Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 8 - 14, 2022

Report Summary:

- **New Threat Detection Added** – 06 (NetDooka Malware Framework , ChromeLoader Malware, Ursnif Malware, Cloud9, IceXLoader, and Worok Malware)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

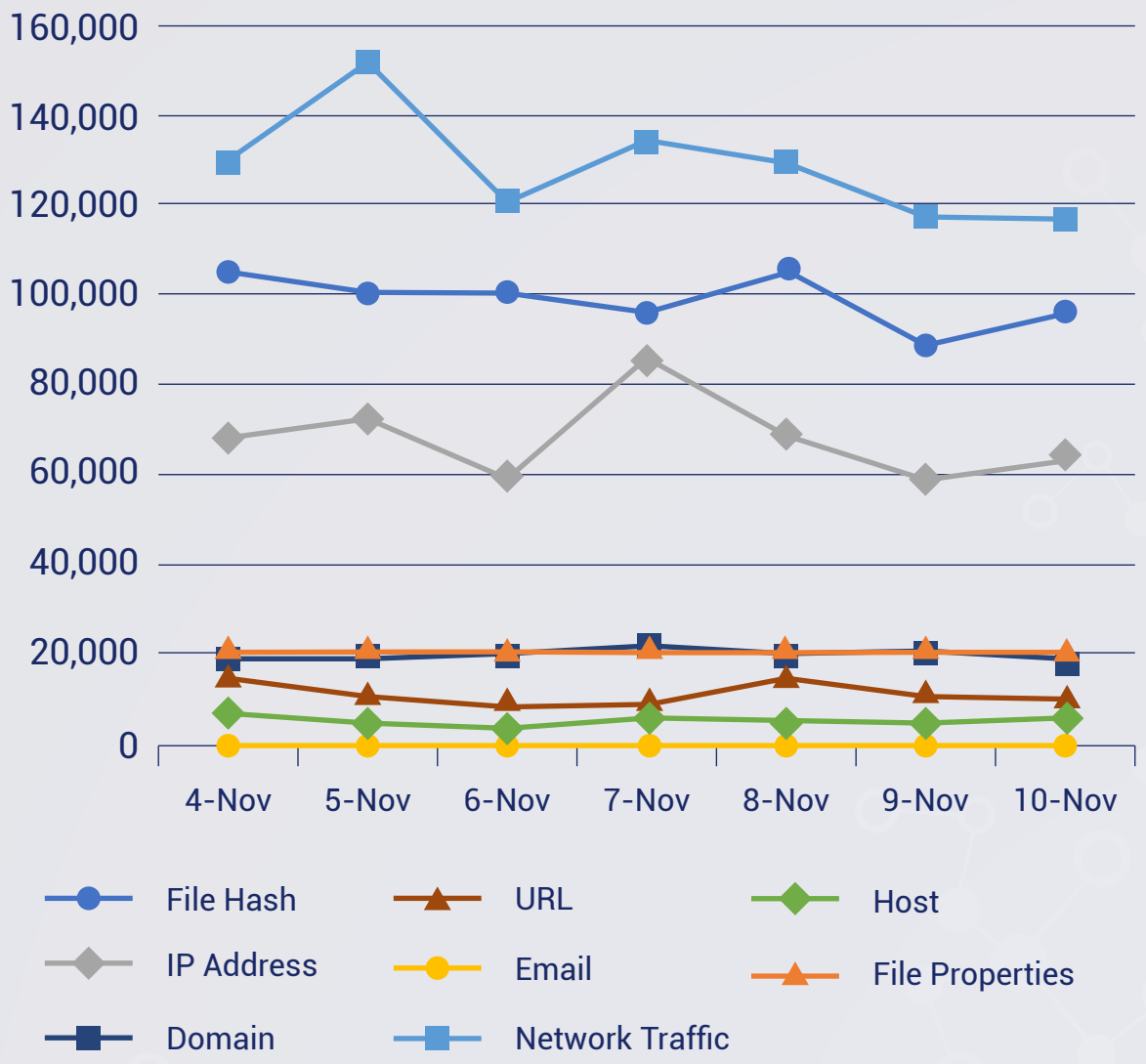
New Threat Protections (Week Ending 14/11/2022):

19

Overall Weekly Observables Count:

2,429,922

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. NetDooka Malware Framework

Researchers recently found a sophisticated malware framework and named it NetDooka after the names of some of its components. This malware is being delivered using a pay-per-install (PPI) service and comprise multiple parts, including a loader, a dropper, a protection driver, and a full-featured remote access trojan (RAT). NetDooka is spread via Private Loader malware which once installed, starts the whole infection chain.

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: Trojan- Activity
Kill Chain: Persistence T1574.002/T1546 - Privilege Escalation T1055/TA0004/T1546 - Defense Evasion T1036/T1497 - Credential Access T1056.001 - Discovery T1010/ T1012/T1082/T1083/T1497 - Collection T1113/T1125 - Command and Control T1571- Impact T1489

2. ChromeLoader Malware

In the beginning of 2022, a new malware named ChromeLoader a.k.a CS_installer was detected, in the wild targeting Chrome browsers. The ChromeLoader uses ISO image malicious files as the initial infection vector. The malware installs itself as a Chrome extension. It works as a browser hijacker capable of stealing users' personal information and track back all browser activities. The ChromeLoader found was developed in .NET programming language and is known as ChromeLoader due to its scheduled task entry for persistence in the infected device.

Threat Protected: 05
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 T1047 - Persistence T1053/T1176- Privilege Escalation T1053/T1055 -Defense Evasion T1036/T1497- Credentials Access T1552 – Discovery T1012/T1082/T1497/T1518- Collection T1185 – Command-in-Command T1071/T1095/T1573

3. Ursnif Malware

Recently, a new Ursnif malware has been observed in the wild. Ursnif was known for bank fraud activities. A new variant of the Ursnif malware seems to have shifted to a backdoor and ransomware-like behaviour. The threat starts from a recruitment email lure that contains links that will lead to the domain of a recruitment company. The email includes documents related to the email that contains the payload when downloaded and executed.

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: Initial Access T1566 - Execution T1059 - Persistence T1053 - Defense Evasion T1027 - Command-and-Control T1102

4. Cloud9

Cloud9 Botnet is a browser extension trojan that has a multitude of functionalities. It steals user sessions, logs keystrokes, can initiate DDoS attacks, mine cryptocurrency, inject ads and exploit browsers. It masquerades itself as an Adobe player plugin that needs to be installed on a browser.

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: Attempted-admin
Kill Chain: Initial Access T1189 - Execution T1203 - Persistence T1176 - Command-and-Control T1102 - Exfiltration T1020

5. IceXLoader

IceXLoader is a commercial malware used to download and deploy additional malware on infected machines. While the version discovered in June (v3.0) looked like a work-in-progress, v3.3.3 loader looks to be fully functional and includes a multi-stage delivery chain.

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: T1105 – Ingress Tool Transfer - T1140 – Deobfuscate/Decode Files or Information - T1620 – Reflective Code Loading -T1497 – Virtualization/Sandbox Evasion -T1055.012 – Process Injection: Process Hollowing - T1592 – Gather Victim Host Information - T1590.005 – Gather Victim Network Information: IP Addresses - T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1059.001 – Command and Scripting Interpreter: PowerShell - T1562.001 –Impair Defenses: Disable or Modify Tools

6. Worok Malware

A threat group tracked as 'Worok' hides malware within PNG images to infect victim's machines with information-stealing malware without raising alarms. The malware is deployed by attackers via ProxyShell vulnerabilities. In some corner cases, exploits against the ProxyShell vulnerabilities were used for persistence in the victim's network. The attackers then used publicly available exploit tools to deploy their custom malicious kits. So, the final compromise chain is straightforward: the first stage is CLRLoader which implements a simple code that loads the next stage (PNGLoader).

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: Reconnaissance T1592 - Resource Development T1588 – Execution T1059 – Persistence T1505 - Defense Evasion T1140 - Credential Access T1003 – Discovery T1082 - Command and Control T1071 – Exfiltration T1041