Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 20 - 26, 2022

Report Summary:

- **New Threat Detection Added** – 06 (DarkTortilla Malware, Venom RAT, RisePro, Vultur Malware, HyperBro RAT, and Adwind RAT)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

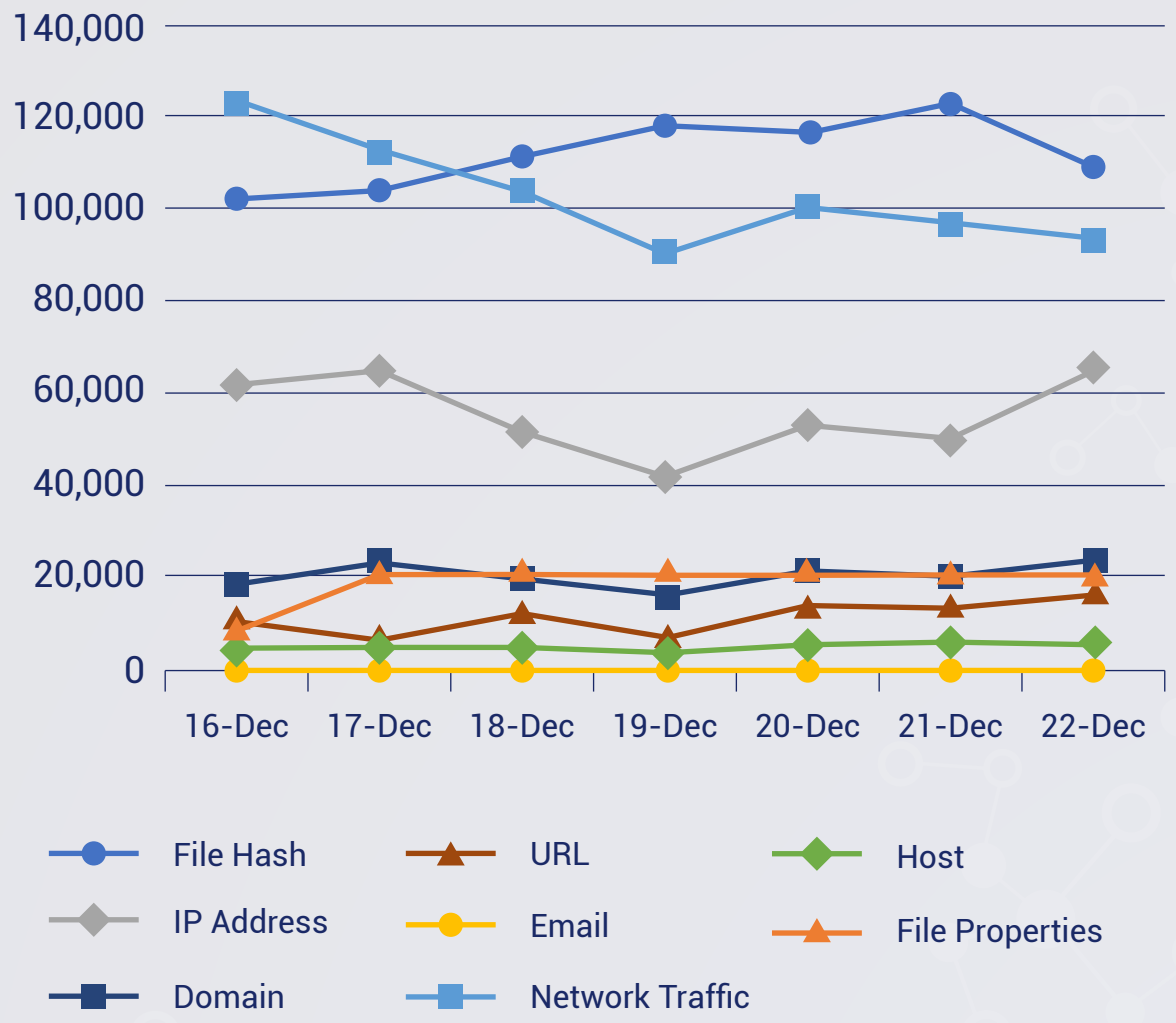
New Threat Protections (Week Ending 26/12/2022):

17

Overall Weekly Observables Count:

2,259,160

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. DarkTortilla Malware

Researchers recently identified a malicious campaign where they observed Threat Actors (TAs) releasing the DarkTortilla malware. DarkTortilla is a complex .NET-based malware that has been active since 2015. This malware is known to remove several thieves and remote access trojans (RATs) such as AgentTesla, AsyncRAT, NanoCore, etc. According to their analysis, DarkTortilla targets users via spam email with malicious attachments. However, researchers discovered that the Threat Actors (TAs) behind DarkTortilla created phishing pages to distribute the malware. Two phishing sites pretending to be legitimate Grammarly and Cisco. A link to phishing sites could reach users through spam emails or online ads, etc. to infect them. In this campaign, TAs use typo phishing pages to deliver the DarkTortilla malware. Files downloaded from phishing sites show different infection techniques, suggesting that TAs should have a sophisticated platform capable of customizing and compiling the binary using various options.

Threat Protected: 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: Initial Access T1566 - Execution T1204 - Persistence T1547.001 - Defense Evasion T1140/T1562 - Command and Control T1071

2. Venom RAT

A newer version of popular remote administration malware called Venom RAT has been detected in the wild. A Remote Access Trojan is a tool used by Threat Actors (TAs) to gain full access and remote control of a victim's machine, including mouse and keyboard control, file access, access to network resources etc. The latest version of the Venom RAT has a thief module that steals sensitive information and exfiltrates the stolen data from the victim's machine to its C&C server. The older version of Venom includes features like remote access, HVNC (Hidden Virtual Network Computing – taking control of the victim's computer without their knowledge), keylogger, etc.

Threat Protected: 01
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 T1204/T1059/T1047- Persistence T1053 - Privilege Escalation T1055 -Defense Evasion T1036/T1562/T1497 - Credential Access 1056/T1003-Discovery T1057/T1082/T1518 - Collection T1005 - Command and ControlT1071/T1105

3. RisePro

RisePro is a stealer malware being sold on Russian Black Markets that also appears to be affiliated with a 'pay-per-install' service called 'PrivateLoader'. It is written in C++ and is created to steal and exfiltrate sensitive information from its victims. The analysis also reveals that it is highly likely to be a clone of another stealer that goes by the name 'Vidar'.

Threat Protected: 10
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: Initial Access T1189/T1566 - Execution T1059 – Command and Control T1102 - Exfiltration T1567

4. Vultur Malware

Vultur is an android malware that steals sensitive information from its victims. Most of the targeted victims reside in Italy, the UK, Australia, and the Netherlands. Its primary goal is to steal banking information from its victim's phones. However, due to its keylogging capabilities, leaked data shows that social media information from TikTok, Facebook and WhatsApp are also affected. The malware is dropped through an app called 'Brunhilda' which was also found on authentication, fitness, and security-related apps that are available in the Google Play Store. One prominent indication of infection is that the 'Casting' icon appears on the phone when it is not.

Threat Protected: 01
Rule Set Type:

Class Type: Trojan-activity

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

5. HyperBro RAT

HyperBro is a RAT that has been observed to target primarily within the gambling industries, though it has been spotted in other places as well. The malware typically consists of 3 or more components:

a) a genuine loader typically with a signed certification
b) a malicious DLL loader loaded from the former component via DLL hijacking
c) an encrypted and compressed blob that decrypts to a PE-based payload that has its C2 information hardcoded within.

HyperBro is a custom in-memory backdoor used by Threat Group-3390. It is used in the last stage of the attacks to gain access to the infected systems.

Threat Protected: 01
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Execution TA0002 - Privilege Escalation TA0004 - Defense Evasion TA0005

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

6. Adwind RAT

Adwind RAT is a cross-platform, multifunctional remote access program which is distributed through a single malware-as-a-service platform. It checks the system to see if it is running in a Virtual Environment. Adwind RAT infects the victim's machine by initial infection vectors of spam campaign with attachment (EML), and a suspicious URL to download the malware. The attachment is a MS Word document (.DOCX). The threat actor can trick the user to click on the blurred image to view the document's content. Once the user opens the .img content, using embedded doc to drop the .JAR file in the %temp% folder to start infecting and perform threat actor's action on objective.

Threat Protected: 03
Rule Set Type:

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

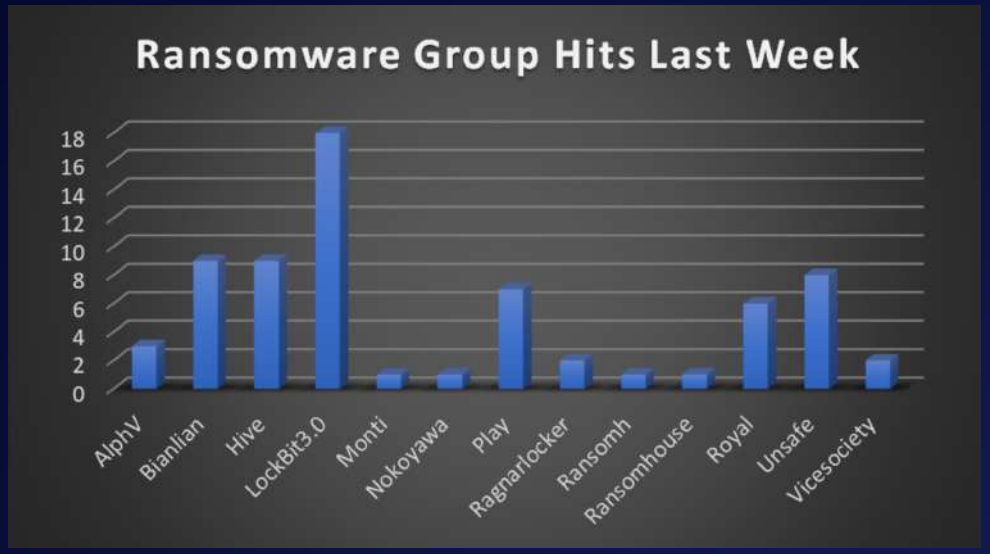
Class Type: Trojan-activity
Kill Chain: Initial Access T1189/T1566 - Execution T1059 - Command-and-Control T1102 - Exfiltration T1567

New Ransomware Victims Last Week: 68

Red Piranha regularly collects information about organizations hit by ransomware from different sources, including the Dark Web. During the previous week, Red Piranha identified a total of 68 new ransomware victim organizations in 26 different countries all over the world.

The ransomware group named LockBit 3.0 once again tallied the greatest number of new victims (18), the locations of which are spread across different countries. This is followed by Hive and Bianlian groups with 9 new victims each. Below are the rest of the ransomware groups and the number of reported victims.

Name of Ransomware Group	No of new Victims last week
AlphV	3
Bianlian	9
Hive	9
LockBit3.0	18
Monti	1
Nokoyawa	1
Play	7
Ragnarlocker	2
Ransomh	1
Ransomhouse	1
Royal	6
Unsafe	8
Vicesociety	2



If we look at the victims as per the country, we can say that the USA has once again become the most affected country by ransomware groups where a total of 22 new victims were reported last week, followed by Canada and New Zealand where 6 and 5 new victims respectively were reported. The number of new ransomware victims per country is listed below:

Name of the effected Country	Number of Victims
Argentina	1
Australia	3
Azerbaijan	1
Brazil	4
Canada	6
Colombia	1
France	2
Germany	1
Greece	1
Hong Kong	1
India	3
Indonesia	1
Italy	1
Japan	2
Kenya	1
Kuwait	1
New Zealand	5
Oman	1
Singapore	1
Spain	1
Sweden	1
Texas	3
UK	1
USA	22
Venezuela	2
West Yorkshire	1