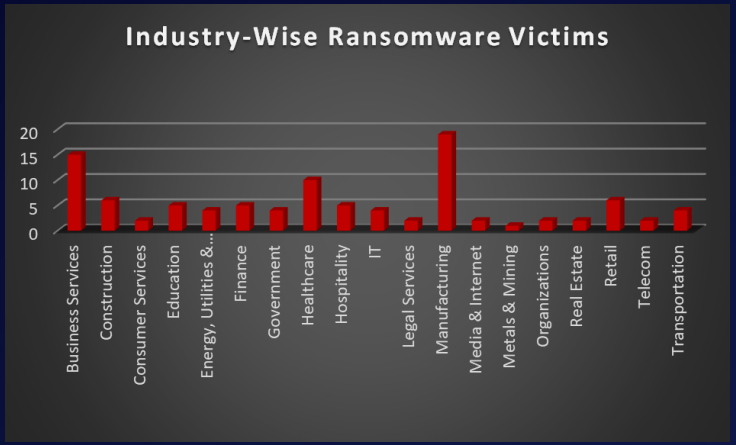

Figure 3: Industry-wise Ransomware Victims