Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 09 - 15, 2022

Report Summary:

- **New Threat Detection Added** – 6 (Woody RAT, CHIMNEYSWEEP Backdoor, RapperBot, Erbium Stealer, CosmicStrand Rootkit and XLoader)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **Total Counts by Observable Type**

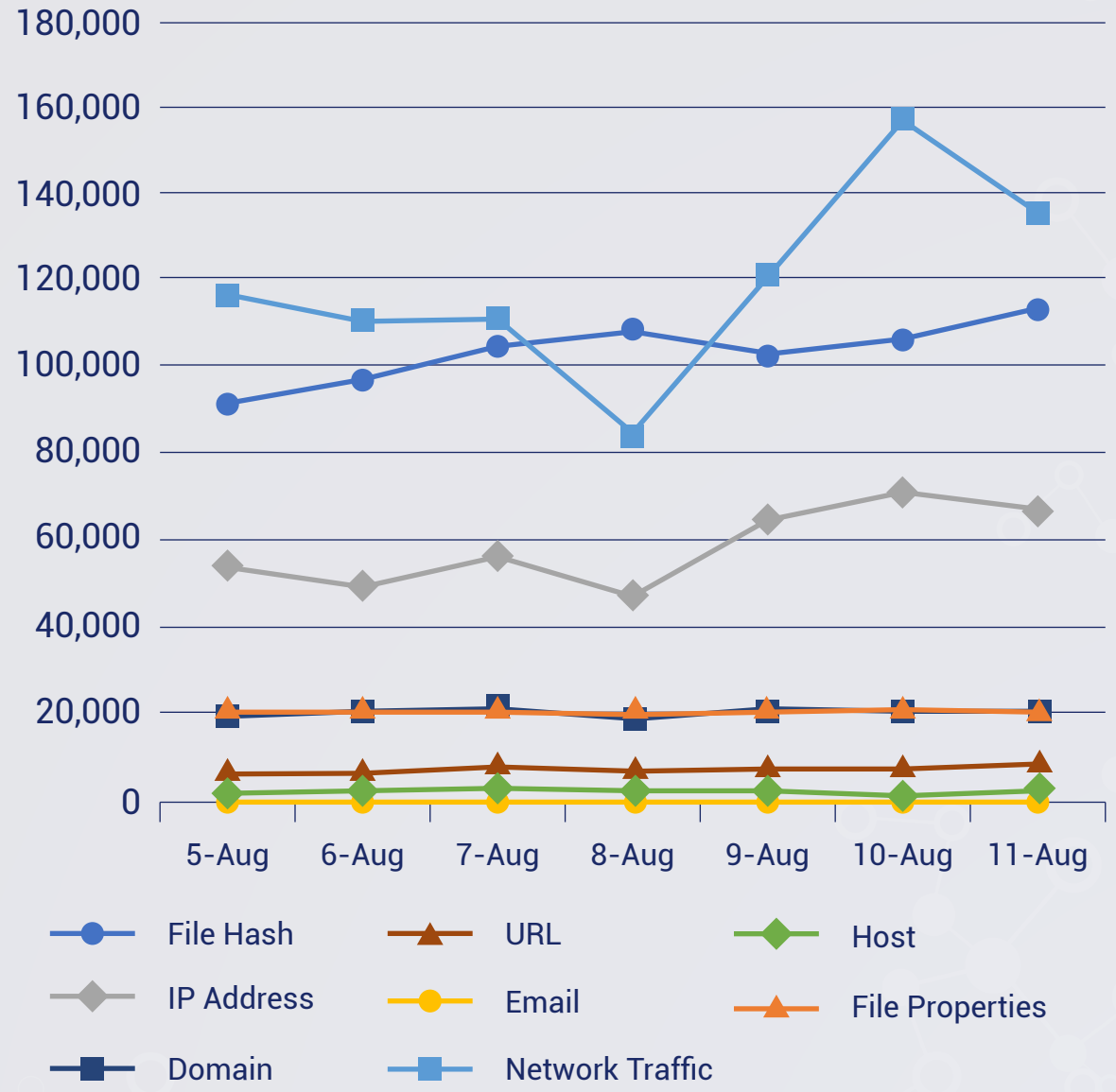
IDPS Rules Created (Week Ending 15/08/2022):

27

Overall Weekly Observables Count:

2,321,355

Daily Submissions by Observable Type:



Newly Detected Threats Added

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

1. Woody RAT

A new Remote Access Trojan (RAT) dubbed as Woody Rat has identified by Malwarebytes Threat Intelligence team. This advanced custom RAT is mainly the work of a threat actor that targets Russian entities by using lures in archive file format and more recently Office documents leveraging the Follina (CVE-2022-30190) vulnerability. A fake domain registered by the threat actors, we know that they tried to target a Russian aerospace and defence entity known as OAK. Based on our knowledge, Woody Rat has been distributed using two different formats: archive files and Office documents using the Follina vulnerability. The earliest versions of this RAT were typically archived into a zip file pretending to be a document specific to a Russian group. When the Follina (CVE-2022-30190) vulnerability became known to the world, the threat actor switched to it to distribute the payload.

Rules Created: 08
Rule Set Type: Balanced
Class Type: Trojan Activity
Kill Chain: Initial Access T1566- Execution T1204- Collection T1185/T1213- Command and Control T1071/T1219 -Exfiltration T1020 -Impact T1531

2. CHIMNEYSWEEP Backdoor

In July 2022, Mandiant identified a new ransomware family dubbed as ROADSWEEP which drops a politically themed ransom note suggesting it targeted the Albanian government. In addition, a front named “HomeLand Justice” claimed credit for the disruptive activity that affected Albanian government websites and citizen services. The “HomeLand Justice” front posted a video of the ransomware being executed on its website and Telegram channel alongside alleged Albanian government documents and residence permits of ostensible members of the Mujahedeen-e-Khalq/People's Mojahedin Organization of Iran (MEK, also known as MKO or PMOI), an Iranian opposition organization that was formerly designated as a terrorist group by the U.S. Department of State.

Mandiant further identified CHIMNEYSWEEP, a backdoor that uses either Telegram or actor-owned infrastructure for command-and-control and can take screenshots, listing and collecting files, spawning a reverse shell, and supports keylogging functionality. CHIMNEYSWEEP shares code with ROADSWEEP and based on observed decoy content has likely been used to target Farsi and Arabic speakers as far back as 2012.CHIMNEYSWEEP and ROADSWEEP share multiple code overlaps, including identical dynamic API resolution code.

Rules Created: 10 | **Rule Set Type**: Balanced
Class Type: Trojan Activity
Kill Chain: System Service Discovery T1007-Query Registry T1012-Obfuscated Files or InformationT1027-System Owner/User Discovery T1033-Process Injection T1055-Process Discovery T1057-File Deletion T1070.004-Timestomp T1070.006-System Information Discovery T1082-File and Directory Discovery T1083-Account Discovery T1087-Modify Registry T1112-Screen Capture T1113-Access Token Manipulation T1134-Service Stop T1489-System Checks T1497.001-Software Discovery T1518-Windows Service T1543.003-Service Execution T1569.002-Debugger Evasion T1622

3. RapperBot

RapperBot exclusively scans and attempts to brute force SSH servers configured to accept password authentication. The bulk of the malware code contains an implementation of an SSH 2.0 client that can connect and brute force any SSH server that supports Diffie-Hellmann key exchange with 768-bit or 2048-bit keys and data encryption using AES128-CTR.

A distinctive feature of the brute forcing implementation in RapperBot is the use of "SSH-2.0-HELLOWORLD" to identify itself to the target SSH server during the SSH Protocol Exchange phase. The appearance of this RapperBot in mid-June coincides with the observation of this same client identification string by SANS Internet Storm Center in their honeypot logs.

Earlier samples had the brute-forcing credential list hardcoded into the binary. From July onwards, samples now retrieve this list from another port on the C2 server. This allows the threat actors to continually add new SSH credentials without having to update infected devices with new samples. This port number ranges from 4343 to 4345 in the latest samples.

Once RapperBot successfully brute forces an SSH server, the valid credentials are reported to the C2 server on a separate port (currently 48109) without executing further commands on the remote victim.

Rules Created: 02
Rule Set Type: Balanced
Class Type: Malware
Kill Chain: T1110 - Brute Force, T1078 - Valid Accounts

4. Erbium Stealer

Erbium Stealer is a malware that is designed to capture data from infected devices.

It obtains data from various applications installed on a computer. It extracts session cookies, passwords, 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 discovered by being recently listed in malware selling marketplaces.

The Crystal Eye has rules that have been deployed to detect and reject the activities related to this threat from initial potential download through to a malware checking to its identified Command-and-Control Server.

Rules Created: 04
Rule Set Type: Security – IDS: Alert – IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access - T1189/T1566 - Execution T1204/T1059 - Persistence T1547 - Collection T1119/T1005 - Command and Control T1102 - Exfiltration T1567

5. CosmicStrand Rootkit

CosmicStrand is a UEFI firmware rootkit that has been attributed to a Chinese malware author. It was discovered in ASUS and Gigabyte motherboards. This sophisticated type of malware is designed to be stealthy and well-hidden. Its main characteristic is to load itself before the actual Operating System. It passes down its malicious code through the boot process through to Windows start-up. To avoid detection, it checks for internet connectivity 10 minutes after it was loaded without the use of native Windows kernel API functions. It contacts its Command-and-Control server to download its payload. The known observed payload creates a user named "aaaabbbb" and is added to the local administrators group. Due to the nature and the privileged access of this malware, it is likely that its functions are not limited to just creating a user account.

Currently, there are two known Command-and-Control domains for this CosmicStrand rootkit. Rules are set to alert and reject traffic going to these domains to prevent the potential download of its payload

Rules Created: 02
Rule Set Type: Security – IDS: Alert – IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access T1195.003 - Persistence T154 - Command and Control T1095

6. XLoader

Threat analysts have spotted a new version of the XLoader botnet malware that uses probability theory to hide its command-and-control servers, making it difficult to disrupt the malware's operation.

This helps the malware operators continue using the same infrastructure without the risk of losing nodes due to blocks on identified IP addresses while also reducing the chances of being tracked and identified.

XLoader is an information-stealer that was originally based on Formbook, targeting Windows and macOS operating systems. It first entered widespread deployment in January 2021.

Recently, a new version of XLoader malware in-the-wild was spotted. The main update in XLoader v2.6 concerns the network communication. The random index of the real C&C server is now saved in the malware state structure. During each communication cycle, when the malware overwrites the first 8 entries in the list of accessed domains, it keeps the values for the real and the fake C&C domains. Therefore, the real C&C server is now accessed in every communication cycle, or once in approximately 80-90 seconds. However, this logic is activated only when the malware runs in an x64 system. When it runs in an x86 system, the variable real_c2_index stores the same value as is stored in the fake_c2_index. This results in the real C&C server being accessed with the same probability as any of the 63 decoys while running in x86 system.

Rules Created: 01
Rule Set Type: Balanced
Class Type: Malware
Kill Chain: Defence Evasion T1480 Command and Control T1001

Total Counts by Observable Type:

The table below shows the total counts of observables we've been collecting for the last four months, the last four weeks, and the total since February 2017.

	Date	File Hash	IP Address	Domain	URL	Email	Network Traffic	Host	File Properties	Total
Month	May 2022	4,029,272	1,798,537	476,808	448,583	168	3,194,022	179,741	590,291	10,717,422
	Jun 2022	4,798,835	2,138,981	548,365	473,164	735	3,645,625	115,609	585,476	12,306,790
	Jul 2022	3,605,153	1,669,888	536,802	237,964	17	3,386,557	78,888	610,772	10,126,041
	Aug 2022	1,179,645	618,378	219,713	99,610	3	1,295,777	40,273	201,715	3,655,114
Week	7/15-7/21	817,762	312,021	117,953	46,922	0	576,167	11,451	137,726	2,020,002
	7/22-7/28	779,941	399,137	126,425	48,629	3	858,242	18,893	138,614	2,369,884
	7/29-8/5	775,710	418,154	134,559	60,051	3	896,342	22,551	122,934	2,430,304
	8/5-8/11	716,626	406,283	137,372	64,791	0	830,271	27,775	138,237	2,321,355
Total	Since Feb 2017	156,293,462	37,649,611	20,491,894	15,954,124	198,907	31,823,320	2,872,817	3,627,035	268,911,170