
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Sept 20 - 26, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Brute Ratel C4 (BRc4) -Tool, Warzone RAT Code RAT, Code RAT, BLINDINGCAN –Malware, DoNot APT, and Gamaredon APT)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

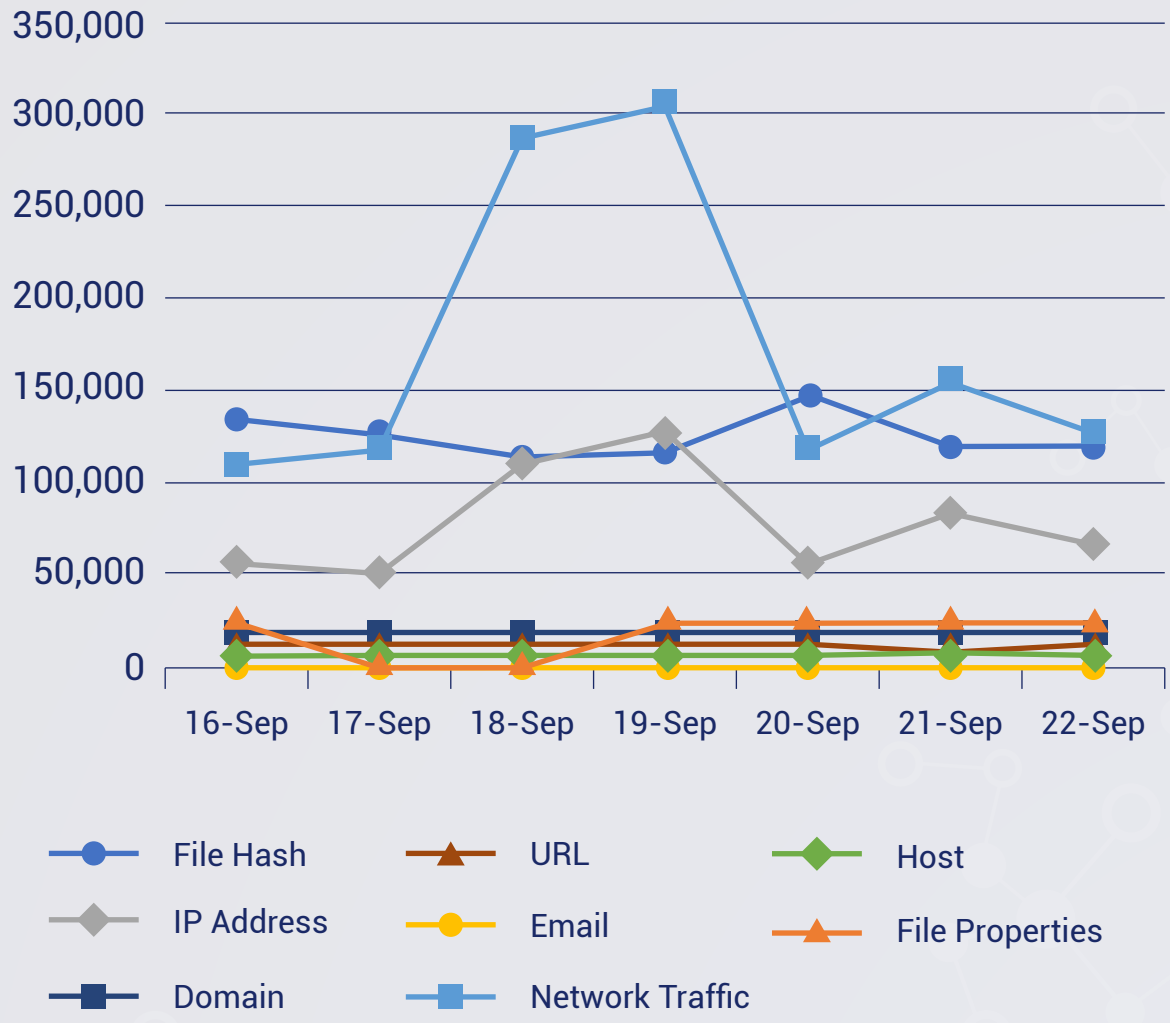
IDPS Rules Created (Week Ending 26/09/2022):

20

Overall Weekly Observables Count:

2,916,764

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Brute Ratel C4 (BRc4) -Tool

Researchers recently discovered an advanced persistent threat (APT) campaign that abused a relatively new, stealthy tool: Brute Ratel C4 (BRc4) pen-testing framework. This campaign was mostly targeting large virtual private server (VPS) hosting providers in various countries and regions. BRc4 remote access payload was packaged in a self-contained ISO with a Windows shortcut (LNK) file, a malicious payload DLL and a legitimate Microsoft executable used by the actors for DLL search order hijacking. This packaging is consistent with known Cozy Bear (APT29) techniques, but the attribution is not definitive.

Rules Created: 04
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: Hijack Execution Flow T1574- User Execution T1204 - Masquerading T1036 - Deobfuscate/Decode Files or Information T1140- Obfuscated Files or Information T1027

2. Warzone RAT

Warzone is a remote access trojan (RAT) that cybercriminals use to remotely access victims' computer. This trojan is advertised using a public website, and thus can be downloaded and used by anyone. Warzone's code is in C++ programming language. This RAT is independent of .NET Framework and controls computers via the VNC module. Warzone uses the HRDP model, which allows it to log into computers without the victims' knowledge. In addition, this model allows cybercriminals to bypass UAC (User Account Control) security. It can control the system using administrative privileges. This feature works on Windows versions from 7 to 10. Warzone can be used to access the victim's webcam, and to steal passwords from Google Chrome, Mozilla Firefox, Internet Explorer, Edge browsers, and Outlook, Thunderbird and Foxmail email clients. Furthermore, cybercriminals can use this trojan to download and upload various files, execute, and delete them. It also includes a key-logging feature, which records every pressed key, even when offline.

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: Initial Access T1566- Execution T1059-Persistance T1564/T1547-Discovery TA0007/T1082-Privilage Escalation T1548-Command-and-Control T1041

3. Code RAT

CodeRAT is a remote access trojan (RAT). The malicious operation, which appears to have originated in Iran, employed a Word document with a Microsoft Dynamic Data Exchange (DDE) exploit to target Farsi-speaking software developers. The source code of a remote access trojan (RAT) dubbed 'CodeRAT' has been leaked on GitHub after malware analysts confronted the developer about attacks that used the tool. CodeRATallows attackers to monitor the victims' activity and have broad monitoring capabilities that support approximately 50 commands. These capabilities are aimed toward webmail, databases, Microsoft Office documents, social media platforms, and Windows. To produce the commands, the attacker uses a UI tool that generates and obfuscates them and then sends them to the malware using one of three methods:

- Telegram bot API with proxy (no direct requests)
- Manual mode (includes USB option)
- Locally stored commands in the 'myPictures' folder.

Rules Created: 04
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 TA0001 - Phishing T1566 – Execution TA0002 – Native API T1106 – Command and Scripting Interpreter T1059 –Defense Evasion TA0005 - Indicator Removal on Host T1070 – Discovery TA0007 – Process Discovery T1057 – File and Directory Discovery T1083 – Collection TA0009 – Screen Capture T1113 – Command and Control TA0011 – Proxy T1090 – Ingress Tool Transfer T1105

4. BLINDINGCAN -Malware

Criminals impersonate recruiters from legitimate companies to lure the victims to open a malicious document — an Office or PDF file that will infect its system. Once criminals gain access to the victim's device, they perform reconnaissance to gather intelligence surrounding key military and energy technologies. The FBI believes that "threat actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation." The malware runs when a loader loads a DLL file. After opening the Word document, a template injection attack is used to install the malware on the target system. This technique allows the download of an external weaponized Word template containing macros that can be executed to infect the victim's device. This evasive attack technique is not new but still very efficient to bypass AVs detection.

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: Malware
Kill Chain: Execution TA0002 - Shared Modules T1129

5. DoNot APT (Update)

DoNot is an APT group known to target and conduct attacks on South Asian countries. They have launched campaigns on South Asian organisations such as Military, Embassies, Ministries of Foreign Affairs. They are shown to be consistent with their techniques which starts with Phishing emails. Upon execution of the attachment from these phishing emails, macros are then leveraged to load their second-stage malware. The malware from the DoNot group function as screenshot and file collectors, keyloggers, browser stealers and establishes reverse shell connections. It uses Google Drive for Command-and-Control traffic.

Red Piranha has deployed rules on Crystal Eye devices that can detect these new DoNot-related domains.

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-activity
Kill Chain: Initial Access T1566 - Execution T1204 - Persistence T1053 - Defense Evasion T1055/T1574 - Command-and-Control T1102 - Exfiltration T1567

6. Gamaredon APT

A Russia-linked threat group that is known to target users from Ukraine with malware that steals information. The technique used is to phish users in the context of current events (Russia-Ukraine conflict), scripts (Powershell, LNK files, VB) are zipped, and malicious software is deployed.

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 - Execution T1059 - Command-and-Control T1102 - Exfiltration T1567