Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 6 - 12, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Orchard Botnet 3.0, Redline stealer, Raspberry Robin, Erbium Stealer, Evilnum APT and MagicRAT)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

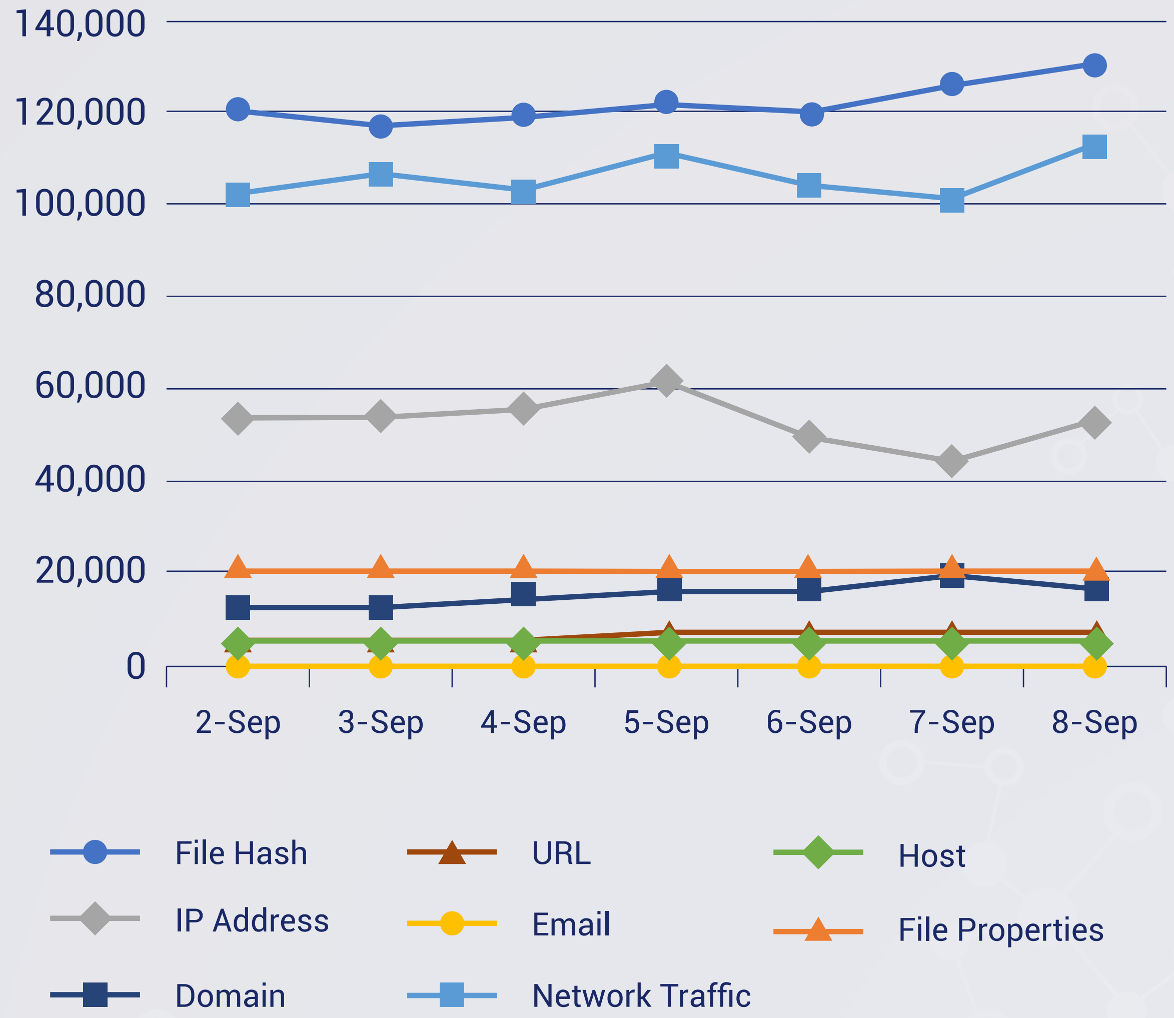
IDPS Rules Created (Week Ending 12/09/2022):

20

Overall Weekly Observables Count:

2,286,781

Daily Submissions by Observable Type:



Newly Detected Threats Added

The following threats were added to Crystal Eye XDR this week:

1. Orchard Botnet 3.0

The Orchard Botnet family was first detected in February 2021. Red Piranha has found that it is undergoing its 3rd round of changes, including switching programming languages between versions. Orchard is a botnet family that uses DGA (Domain Generation Algorithm) technology. The latest version is dedicated to mining and began using more unpredictable information such as Satoshi Nakamoto's Bitcoin account transaction information as input to DGA, increasing the difficulty of detection.

In more than 1 year, Orchard has appeared at least 3 different versions, programming language and DGA implementation have changed. This shows that Orchard is a botnet family that is still active, and is expected with more variants in the future, which is worth our vigilance. The development language for v3 is written back in C++, that also includes C2 communication and USB infection capabilities. C2 communication logic runs in a thread that also includes a worker thread bound to XMRig mining. When Orchard receives the XMrig, program issued and creates a puppet process to run, the worker thread will send mining-related hardware information to C2 again, trying to read the configuration of the mining software from C2, to check whether it is necessary to dynamically modify the configuration of the XMRig runtime. Combined with long-term tracking results and other dimensions of information, we believe that Orchard will be a long-term active, sustainable botnet family that deserves vigilance.

Rules Created: 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: Privilege Escalation T1055- Défense Evasion T1497 - Discovery TA1124 – Collection TA0007-Command and Control TA0011

2. Redline stealer

Hacked Facebook accounts belonging to a Brazilian ISP, Mexican sporting goods store, mountain tourism site from Slovakia, and a computer repair shop in the Philippines are spreading posts linking to malware to users around the world.

Stealer functionality:

- Collects information from browsers
- Login and passwords
- Cookies
- Autocomplete fields
- Credit cards
- Supported browsers:
- All browsers based on Chromium (even the latest version of Chrome)
- All Gecko-based browsers (Mozilla, etc.)
- Data collection from FTP clients, IM clients
- File-grabber customizable by Path, Extension, Search-in-subfolders (can be configured for the necessary cold wallets, Steam, etc.)
- Settings by country. Setting up a blacklist of countries where the build will not work.
- Settings for anti-duplicate logs in the panel

It collects information about the victim's system: IP, country, city, current username, HWID, keyboard layout, screenshot, screen resolution, operating system, UAC Settings, the current build running with administrator privileges, User-Agent, information about PC hardware (video cards, processors), installed antiviruses.

Performing tasks:

- Download - download a file from the link to the specified path
- RunPE - injection of a 32-bit file downloaded from a link into another file
- DownloadAndEx - download a file from the link to the specified path with the subsequent launch
- OpenLink - open a link in the default browser

Rules Created: 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

Kill Chain: Execution TA0002- Privilege Escalation TA0004- Defense Evasion TA0005 - Credential Access TA0006 - Discovery TA0007 - Collection TA0009 - Command and Control TA0011

3. Raspberry Robin

Raspberry Robin is a worm that spreads over an external drive. After the initial infection, it downloads its payload through msiexec.exe from QNAP cloud accounts, executes its code through rundll32.exe, and establishes a command and control (C2) channel through TOR connections. Raspberry Robin is delivered through infected external disks. Once attached, cmd.exe tries to execute commands from a file within that disk. This file is either a .lnk file or a file with a specific naming pattern. Files with this pattern exhibit a 2 to 5 character name with a usually obscure extension, including; .swy, .chk, .ico, .usb, .xml, and .cfg. Also, the attacker uses an excessive amount of whitespace/non-printable characters and changes the letter case to avoid string matching detection techniques.

Rules Created: 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: Input Capture T1056 - Deobfuscate/Decode Files or Information T1140 - Trusted Relationship T1199 - Native API T1106 - Signed Binary Proxy Execution T1218 - Boot or Logon Autostart Execution T1547 - Obfuscated Files or Information T1027 - Command and Control TA0011

4. Erbium Stealer

Erbium is a piece of malicious software classified as a stealer. Malware within this category is designed to extract vulnerable data from infected devices. Erbium begins its operations by gathering device data, such as CPU, GPU, RAM, operating system version and architecture, monitor number, username, Windows license key, and so forth. The program can take screenshots from all monitors connected to the infected machine. This stealer can obtain information from various installed applications. From Chromium and Gecko, Erbium can extract browsing histories, Internet cookies, autofill, passwords, and other data. This malware also targets cryptocurrency wallets. From over fifty desktop and browser crypto wallets, this malicious program seeks to obtain log-in credentials and stored funds.

Rules Created: 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: Kill Chain: Privilege Escalation T1055- Défense Evasion T1497 - Discovery TA1124 – Collection TA0007-Command and Control TA0011

5. Evilnum APT

Evilnum APT is a financially motivated hacking group known to target European organizations involved in international migration. Due to the ongoing Russia-Ukraine crisis, a spike of malicious emails containing malicious documents has been observed. These documents are loaded with a macro which executes an obfuscated JavaScript. This JavaScript drops a malware loader and creates a scheduled task as a persistence mechanism. Once the malware is loaded, it establishes communications with its Command-and-Control servers for further instructions.

Red Piranha has obtained new and updated information on the Command-and-Control domains that Evilnum is currently using. These rules are deployed to detect DNS requests for these domains.

Rules Created: 01
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1204 - Persistence T1053 - Command and Control T1102

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

6. MagicRAT

MagicRAT is a new remote access trojan operated by the Lazarus threat group. It is observed that it drops on machines that were previously attacked through a vulnerability found on VMware Horizon. Along with the usual features of a remote access trojan, such as but not limited to Screen Capture, Network tunnelling, Keylogging etc. This trojan intends to make detection and analysis harder.

Rules Created: 07
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Initial Access T1190 - Persistence T1053 - Collection T1119 - Command-and-Control T1102

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