Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 12 - July 18, 2022

Report Summary:

- **New Threat Detection Added** – 6 (SilentLibrarian APT, YourCyanide Ransomware, NoMercy Stealer Malware, ABCsoup Adware, CVE-2019-0708 and CVE-2020-1350)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **Total Counts by Observable Type**

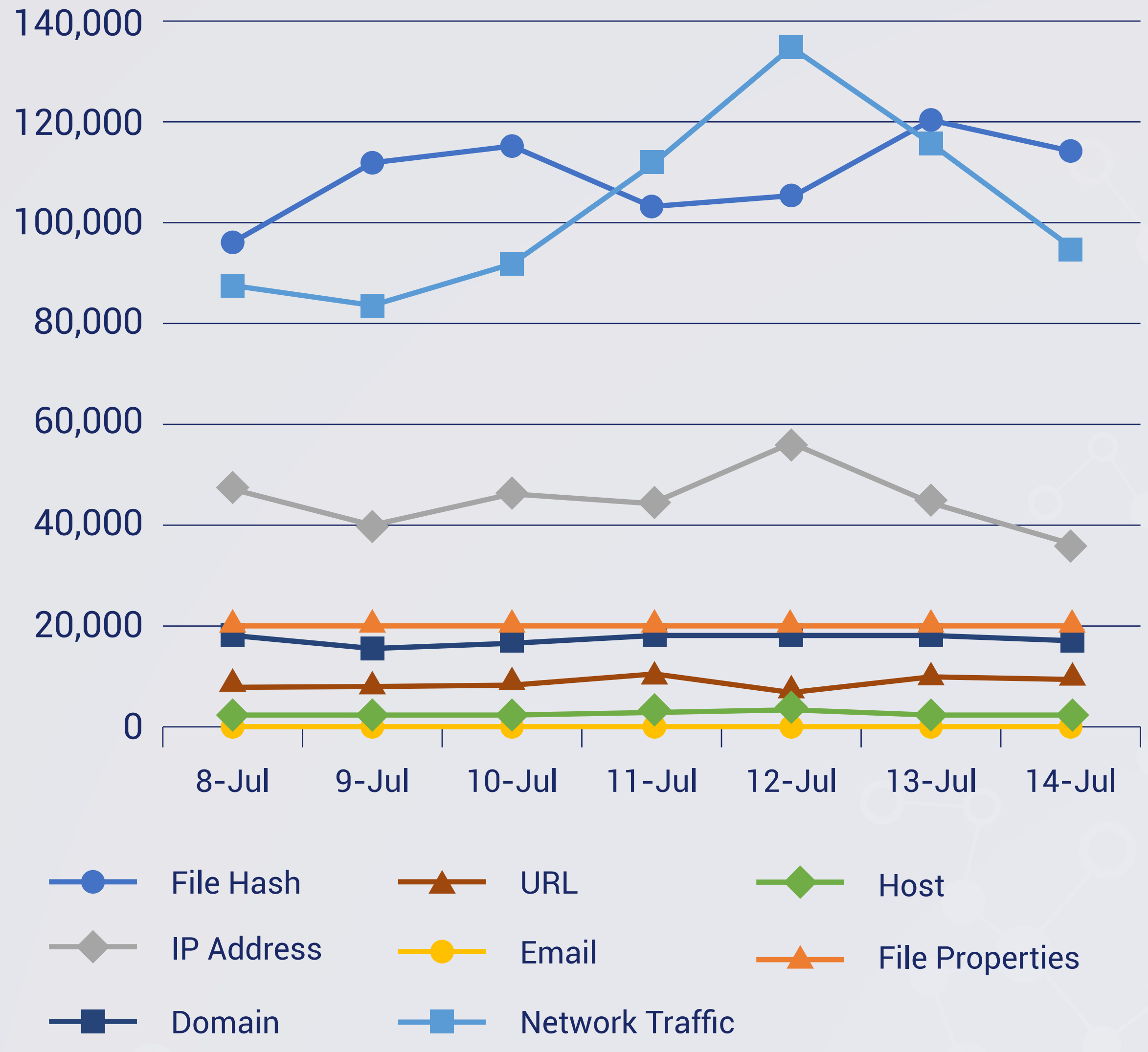
IDPS Rules Created (Week Ending 18/07/2022):

13

Overall Weekly Observables Count:

2,099,908

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Threat name: SilentLibrarian APT

SilentLibrarian is an APT group that primarily targets universities for research data. This group has been active since 2013 and its members are said to be affiliated with Iran. Their primary motive is to steal proprietary research data from the academe and other private research agencies. Their main observed technique is to gather and use compromised accounts from university domains. They then use these accounts to phish and trick their specific targets into authenticating into their own fake university login portal.

Red Piranha is continuously monitoring the domains that this APT group is known to be using. Rules are being updated to include the most recent domains that have been observed.

Rules Created: 03
Rule Set Type: Security – IDS: Alert – IPS: Reject
Class Type: Bad-unknown
Kill Chain: Initial Access T1566 – Credential Access T1056

2. Threat name: YourCyanide Ransomware

YourCyanide is a newly observed ransomware that is distributed via Discord as an attachment. Upon execution, it creates a .lnk file that retrieves and executes the main dropper malware. Once the dropper is executed, it creates a new directory where it will save a batch script that it will fetch from Pastebin and execute. The dropper deletes the directory where it stored the files. It achieves persistence through the Registry by adding itself as a startup item. Upon locking the user's machine, it fetches another batch script which uploads data to a Telegram bot. It also downloads a token stealer that is used on the user's web browser local storage and sends the contents to the Telegram bot.

This malware can also spread via email by sending a copy of itself through Outlook. It retrieves the user's contact list and sends an email that resembles a love letter.

The rules in place are to detect the usage of Discord and an unusual user-agent that is observed being used by the malware.

Rules Created: 02
Rule Set Type: Security – IDS: Alert – IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 – Execution T1059 – Defense Evasion T1140/T1562 – Persistence T1547 – Command and Control T1102 – Impact T1486

3. Threat name: NoMercy Stealer Malware

Threat researchers came across a post on Telegram selling NoMercy stealer malware for 10 USD. The stealer is very offensive and studies indicate that it is at the initial stages of development. This stealer is a 32-bit, console-based C# executable file that after execution, initially checks for the system's public IP using hxxp://api.ipify[.]org. After getting the public IP, the stealer registers itself with the Command-and-Control server (C&C). After registration, the stealer sends various system information to the C&C server. The stealer then proceeds to continuously send screenshots, keystrokes, webcam photos and device audio to the C&C server. One such emerging trend is adding clipper capabilities to the malware.

Rules Created: 02
Rule Set Type: Security – IDS: Alert – IPS: Reject
Class Type: Trojan-activity
Kill Chain: Execution T1204 – Persistence T1547
Discovery T1087/T1046/T1012/T1518/T1082/T1016/T1033
Collection T1119/T1115/T1056/T1113/T1125 – Command and Control T1071

4. Threat name: ABCsoup Adware

Recently, researchers discovered the growth of a wide range of malicious browser extensions such as ABCSoup family with the same extension ID as that of Google Translate, deceiving users into believing that they have installed a legitimate extension. The ABCsoup targets three popular browsers: Google Chrome, Opera and Firefox. This Google Translate spoofing browser extensions are installed onto the victim's machine via a Windows-based executable, bypassing most endpoint security solutions, along with the security controls found in the official extension stores. Like app spoofing and cloning, these malicious applications look legitimate, but underneath the surface lies code that puts personal and enterprise data at risk. These malicious extensions can perform a wide variety of attacks based on the attacker's purpose, as the malware includes a JavaScript injection method from the attacker's-controlled server. The extension's main logic confirms that this family is an Adware campaign along with some script injection functionality which can be further abused for other malicious actions such as phishing, stealing credentials/cookies, etc.

Rules Created: 04
Rule Set Type: Balanced/ Security – IDS: Alert – IPS: Alert
Class Type: Trojan
Kill Chain: Initial Access T1190/T1133 – Execution T1203 – Persistence T1098 – Discovery T1046 – Command and Control T1102

5. Threat name: CVE-2019-0708

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

Rules Created: 01
Rule Set Type: Exploit
Class Type: RCE
Kill Chain: Initial Access T1133 – ExecutionT1059.001

6. Threat name: CVE-2020-1350

The CVE-2020-1350 is an integer overflow vulnerability that leads to a heap-based buffer overflow when processing malformed DNS SIG resource records. A SIG record is a type of DNS resource record that contains a digital signature for a record set (one or more DNS records with the same name and type). To exploit SIGRed, an attacker can configure an “evil” domain whose NS record points to a malicious DNS server. When a client makes a DNS query for the “evil” domain to the victim server, the victim server will query the DNS server above it. The DNS server will respond back with an NS record indicating that the malicious DNS server is the authority for that domain, and the record will be cached by the victim. Afterwards, when a client sends the victim a DNS SIG query for the domain, the victim server will query the malicious DNS server. The malicious DNS server will send a malformed DNS SIG record as a response.

Rules Created: 01
Rule Set Type: Exploit
Class Type: Authentication Bypass
Kill Chain: Initial Access T1190 – Command and Control – T1071.004

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	Apr 2022	4,124,667	1,837,957	396,073	637,235	592	3,514,384	371,365	563,861	11,446,134
	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	1,694,756	752,669	240,205	117,181	14	1,521,309	38,491	274,976	4,639,601
Week	6/17-6/23	1,219,545	557,275	124,005	162,316	1	952,911	26,917	138,334	3,181,304
	6/24-6/30	1,350,886	480,717	141,554	58,788	1	858,740	25,749	137,433	3,053,868
	7/1-7/7	943,452	438,030	126,350	62,360	0	810,711	23,358	135,432	2,539,693
	7/8-7/14	751,304	314,639	113,855	54,821	14	710,598	15,133	139,544	2,099,908
Total	Since Feb 2017	153,203,420	36,114,014	19,975,584	15,733,731	198,901	28,662,295	2,792,147	3,089,524	259,769,616