Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 11 - 17, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Allcome Clipper, CreepySnail Backdoor, Insekt RAT, Triada Trojan, Fortinet CVE-2022-40684 and Maggie MSSQL Backdoor)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

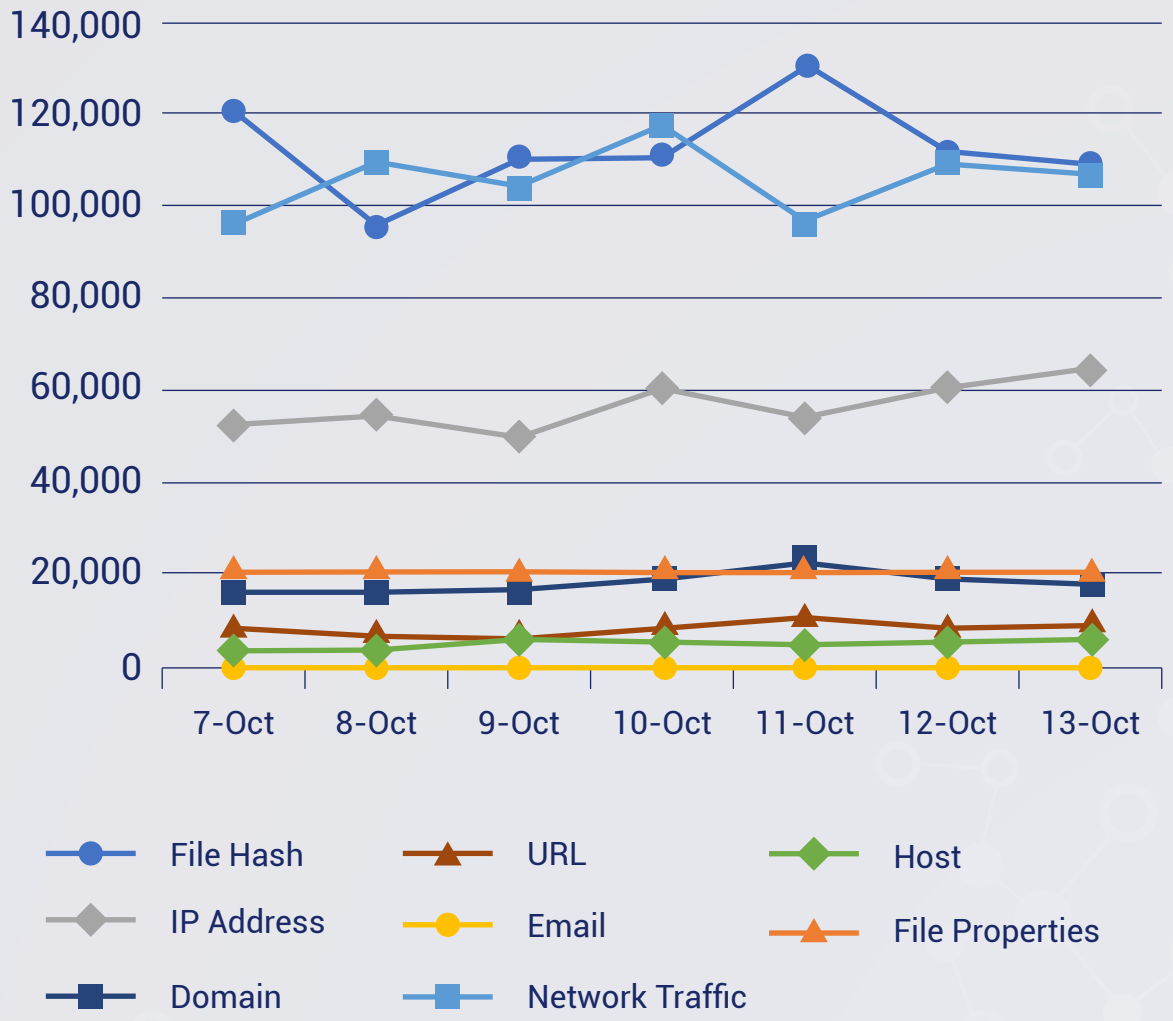
IDPS Rules Created (Week Ending 17/10/2022):

14

Overall Weekly Observables Count:

2,247,434

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Allcome Clipper

Allcome is a clipper-type malicious program that targets cryptocurrencies by replacing clipboard (copy-paste buffer) data for outgoing transactions. The Allcome's developers emphasize their program's versatility and uniqueness. They promise to add content (i.e., cryptocurrency, wallet, card, etc.) per buyer request. Clippers operate by replacing data copied into the clipboard; this feature replaces crypto wallet addresses with ones owned by cyber criminals - when victims make a cryptocurrency transfer/transaction. Therefore, the funds end up in the criminals' possession. According to Allcome's advertising, it can take screenshots when victims are on their online payment journey (thereby obtaining banking and other financial information). This malware also targets credit card details (i.e., cardholder's name, card number, expiration date, and CVV/CVC value/code). With this vulnerable data, cyber criminals may make fraudulent transactions or online purchases. Allcome clipper malware infections can result in severe privacy issues, significant financial losses, and identity theft.

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: Execution TA0002- Privilege Escalation T1055- Defence Evasion T1036/T1055- Collection T1005- Command and Control T1071/T1571

2. CreepySnail Backdoor

POLONIUM has also been observed deploying a custom PowerShell implant detected as Backdoor: PowerShell/CreepySnail.B!dha.. CreepySnail is another PowerShell backdoor that sends HTTP requests to a C&C server and receives and executes PowerShell commands. We saw various versions of this backdoor in the wild, with minimal differences. One version can run any executable specified by the C&C server (if it's in the malware folder). The CreepySnail PowerShell implant, once deployed on a target network, attempts to authenticate using stolen credentials and connect to POLONIUM C2 for further actions on objectives, such as data exfiltration or further abuse as C2.

Rules Created: 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: Trojan- Activity
Kill Chain: Execution- T1588.001/T1059.001/T1059.003/T1129- Collection T1071.001/T1132.001- Command and Control T1095- Exfiltration T1041

3. Insekt RAT

"Alchimist" is a 64-bit Linux executable written in GoLang and packed with assets that includes resources for the web interface and Insekt RAT payloads compiled for Windows and Linux.

Insekt RAT, a new trojan is Alchimist's beacon implant is written in GoLang. It has a variety of remote access capabilities that can be instrumented by the Alchimist C2 server.

Alchimist C2 has a web interface written in Simplified Chinese. It can generate a configured payload, establish remote sessions, deploy payload to the remote machines, capture screenshots, perform remote shellcode execution and run arbitrary commands.

Alchimist C2 panel further features the ability to generate PowerShell and wget code snippets for Windows and Linux, potentially allowing an attacker to flesh out their infection chains to distribute the Insekt RAT payload.

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: Trojan
Kill Chain: Execution TA0002 - Command and Control TA0011 - Discovery TA0007 - Privilege Escalation TA0004

5. Triada Trojan

An unofficial version of the popular WhatsApp messaging app called YoWhatsApp has been observed deploying an Android trojan known as Triada.

The goal of the malware is to steal the keys that "allow the use of a WhatsApp account without the app," YoWhatsApp offers the ability for users to lock chats, send messages to unsaved numbers, and customize the app with a variety of theme options. It's also said to share overlaps with other modded WhatsApp clients such as FMWhatsApp and HeyMods. Typically spread through fraudulent ads on Snaptube and Vidmate, the app, upon installation, requests the victims to grant it permission to access SMS messages, enabling the malware to enrol them to paid subscriptions without their knowledge.

Rules Created: 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: Command and Control TA0011 - Defense Evasion TA0030 - Impact TA0034 - Collection TA0035 - Network Effects TA0038

5. Fortinet CVE-2022-40684

An authentication bypass has been discovered affecting FortiOS, FortiProxy and FortiSwitchManager. This vulnerability can be exploited through specially crafted HTTP Requests to the exposed management interface. Attackers can modify admin users' SSH Keys for login, add new users, modify configurations for traffic manipulation, and capture network traffic.

While exploit attempts can be detected through the rules deployed on Crystal Eye devices, Fortinet has also released patches for this vulnerability.

Rules Created: 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: attempted-admin
Kill Chain: Initial Access T1190 - Execution T1059 - Persistence T1556 - Collection T1602/T1005

6. Maggie MSSQL Backdoor

An MSSQL Backdoor has been recently discovered tagged as "Maggie". It is loaded in the form of a DLL and can be controlled using SQL Queries. It can perform bruteforce attacks against other MSSQL servers within the network and add a user upon successful login. It can execute commands/programs, collect information, manipulate network traffic and act as a proxy. It is still unclear how the Maggie backdoor is initially deployed.

Rules Created: 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: Credential Access T1110 - Command-and-Control T1090 - Collection T1005