Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

Nov 1 - 7, 2022

# Report Summary:

- **New Threat Detection Added** – 06 [Juniper SSLVPN: Multiple vulnerabilities, Manjusaka: The Chinese Cobalt Strike, Drinik Malware, VMware NSX (CVE-2021-39144), Spooky SSL, and RomCom RAT]
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

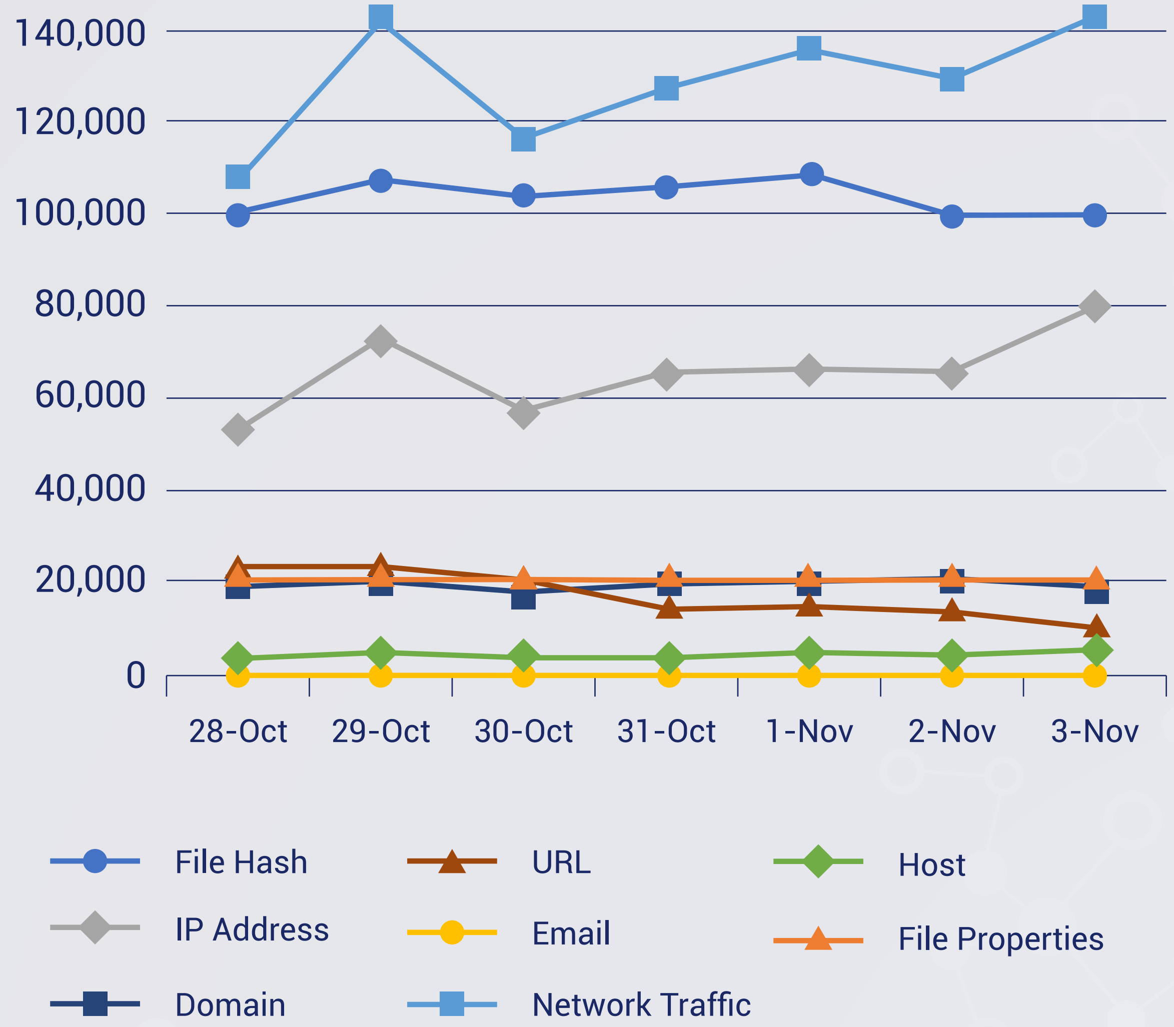
## New Threat Protections (Week Ending 07/11/2022):

**14**

## Overall Weekly Observables Count:

**2,503,637**

## Daily Submissions by Observable Type:



# Newly Detected Threats Added

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

## 1. Juniper SSLVPN: Multiple vulnerabilities

Juniper, an American multinational corporation that develops networking products such as routers, switches, network management software and network security products, has recently reported multiple vulnerabilities in its J-Web component of Junos OS. These vulnerabilities lead to unauthorized local file access, cross-site scripting attacks, path injection and traversal, or local file inclusion of the said component. The details of the vulnerabilities are given below:

1. CVE-2022-22241-An improper input validation vulnerability allows an attacker to access data without proper authorization.

2. CVE-2022-22242 - A Cross-site Scripting (XSS) vulnerability allows attacker to run malicious scripts.

3. CVE-2022-22243- An XPath Injection vulnerability due to Improper Input Validation allows an attacker to add an XPath command to the XPath stream leading to a partial loss of confidentiality.

4. CVE-2022-22244- An XPath Injection vulnerability allows an attacker to send crafted POST requests to reach the XPath channel leading to a partial loss of confidentiality.

5. CVE-2022-22245- A Path Traversal vulnerability allows attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The exploitation of this vulnerability could lead to loss of filesystem integrity.

6. CVE-2022-22246- A PHP Local File Inclusion (LFI) vulnerability allows an attacker to execute an untrusted PHP file. The exploitation of the same could lead to a complete system compromise.

The affected versions of Juniper Junos OS are as under:
All versions prior to 19.1R3-S9
19.2 versions prior to 19.2R3-S6
19.3 versions prior to 19.3R3-S7
19.4 versions prior to 19.4R3-S9
20.1 versions prior to 20.1R3-S5
20.2 versions prior to 20.2R3-S5
20.3 versions prior to 20.3R3-S5
20.4 versions prior to 20.4R3-S4
21.1 versions prior to 21.1R3-S2
21.2 versions prior to 21.2R3-S1
21.3 versions prior to 21.3R3
21.4 versions prior to 21.4R3
22.1 versions prior to 22.1R2

**Threat Protected:** 05
**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:** File and Directory Traversal T1083 - Drive-By Compromise T1456

## 2. Manjusaka: The Chinese Cobalt Strike

A researcher recently reported a new cyber-attack framework named "Manjusaka" which was found used in the wild that can become dominant across the threat landscape. It is said that the Manjusaka framework is a copy of the world-famous Cobalt Strike cyber-attack framework. Manjusaka malware is written in the Rust language for Windows and Linux, and the command and control (C2) of the same is written in GoLang with a User Interface in the Simplified Chinese language freely available and can easily generate new payloads with custom configurations.

**Threat Protected:** 02
**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:** Defense Evasion T1497- Discovery T1033/T1082/T1497- Command and Control T1071/T1095/T1105

## 3. Drinik Malware

A malware variant known for targeting Indian bank customers has been recently observed to have been updated. Drinik android malware was discovered in September of 2021. Initially observed to be stealing PII from customers, but recent updates to the malware have provided new capabilities. It is now used for screen recording, keylogging, and manipulating the devices' Call and Messaging functions.

**Threat Protected:** 04
**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:**Initial Access T1456 - Execution T1575 - Credential Access T1417 - Collection T1417/T1513/T1512 - Command-and-Control T1481 - Impact T1616/T1582

## 4. VMware NSX (CVE-2021-39144)

A remote code execution vulnerability has been recently discovered on VMware Cloud Foundation. The NSX-V plug-in is affected by a flaw in its XStream library through input serialization. The successful exploitation of this vulnerability results in code execution with root privileges on the appliance. A patch has been released by VMware. It is also confirmed that a Proof-of-Concept exploit was made available to the public.

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

**Class Type:** Attempted-admin
**Kill Chain:** Initial Access T1190

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

## 5. VMware NSX (CVE-2021-39144)

Two high-severity vulnerabilities in the OpenSSL security framework (CVE-2022-3602 & CVE-2022-3786), also known as “Spooky SSL.” These vulnerabilities were announced as a “Critical” severity rating but downgraded to “High” upon further analysis by OpenSSL. These CVEs are related to buffer overruns in the security certificate verification code, and more information can be found on the OpenSSL site.

Potentially Affected Products

These products and versions include OpenSSL 3.0 and patches are in development:

Server 22.1+

Designer 22.1+

Server FIPS 22.1+

Designer FIPS 22.1+

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

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

**Class Type:** Exploit
**Kill Chain:** Initial Access T1190

## 6. ROMCOM RAT

The initial "Advanced IP Scanner" campaign occurred on July 23, 2022. Once the victim installs a Trojanized bundle, it drops RomCom RAT into the system. On October 10, 2022, the threat actor improved evasion techniques by obfuscation all strings, executing as a COM object, and others. The development marks a shift in the attacker's modus operandi, which previously attributed to spoofing legitimate apps like Advanced IP Scanner and pdfFiller to drop backdoors on compromised systems. While previous iterations of the campaign involved the use of trojanized Advanced IP Scanner, the unidentified adversarial collective has since switched to pdfFiller as of October 20, indicating an active attempt on part of the adversary to refine tactics and thwart detection. These lookalike websites host a rogue installer package that results in the deployment of the RomCom RAT, which can harvest information and capturing screenshots, all of which are exported to a remote server.

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

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

**Class Type:** Trojan
**Kill Chain:** Persistence TA0003 - Privilege Escalation TA0004 - Defense Evasion TA0005 - Discovery TA0007 - Command and Control TA0011