
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Aug 23 - 29, 2022

Report Summary:

- **New Threat Detection Added** – 6 (DoNot APT Group, VileRAT, AtomSilo Ransomware -Lockbit Affiliate, SVCReady, Amadey trojan, and HyperScrape Tool.)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

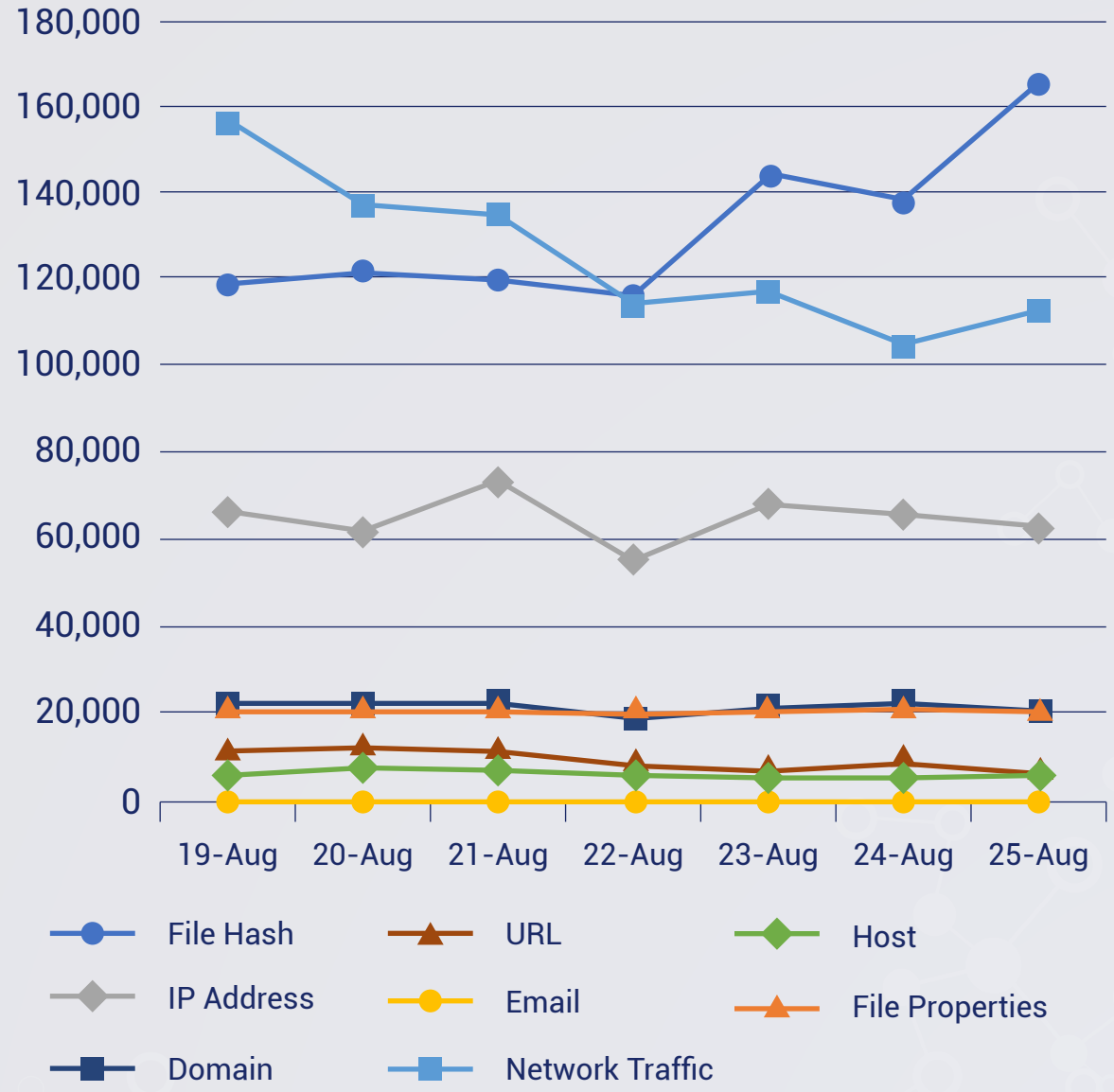
IDPS Rules Created (Week Ending 29/08/2022):

17

Overall Weekly Observables Count:

2,618,512

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. DoNot APT Group

DoNot is an APT group known to target and conduct attacks on South Asian countries. They have launched campaigns on South Asian organisations such as Military, Embassies, Ministries of Foreign Affairs. They are consistent with their techniques which starts with Phishing emails. Upon execution of the attachment from these phishing emails, macros are then leveraged to load their second-stage malware. The malware from the DoNot group is observed to function as screenshot and file collectors, keyloggers, browser stealers and also establishes reverse shell connections. It uses Google Drive for Command-and-Control traffic.

Red Piranha has deployed rules on Crystal Eye devices that can detect these DoNot-related domains. Traffic going to and from these domains are rejected upon detection.

Rules Created: 08
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1204 - Persistence T1053 - Defense Evasion T1055/T1574 - Command-and-Control T1102 - Exfiltration T1567

2. VileRAT Malware

VileRAT is the name of a Remote Access Trojan (RAT) malware that gives the attacker administrative control over a compromised computer. It is known that cybercriminals behind VileRAT are targeting foreign and cryptocurrency exchanges. This RAT can execute remote commands, keylogging, and other things. Threat actors distribute VileRAT by sending emails containing MS Word document. This document further downloads a malicious and macro-enabled document. The Word document starts the infection chain after users enable macros commands (editing/content). Emails used to deliver VileRAT are disguised as official letters from legitimate companies. VileRAT's ability to execute arbitrary remote commands allows cybercriminals to perform malicious activities via Command Prompt. Threat actors can use this feature to download and execute files, delete (or manage) files stored on a computer, open websites, end/kill processes, and many more. Additionally, VileRAT can update itself from a Command-and-Control server, list antivirus software installed on the infected computer, establish SSH connections to a remote server, and set up persistence using Windows Task Scheduler by creating scheduled tasks. Cybercriminals behind VileRAT frequently update their malware and improve techniques that allow this RAT to avoid antivirus detection. Judging by the capabilities of VileRAT, it is used to steal sensitive information, spy on victims, or even distribute other malware. More examples of RATs with similar features are Woody RAT, ApolloRAT, and Nerbian RAT.

Rules Created: 02
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1204 - Persistence T1053 -Command-and-Control T1102

3. AtomSilo Ransomware (Lockbit Affiliate)

AtomSilo ransomware (Lockbit Affiliate) is on the rise since April 2022. This malware leverages Windows Defender (MpCmdRun.exe) in sideloading its CobaltStrike payloads. The infection chain starts with an exploitation of a Log4j vulnerability. Upon initial access, system information is gathered, and post-exploitation techniques are executed. This is where it was observed that Windows Defender was utilized to side-load and decrypt its CobaltStrike payload.

Red Piranha has deployed rules created out of indicators of compromise that will detect communications to the stored malicious payloads and Command-and-Control server.

Rules Created: 01
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: Trojan-activity
Kill Chain: Initial Access T1190 - Execution T1059 - Defense Evasion T1218 - Command-and-Control T1102

4. SVCReady

The world is observing a new emerging malware called SVCReady, a loader for various crimeware (Vidar, Ursnif and others). The malware is notable for its unusual way it is delivered to target PCs – using shellcode hidden in the properties of Microsoft Office documents. As in many other malware campaigns, the documents contain Visual Basic for Applications (VBA) AutoOpen macros that are used to execute malicious code. But unlike other Office malware, the document does not use PowerShell or MSHTA to download further payloads from the web. Instead, the VBA macro runs shellcode stored in the properties of the document, which then drops and runs SVCReady malware.

Functionalities of the malware are:

- Download a file to the infected client
- Take a screenshot
- Run a shell command
- Check if it is running in a virtual machine
- Collect system information (a short and a “normal” version)
- Check the USB status, i.e. the number of devices plugged-in
- Establish persistence through a scheduled task
- Run a file
- Run a file using RunPeNative in memory

Rules Created: 01
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: Malware
Kill Chain: Defense Evasion T1218

5. Amadey Trojan

Amadey infects a victims' computer and incorporates it into a botnet. The Amadey trojan can also download additional malware and exfiltrate user information to a command and control (C2) server. Moreover, it can engage the victims' system in distributed denial-of-service attacks2 and have it send spam with additional malware. The threat actor sends spam emails that reference a package or shipment. Many emails claim in the subject line that the package or shipment; is from the shipping company DHL. For example, "You have a package coming from DHL." However, the email body in this campaign are blank. Each email has a ZIP attachment containing a Visual Basic Script (VBS) file. Each file name for the ZIP files is a series of numbers separated by an underscore, such as 410044450_64504154.zip. The VBS files have the same name as their ZIP file, except they have the VBS extension rather than the ZIP extension. The victim receives an email with an attached ZIP file. After extracting and opening the VBS file it contains, a window with the title "MS Word" appears. However, it is not a Microsoft Word document; it is a pop-up from the VBS file imitating an error that Word might throw. The window states that an unexpected error has occurred and to try again later. In the background, the script extracts and executes the file FgdkHbrze.txt. Although it has the TXT extension, it is actually an executable file. FgdkHbrze.txt extracts and executes the final Amadey payload, kntd.exe, which contacts its C2 and adds a key to the Windows Startup Registry to maintain persistence.

Rules Created: 02
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: Trojan
Kill Chain: Ingress Tool Transfer T1105 - Screen Capture T1113 - Process Injection T1055 - Abuse Elevation Control Mechanism T1548 - Obfuscated Files or Information T1027 - Signed Binary Proxy Execution T1218 - Network Sniffing T1040 - Boot or Logon Autostart Execution T1547 –Phishing T1566

6. HyperScrape Tool

A novel Charming Kitten tool named HYPERSCRAPE, used to steal user data from Gmail, Yahoo!, and Microsoft Outlook accounts has been detected by the Researchers from Google. The attacker runs HYPERSCRAPE on their own machine to download victims' inboxes using previously acquired credentials. Researchers have seen it deployed against fewer than two dozen accounts located in Iran. The oldest known sample is from 2020, and the tool is still under active development. HYPERSCRAPE requires the victim's account credentials to run using a valid, authenticated user session the attacker has hijacked, or credentials the attacker has already acquired. It spoofs the user agent to look like an outdated browser, which enables the basic HTML view in Gmail. Once logged in, the tool changes the account's language settings to English and iterates through the contents of the mailbox, individually downloading messages as .eml files and marking them unread. After the program has finished downloading the inbox, it reverts the language back to its original settings and deletes any security emails from Google. Earlier versions contained the option to request data from Google Takeout, a feature which allows users to export their data to a downloadable archive file.

Rules Created: 03
Rule Set Type: Balanced – IDS: Reject – IPS: Drop
Class Type: Trojan- Activity
Kill Chain: Privilege Escalation TA0004- Defense Evasion TA0005 - Discovery TA0007 -Collection TA0009 -Command and Control TA0011