
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Nov 15 - 21, 2022

Report Summary:

- **New Threat Detection Added** – 07 (IceXLoader v3.3.3, Laplas Clipper, Fodcha DDoS botnet V4.0, Typhon Reborn, RatMilad, Earth Longzhi, and Fangxiao)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

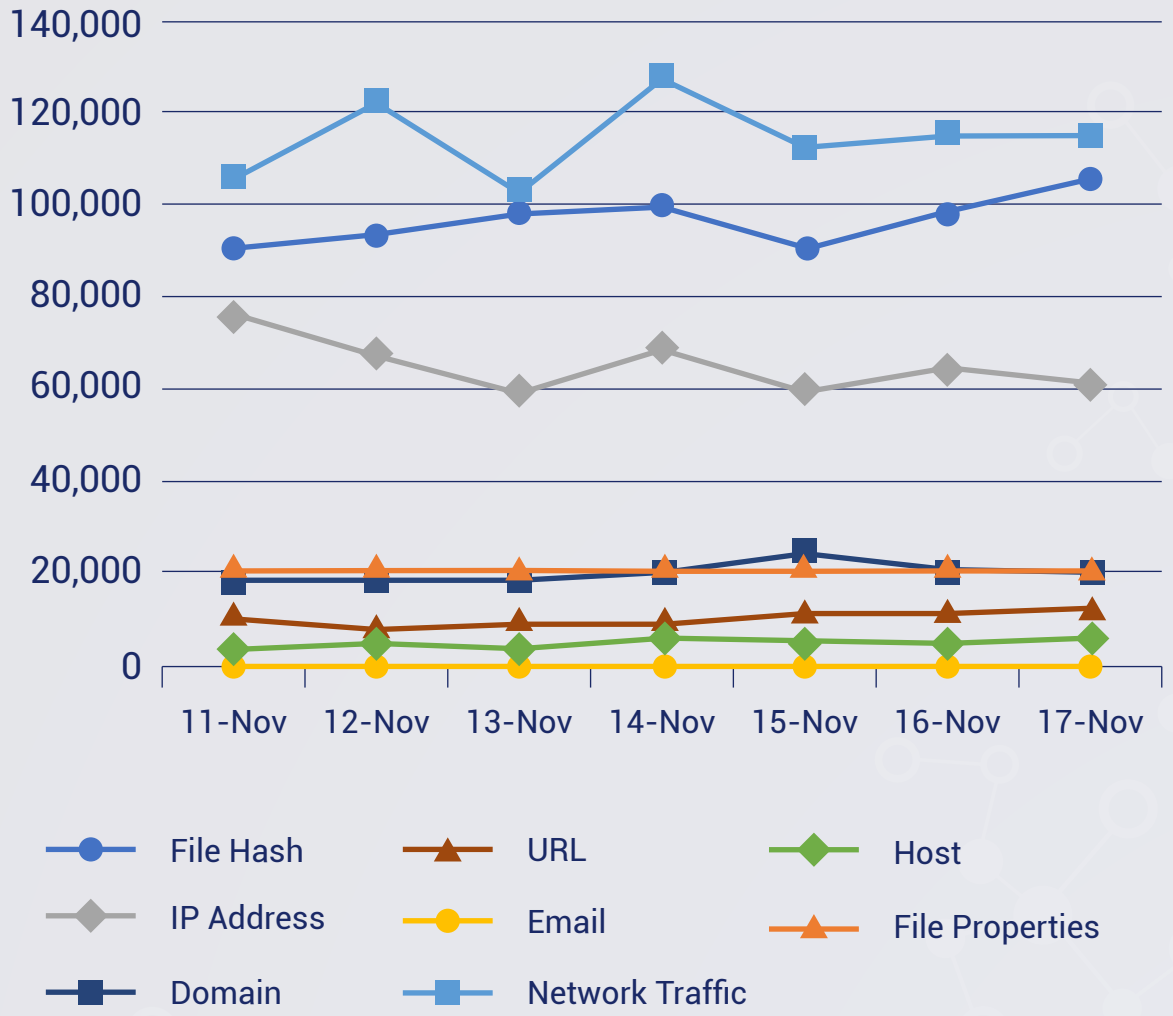
New Threat Protections (Week Ending 21/11/2022):

19

Overall Weekly Observables Count:

2,289,140

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. IceXLoader v3.3.3

Researchers recently detected a new version (Version 3.3.3) of famous Loader malware named IceXLoader. The IceXLoader Version 3.3.3 is written in the Nim language, compiled into C, C++, and JavaScript. IceXLoader can collect the following information about the victim and send it to the C&C server:

a. IP address
b. UUID
c. Username and machine name
d. Windows OS version
e. Installed security products
f. Presence of .NET Framework v2.0 and/or v4.0
g. Loader Version – in our case is v3.3.3
h. RAM information
i. CPU information
j. GPU information
k. Timestamp.

Threat Protected: 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 T1064- Persistence T1055/T1547.001- Privilege Escalation T1055 - Defense Evasion T1036/T1055/T1064/T1497 - Discovery T1010/T1012/T1018/T1057/T1082/T1083/T1497 - Command and Control T1071/T1095

2. Laplas Clipper

Laplas Clipper is a malicious application which targets user's cryptocurrency accounts. This malware seizes a cryptocurrency transaction by exchanging a victim's wallet address with the wallet address owned by Threat Actors (TAs). When a user tries to make a payment from their cryptocurrency account, it redirects the transaction to TAs account instead of their original recipient. Malware performs this swap by monitoring the clipboard of the victim's system, where copied data is stored. Whenever the user copies data, the clipper verifies if the clipboard data contains any cryptocurrency wallet addresses. The malware replaces it with the TAs wallet address, resulting in the victim's financial loss.

Threat Protected: 04
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 T1204/T1203- Persistence T1053- Privilege Escalation T1055/T1574 - Defense Evasion T1027/T1562/T1497/T1036/T1070/T1564- Discovery T1057/T1082/T1518- Command and Control T1071/T1105/T1571

3. Fodcha DDoS botnet V4.0

A new version of the Fodcha DDoS botnet has been detected by the researcher recently which is a highly sophisticated malware capable of ransom demands injected into packets and features to evade detection measures. The Fodcha DDoS botnet was detected by 360Netlab researchers back in April 2022. According to a new report published by the researchers, the latest Fodcha version 4 has grown to an unprecedented scale, with its developers taking measures to prevent analysis after Netlab's last report. The most notable improvement in this botnet version is the delivery of ransom demands directly within DDoS packets used against victims' networks. In addition, the botnet now uses encryption to establish communication with the C2 server, making it harder for security researchers to analyse the malware and potentially take down its infrastructure.

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: Persistence T1543.002 -Defense Evasion T1070.004/T1222-Discovery T1082/T1083/T1518.001

4. Typhon Reborn

Typhon Reborn is the new and updated version of the Typhon Stealer. Both variants are mainly used to steal crypto wallets, and log keystrokes are used in both personal and banking applications. The updated variant Typhon Reborn, however, is now capable of anti-analysis. These techniques range from checking for a debugging environment, default or VM-related user account to checking the hard disk space.

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 T1566/T1189 - Execution T1059 - Collection T1119 - Command-and-Control T1102

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: Trojan-activity
Kill Chain: Initial Access T1456 - Execution T1623 - Collection T1119 - Command-and-Control T1102 - Exfiltration T1041

6. Earth Longzhi

Earth Longzhi campaigns used spear-phishing emails as the primary entry vector to deliver Earth Longhzhi's malware. The attacker embeds the malware in a password-protected archive or shares a link to download malware, luring the victim with information about a person. Upon opening the link, the victim is redirected to a Google Drive hosting a password-protected archive with a Cobalt Strike loader we call CroxLoader. In addition, many TTPs and code spreads throughout the threat landscape in various ways; leaks that are coopted by other actors and selling of tools as a service by threat groups or rogue developers.

Threat Protected: 06
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: Execution TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defense Evasion TA0005 - Defense Evasion TA0005 - Discovery TA0007 - Command and Control TA0011

7. Fangxiao

Fanxgiao uses various strategies to maintain anonymity: most of its infrastructure is protected behind CloudFlare, and domain names are changed regularly and quickly: on one day in October 2022 alone, the group used over 300 new unique domains.

Users arrive at a Fangxiao-controlled site through a link sent in a WhatsApp message, which in turn sends them to a landing domain impersonating a well-known, trusted brand: over 400 organisations are currently being imitated, with that number continuing to rise. Companies affected include Emirates, Singapore's Shopee, Unilever, Indonesia's Indomie, Coca-Cola, McDonald's and Knorr.

Victims are then redirected to the main survey domain. When they click the link, they are sent through a series of advertising sites to one of a set of constantly changing destinations. A click on the "Complete registration" button with an Android user agent will sometimes result in a download of the Triada malware. As victims are invested in the scam, keen to get their "reward", and the site tells them to download the app, this has likely resulted in a significant number of infections.

Threat Protected: 03
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: Command and Control TA0011/ T1071/ T1571/ T1573