
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Dec 6 - 12, 2022

Report Summary:

- **New Threat Detection Added** – 06 (Electron Bot, RecordBreaker, CodeRat, Irafau Backdoor, Impersoni-fake-ator, and Scattered Spider)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

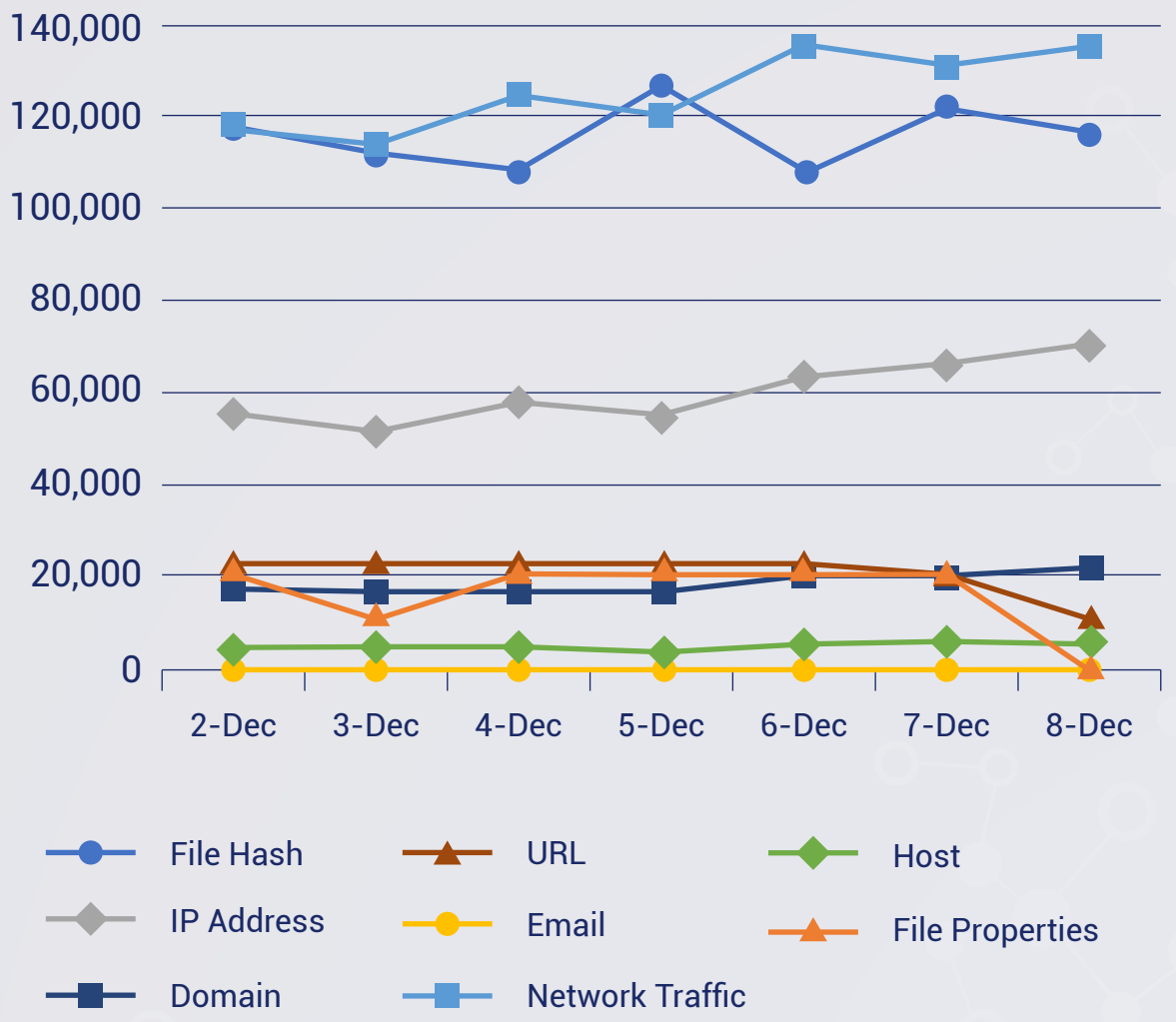
New Threat Protections (Week Ending 12/12/2022):

29

Overall Weekly Observables Count:

2,533,410

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. Electron Bot

In February 2022, researchers discovered a new malware called Electron Bot, which has reportedly infected more than 5,000 active machines worldwide to date. The malware was named based on the last campaign's C&C Electron-Bot[.]s3[.]eu-central-1[.]amazonaws domain. com. Electron Bot is a modular SEO annoying malware for social media promotion and click fraud.

It is distributed mainly through the Microsoft store platform and removed from dozens of infected applications, mostly games, which are constantly uploaded by attackers. The malware executes the attackers' commands, such as checking Facebook, Google, and Sound Cloud social media accounts. Malware can register new accounts, login, comment and "like" other posts. Electron bot is also capable of poisoning SEO, Ad Clicker, promoting social media accounts, promoting online products to generate profits with ad clicks or increase store ranking for more sales.

Threat Protected: 03
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 T1543.003/T1547.008/T1574.002 - Privilege Escalation T1543.003/ T1547.008/T1574.002 - Defense Evasion T1574.002/ TA0007 - Discovery T1082-Command and Control T1071 T1095

2. RecordBreaker

RecordBreaker is a stealth malware designed to extract and exfiltrate data and content. RecordBreaker is actively distributed through various websites offering cracked software. After successful infiltration, supported by various anti-detection measures, RecordBreaker will start collecting relevant system data. It also gets information related to installed applications. This thief can also take screenshots. However, its most harmful function is to steal cryptocurrency wallets by extracting their credentials and related data. RecordBreaker focuses on cryptocurrency-related cryptocurrency wallets and browser extensions such as AuroWallet, BinanceChain, CloverWallet, Coin98, Coinbase, CyanoWallet, Goby, GuildWallet, ICONex, Keplr, KHC, Liquality, PolyMask, MetaX, MEWne_CXme, NeoLine_CX, Ronin, SaturnWallet, Solflare, Sollet, Temple, TeraStation, TezBox, TON, TronLink, WavesKeeper, XDEFI and so on. This malicious program may also collect other data from browsers, such as Internet cookies. RecordBreaker infections can lead to serious privacy issues, significant financial losses, and even identity theft.

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- Defense Evasion T1140/T1497/T1055.012- Credential Access T1555/T1539/T1552/T1528- Collection T1113-Discovery T1518/T1124/T1007 - Command and ControlT1071-ExfiltrationT1041

3. CodeRAT

A new targetted attack has been discovered towards Farsi-speaking code developers by using a Microsoft Word document that includes a Microsoft Dynamic Data Exchange (DDE) exploit. It has been found leveraging CODERAT to gain access and control of victim devices. After gaining access, the attacker's main goal seems to be monitoring the victim's activities on the local machine and social media. This type of monitoring makes us believe that the RAT is used as an intelligence-gathering tool.

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: Execution TA0002 - Defense Evasion TA0005 - Discovery TA0007

4. Irafau Backdoor

Irafau is a backdoor used in recently discovered cyber espionage campaign in the Middle East. Upon successful delivery and execution, Irafau gathers information on target machines. It is capable of lateral movement by copying and adding itself on accessible C$ shares within the network. It uses scheduled tasks and WMI for persistence. It enables a threat actor to download and upload files from the victim machine, spawn a remote shell and execute commands.

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: Initial Access T1566 - Execution T1059/T1106 - Persistence T1053 - Command-and-Control T1102

5. Impersoni-fake-ator

Another malware recently discovered in a cyber espionage campaign in the Middle East. It is embedded into legitimate versions of Putty and DbgView. The legitimate binaries of the software were modified to execute the embedded shellcode. It will contact its Command-and-Control server for further instructions.

Threat Protected: 21
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/T1189 - Execution T1106/T1059 - Command-and-Control T1102

6. SCATTERED SPIDER

An increase in the targeting of BPO and Telcom industries has been observed. These investigations appear to be tied to a financially motivated campaign with links to an adversary known as SCATTERED SPIDER. In this attack campaign, the adversary demonstrates persistence in trying to gain access to victim environments and performs consistent activity within the target environment. It has been noticed that if mitigation measures are slowly implemented, the adversary becomes even more active, setting up additional persistence mechanisms, i.e., multiple RMM tools and/or VPN access.

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: Malware
Kill Chain: Execution TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defense Evasion TA0005 - Command and Control TA0011