
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
July 4 - July 11, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Shuckworm, Evilnum APT ZuoRAT, YamaBot, CVE-2022-30190, CVE-2022-23131)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **Total Counts by Observable Type**

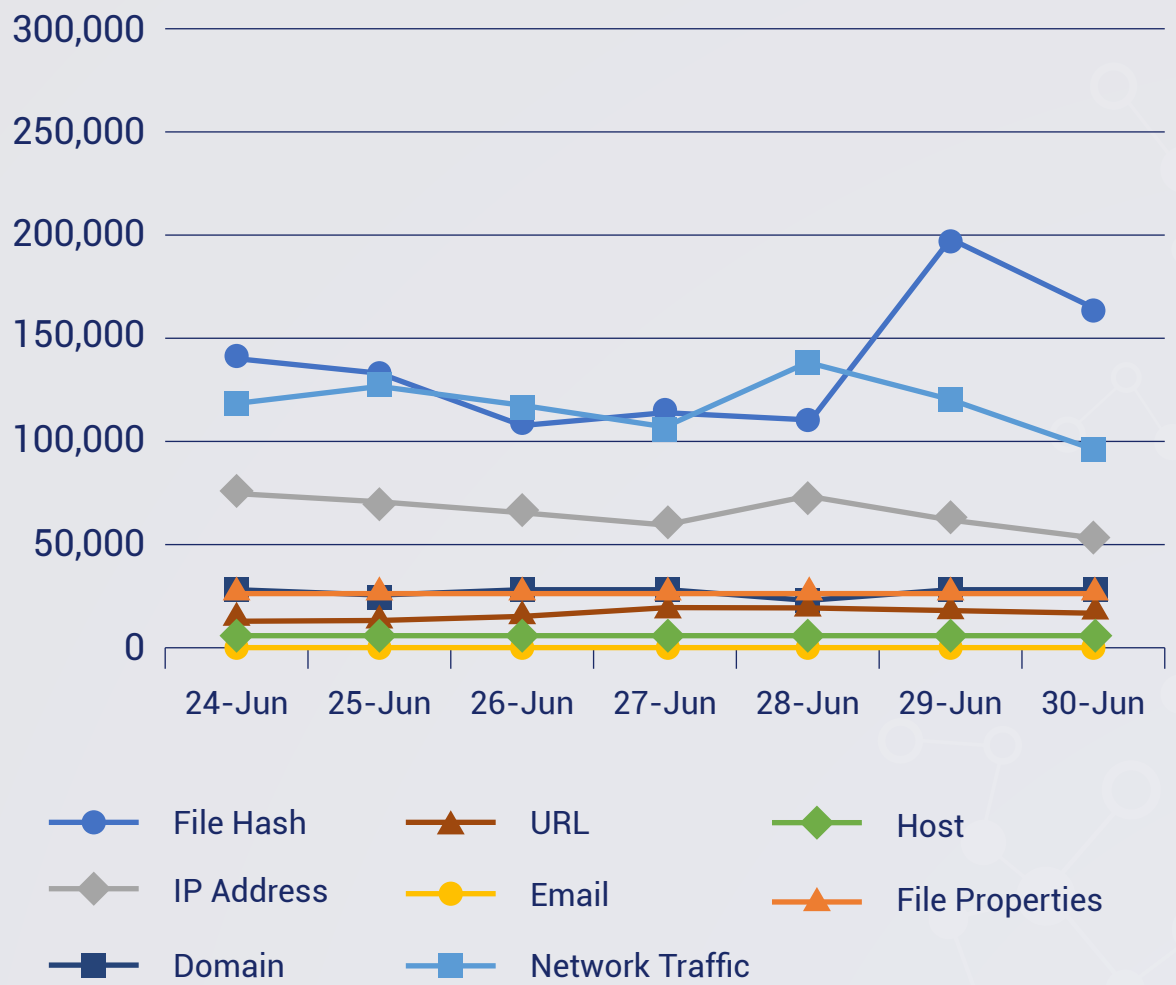
IDPS Rules Created (Week Ending 11/07/2022):

17

Overall Weekly Observables Count:

2,539,693

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Threat name: Shuckworm
Shuckworm is a Russia-linked cyber-espionage group that is still continuously conducting operations. Recent activity shows that attacks have shown how sophisticated the attacks have become since 2013. Shuckworm now leverages living-off-the-land tools to move laterally on networks.

Upon receipt and execution of a malicious document through phishing, a malicious VBS script is launched to create a persistent backdoor as a scheduled task. Communications to its Command-and-Control server are established, where recent methodologies include HTA files being executed and using W-script to execute VBS files.

Red Piranha has obtained information on the new domains linked to Shuckworm. A rule was created to detect and alert the DNS requests to these domains as well as their specific requests.

Rules Created: 03
Rule Set Type: Security – IDS: Alert – IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1059 - Persistence T1053 - Lateral Movement T1021 - Command and Control T1219

2. Threat name: Evilnum APT
Evilnum APT is a financially motivated hacking group known to target European organisations involved in international migration. Due to the ongoing Russia-Ukraine crisis, a spike of malicious emails containing malicious documents has been observed. These documents are loaded with a macro that executes an obfuscated JavaScript. This JavaScript drops a malware loader and creates a scheduled task as a persistence mechanism. Once the malware is loaded, it establishes communications with its Command-and-Control servers for further instructions.

Rules Created: 05
Rule Set Type: Balanced – IDS: Alert – IPS: Drop
Class Type: Bad-unknown
Kill Chain: Initial Access T1566 - Execution T1204 - Persistence T1053 - Command and Control T1102

3. Threat name: ZuoRAT (Remote Access Trojan)

Recently, researchers identified at least 80 infected routers made by Cisco, Netgear, Asus, and DrayTeby by a stealthy malware Dubbed ZuoRAT Remote access Trojan. The researchers reported that the remote access Trojan is part of a broader hacking campaign that has existed since at least the fourth quarter of 2020 and continues to operate. This advanced hacking group has spent almost two years infecting a wide range of routers in North America and Europe with malware that takes full control of connected devices running Windows, macOS, and Linux.

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

4. Threat name: YamaBot Malware

YamaBot is malware written in the Go language, and its functions are slightly different between the malware written for each platform. In the past, the YamaBot usually detected targeting Linux OS but in the recent activity by the malware was found to be targeting Windows OS as well. YamaBot communicates with the C2 server using HTTP requests. The said BOT sends its first HTTP POST request to its C2 but in this first POST request did not detect sending any data. It encodes the User-Agent in Base64. YamaBot is a malware that is still used by attackers. Since it targets not only Windows OS but also Linux OS, it is necessary to carefully investigate the server when investigating an incident. The famous cybercrime group named Lazarus has been identified as using YamaBot malware in Japan to compromise the targets.

Rules Created: 03
Rule Set Type: Balanced/ Security– IDS: Alert – IPS: Alert
Class Type: Trojan
Kill Chain: Initial Access T1566 - Execution T1204 - Persistence T1053 - Command and Control T1102

5. Threat name: CVE-2022-30190
A new remote code execution vulnerability has been found lurking in most Microsoft products.

Here are the steps we observed:

Step 1: The attacker sends an email containing a malicious Microsoft Office document (.docx, etc.) to the targeted user.
Step 2: The user executes this file, which resolves and executes the attacker-controlled external resource from the document.xml.ref file.
Step 3: Code exploiting the vulnerability is now served to the user.
Step 4: This code then launches additional commands like downloading Remote Access Trojans, etc.

Rules Created: 01
Rule Set Type: Exploit
Class Type: RCE
Kill Chain: Initial AccessT1566.001–ExecutionT1059.001/T1203

6. Threat name: CVE-2022-23131
In the case of instances where the SAML SSO authentication is enabled (non-default), session data can be modified by a malicious actor, because a user login stored in the session was not verified. The malicious unauthenticated actor may exploit this issue to escalate privileges and gain admin access to Zabbix Frontend. To perform the attack, SAML authentication is required to be enabled and the actor must know the username of the Zabbix user (or use the guest account, which is disabled by default). CVE-2022-23131 involves unsafe client-side session storage leading to authentication bypass/instance takeover via Zabbix Frontend with configured SAML. The affected versions are 5.4.0 –5.4.8; 6.0.0 alpha1.

Rules Created: 01
Rule Set Type: Exploit
Class Type: Authentication Bypass
Kill Chain: Discovery T1087–Initial Access T1078–Privilege Escalation -T1078

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	943,452	438,030	126,350	62,360	0	810,711	23,358	135,432	2,539,693
Week	6/10-6/16	1,055,363	487,876	131,196	110,600	728	843,783	26,699	136,433	2,792,678
	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
	7/1-7/8	943,452	438,030	126,350	62,360	0	810,711	23,358	135,432	2,539,693
Total	Since Feb 2017	152,452,116	35,799,375	19,861,729	15,678,910	198,887	27,951,697	2,777,014	2,949,980	257,669,708