Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 25 - 31, 2022

Report Summary:

- **New Threat Detection Added** – 5 (CVE-2022-40684, ROMCOM RAT, WarHawk Malware, Gamaredon APT, and SocGholish)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

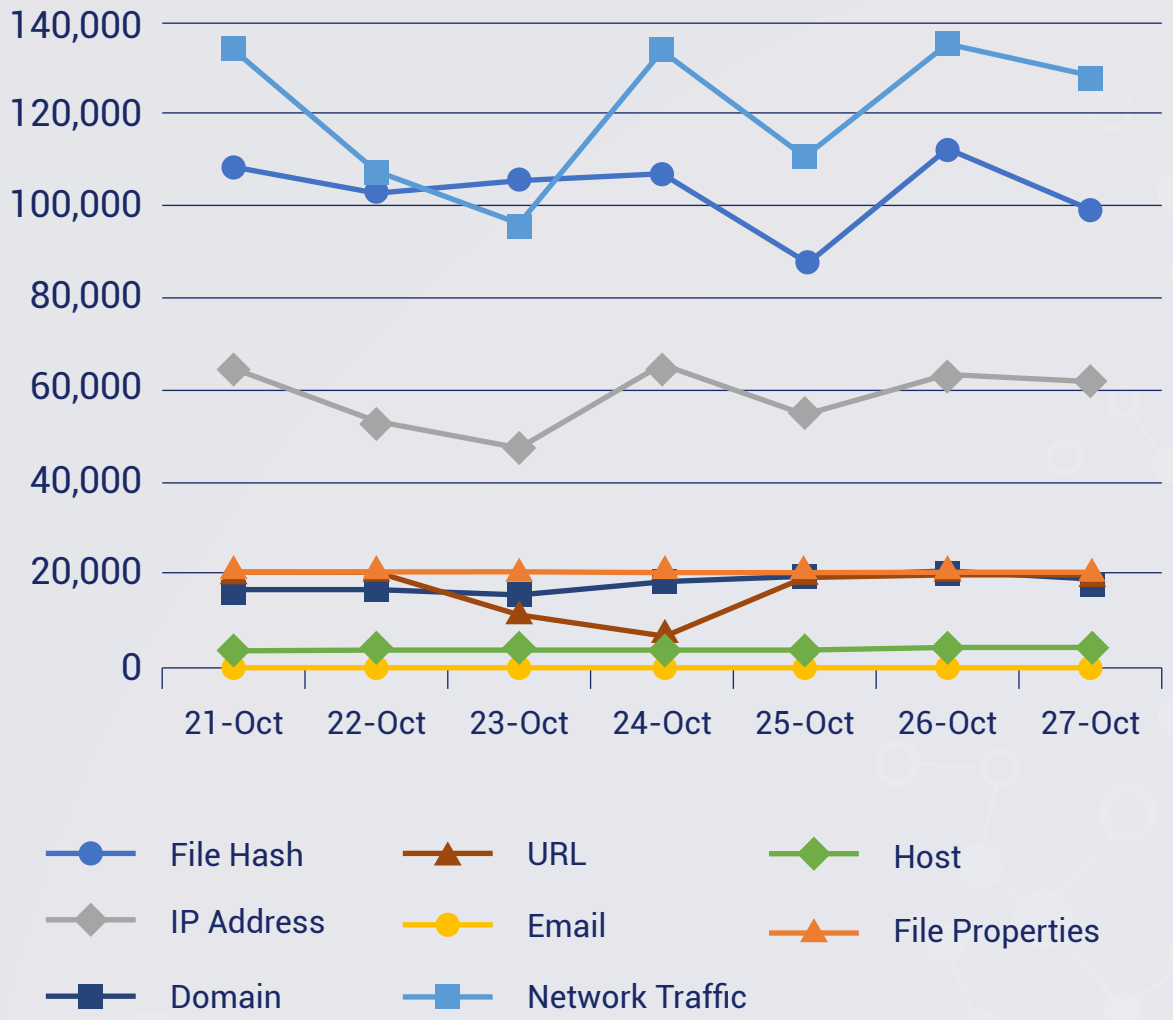
New Threat Protections (Week Ending 31/10/2022):

17

Overall Weekly Observables Count:

2,360,019

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. CVE-2022-40684

Fortinet recently patched a critical authentication bypass vulnerability (CVE-2022-40684) in their FortiOS, FortiProxy, and FortiSwitchManager projects. This vulnerability gives an attacker the ability to log in as an administrator on the affected system. Any HTTP requests to the management interface of the system that match the conditions above should be cause for concern. An attacker can use this vulnerability to do just about anything they want to the vulnerable system. This includes changing network configurations, adding new users, and initiating packet captures. Note that this is not the only way to exploit this vulnerability and there may be other sets of conditions that work. For instance, a modified version of this exploit uses the User-Agent “Node.js”. This exploit seems to follow a trend among recently discovered enterprise software vulnerabilities where HTTP headers are improperly validated or overly trusted. We have seen this in recent F5 and VMware vulnerabilities.

Affected Products:

FortiOS version 7.2.0 through 7.2.1
FortiOS version 7.0.0 through 7.0.6
FortiProxy version 7.2.0
FortiProxy version 7.0.0 through 7.0.6
FortiSwitchManager version 7.2.0
FortiSwitchManager version 7.0.0

Threat Protected: 04
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 T1190 - Execution T1059

2. ROMCOM RAT (updated)

Researchers recently discovered a custom remote access Trojan/backdoor and named it ROMCOM RAT. It contains a unique command and control (C2) protocol. ROMCOM RAT can be executed using one of its two exports named ServiceMain and startWorker. Both exports lead to the execution of the same function. However, the difference is the string passed as a parameter ServiceMain passes the string _inet, while startWorker passes the string _file. Based on this string alone, the flow of execution within the sample is completely different, with ServiceMain causing the sample to beacon out to its C2 server, and startWorker resulting in the sample opening a backdoor on the system and waiting for connections.

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: Persistence T1574.002-Privilege Escalation T1055- Defense Evasion T1036/T1055/T1497-Discovery T1010/T1012/T1018/T1057/T1082/T1083/T1497 -Command and Control T1071/T1095/T1571

3. WarHawk Malware

Recently, researchers discovered a new malware used by the SideWinder APT threat group in campaigns targeting Pakistan: a backdoor called WarHawk. SideWinder APT, aka Rattlesnake or T-APT4, is a suspected Indian Threat Actor Group active since at least 2012, with a history of targeting government, military, and businesses throughout Asia, particularly Pakistan. The newly discovered WarHawk backdoor contains various malicious modules that deliver Cobalt Strike, incorporating new TTPs such as KernelCallBackTable Injection and Pakistan Standard Time zone check in order to ensure a victorious campaign. The WarHawk Backdoor consists of four modules:

- Download & Execute Module
- Command Execution Module
- File Manager InfoExfil Module
- UploadFromC2 Module

Threat Protected: 05
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- Activity
Kill Chain: Initial Access T1566/T1190-Execution T1204/T1059-Defense Evasion T1140/T1564/T1055-Command and Control T1071.001-Exfiltration T1041

4. Gamaredon APT

A Russia-linked threat group that is known to target users from Ukraine with malware that steals information. The main technique used is to phish users in the the context of current events (Russia-Ukraine conflict), scripts (Powershell, LNK files, VB) are zipped, and malicious software are deployed.

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: Initial Access T1566 - Execution T1059 - Command-and-Control T1102 - Exfiltration T1567

5. SocGholish

SocGholish is a framework for drive-by attacks. It has been active since 2018 linked to the cybercrime group Evil Corp. It is possible for an unsuspecting victim who visits a compromised website to execute a malicious Javascript code from the legitimate site. Since the sites are known to be legitimate, users often trust the objects seen on the site. An example is a company website that has been exploited through a WordPress vulnerability, malicious javascript code was embedded, and an employee visits the site and unknowingly executes the script on their machine.

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: Trojan-activity
Kill Chain: Initial Access T1189/T1566 - Execution T1059 - Command and Control T1071 - Exfiltration T1020