Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

June 26 - July 03, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Grandoreiro – Banking Trojan, SocGholish, ToddyCat APT (Advanced Persistent Threat), DarkCrystal RAT (Remote Access Trojan), CVE-2022-1388, CVE-2021-42292)
- **New IDPS Rules Created - 10**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **Total Counts by Observable Type**

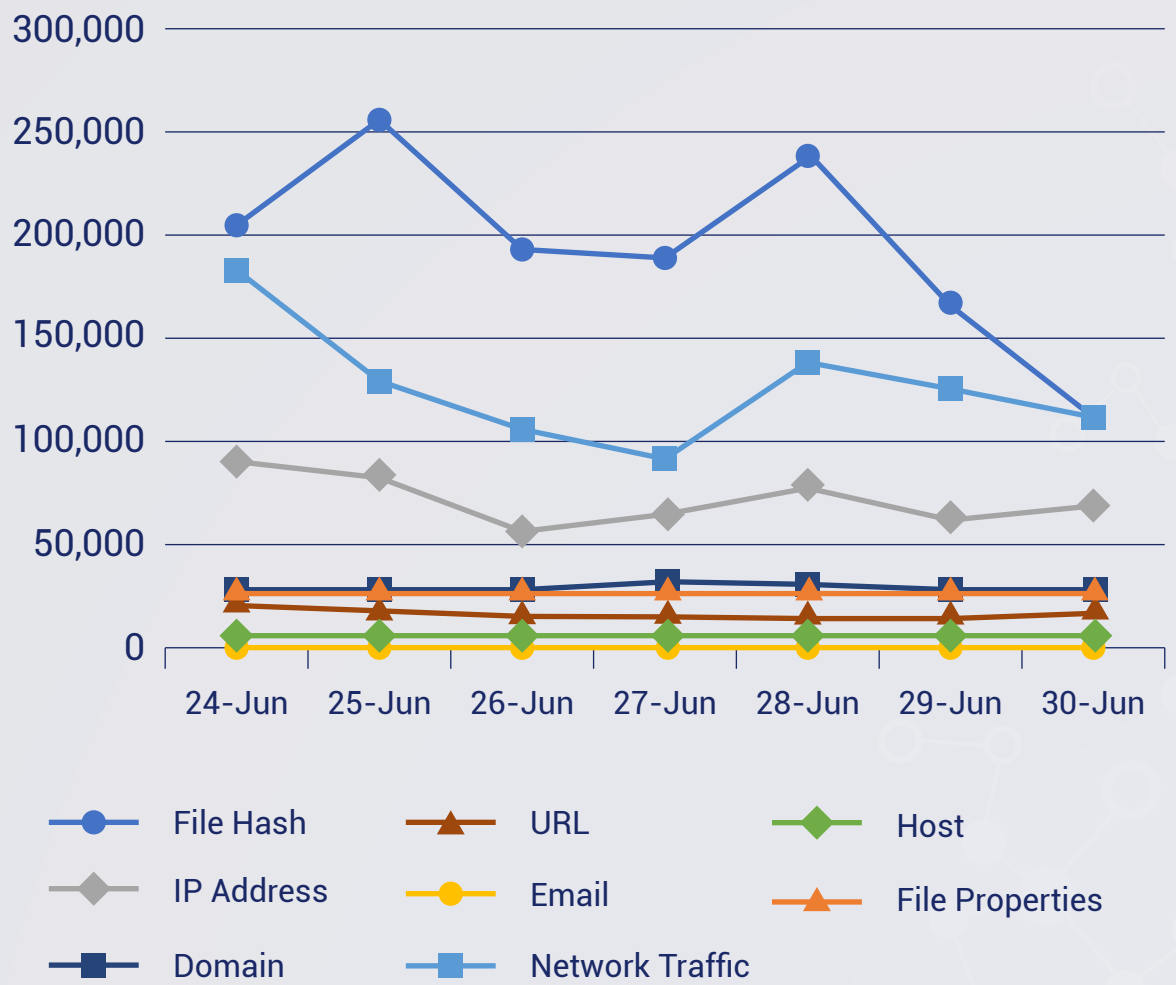
IDPS Rules Created (Week Ending 03/07/2022):

10

Overall Weekly Observables Count:

3,053,868

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1.Threat name: Grandoreiro – Banking Trojan
Grandoreiro is a banking trojan that originated in Brazil, South America. It has been active since 2015 and has spread its operations across other regions of South America and Europe. The main interesting behavior of this malware is that it only executes on Spanish language. Once it has detected English as the victims' language, it stops. It starts with a URL from a malicious email that leads to a specific zip file. The zip file contains an MSI installer which unpacks a series of files. The included malicious DLL is executed by a legitimate MS Visual Studio instance in the guise of Solodriver.exe (A part of Advanced Installer). The malware will take over victims' computers and when a targeted banking website is visited, the threat actors will create fraudulent money transfers from the user's session.

Red Piranha has created a rule for the detection of the specific zipped archive that is associated and observed with Grandoreiro. By having this rule in place, we will be able to monitor first-hand if a machine is downloading this zipped archive and prevent any further actions and/or executions.

Rules Created: 01
Rule Set Type: Security – IDS: Alert – IPS: Reject. The IDS will alert if traffic is observed and IPS will automatically reject the traffic.
Class Type: Trojan
Kill Chain: Initial Access T1566 - Execution T1204 - Credential Access T1539 - Collection T1185/T1056/T1113/T1125 - Command and Control T1071

2. Threat name: SocGholish
SocGholish is a framework for drive-by attacks. It has been active since 2018 and has been linked to the cybercrime group Evil Corp. It is possible for an unsuspecting victim who visits a compromised website to execute a malicious Javascript code from the legitimate site. Since the sites are known to be legitimate, users often trust the objects that are seen from the site. An example is a company website that has been exploited through a Wordpress vulnerability, malicious javascript code was embedded, an employee visits the site and unknowingly executes the script on their machine.

Red Piranha has created a rule for the detection of an outgoing remote access traffic using NetSupport (ctfmon.exe). The detection is specific to a traffic going to an observed URI 'fakeurl.htm' using NetSupport (ctfmon.exe).

Rules Created: 01
Rule Set Type: Security – IDS: Alert – IPS: Reject. The IDS will alert if traffic is observed and IPS will automatically reject the traffic.
Class Type: Trojan
Kill Chain: Initial Access T1189/T1566 - Execution T1059 - Command and Control T1071 - Exfiltration T1020

3. Threat name: ToddyCat APT (Advanced Persistent Threat)

A relatively new APT group named ToddyCat was detected targeting high profile entities of Europe and Asia. The said APT using two well-known malware named Samurai backdoor and Ninja Trojan as a main weapon to destroy the targets. Samurai backdoor is a sophisticated backdoor which works on ports 80 and 443. The malware uses multiple modules that allow the attacker to administrate the remote system and move laterally inside the targeted network. Ninja has a feature like Cobalt Strike pivot listeners, which can limit the number of direct connections from the targeted network to the remote C2 and control systems without internet access. It appears that this group started exploiting the Microsoft Exchange vulnerability and compromise Microsoft Windows Exchange servers.

Rules Created: 01
Rule Set Type: Connectivity & Security – IDS: Alert – IPS: Reject. The IDS will alert if traffic is observed and IPS will automatically reject the traffic.
Class Type: Trojan
Kill Chain: Initial Access T1190/T1566 - Execution T1059 - Command and Control T1071 - Exfiltration T1020

4. Threat name: DarkCrystal RAT (Remote Access Trojan)

Recently in June 2022, The DarkCrystal also dubbed as DCRAT Remote Access Trojan was reported by CERT-UA targeting Ukraine. The DCRat is commercial .NET malware and designed primarily to steal data from a host that has been compromised. In early May this year, RAT was being sold in Russian underground forums. The primary focus of DCRat is data exfiltration as it supports keylogging as well as the theft of confidential information such as credentials from installed web browsers and FTP clients.

DCRat functions include:

- Keylogging
- Taking screenshots
- Stealing cookies, passwords, and form contents from installed web browsers
- Stealing credentials from installed FTP clients such as FileZilla
- Stealing clipboard contents
- Collecting machine information (host computer name, host username, country location, installed security products, etc.) and sends the collected information to a C2 server.

Rules Created: 02
Rule Set Type: Connectivity & Security – IDS: Alert – IPS: Reject. The IDS will alert if traffic is observed and IPS will automatically reject the traffic.
Class Type: Trojan
Kill Chain: Initial Access T1190/T1566 - Command and Control T1071 - Exfiltration T1020

5. Threat name: CVE-2022-1388
This vulnerability may allow an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands, create or delete files, or disable services. Threat actors can exploit this vulnerability to bypass authentication and run arbitrary code on unpatched systems. This is a critical vulnerability that was given a 9.8 CVSS score.

Rules Created: 01
Rule Set Type: Security
Class Type: Remote Code Execution
Kill Chain: Initial Access - T1190 - command and control -T1105/T1071.001 - Discovery T1083/1069

6. Threat name: CVE-2021-42292 is a security bypass vulnerability in Microsoft Excel that could lead to local code execution via a specially crafted Excel file. It was marked by Microsoft as a local file format vulnerability. It is an actively exploited Microsoft Excel vulnerability utilizing security feature bypass. Adversaries can install malicious code by tricking users into opening a “booby-trapped” Excel file. This vulnerability affects 18 versions of Microsoft Excel. Attack takes place either locally or remotely (e.g., via SSH) following a social engineering attack, generally by tricking a legitimate user into downloading and opening an unsafe Excel file (spear phishing)

Rules Created: 04
Rule Set Type: Exploit
Class Type: Privilege escalation
Kill Chain: Initial access - T1556 - Execution - T1204.004 - Persistence - T1546

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	Mar 2022	4,103,469	1,972,596	506,654	884,326	2,987	4,263,651	382,267	555,389	12,671,339
	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	4,798,833	2,138,980	548,364	473,164	735	3,645,625	115,609	585,476	12,306,786
Week	6/3-6/9	946,608	482,287	118,066	119,802	2	827,414	31,130	133,749	2,659,058
	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
Total	Since Feb 2017	151,508,664	35,361,345	19,735,379	15,616,550	198,887	27,140,986	2,753,656	2,814,548	248,894,843