Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 02 - 08, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Manjusaka Attack Framework, Knotweed Subzero Malware, Ave Maria RAT (Updated), Luca Stealer, T-RAT 2.0 and SHARPEXT)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **Total Counts by Observable Type**

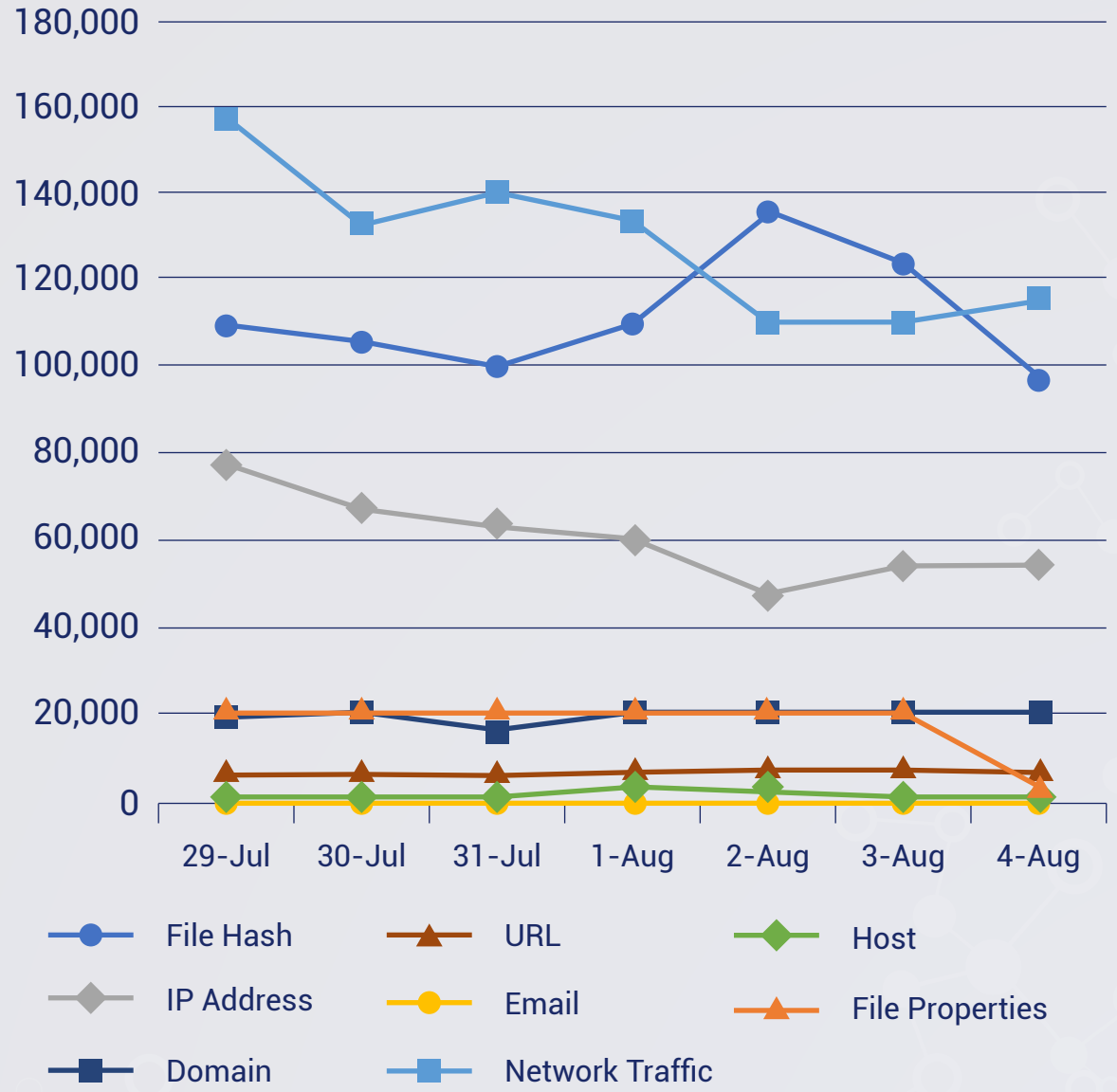
IDPS Rules Created (Week Ending 08/08/2022):

15

Overall Weekly Observables Count:

2,430,304

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Manjusaka Attack Framework

A new attack framework like Cobalt Strike named "Manjusaka" found being used in the wild that has the potential to become rampant across the threat landscape. The new malware family is written in the Rust language for targeting both operating Systems Windows and Linux. A fully functional command and control (C2) dashboard is written in GoLang with a user Interface in Simplified Chinese language which is freely available. It generates new grafts with custom configurations with ease, increasing the likelihood of wider adoption of this framework by malicious actors. A campaign recently discovered in the wild using lure documents themed around COVID-19, the Haixi Mongol and Tibetan Autonomous Prefecture, Qinghai Province.

Rules Created: 02
Rule Set Type: Balanced - IDS: Alert - IPS: Drop
Class Type: Trojan Activity
Kill Chain: Initial Access T1566 - Execution T1204 - Persistence T1053 - Command and Control T1102

2. Knotweed Subzero Malware

Knotweed is an Austria-based Private Sector Offensive Actor (PSOA) known to use Windows and Adobe 0-day exploits. They sell offensive tools or services as their business. They are well-known for having developed and sold a malware called Subzero which leverages Windows' and Adobe products' vulnerabilities. They are directly involved in the usage of the Subzero malware but recent discoveries indicate otherwise. Recently observed activities have originated from Knotweed-associated infrastructure. A common tactic from Knotweed is to distribute an Adobe remote code execution along with Windows privilege escalation exploits; packaged into a PDF document through an email.

These Indicators of Compromise are blended into Crystal Eye as rules for detection and response to such threats.

Rules Created: 06
Rule Set Type: Balanced - IDS: Alert - IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access - T1566 - Execution T1204/T1059 - Privilege Escalation T1068 - Command and Control T1102

3. Ave Maria RAT (Updated)

Ave Maria RAT is a trojan that is used to steal sensitive information, remote access, and camera manipulation among others. It is known to be distributed via phishing emails with attached documents. Upon opening the attachment, it uses PowerShell to download additional malicious files, creates a scheduled task for persistence and exfiltrates data via web traffic to its Command-and-Control server.

Red Piranha has deployed new rules to the Crystal Eye platform as recent Ave Maria RAT activities that include data exfiltration have been observed.

Rules Created: 01
Rule Set Type: Security - IDS: Alert - IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1059 - Persistence T1053 - Command and Control T1102 - Exfiltration T1567

4. Luca Stealer

The source code for an information-stealing malware coded in Rust has been released for free on hacking forums, with security analysts already reporting that the malware is actively used in attacks. As the info-stealer is written in Rust, a cross-platform language, it allows threat actors to target multiple operating systems. However, in its current form, the new info-stealer only targets Windows operating systems. When executed, the malware attempts to steal data from thirty Chromium-based web browsers, where it will steal stored credit cards, login credentials, and cookies. The stealer also targets a range of "cold" cryptocurrency and "hot" wallet browser addons, Steam accounts, Discord tokens, Ubisoft Play, and more. Where Luca Stealer stands out against other info-stealers is the focus on password manager browser addons, stealing the locally stored data for 17 applications of this kind. In addition to targeting applications, Luca also captures screenshots and saves them as a .png file and performs a "whoami" to profile the host system and send the details to its operators.

Rules Created: 02
Rule Set Type: Security - IDS: Alert - IPS: Reject
Class Type: Malware
Kill Chain: Execution T1047/ T1059 - Privilege Escalation T1055 - Defense Evasion T1036 / T1562.001/ T1055 – Discovery T1518.001/ T1057/ T1082 - Command and Control T1105/ T1071

5. T-RAT 2.0

Recently researchers discovered T-RAT 2.0 selling on a Russian cybercrime forum which can be controlled via smartphone with the Telegram app. The attacker controls T-RAT 2.0 via Telegram using text-based commands and command buttons provided by the RAT. The commands are in English, and the help messages are mostly in Russian. One section of the advertisement banner demonstrates the controls and how they look on the phone. The first known stage of infection is the downloader which obtains an encrypted file. For decrypting the payload, the downloader applies XOR with the key 0x01. For the second part of the malware path the downloader generates a random number between 347 and 568203, converts that to a string, and then generates the hash either using MD5, SHA1 or SHA256. It uses the hash's hexadecimal representation as the second part of the malware path. The archive contains the actual T-RAT executable as well as several DLLs that the RAT needs. Some notable libraries are the Telegram.Bot.dll and socks5.dll. A subfolder named service contains six more files. The T-RAT 2.0 has 98 commands and provides the feature to Threat Actors like Stealer, clipper, keylogger, create a screenshot, record audio via microphone, take picture from webcam, and UAC bypass. It can disable Windows Defender and Smart Screen notifications. The malware provides a PowerShell or CMD terminal via Telegram. Remote control can also be done via HRDP or VNC.

Rules Created: 03
Rule Set Type: Balanced
Class Type: Trojan-activity
Kill Chain: Initial Access T1190/T1133 - Execution T1203 - Persistence T1098 – Discovery T1046-Command and Control T1102

6. SHARPEXT

Sharpext is a malicious browser extension deployed by SharpTongue following successful compromise of a target system. In the first versions of SHARPEXT investigated by Volexity, the malware only supported Google Chrome. The latest version (3.0 based on the internal versioning) supports three browsers: Chrome, Edge, and Whale.

Prior to deploying SHARPEXT, the attacker manually exfiltrates files required to install the extension (explained below) from the infected workstation. SHARPEXT is then manually installed by an attacker-written VBS script. The workflow of the installation script is as follows:

1. Download supporting files:
    - The malicious browser extension files
    - Browser configuration files
    - Additional scripts (pow.ps1 and dev.ps1) to ensure the extension is loaded
2. Run the setup script (pow.ps1)

Rules Created: 01
Rule Set Type: Balanced
Class Type: Malware
Kill Chain: Collection T1114 – Command and Control T1071

Total Counts by Observable Type:

The table below shows the total counts of observables we've been collecting for the last four months, the last four weeks, and the total since February 2017.

	Date	File Hash	IP Address	Domain	URL	Email	Network Traffic	Host	File Properties	Total
Month	May 2022	4,029,272	1,798,537	476,808	448,583	168	3,194,022	179,741	590,291	10,717,422
	Jun 2022	4,798,835	2,138,981	548,365	473,164	735	3,645,625	115,609	585,476	12,306,790
	Jul 2022	3,292,459	1,463,827	484,583	212,732	17	2,955,718	68,835	551,316	9,029,487
	Aug 2022	463,019	212,095	82,341	34,819	3	465,506	12,498	63,478	1,333,759
Week	7/8-7/14	751,304	314,639	113,855	54,821	14	710,598	15,133	139,544	2,099,908
	7/15-7/21	817,762	312,021	117,953	46,922	0	576,167	11,451	137,726	2,020,002
	7/22-7/28	779,941	399,137	126,425	48,629	3	858,242	18,893	138,614	2,369,884
	7/29-8/5	775,710	418,154	134,559	60,051	3	896,342	22,551	122,934	2,430,304
Total	Since Feb 2017	155,576,836	37,243,328	20,354,522	15,889,333	198,907	30,993,049	2,845,042	3,488,798	266,589,815