
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Aug 30 - Sept 5, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Nitrokod Crypto Miner, Parrot Stealer, IBAN Clipper Malware, IRATA Android Malware, PureCrypter, and DotCMS RCE: CVE-2022-26352)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

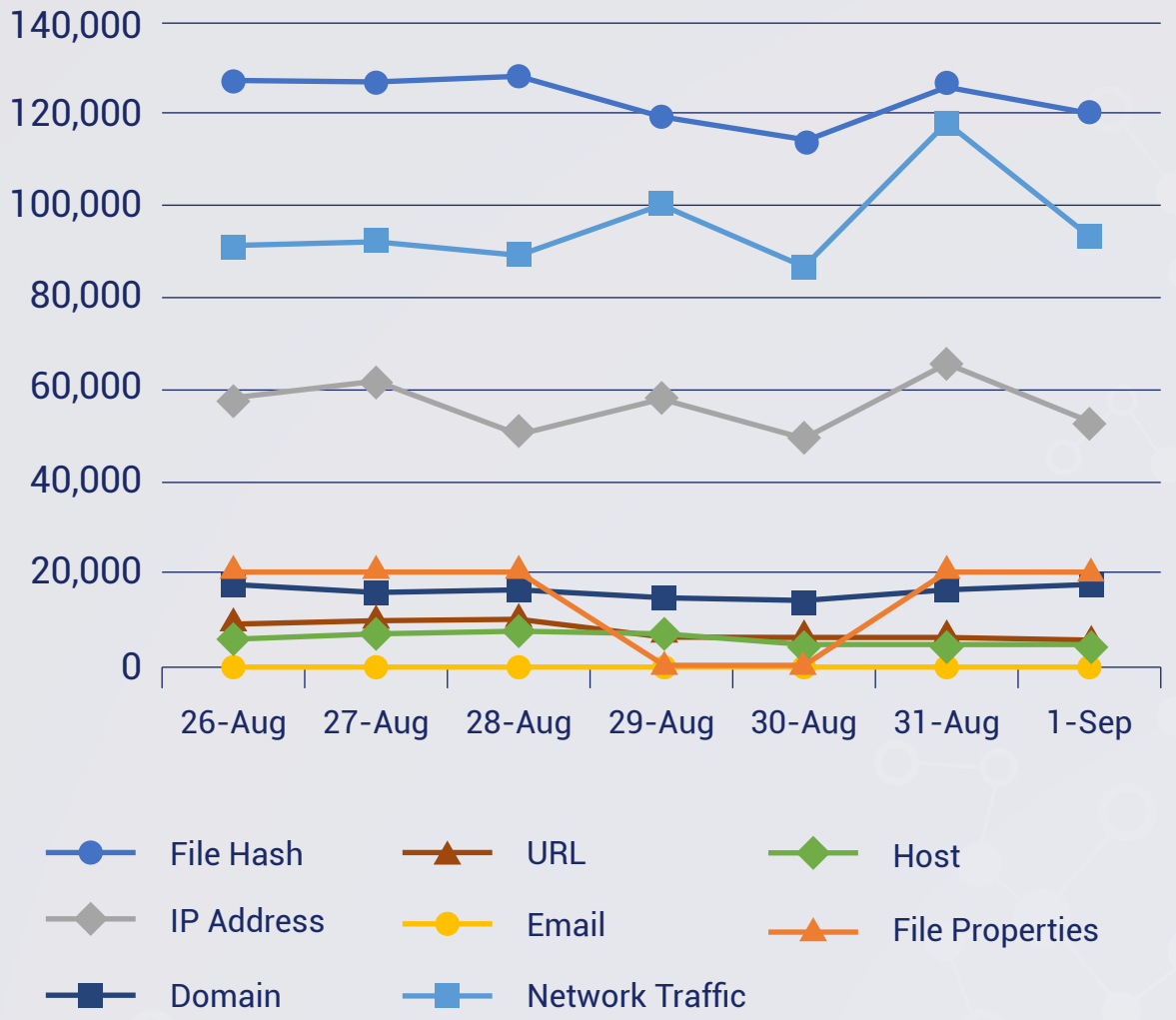
IDPS Rules Created (Week Ending 05/09/2022):

20

Overall Weekly Observables Count:

2,208,259

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Nitrokod Crypto Miner

A new malware campaign disguised as Google Translate or MP3 downloader programs was found distributing cryptocurrency mining malware across 11 countries. The fake applications are being distributed through legitimate free software sites, providing broad exposure to the malicious applications to both regular visitors of the sites and search engines. According to a report by Check Point, the malware is created by a developer named 'Nitrokod,' which at first look appears to be a legitimate application free of malware and provides the advertised functionality. These are the steps the Nitrokod attacker followed to avoid detection:

- Executing the malware almost a month after the Nitrokod program was installed.
- Delivering the payload after 6 earlier stages of infected programs.
- A continuous infection chain initiated after a long delay using a scheduled task mechanism, giving the attackers time to clear the evidence.

Rules Created: 02
Rule Set Type: Balanced IDS: Reject IPS: Drop
Class Type: Trojan
Kill Chain: T1053 - Scheduled Task/Job, T1547 - Boot or Logon Autostart Execution, T1036 - Masquerading, T1049 - System Network Connections Discovery, T1070 - Indicator Removal on Host, T1560 - Archive Collected Data

2. Parrot Stealer

A threat actor (TAs) has released the source code of Parrot Stealer, a malware that can steal data from a target network and send it to the dark web in a post on a cybercrime forum. Parrot Stealer is a 64-bit .NET-binary that uses Timestomping (a technique that modifies the timestamps of a file). Adversaries use this technique on their payloads to deflect any unnecessary attention during forensic investigations. The stealer uses multiple AntiAnalysis checks to prevent debugging of the sample. To detect profiling, the code verifies if the COR_ENABLE_PROFILING environment variable is present and set to 1. Profilers are designed to monitor, troubleshoot, and debug managed code executed by the .NET Common Language Runtime. This stealer payload steals data from the following Chromium-based browsers and FTP applications. The stealer appears to be in the development stage as several FTP applications are hardcoded in the stealer, but it does not appear to target all of them.

Rules Created: 01
Rule Set Type: Balanced IDS: Reject IPS: Drop
Class Type: Trojan
Kill Chain: T1566 - Phishing, T1003 - OS Credential Dumping, T1127 - Trusted Developer Utilities Proxy Execution, T1007 - System Service Discovery, T1041 - Exfiltration Over C2 Channel, T1057 - Process Discovery, T1070 - Indicator Removal on Host, T1071 - Application Layer Protocol, T1087 - Account Discovery, T1204 - User Execution, T1497 - Virtualization/Sandbox Evasion, T1518 - Software Discovery, T1528 - Steal Application Access Token, T1539 - Steal Web Session Cookie, T1552 - Unsecured Credentials, T1555 - Credentials from Password Stores

3. IBAN Clipper Malware

An International Bank Account Number (IBAN) Clipper Malware was identified selling by a Threat Actor (TA) on a cybercrime forum offering monthly subscription-based services of clipper malware targeting Windows operating systems. IBAN is an internationally agreed system developed to identify an overseas bank account. Clipper malware targets a victim's clipboard to perform unauthorized swapping operations by replacing the victim's data with the TA's data to carry out financial theft. Most popular clippers target crypto transactions where the malware swaps the victim's crypto address with the TA's crypto address and tricks unsuspecting victims into sending money to the TA's crypto address. Similarly, IBAN clipper targets bank account numbers.

Rules Created: 02
Rule Set Type: Balanced IDS: Reject IPS: Drop
Class Type: Trojan- Activity
Kill Chain: Execution T1204 -Persistence T1547.001- Credential Access T1555/T1539/T1552/T1528- Collection T1115- Command and Control T1071- Impact T1565.002

4. IRATA Android Malware

IRATA (Iranian Remote Access Trojan) Android Malware is a new malware detected in the wild. It originates from a phishing attack through SMS. The theme of the message resembles information coming from the government that will ask you to download this malicious application. IRATA can collect sensitive information from your mobile phone including bank details. Since it infects your mobile, it can also gather your SMS messages which then can be used to obtain 2FA tokens.

The domains for these command-and-control servers have been identified and are deployed on the Crystal Eye platform to reject such traffic when triggered.

Rules Created: 05
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Collection T1005 - Command and Control T1102 - Exfiltration T1567

5. PureCrypter

PureCrypter is a malware loader known to be used in Malware-as-a-Service (MaaS). This loader is currently active and is known to promote at least 10 malware families with hundreds of Command-and-Control servers in their arsenal. Once they are loaded on a victim's machine, it downloads malware such as Formbook, AgentTesla, Mars Stealer, etc.

A list of Domains and Command-and-Control servers for PureCrypter have been identified, and rules are in place to detect and reject this traffic.

Rules Created: 07
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: Trojan-activity
Kill Chain: Initial Access T1189/T1566 - Execution T1059 - Command-and-Control T1102

6. DotCMS Remote Code Execution (CVE-2022-26352)

A pre-auth remote code execution vulnerability was found in DotCMS which was achievable by performing a directory traversal attack during file upload. This vulnerability ultimately allows attacker to execute arbitrary commands on the underlying system. This vulnerability is exploitable with the default configuration of DotCMS and tested on version 22.01. An attacker can upload arbitrary files to the system. By uploading a JSP file to the tomcat's root directory, it is possible to achieve code execution, leading to command execution. An attacker can ultimately execute arbitrary commands on the underlying system. The vulnerability was confirmed on 22.01 and below. This vulnerability may also work on 22.02, however not yet confirmed. DotCMS is an open-source content management system written in Java for managing content and content driven sites and applications. DotCMS provides a community edition of their content management system that is free to download and use. They also provide an Enterprise edition, a SaaS-based product, that you can purchase on an annual or monthly subscription.

Rules Created: 03
Rule Set Type: Balanced IDS: Alert IPS: Alert
Security IDS: Reject IPS: Drop
Class Type: Exploit-Rules
Kill Chain: Initial Access T1190