
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
July 19 - July 25, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Cloaked Ursa APT Group, ChromeLoader, Raspberry Robin USB Worm, H0lyGh0st Ransomware, CVE-2021-24284 and Maui Ransomware)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **Total Counts by Observable Type**

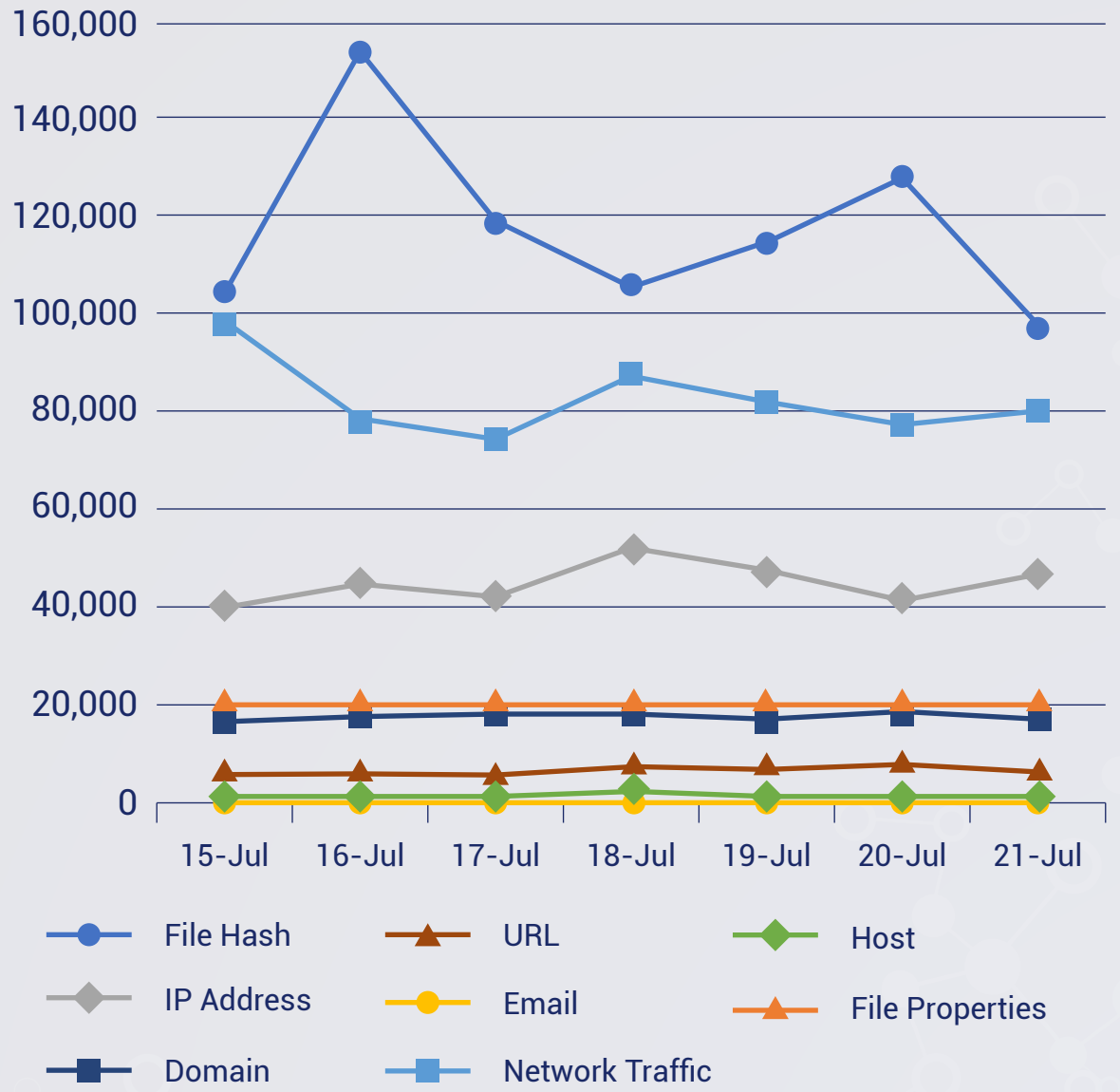
IDPS Rules Created (Week Ending 25/07/2022):

14

Overall Weekly Observables Count:

2,020,002

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Threat name: Cloaked Ursa APT Group

Cloaked Ursa (APT29) is a threat group that has been traced back to Russia. They are popularly known to be the threat actors behind the Solarwinds supply chain attack in 2020. They have operated since 2008 and have been targeting large organizations such as governments and research institutes.

A newly observed campaign from Cloaked Ursa leverages trusted cloud services such as Google Drive to deliver malware. The most recent incidents were targeted at embassies in Portugal and Brazil. The phishing documents delivered to these targets contained a link to a malware dropper that would gather additional malicious files and payloads.

Red Piranha has rules in place to detect requests for domains that are related to Cloaked Ursa, a specific parameter for suspicious Google Drive authentication events, and download traffic for the malware dropper.

Rules Created: 04
Rule Set Type: Balanced and Security, IDS: Alert – IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1059 - Command and Control T1102 - Exfiltration T1567-T1537-T1041

2. Threat name: ChromeLoader

ChromeLoader is a malware used to hijack a user's browser and usually originates from malicious advertisements. Historically, the events start with a user downloading a cracked version of software through malicious adverts. Installing this malicious software means installing the malware on your machine. Through the years, the ChromeLoader has been observed to be improving on its techniques. The most recent ChromeLoader activity started with malicious advertisements and ended up with deploying a browser extension instead. This browser extension is used as an infostealer and will present you with advertisements.

Red Piranha has deployed rules to detect a pattern used by the authors of this malware. It detects outgoing requests for domains associated with ChromeLoader.

Rules Created: 01
Rule Set Type: Balanced – IDS: Alert – IPS: Alert
Class Type: Trojan
Kill Chain: Initial Access T1189 - Execution T1059 - Persistence - Command and Control T1102

3. Threat name: Raspberry Robin USB Worm

Raspberry Robin is usually launched via infected removable drives, often USB devices. The Raspberry Robin worm often appears as a shortcut .lnk file hidden as a legitimate folder on the infected USB device. Soon after the Raspberry Robin infected drive is connected to the system, the User Assist registry entry is updated and records the execution of a ROT13-ciphered value referencing a .lnk file when deciphered.

Rules Created: 03
Rule Set Type: Balanced - IDS: Alert - IPS: Alert
Class Type: Trojan
Kill Chain: Initial Access T1091 - Execution T1059.003 - Defence Evasion T1218.008 - Command and Control T1218.007/T1071.001

4. Threat name: H0lyGh0st Ransomware

The Microsoft Threat Intelligence Center (MSTIC) recently reported a new malware strain attacking small to middle-sized businesses across the globe since June 2021. The ransomware named H0lyGh0st has been initially developed by an emerging North Korean APT tracked under the DEV-0530 moniker. The ransomware attacks are explicitly financially motivated, targeting such sectors as manufacturing, education, financial services, and tech. Analysis of DEV-0530 activity reveals the ties to another North Korea-backed threat actor known as Plutonium (aka Andariel), an active unit of the Lazarus umbrella.

Rules Created: 04
Rule Set Type: Balanced - IDS: Alert - IPS: Alert
Class Type: Trojan
Kill Chain: Initial Access T1078 - Execution T1059 - Privilege Escalation T1548 - Defence Evasion T1112 - Discovery T1082 - Impact T1490

5. Threat name: CVE-2021-24284

A vulnerability classified as critical has been found in Kaswara Modern VC Addons Plugin up to 3.0.1 on WordPress (WordPress Plugin). Affected is the function uploadFontIcon of the file wp-content/uploads/kaswara/fonts_icon. The manipulation with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-434. The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. The critical-severity security bug allows an unauthenticated attacker to upload malicious PHP files to a vulnerable site, potentially achieving remote code execution. An attacker can exploit the flaw to inject malicious JavaScript code into any file on the WordPress installation and completely take over a vulnerable site. Over the past two weeks, Wordfence has seen a massive surge in the number of attack attempts targeting the vulnerability.

Rules Created: 01
Rule Set Type: Balanced - IDS: Alert - IPS: Alert
Class Type: Privilege escalation
Kill Chain: Stage Capabilities: Upload Tool T1608:002

6. Threat name: Maui Ransomware

Maui ransomware (maui.exe) is an encryption binary. The ransomware appears to be designed for manual execution by a remote actor. The remote actor uses a command-line interface to interact with the malware and to identify files to encrypt. Maui uses a combination of Advanced Encryption Standard (AES), RSA, and XOR encryption to encrypt target files:

Maui encrypts target files with AES 128-bit encryption. Each encrypted file has a unique AES key, and each file contains a custom header with the file's original path, allowing Maui to identify previously encrypted files. The header also contains encrypted copies of the AES key.Maui encrypts each AES key with RSA encryption.Maui loads the RSA public (maui.key) and private (maui.evd) keys in the same directory as itself. Maui encodes the RSA public key (maui.key) using XOR encryption. The XOR key is generated from hard drive information (\\.\PhysicalDrive0).

Rules Created: 01
Rule Set Type: Balanced - IDS: Alert - IPS: Alert
Class Type: Ransomware
Kill Chain: manual execution TA0002 - command-line interface T1059.008 - Data Encryption - T14867

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	2,512,518	1,064,690	358,158	164,103	14	2,097,476	49,942	412,702	6,659,603
Week	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
	7/15-7/21	817,762	312,021	117,953	46,922	0	576,167	11,451	137,726	2,020,002
Total	Since Feb 2017	154,021,182	36,426,035	20,093,537	15,780,653	198,901	29,238,462	2,803,598	3,227,250	261,789,618