
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Sept 13 - 19, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Worok Group, Dracarys Android Spyware, CVE-2022-28958 D-Link RCE, EvilProxy/Moloch- PhaaS, OriginLogger, and ShadowPad RAT)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

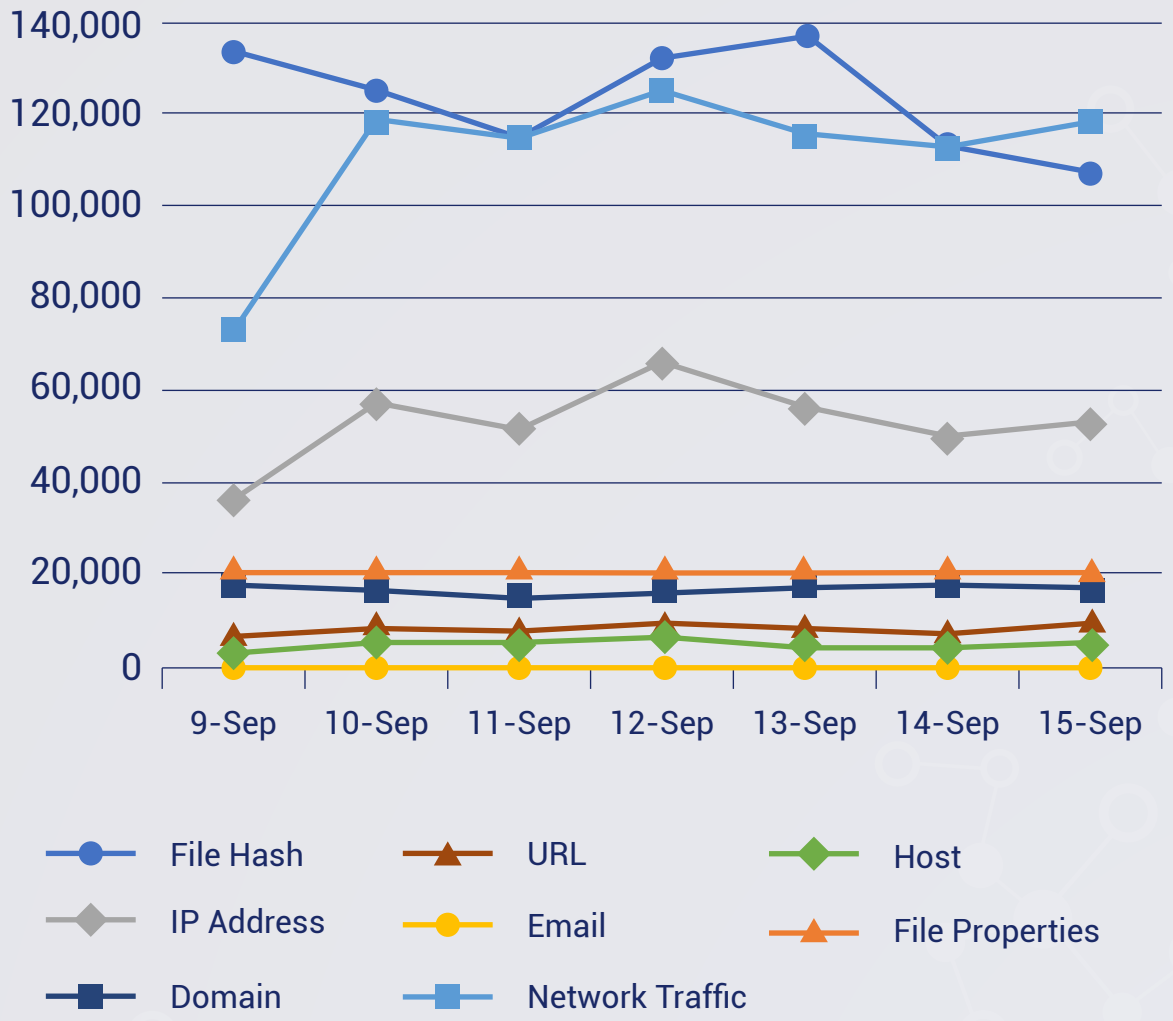
IDPS Rules Created (Week Ending 19/09/2022):

14

Overall Weekly Observables Count:

2,310,680

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Worok Group

Researchers recently found targeted attacks that used undocumented tools against various high-profile companies and local governments mostly in Asia. These attacks were conducted by a previously unknown espionage group named-Worok and which has been active since 2020. Worok's toolset includes a C++ loader CLRLoad, a PowerShell backdoor PowHeartBeat, and a C# loader PNGLoad that uses steganography to extract hidden malicious payloads from PNG files.

Rules Created: 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: Trojan-Activity
Kill Chain: Reconnaissance T1592/T1590-Resource Development T1583/T1588/T1587- Execution T1059- Persistence T1505- Defense Evasion T1140/T1036-Credential Access T1003 - Discovery T1082/T1083/T1046/T1124 -Collection T1005- Command and Control T1071/T1090/T1001/T1095- Exfiltration T1041

2. Dracarys Android Spyware

The Dracarys Spyware is an android-based threat recently observed to be distributed by the Bitter APT group. It is distributed as a trojanized messaging application such as Signal/Telegram. It is sent to its victims via phishing. This android spyware captures data found on your android mobile such as SMS, Contacts list, Call logs, etc. In addition, it can also capture the audio.

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: Initial Access T1476/T1444 - Collection T1412/T1432/T1433/T1517/T1533/T1429 - Exfiltration T1437

3. CVE-2022-28958 D-Link RCE

A remote command execution (RCE) vulnerability in D-Link devices' "/shareport.php" component has been discovered. Shareport.php doesn't sanitize the value that is passed to it, leading to a command execution. Upon successful exploitation, MooBot is dropped which contacts it Command-and-Control server and adds the impacted device to its botnet. MooBot, on the other hand, is a malware which targets networking devices that are running Linux. It is usually utilized to conduct DDoS.

Red Piranha has deployed rules to detect and reject these exploit attempts against D-Link routers.

Rules Created: 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 T1190 - Execution T1059 - Persistence T1542 - Command-and-Control T1095

4. EvilProxy/Moloch

Researchers have recently identified a new Phishing-as-a-Service (PhaaS) called EvilProxy advertised on the Dark Web. In some sources, the alternative name is Moloch, which has some connection to a phishing-kit developed by several notable underground actors who targeted financial institutions and the e-commerce sector. EvilProxy actors use Reverse Proxy and Cookie Injection methods to bypass 2FA authentication – proxyfying victim's session. Previously such methods have been seen in targeted campaigns of APT and cyberespionage groups. However, now these methods have been successfully productized in EvilProxy which highlights the significance of growth in attacks against online services and MFA authorization mechanisms. EvilProxy was first detected in early May 2022, this is when the actors running it released a demonstration video detailing how it could be used to deliver advanced phishing links with the intention to compromise consumer accounts belonging to major brands such as Apple, Facebook, GoDaddy, GitHub, Google, Dropbox, Instagram, Microsoft, Twitter, Yahoo, Yandex and others.

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: Initial Access T1566/T1195

5. OriginLogger

As the name suggests, its primary purpose is logging keystrokes, clipboard data, HTTP cookies, taking periodic screenshots, and viewing the webcam of infected computers. When a device is infected with the Origin Logger malware, it becomes easy for an attacker to familiarize themselves with an employee's sensitive information, including schedules and communications. For industries that use expensive equipment or large orders, this intel can create plethora of opportunities for the attacker. The Origin Logger malware provided additional information to the attacker by taking a screenshot as the supervisor writes an email to management.

Rules Created: 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: Defense Evasion TA0005 - Discovery TA0007

6. ShadowPad RAT

Threat actors associated with the ShadowPad remote access Trojan have implemented a new toolset to assist its campaigns. The group is targeting various government and state-owned organizations spanning multiple Asian countries. The attack method leveraged by ShadowPad consists of placing a malicious dynamic link library in a legitimate DLL directory. The attacker runs the legitimate application, which then executes the previously-dropped payload. These types of attacks are often associated with multiple software packages, such as graphics software, web browsers, and outdated versions of security software. Most current versions of the software used would possess mitigation against this type of attack, hence why the attackers target older versions. The group then uses Mimikatz and ProcDump to steal user credentials and network scanning tools to identify other devices on the network that could facilitate lateral movement.

Rules Created: 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 - Privilege Escalation TA0004 - Defense Evasion TA0005 - Discovery TA0007