
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Oct 4 - 10, 2022

Report Summary:

- **New Threat Detection Added** – 6 (ZINC Group, MS Exchange - CVE-2022-41040, CVE-2022-41082, Trojanized Comm100 Installer, NetDooka Malware Framework, TraderTraitor Malware and HyperBro)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

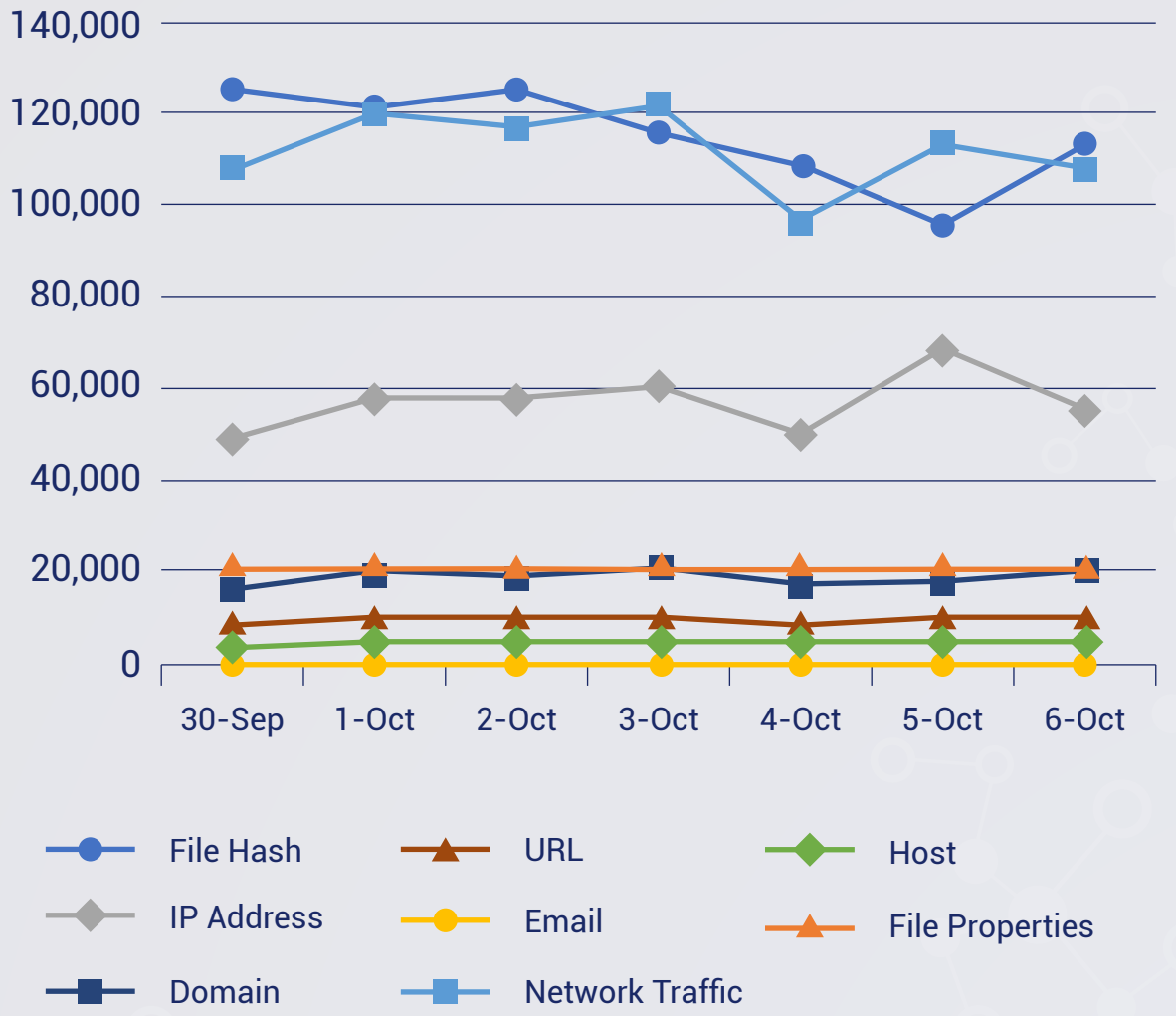
IDPS Rules Created (Week Ending 10/10/2022):

19

Overall Weekly Observables Count:

2,335,112

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. ZINC Group

ZINC is a highly operational, destructive, and sophisticated nation-state activity group. Active since 2009, the activity group gained further public notoriety in 2014 following their successful attack against Sony Pictures Entertainment. ZINC is known to use various custom remote access tools (RATs) as part of their arsenal, including those detected as FoggyBrass and PhantomStar.

Spear-phishing campaign has been observed as a primary tactic of ZINC actors, but they have also been using strategic website compromises and social engineering across social media to achieve their objectives.

ZINC targets employees of companies by attempting to infiltrate and seek to coerce these individuals into installing seemingly benign programs or opening weaponized documents that contain malicious macros. Targeted attacks have also been carried out against security researchers over Twitter and LinkedIn.

ZINC attacks appear to be motivated by traditional cyberespionage, theft of personal and corporate data, financial gain, and corporate network destruction.

ZINC attacks bear many hallmarks of state-sponsored activities, such as heightened operational security, sophisticated malware that evolves over time, and politically motivated targeting. ZINC, tracked by other security companies as Labyrinth Chollima and Black Artemis, has been observed conducting this campaign from late April to mid-September 2022.

Rules Created: 02
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: Initial Access T1566 - Execution T1204 - Persistence T1053 - Defense Evasion T1055 - Command-and-Control T1102 - Exfiltration T1567

2. MS Exchange - CVE-2022-41040, CVE-2022-41082

A Zero-day vulnerability was recently discovered targeting Microsoft Exchange servers with assigned identifier CVE-2022-41040 (SSRF) and CVE-2022-41082 (RCE). The SSRF vulnerability (CVE-2022-41040) is used to trigger the Remote Code Execution vulnerability (CVE-2022-41082). However, a successful authentication (standard low-privileged user) is required for the chain of attacks to work. Upon initial access through exploitation, a web shell known as Chopper is deployed on the server. Reconnaissance, lateral movement, and data exfiltration shortly followed as observed in the wild.

Rules Created: 01
Rule Set Type:

Class Type: Attempted admin
Kill Chain: Initial Access T1190 - Persistence T1505 - Exfiltration T1567

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

3. Trojanized Comm100 Installer

Comm100 is known for providing automated Chat solutions. There has been a recent discovery of a supply chain attack regarding Comm100's Live Chat installer. The trojanized live chat installer was signed using a valid Comm100 certificate and was available for download. An updated installer has been released by Comm100. The backdoor downloads a script from its external Command-and-Control site which then gathers information from the victim's computer as well as providing a remote shell access.

Rules Created: 05
Rule Set Type:

Class Type: Trojan-Activity
Kill Chain: Initial Access T1195 - Execution T1059 - Command-and-Control T1102

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

4. NetDooka Malware Framework

We recently encountered a sophisticated malware framework that we named NetDooka after the names of some of its components. The framework is distributed via a pay-per-install (PPI) service, containing multiple parts, including a loader, a dropper, a protection driver, and a full-featured remote access trojan (RAT) that implements its own network communication protocol. During analysis, we discovered that NetDooka spread via the Private Loader malware upon installation starts the whole infection chain.

The PrivateLoader malware is a downloader responsible for downloading and installing multiple malwares into the infected system as part of the PPI service. Due to the way PPI service works, the installed payloads might differ depending on the malware version. Some known malware families distributed via PPI services include SmokeLoader, RedLine, and Anubis.

This report focuses on the components and infection chain of the NetDooka framework. The scope ranges from the release of the first payload dropping a loader that creates a new virtual desktop to execute an antivirus software uninstaller and interact with it by emulating the mouse and the pointer position — a necessary step to complete the uninstallation process and preparing the environment for executing other components — up until the release of the final RAT that is protected by a kernel driver.

Rules Created: 08
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: Initial Access T1566 - Execution T1204 - Persistence T1053 - Command-and-Control T1102 - Exfiltration T1567

5. TraderTraitor Malware

Intrusions begin with many spear-phishing messages sent to employees of cryptocurrency companies—often working in system administration or software development/IT operations (DevOps)—on various communication platforms. Messages often mimic a recruitment effort and offer high-paying jobs to entice the recipients to download malware-laced cryptocurrency applications.

TraderTraitor describes a series of malicious applications written using cross-platform JavaScript code with the Node.js runtime environment using the Electron framework. The malicious applications are derived from a variety of open-source projects and purport to be cryptocurrency trading or price prediction tools. TraderTraitor campaigns feature websites with modern design advertising the alleged features of the applications. The JavaScript code providing the core functions of the software, is bundled with Webpack. Within the code is a function that purports to be an "update," with a name such as UpdateCheckSync(), that downloads and executes a malicious payload.

Rules Created: 02
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: Malware
Kill Chain: Defense Evasion TA0005 - Discovery TA0007 - Command and Control TA0011

6. HyperBro

HyperBro is a RAT that has been observed to target primarily within the gambling industries, also been spotted in other places as well. The malware typically consists of 3 or more components:

a) A genuine loader typically with a signed certification

b) A malicious DLL loader loaded from the former component via DLL hijacking

c) An encrypted and compressed blob that decrypts to a PE-based payload which has its C2 information hardcoded within.

HyperBro is a custom in-memory backdoor used by Threat Group-3390. It is used in the last stage of the attacks to gain access to the infected systems. The operation target organizations associated with the government to steal sensitive information. HyperBro can delete a specified file, download additional files, run an application or script/file via API, take screenshots, list all services and their configurations, start and stop a specified service and injects into a newly created process.

Rules Created: 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: Malware
Kill Chain: T1543.003 Persistence - T1574.002 Hijack Execution Flow - T1567.000 Exfiltration - T1560.000 Collection