
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Oct 18 - 24, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Lumma Stealer, Snake Keylogger, Spyder Loader, Witchetty, Text4Shell CVE-2022-42889, and Polonium)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

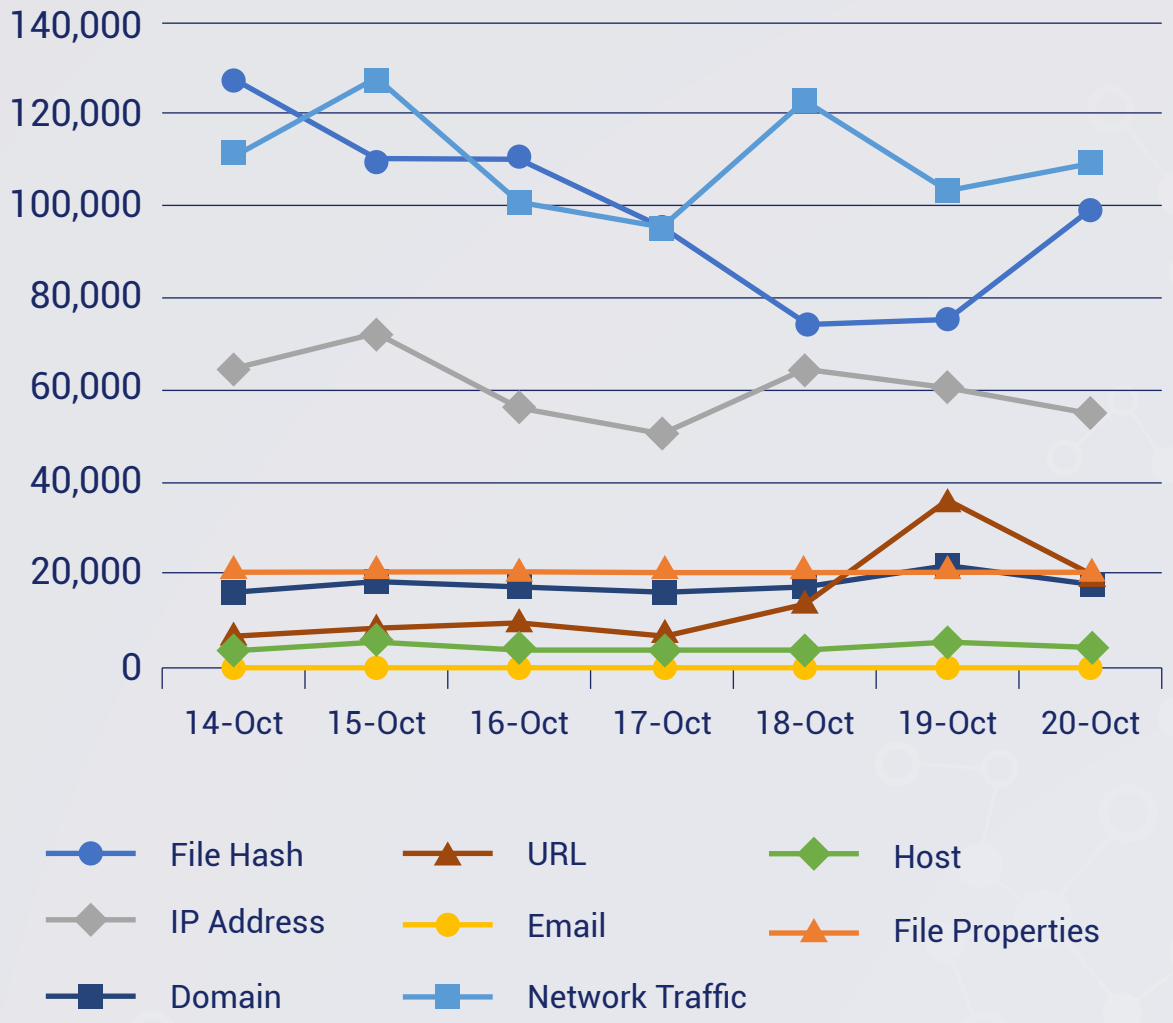
New Threat Protections (Week Ending 24/10/2022):

23

Overall Weekly Observables Count:

2,246,451

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Lumma Stealer

Lumma is a piece of malicious software categorized as a stealer. Malware within this category is designed to steal sensitive data. These programs are capable of exfiltrating data from infected systems and the applications installed onto them. Lumma's behaviour is like that of the Mars, Arkei, and Vidar stealers. Stealer-type malware can exfiltrate both device/system and personal data. The latter entails downloading various files (e.g., databases, images, documents, videos, etc.) from the compromised system. Typically, these malicious programs can extract information from browsers, which could include browsing and search engine data, autofill's, usernames/passwords, personally identifiable details, credit card numbers, and so forth. Stealers often target various accounts like emails, social media, social networking, messengers, gaming-related software, online banking, e-commerce, cryptocurrency wallets, FTPs, password managers, authentication software, VPNs, and many others.

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: Privilege Escalation T1055- Defense Evasion T1055/T1497- Discovery T1018/T1082/T1497/T1518.001- Collection T1056.004- Command-and-Control T1071/T1095

2. Snake Keylogger

A new variant of Snake Keylogger has been recognized by researchers recently. Snake Keylogger is a malware developed using .NET. It first appeared in late 2020 and focused on stealing sensitive information from a victim's device, including saved credentials, keystrokes, screenshots of the victim's screen, and clipboard data. In July 2021, Snake Keylogger first entered TOP 10 popular malware families report, meaning that the Snake Keylogger family is increasing its influence and impacting more people's devices and sensitive data.

Historically, Snake arrived in the form of a .docx or .xlsx attachment. The snake keylogger can take screenshots of the machine, collect system clipboard data, steal saved credentials in all internet browsers, and send an email to the attacker (using SMTP protocol) to submit the stolen credentials data of the victim.

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: Execution T1059/T1203/T1064/T1203- Persistence T1546.001- Privilege Escalation T1055- Defense Evasion T1497.003/T1564.003- Discovery T1016/T1082/T1083-Command-and Control T1071/T1095/T1105

3. Spyder Loader

The Spyder Loader malware is used for targeted attacks on information storage systems, collecting information about corrupted devices, executing mischievous payloads, coordinating script execution, and C&C server communication. The attackers exfiltrated hundreds of gigabytes of information, and they "targeted intellectual property developed by the victims, including sensitive documents, blueprints, diagrams, formulas, and manufacturing-related proprietary data." They also stole data for future cyber-attacks — such as credentials, customer data, and information about network architecture. This backdoor is written in C++ and designed to run on 64-bit Windows. This module is used for targeted attacks on information storage systems, collecting information about corrupted devices, executing mischievous payloads, coordinating script execution, and C&C server communication. The module is loaded by the MSDTC system service using a well-known DLL Hijacking method. The function names within the modules export table are related to the exported functions of the apphelp.dll system library.

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: Malware
Kill Chain: Execution TA0002 - Privilege Escalation TA0004 - Defense Evasion TA0005 - Discovery TA0007 - Discovery TA0007 - Command and Control TA0011

4. Witchetty

The Witchetty espionage group (aka LookingFrog) has been progressively updating its toolset, using new malware in attacks on targets in the Middle East and Africa. A new tool used by the group is a backdoor Trojan (Backdoor.Stegmap) that employs steganography, a rarely seen technique where malicious code is hidden within an image. While the group has continued to use the LookBack backdoor, several new pieces of malware appear to have been added to its toolset. One is Backdoor.Stegmap, which leverages steganography to extract its payload from a bitmap image. Although rarely used by attackers, if successfully executed, steganography can be leveraged to disguise malicious code in seemingly innocuous-looking image files.

A DLL loader downloads a bitmap file from a GitHub repository. The file appears to be simply an old Microsoft Windows logo. However, the payload is hidden within the file and is decrypted with an XOR key. Disguising the payload in this fashion allowed the attackers to host it on a free, trusted service. Downloads from trusted hosts such as GitHub are far less likely to raise red flags than downloads from an attacker-controlled command-and-control (C&C) server.

Threat Protected: 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: Privilege Escalation TA0004 - Defense Evasion TA0005 - Discovery TA0007

5. Text4Shell CVE-2022-42889

A new remote code execution Apache Commons Text vulnerability was discovered like Spring4Shell and Log4Shell. The issue lies on the StringSubstitutor interpolator class which is used for string lookups. The payload "${prefix:name}" is used to trigger the String Lookup in which "script", "DNS", and "URL" are the strings to be used as "prefix". Upon successful exploitation, an attacker is given access to the target with code execution in the context of the user account running the service. It is highly recommended to upgrade to the latest version of Apache Commons Text as versions 1.5 to 1.9 are affected.

Threat Protected: 08
Rule Set Type:

Class Type: attempted-admin
Kill Chain: Initial Access T1190

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

6. Text4Shell CVE-2022-42889

An APT group is known to conduct cyber-espionage operations against its target organizations in Israel. Recently, the group has been observed to use a malware family dubbed Creepy. The Creepy Malware family consists of different modules for different purposes such as: Keylogging, Remote Access, and Information gathering among many others.

Threat Protected: 08
Rule Set Type:

Class Type: Trojan-activity
Kill Chain: Execution T1059 - Persistence T1547/T1053 - Collection T1560/T1005 - Command-and-Control T1102/T1071 - Exfiltration T1041

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