Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 16 - 22, 2022

Report Summary:

- **New Threat Detection Added** – 6 (ROMCOM RAT, MikuBot, CVE-2022-31656, Kolobko, CopperStealer, and CVE 2022-27925)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

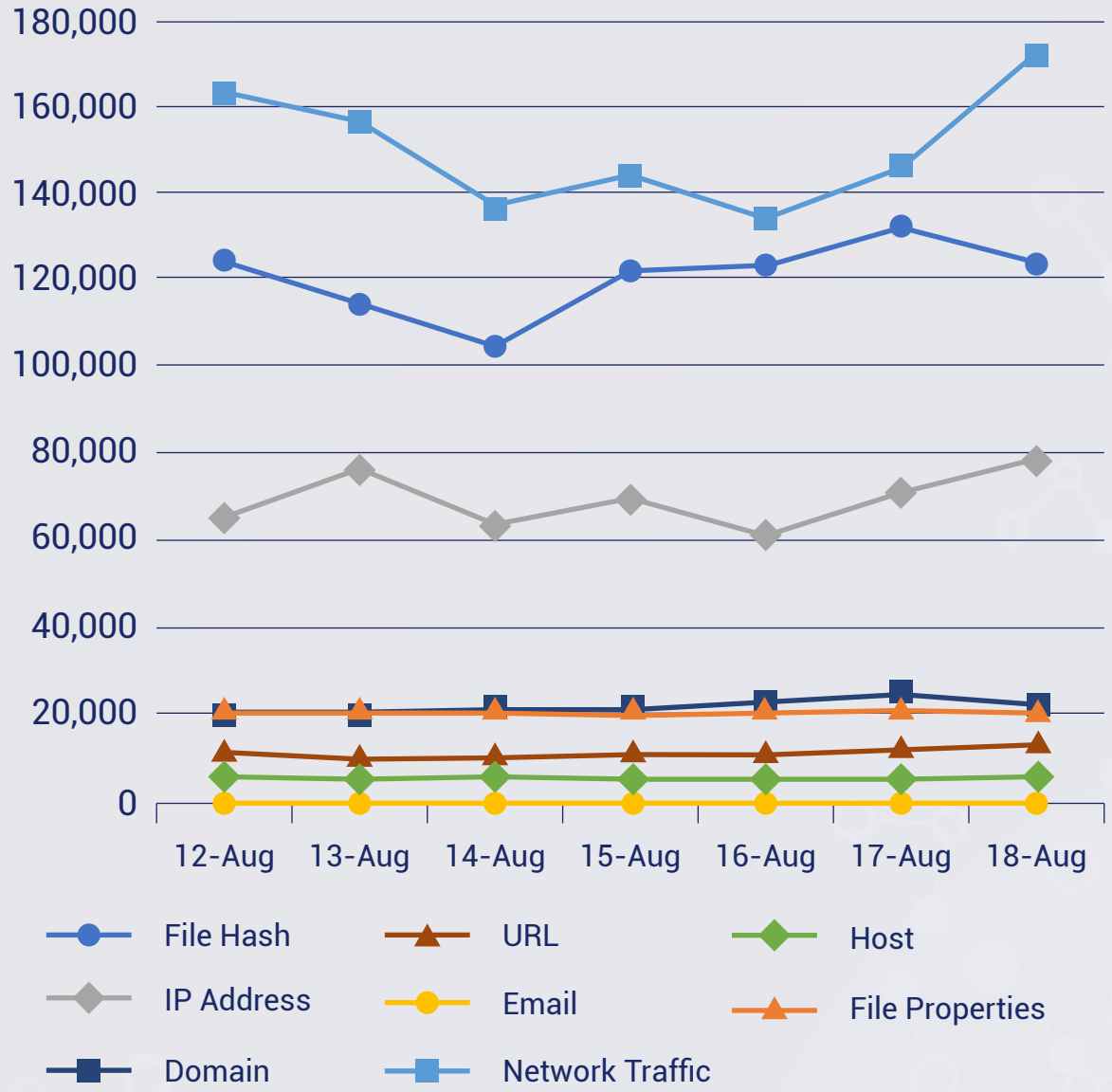
IDPS Rules Created (Week Ending 22/08/2022):

23

Overall Weekly Observables Count:

2,776,050

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. ROMCOM RAT

Unit 42 discovered a custom remote access Trojan/backdoor and named it ROMCOM RAT which contains a unique command and control (C2) protocol.

ROMCOM RAT can be executed using one of its two exports named ***ServiceMain*** and ***startWorker***. Both exports lead to the execution of the same function; however, the difference is the string passed as a parameter: ServiceMain passes the string _inet, while startWorker passes the string _file. Based on this string alone, the flow of execution within the sample is completely different, with ServiceMain causing the sample to beacon out to its C2 server, and startWorker resulting in the sample opening a backdoor on the system and waiting for connections.

Rules Created: 02
Rule Set Type: Balanced - IDS: Reject – IPS: Drop
Class Type: Trojan Activity
Kill Chain: Privilege Escalation TA0004 - Défense Evasion TA0005 - Credential Access TA0006 - Discovery TA0007 - Collection TA0009

2. MikuBot

Researchers recently came across a new malware bot named “MikuBot” selling on a cyber-crime forum. Mikubot is a malicious bot that steals sensitive data and launches hidden VNC sessions that allow the attacker to access the victim's machine remotely, spread through USB, download and execute other malware. The bot is written in C++ and works on operating systems ranging from Windows Vista to Windows 11. The malware is standalone and does not require any dependencies to run. It is capable to use encrypted strings, dynamic API functions, unique object names, anti-emulation methods, and tricks to evade detection by antivirus products.

Rules Created: 02
Rule Set Type: Balanced - IDS: Reject – IPS: Drop
Class Type: Trojan Activity
Kill Chain: Execution T1204/T1059-Defense Evasion T1497/T1027-Persistence T1053/T1547-Discovery T1082-Collection T1005- Command and Control T1071

3. CVE-2022-31656

VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. Updated advisory with information that VMware has confirmed malicious code that can exploit CVE-2022-31656 in impacted products is publicly available.

The UrlRewriteFilter layer is responsible for mapping requests to some internal servlets based on predefined rules (in the WEB-INF/urlrewrite.xml file). If the request has path math with the regex matching the predefined one, then it will map to the servlet. After having RequestDispatcher (rq variable), the program calling rq.forward this function will forward (forward) the request from one servlet to another so it can also pass the request to "ResourceServlet" to get resources. This means that the ServletPath having the value of the requested URL corresponds to a resource and is accessible.

Rules Created: 02
Rule Set Type: Balanced - IDS: Alert – IPS: Alert
Security – IDS: Reject – IPS: Drop
Class Type: Exploit
Kill Chain: Initial Access T1190 - Command and Control T1071

4. Kolobko

Cisco has suffered a cyber-attack when one if its employees' personal email account was obtained. The threat actor conducted phishing and vishing attacks that led to obtaining the VPN access to Cisco's corporate environment. After gaining access, attempts to maintain persistence, escalate privileges, and minimise activity artifacts were conducted. Through these indicators of compromise, Red Piranha has deployed signatures that will detect similar activities and sources that were used in this incident.

Rules Created: 15
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: trojan-activity
Kill Chain: Initial Access T1566 - Execution T1569 - Persistence T1136 - Command and Control T1071

5. CopperStealer

CopperStealer is a browser extension-based stealer and its updated version is on the rise. Once installed on a victim's browser:

- It contacts its Command-and-Control server.
- Creates a follow up POST request to its Command-and-Control with the domains of the cryptocurrency domains found on the browser's data.
- Looks for crypto wallet information and sends 85% of the available funds to a wallet controlled by the malware authors.

Rules Created: 1
Rule Set Type: Balanced/Security – IDS: Reject – IPS: Drop
Class Type: trojan-activity
Kill Chain: Initial Access T1189 - Execution T1204 - Persistence T1176 - Collection T1185 - Command and Control T1102

6. CVE 2022-27925

CVE-2022-27925 is a high severity vulnerability in ZCS releases 8.8.15 and 9.0 that have mboximport functionality to receive a ZIP archive and extract files from it. An authenticated user can upload arbitrary files to the system thereby leading to directory traversal.

The vulnerability entails following steps to be taken -

- Set up a vulnerable instance of ZCS.
- Create a specially crafted ZIP file containing a file with a name that contains a relative path, allowing it to be dropped to the correct directory.
- Send an HTTP POST request to the ZCS instance's MailboxImport servlet with the ZIP file in the body of the post.
- Use an authentication token belonging to a logged-in administrator in the correct HTTP header (this can be done by logging in and inspecting requests manually) to authenticate with the server.

In summary, an unauthenticated user was able to access this endpoint (which is intended as a feature used by administrators), and further means that CVE-2022-27925 can effectively be turned into an unauthenticated RCE exploit. Even after the patch for CVE-2022-27925, which fixed the directory traversal issue, an attacker could overwrite any user's mailbox using a specially crafted request, as the initial patch did not resolve the authentication issue.

Rules Created: 01
Rule Set Type: Balanced – IDS: Alert – IPS: Alert
Security – IDS: Reject – IPS: Drop
Class Type: Exploit
Kill Chain: T1059 - Command and Scripting Interpreter, T1134 - Access Token Manipulation, T1027 - Obfuscated Files or Information, T1057 - Process Discovery, T1505 - Server Software Component