Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

Nov 22 - 28, 2022

# Report Summary:

- **New Threat Detection Added** – 06 (Hyperscrape Malware, HGRat Malware, HCRootkit, Micropsia, SCANBOX, and KOLOBKO)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

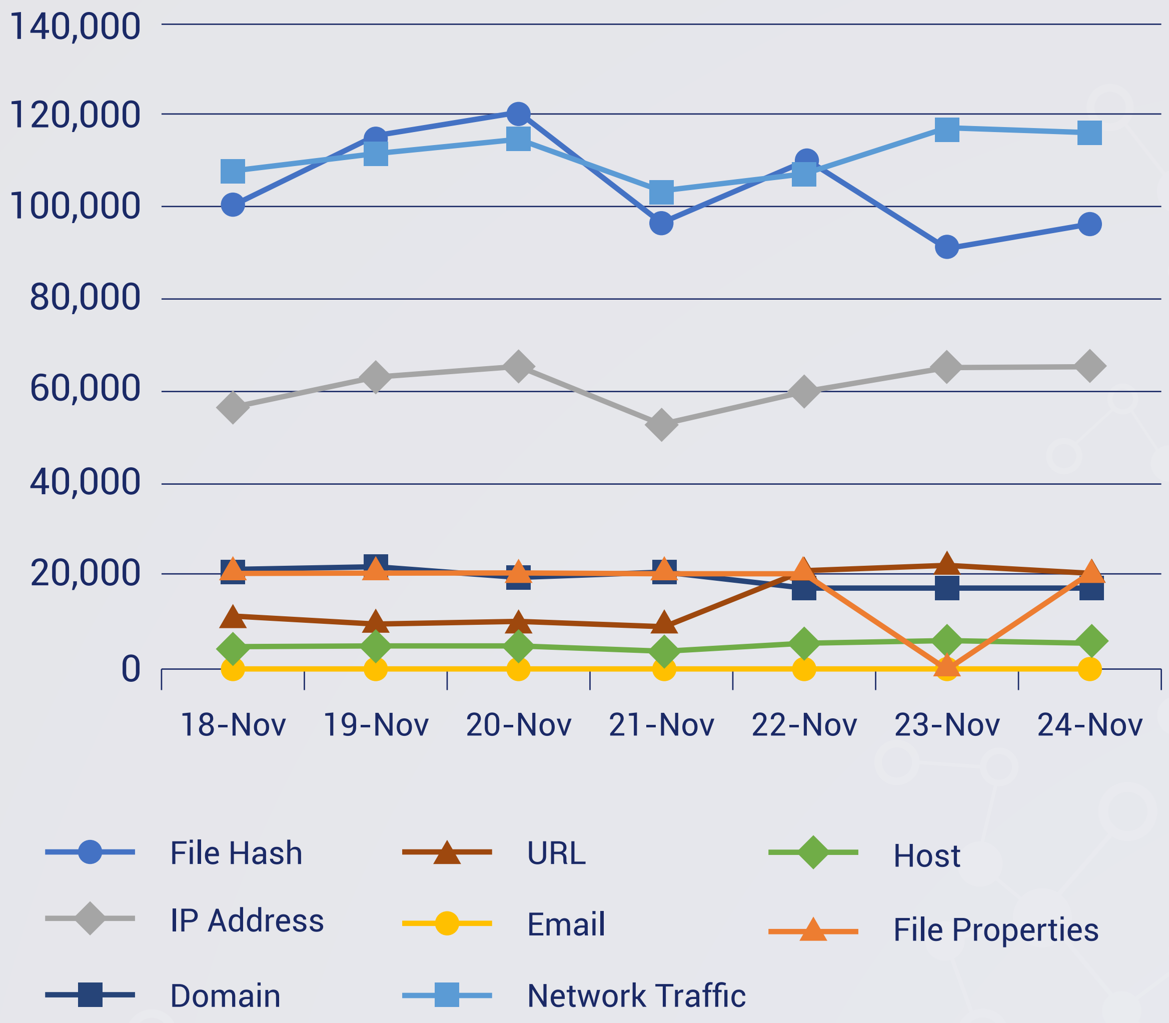
## New Threat Protections (Week Ending 28/11/2022):

**20**

## Overall Weekly Observables Count:

**2,298,067**

## Daily Submissions by Observable Type:



# Newly Detected Threats Added

## 1. Hyperscrape Malware

The Iranian Advanced Persistent Threat (APT) cyberespionage group, APT35, also known as Charming Kitten or Phosphorus, has been found using a new malicious tool called  Hyperscrape  to extract emails from victims' mailboxes. The emails associated with the campaigns contained links that led to installation of malware. In addition, domains were used as a part of the command-and-control infrastructure of the group. Hyperscrape checks its connectivity to a particular command control server after it is executed from a folder with specific file dependencies. Hyperscrape then terminates if there is no connectivity. Next, it opens a form to specify parameters if everything is okay. Once the parameters are provided, data is sent to the command and control for confirmation. Subsequently, a new form appears, and APT35 provides a valid cookie file unless it was provided via the command line. After starting an embedded web browser, Hyperscrape stores the cookies in a local cache used by the browser. The browser is configured to look like it is outdated. Finally, the browser navigates to the targeted email server (Gmail, Outlook, etc.).

**Threat Protected:** 03
**Rule Set Type:**

| Ruleset | IDS: Action | IPS: Action |
|---|---|---|
| Balanced | Reject | Drop |
| Security | Reject | Drop |
| WAF | Disabled | Disabled |
| Connectivity | Alert | Alert |
| OT | Disabled | Disabled |

**Class Type:** Malware
**Kill Chain:** Resource Development T1586 – Reconnaissance T1595 – Initial Access T1566 Credential Access T1003 – Collection T1560/T1114

## 2. HGRat Malware

Researchers recently detected a new Remote Access Trojan (RAT) malware called HZRat. Based on research, at least three versions of HZ Rat (HZ_2.8.2, HZ_2.9.0, HZ_2.9.1) have been submitted so far. Threat actors (TAs) reported using two different attack vectors to deliver backdoors to their targets. Embedded as a self-extracting zip archive or a malicious RTF document created using the Royal Road framework. It is believed that the campaign is still ongoing and active since at least October 2020. HZRat itself is used as an initial access tool with limited capabilities such as executing commands and uploading files. Reports showed that this malware was used to steal credentials and identify the system. The second distribution method is simply tricking the user into running a malicious self-extracting archive and then piggybacking the process of extracting. Pretending that the archive installs OpenVPN, puTTYgen or EasyConnect, it runs install.VBS. Firstly, it runs default.exe (HZ Rat) and then the actual lure program. Once started, it iterates through a list of C2 servers to connect to and receive commands. The malware itself acts like a client and executes the commands it receives.

**Threat Protected:** 01
**Rule Set Type:**

| Ruleset | IDS: Action | IPS: Action |
|---|---|---|
| Balanced | Alert | Alert |
| Security | Reject | Drop |
| WAF | Disabled | Disabled |
| Connectivity | Alert | Alert |
| OT | Disabled | Disabled |

**Class Type:** Trojan- Activity
**Kill Chain:** Execution T1059/T1064 – Persistence T1543.003/T1547.001/T1547.008 – Privilege Escalation T1055 – Defence Evasion T1036/T1055/T1055/T1064/T1497 – Credential Access T1040 – Discovery T1010/T1012/T1040/T1057/T1082/T1083/T1497 – Command-and- control T1571

## 3. HCRootkit

HCRootkit is a Linux rootkit that affects 32-bit, 64-bit, and ARM architectures. The rootkit includes a keylogger, a module used for downloading and executing commands as well as an ICMP module for monitoring bytes before triggering events (download/execution). It is based on a backdoored version of the Coreutils 'kill' binary. The main goal of the rootkit is to hide its second-stage payload. It hides the Command-and-Control traffic from the firewall by masking it as traffic from the local host.

**Threat Protected:** 06
**Rule Set Type:**

| Ruleset | IDS: Action | IPS: Action |
|---|---|---|
| Balanced | Reject | Drop |
| Security | Reject | Drop |
| WAF | Disabled | Disabled |
| Connectivity | Alert | Alert |
| OT | Disabled | Disabled |

**Class Type:** Trojan- Activity
**Kill Chain:** Execution T1059 - Persistence T1547 - Command-and-Control T1205

## 4. Micropsia

Micropsia is a python-based stealer trojan but is made into windows executable. It is capable of keylogging, creating screenshots, recording audio, collecting email information, and uploading information to its command-and-control server via HTTP traffic. It is persistence via creating registry keys. This trojan is attributed to the threat group AridViper.

**Threat Protected:** 01
**Rule Set Type:**

**Class Type:** Trojan-activity
**Kill Chain:** Execution T1059 - Persistence T1547 - Command-and-Control T1102

| Ruleset | IDS: Action | IPS: Action |
|---|---|---|
| Balanced | Reject | Drop |
| Security | Reject | Drop |
| WAF | Disabled | Disabled |
| Connectivity | Alert | Alert |
| OT | Disabled | Disabled |

## 5. SCANBOX

The China-based espionage-motivated APT group “APT TA423”, AKA “Red Ladon”, has been observed conducting a campaign targeting local and federal Australian government agencies, Australian media organizations, and energy firms in the South China Sea. The malware in these campaigns are hosted on OneDrive and GitHub sites. They are distributed by phishing emails and hiding malicious links between various legitimate links to avoid detection. Gmail, Outlook and SendGrid email addresses are used to bypass security controls and to convince the recipient the email is authentic.

**Threat Protected:** 01
**Rule Set Type:**

| Ruleset | IDS: Action | IPS: Action |
|---|---|---|
| Balanced | Reject | Drop |
| Security | Reject | Drop |
| WAF | Disabled | Disabled |
| Connectivity | Alert | Alert |
| OT | Disabled | Disabled |

**Class Type:** Malware
**Kill Chain:** Execution TA0002 - Discovery TA0007

## 6. KOLOBKO

A financially motivated offensive group named  UNC2447  was found to exploit a zero-day vulnerability in SonicWall VPN before a patch was made available to deploy advanced malware previously reported as SOMBRAT. It is linked to the deployment of ransomware, which has never been publicly reported. UNC2447 first used FIVEHANDS ransomware to extort victims, followed by aggressive pressure by threatening media attention and selling victims' data on hacker forums to force intrusion. UNC2447 has been seen targeting organizations in Europe and North America and has consistently demonstrated advanced capabilities to evade detection and minimize post-breach forensics.

**Threat Protected:** 06
**Rule Set Type:**

| Ruleset | IDS: Action | IPS: Action |
|---|---|---|
| Balanced | Reject | Drop |
| Security | Reject | Drop |
| WAF | Disabled | Disabled |
| Connectivity | Alert | Alert |
| OT | Disabled | Disabled |

**Class Type:** Malware
**Kill Chain:** Initial Access T1566/T1079 - Execution T1569 – Persistence T1176/T1098 - Privilege Escalation T1546 - Command and Control T1071