
Red Piranha
unified threat management
THREAT INTELLIGENCE REPORT
Sept 27 - Oct 3, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Metador APT, GO#WEBBFUSCATOR Malware, LuckyMouse RShell, Ginp Malware, SocGholish and Erbium Stealer)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**

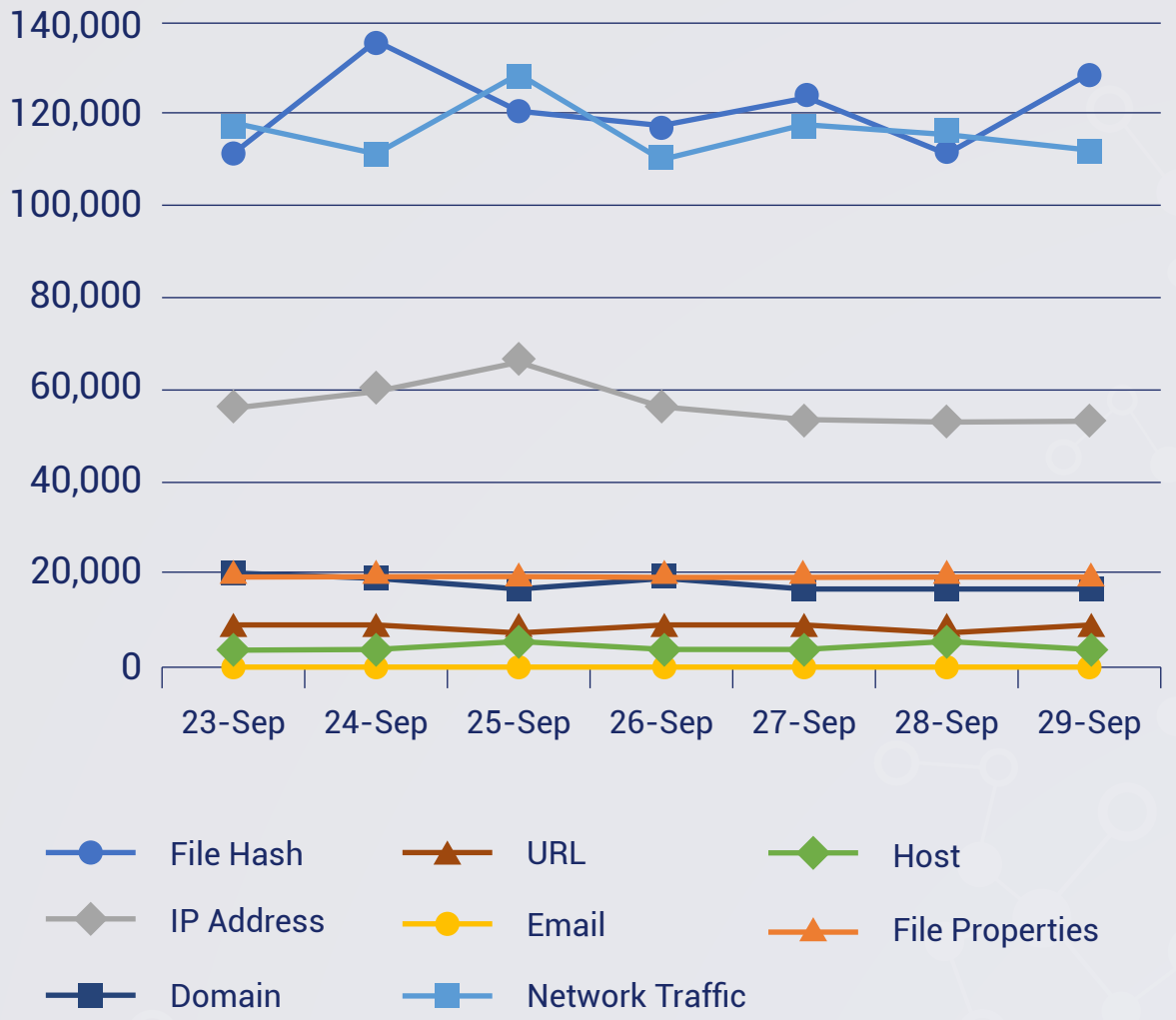
IDPS Rules Created (Week Ending 03/10/2022):

14

Overall Weekly Observables Count:

2,373,547

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Metador APT

Researchers have recently discovered a never-before-seen advanced threat actor dubbed as Metador. It primarily targets telecommunications, internet service providers, and universities in several countries in the Middle East and Africa. The operators are highly aware of operations security, managing carefully segmented infrastructure per victim and quickly deploying complex countermeasures in the presence of security solutions. Despite their care for OPSEC, Metador operators do not prioritize deconfliction and regularly cohabitate with other known APTs while remaining undiscovered. Metador's attack chains are designed to bypass native security solutions while deploying malware platforms directly into memory. Researchers discovered variants of two long-standing Windows malware platforms, and indications of an additional Linux implantation. Traces point to multiple developers and operators that speak both English and Spanish, alongside varied cultural references including British pop punk lyrics and Argentinian political cartoons. While Metador appears primarily focused on enabling collection operations aligned with state interests, the possibility of a high-end contractor arrangement not tied to a specific country.

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

2. GO#WEBBFUSCATOR Malware

Threat researchers have recently identified a unique sample of a persistent Golang-based attack campaign tracked by Securonix as GO#WEBBFUSCATOR. The new campaign incorporates an equally interesting strategy by leveraging the infamous deep field image taken from the James Webb telescope and obfuscated Golang programming language payloads to infect the target system with the malware.

Initial infection begins with a phishing email containing a Microsoft Office attachment (Geos-Rates.docx in our case). The document includes an external reference hidden inside the document's metadata which downloads a malicious template file. When the document is opened, the malicious template file is downloaded and saved on the system. Like that of a traditional Office macro, the template file contains a VB script that will initiate the first stage of code execution for this attack once the user enables macros. The deobfuscated code executes the command that downloads a file named OxB36F8GEEC634.jpg, use certutil.exe to decode it into a binary (msdllupdate.exe) and then finally, execute it. Upon execution, the malware makes unique DNS connections. By looking at the URL strings we can determine that the binary file was leveraging a DNS data exfiltration technique by sending unique DNS queries to a target C2 DNS server.

Overall, TTPs observed with GO#WEBBFUSCATOR during entire attack chain are interesting. Using a legitimate image to build a Golang binary with Certutil is not very common in our experience, and we are tracking closely. It's clear that the original author of the binary designed the payload with some trivial counter-forensics and anti-EDR detection methodologies in mind.

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: Trojan-Activity
Kill Chain: Initial access T1566.001 -Execution T1059.003 -Persistence T1547.001 -Defense evasion T1140 -Discovery T1420 -Command and control T1071.001 -Exfiltration T1041

3. LuckyMouse RShell

“MìMì” Messenger's MacOS version has been trojanized since May 26, 2022 to download and execute a Mach-O binary dubbed “rshell”. Infrastructure links were established between China-nexus Intrusion Set- LuckyMouse and this operation. The downloaded implant, named RShell by its developers, is written in C++ and embeds the Boost.Asio and nlohmann/json libraries. This backdoor uses BJSON (Binary JSON) over TCP sockets to communicate with its command-and-control server without any encryption and does not display a persistence mechanism. Upon execution, RShell backdoor attempts to connect with the C2 server. This “Hello message” sent to the C2 server contains:

- a random GUID added to each response to the C2 server
- the hostname
- the IPv4 addresses
- the type of connection (For instance; “login”)
- the current username
- the kernel version.

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: Malware
Kill Chain: Discovery TA0007/T1082 - Command and Control TA0011/T1071/T1095/ T1573

4. Ginp Malware

The Ginp mobile banking malware emerged in late 2019, and is one of the most prevalent Android banking malware families today. It started as an SMS stealer and rapidly evolved into one of the most advanced actors in the financial fraud landscape. Ginp has primarily targeted Spanish banks, but recent evidence suggests the malware has changed or may change its targeting strategy soon to focus on Turkey. New Ginp overlay pages are intended for overlay attacks on mobile devices residing on the malware's command-and-control (C&C) servers. These overlay pages are spoofs of legitimate banking pages meant to deceive mobile device users into sharing confidential banking and other information. Several such fake overlays mimic banks in Turkey, suggesting that malware operators intend to use these pages in future campaigns to target customers of Turkish banks.

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: Command and Control TA0011- Defense Evasion TA0030 - Credential Access TA0031- Discovery TA0032 - Impact TA0034 - Collection TA0035 - Network Effects TA0038

5. SocGholish

SocGholish is a framework for drive-by attacks. It has been active since 2018 and 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 legit, users often trust the objects seen on the site. For example, 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.

Rules Created: 05
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

6. Erbium Stealer

Erbium Stealer is a malware designed to capture data from infected devices. It obtains data from various applications installed on a computer, extracts session cookies, passwords, and browser history on browsers. It also targets desktop-installed or browser extension-based cryptocurrency wallets. Other applications that utilise authentication such as password managers, FTP clients, Gaming and Messaging software are also affected. The Erbium Stealer has been recently listed in malware-selling marketplaces.

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 - T1189/T1566 - Execution T1204/T1059 - Persistence T1547 - Collection T1119/T1005 - Command and Control T1102 - Exfiltration T1567