Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 29 - Dec 5, 2022

Report Summary:

- **New Threat Detection Added** – 06 (Vidar, Mustang Panda, LoanBee Fraud App, Xiongmai IoT Exploit, DTrack, and Vultur)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

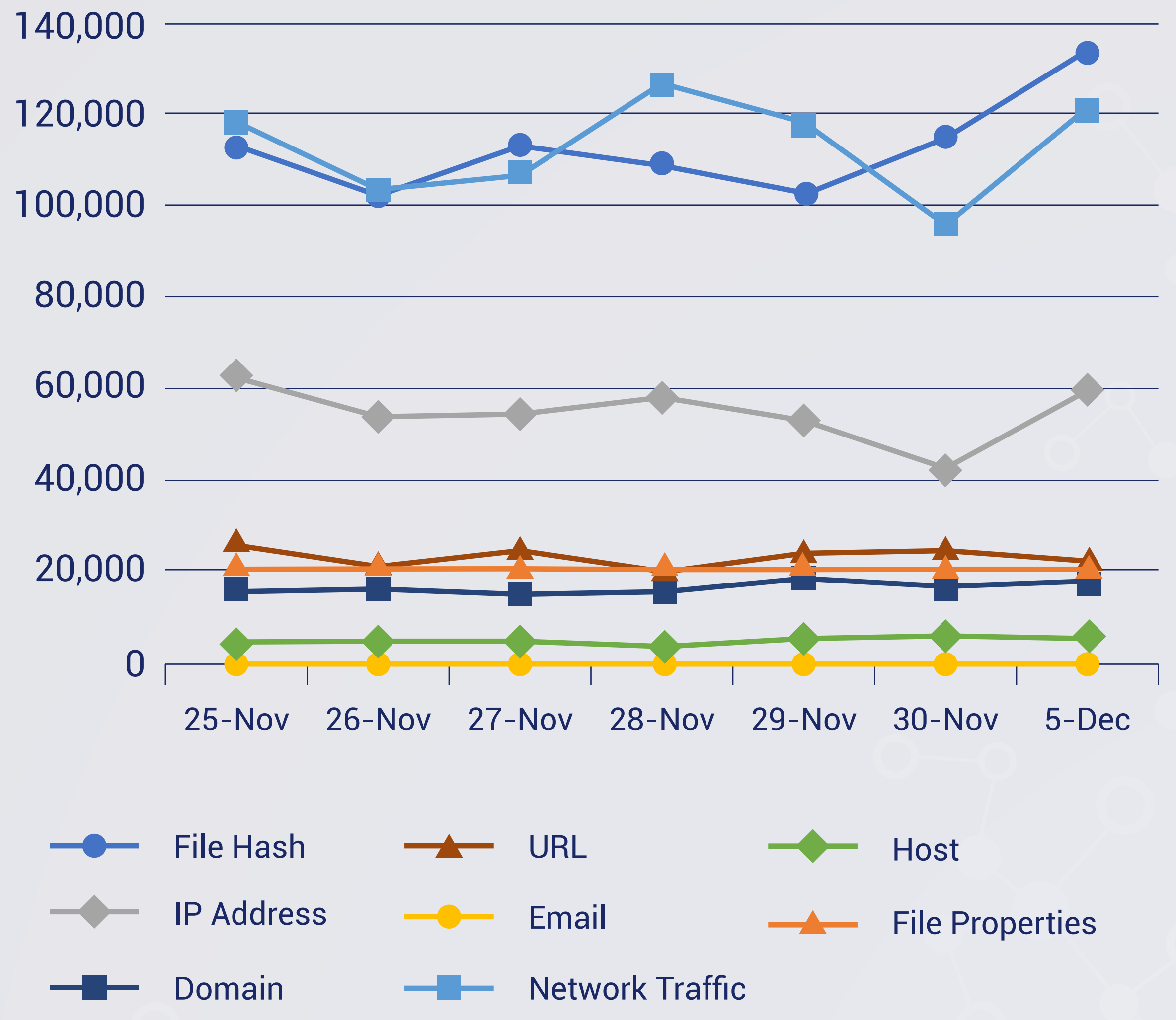
New Threat Protections (Week Ending 05/12/2022):

14

Overall Weekly Observables Count:

2,390,769

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Vidar

Threat Actors (TAs) found using the latest variant of stealer malware named Vidar malware to steal credentials from victims' devices. The Vidar malware was first identified in 2018. It is capable of stealing sensitive data from the victim's PC, including banking information, saved passwords, IP addresses, browser history, login credentials, and crypto wallets. It then transferred all stolen data to the TAs Command and Control (C&C). Researchers identified that the TAs use delivery mechanisms such as spam mail, cracked software, keygens, etc., to distribute this malware. The malware downloads configuration data from the C&C and other payloads/modules to extract credentials from the victim's device and perform data exfiltration.

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 - Credential Access T1555 /T1539 /T1552 - Collection T1113 - Discovery T1087/ T1518/T1057/ T1007/T1614 - Command and Control T1095 - Exfiltration T1041

2. Mustang Panda (APT)

A notorious advanced persistent threat (APT) group named Earth Preta AKA Mustang Panda or Bronze President used malware families in campaigns and attributed the incidents to them. The APT group targets people using spear-phishing attacks targeting the government, academic, foundations, and research sectors around the world. Based on the lure documents observed in the wild, this is a large-scale cyberespionage campaign that began around March 2022. After months of tracking, the seemingly wide outbreak of targeted attacks includes but is not limited to Myanmar, Australia, the Philippines, Japan, and Taiwan.

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: Resource Development T1583.004/T1587.001/T1585.002 -Inital access T1566.002 - Execution T1204.001 - Persistence T1547.001/ T1574.002/T1053.005 - Defense Evasion T1140/T1036.005 - Command -and- Control T1071.001/T1573.001/T1104/T1095

3. LoanBee Fraud App

LoanBee is a fraudulent Android app that steals its users' data. Although the app has been removed from Google Play Store, it has garnered over 100,000 installations. Upon installation, the app will require excessive permissions that will allow it to gather Device Information, Contacts, and Messages and upload it to a remote server.

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	

Class Type: Trojan- Activity
Kill Chain: Initial Access T1475/T1476 - Execution T1575 - Collection T1636 - Command-and-Control T1436

4. Xiongmai IoT Exploit

Xiongmai is a Chinese company that manufactures IP Camera/DVR/NVR modules. Through public information, there are approximately 200,000 devices exposed on the public internet. Although, there aren't many reliable public exploit codes available. Information about the firmware used by Xiongmai devices is listed on their Huawei Cloud space.

Due to the amount of exposed Xiongmai devices, combined with information about their firmware, and the availability of the actual product for purchase, these devices are likely being studied and freely exploited in the wild.

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: Web-application-attack
Kill Chain: Initial Access T0819

5. DTrack

DTrack is a backdoor used by the Lazarus group. It allows its users to upload, download, start or delete files on the victim host. Dtrack unpacks the second stage from its PE file. This process has two approaches – offset or resource-based. After retrieving the location of the next stage and its key, the malware decrypts the buffer (with a modified RC4 algorithm) and passes control to it.

Threat Protected: 08
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: Malware
Kill Chain: Execution TA0002 - Privilege Escalation TA0004 - Defense Evasion TA0005 - Credential Access TA0006 - Command and Control TA0011

6. Vultur

Unlike other banking trojans, Vultur uses screen recording based on VNC to obtain all the PII (Personal Identifiable Information). After installation, the dropper uses advanced evasion techniques, including steganography, file deletion and code obfuscation in addition to multiple checks before downloading the malware.

Upon download, the trojan gives the threat actor a clear view of everything that happens on the compromised device.

Threat Protected: 01
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
Kill Chain: Initial Access T1199 – Collection T1113