

Date of Publication
June 26, 2023



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

19 to 25 JUNE 2023

Table Of Contents

<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	15
<u>Adversaries in Action</u>	24
<u>Recommendations</u>	27
<u>Threat Advisories</u>	28
<u>Appendix</u>	29
<u>What Next?</u>	32

Summary

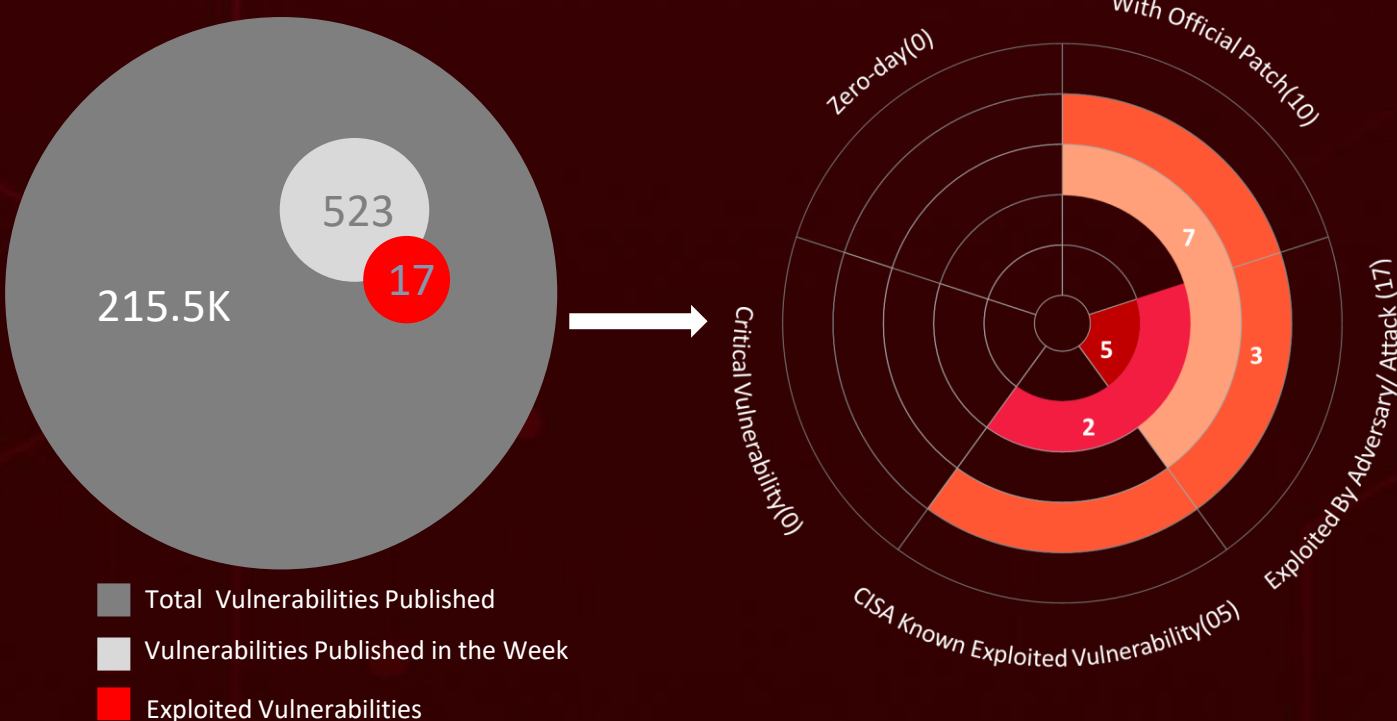
HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **twelve** attacks executed, taking advantage of **seventeen** different vulnerabilities in various systems, and involving **four** different adversaries highlights the ever-present danger of cyberattacks.

Interestingly, out of seventeen vulnerabilities five are part of the known exploited vulnerability catalog by CISA.

Moreover, HiveForce Labs also found that **Flea APT** threat group was exploiting a three-year-old Microsoft Netlogon vulnerability (**CVE-2020-1472**).

Furthermore, a new info stealer called **FadeStealer** has been identified, which has various features of information theft capabilities.

In addition to these threats, there is also a Romanian threat group "**Diicot**" which has been actively employing SSH brute-forcing and deploying malware loaders to compromise systems for the purpose of cryptocurrency mining. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

12

Attacks
Executed

17

Vulnerabilities
Exploited

4

Adversaries in
Action

- [Mystic Stealer](#)
- [XMRig](#)
- [Cayosin](#)
- [Shampoo](#)
- [Condi](#)
- [Tsunami](#)
- [Mirai](#)
- [Shellbot](#)
- [FadeStealer](#)
- [CHM malware](#)
- [AblyGo](#)
- [backdoor](#)
- [Backdoor.Graphical](#)

- [CVE-2023-1389](#)
- [CVE-2020-1472](#)
- [CVE-2019-17621](#)
- [CVE-2019-12725](#)
- [CVE-2019-20500](#)
- [CVE-2021-25296](#)
- [CVE-2021-46422](#)
- [CVE-2022-27002](#)
- [CVE-2022-29303](#)
- [CVE-2022-30023](#)
- [CVE-2022-30525](#)
- [CVE-2022-31499](#)
- [CVE-2022-37061](#)
- [CVE-2022-40005](#)
- [CVE-2022-45699](#)
- [CVE-2023-25280](#)
- [CVE-2023-27240](#)

- [STORM-1359](#)
- [Diicot](#)
- [Flea](#)
- [Red Eyes](#)



Insights

Mystic Stealer Targeting Healthcare, Cryptocurrency, Finance, and Technology

ChromeLoader Shampoo

In this campaign where users unknowingly download and execute VBScript files from malicious websites.

Mirai botnet is actively exploiting vulnerabilities in various devices.

Tsunami(aka Kaiten)

Botnet hacking campaign targets Linux SSH servers for DDoS botnets and other malware.

Condi

Malware exploits TP-Link Archer Wi-Fi routers for DDoS botnet.

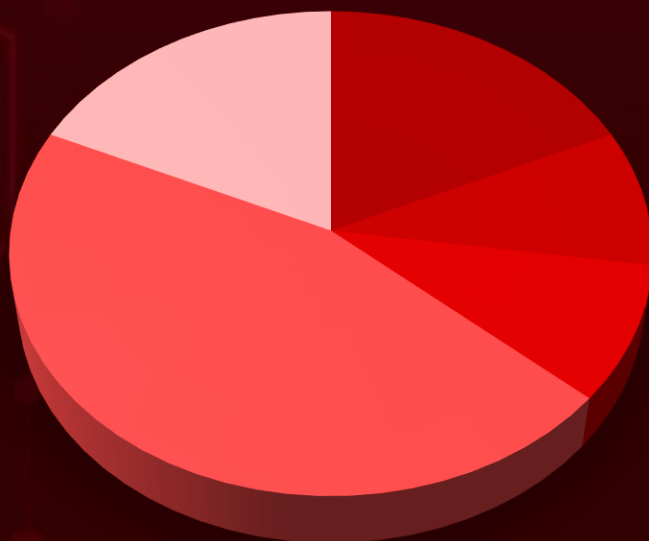
Flea APT Group

Targeted foreign ministries with their new backdoor, Backdoor.Graphican

STORM-1359

Threat Group Targeting Technology Companies, Government, Aviation Industries

Threat Distribution



■ InfoStealer ■ Miner ■ Browser extension ■ Botnet ■ Backdoor

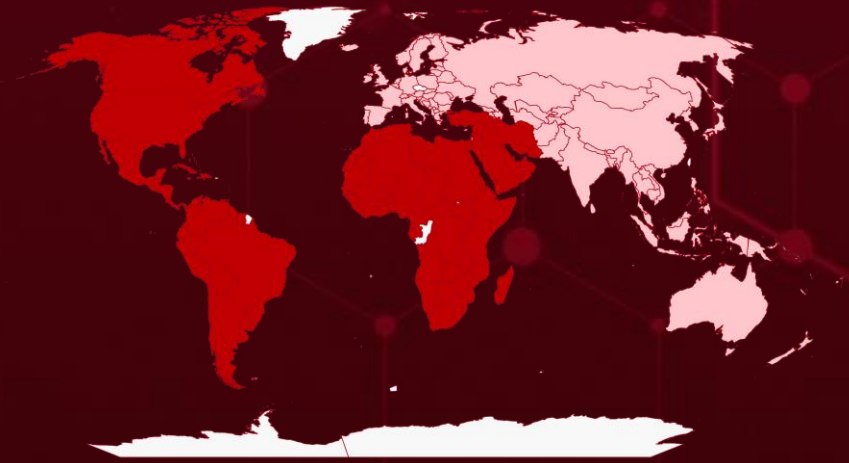


Targeted Countries

Most



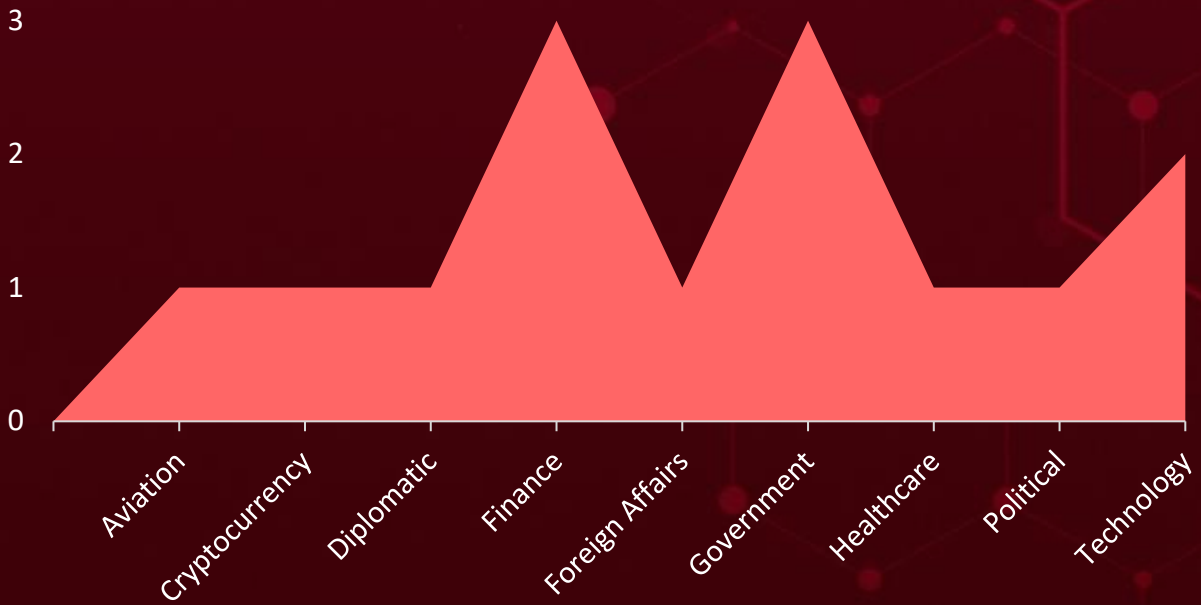
Least



© Australian Bureau of Statistics, GeoNames, Microsoft, NavInfo, OpenStreetMap contributors, Power by Bing

Countries	Countries	Countries	Countries	Countries
Mexico	Mauritania	Madagascar	Guatemala	Solomon Islands
United States	Burundi	Dominica	Tanzania	Afghanistan
Senegal	Mozambique	Mali	Guinea	State of Palestine
Algeria	Cabo Verde	Dominican Republic	Trinidad and Tobago	Liechtenstein
Lebanon	Nigeria	Mauritius	Guinea-Bissau	Timor-Leste
Angola	Cameroon	DR Congo	Turkey	Lithuania
Panama	Peru	Morocco	Guyana	Ireland
Antigua and Barbuda	Canada	Ecuador	United Arab Emirates	Luxembourg
Syria	Sao Tome & Principe	Namibia	Haiti	Vietnam
Argentina	Central African Republic	Egypt	Uruguay	Andorra
Jamaica	Sierra Leone	Niger	Honduras	Saint Kitts & Nevis
Bahamas	Chad	El Salvador	Yemen	Bangladesh
Malawi	Sudan	Oman	Iran	China
Bahrain	Chile	Equatorial Guinea	Zimbabwe	Malaysia
Nicaragua	Togo	Paraguay	Iraq	Slovakia
Barbados	Colombia	Eritrea	Libya	Maldives
Rwanda	Uganda	Qatar	Austria	Bosnia and Herzegovina
Belize	Comoros	Eswatini	Russia	Cambodia
South Africa	Venezuela	Saint Lucia	Croatia	Sri Lanka
Benin	Congo	Ethiopia	Kyrgyzstan	Malta
Tunisia	Israel	Saudi Arabia	Bhutan	Sweden
Bolivia	Costa Rica	Gabon	Laos	Marshall Islands
Zambia	Jordan	Seychelles	Hungary	Iceland
Botswana	Côte d'Ivoire	Gambia	Latvia	Albania
Kenya	Kuwait	Somalia	Cyprus	Tonga
Brazil	Cuba	Ghana	Brunei	Belarus
Liberia	Lesotho	South Sudan	Samoa	Turkmenistan
Burkina Faso	Djibouti	Grenada	Bulgaria	Estonia
		Suriname	Guatemala	Solomon Islands

Targeted Industries



TOP MITRE ATT&CK TTPS

T1498

Network Denial of Service

T1560

Gather Victim Network Information

T1071

Application Layer Protocol

T1027

Obfuscated Files or Information

T1190

Exploit Public-Facing Application

T1059

Command and Scripting Interpreter

T1095

Non-Application Layer Protocol

T1212

Exploitation for Credential Access

T1552

Unsecured Credentials

T1525

Implant Internal Image

T1036

Masquerading

T1055

Process Injection

T1021

Remote Services

T1057

Process Discovery

T1564

Hide Artifacts

T1078

Valid Accounts

T1083

File and Directory Discovery

T1068

Exploitation for Privilege Escalation

T1505

Server Software Component

T1518

Software Discovery

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mystic Stealer	Mystic Stealer is an advanced information stealer malware known for its low detection rate, code manipulation techniques and is stealing sensitive data from browsers, wallets & messaging platforms, posing significant risks to individuals and organizations.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
InfoStealer		Data theft, Financial loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	7c185697d3d3a544ca0cef987c27e46b20997c7ef69959c720a8d2e8a03cd5dc5c0987d0ee43f2d149a38fc7320d9ffd02542b2b71ac6b5ea5975f907f9b9bf88592e7e7b89cac6bf4fd675f10cc9ba319abd4aa6eaa00fb0b1c42fb645d341045d29afc212f2d0be4e198759c3c152bb8d0730ba20d46764a08503eab0b454fce56e45ad63065bf16bf736dccb452c48327803b434e20d58a6fed04f1ce2da9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XMRig	XMRig is a prevalent form of malware often employed by botnets to mine cryptocurrencies such as Monero. It discreetly exploits infected systems' computing power, enabling unauthorized mining activities.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Miner		Financial loss	-
ASSOCIATED ACTOR			PATCH LINK
Diicot (aka Mexals)			-
IOC TYPE	VALUE		
MD5	0014403121eeaebaeede796e4b6e5dbe125951260a0cb473ce9b7acc406e83e1		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Cayosin</u>	Cayosin is a Mirai-based botnet agent utilized by the threat group Diicot for DDoS attacks, primarily targeting routers running OpenWrt. Its deployment showcases Diicot's expanding attack capabilities beyond cryptojacking campaigns.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet			
ASSOCIATED ACTOR			
Diicot (aka Mexals)			
IOC TYPE	VALUE		
-	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Shampoo</u>	Shampoo malware is a variant of ChromeLoader targeting Google Chrome browsers, installing a malicious extension to collect personal information and manipulate browsing activities. It employs persistence mechanisms and encryption to evade detection, aiming to generate revenue through aggressive advertising.	Malicious VBScript files from malicious websites	-
TYPE		IMPACT	AFFECTED PRODUCTS
Browser extension			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
-	-		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>Condi</u>	Condi, a recently discovered malware, utilizes a security vulnerability within TP-Link Archer Wi-Fi routers to ensnare these devices into a botnet specifically designed for launching distributed denial-of-service (DDoS) attacks.	Unknown	CVE-2023-1389	
TYPE		IMPACT	AFFECTED PRODUCTS	
Botnet				TP-Link Archer AX21 versions before 1.1.4 Build 20230219
ASSOCIATED ACTOR				PATCH LINK
-		https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware		
IOCTYPE	VALUE			
SHA256	091d1aca4fcd399102610265a57f5a6016f06b1947f86382a2bf2a668912554f291e6383284d38f958fb90d56780536b03bcc321f1177713d3834495f64a3144449ad6e25b703b85fb0849a234cbb62770653e6518cf1584a94a52cca31b11904e3fa5fa2dcc6328c71fed84c9d18dfdbd34f8688c6bee1526fd22ee1d749e5a			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>Tsunami</u>	Tsunami botnet is a powerful DDoS botnet known for its open-source nature and widespread usage by threat actors, causing significant disruptions on the internet.	Exploit kits	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
Botnet				-
ASSOCIATED ACTOR				PATCH LINK
-		-		
IOCTYPE	VALUE			
MD5	822b6f619e642cc76881ae90fb1f8e8e			
C2	ircx.us[.]to:53 ircxx.us[.]to:53			

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Mirai</u>	<p>Mirai is a notorious botnet malware that targets vulnerable Internet of Things (IoT) devices, turning them into a network of compromised devices used for launching massive DDoS attacks</p>	Exploiting vulnerabilities	CVE-2019-12725 CVE-2019-17621 CVE-2019-20500 CVE-2021-25296 CVE-2021-46422 CVE-2022-27002 CVE-2022-29303 CVE-2022-30023 CVE-2022-30525 CVE-2022-31499 CVE-2022-37061 CVE-2022-40005 CVE-2022-45699 CVE-2023-1389 CVE-2023-25280 CVE-2023-27240
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		Internet-of-Things (IoT) disruption	Zeroshell; D-Link DIR-859 Wi-Firouter; D-Link DWL-2600AP; TelesquareSDT-CW3B11.1.0; Arris TR3300v1.0.13; SolarViewCompact; Tenda ONTGPON AC1200Dual bandWiFi HG9v1.0.1; Zyxel MultipleFirewalls; Nortek LineareMerge E3-Series devicesbefore 0.32-08f; All FLIR AX8
ASSOCIATED ACTOR			
Diicot (aka Mexals)			

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	PATCH LINK
<u>Mirai</u>	https://www.zeroshell.org/download/ ; https://www.dlink.com/en/security-bulletin ;
	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113 ; https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls ; https://na.niceforyou.com/solutions/access-control/ ;
TYPE	https://www.flir.com/products/ax8-automation/ ;
Botnet	https://seclists.org/fulldisclosure/2022/Dec/13 ;
Diicot (aka Mexals)	https://github.com/0xst4n/APSystems-ECU-R-RCE-Timezone ;
	https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware ;
	https://www.fortiguard.com/encyclopedia/ips/52742 ;
	https://github.com/migraine-sudo/D_Link_Vuln/tree/main/cmd%20Inject%20in%20pingV4Msg ;
IOC TYPE	VALUE
SHA256	b43a8a56c10ba17ddd6fa9a8ce10ab264c6495b82a38620e9d54d66ec8677b0c b45142a2d59d16991a38ea0a112078a6ce42c9e2ee28a74fb2ce7e1edf15dce3 366ddbbaa36791cdb99cf7104b0914a258f0c373a94f6cf869f946c7799d5e2c6 413e977ae7d359e2ea7fe32db73fa007ee97ee1e9e3c3f0b4163b100b3ec87c2 2d0c8ab6c71743af8667c7318a6d8e16c144ace8df59a681a0a7d48affc05599

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Shellbot</u>	Shellbot is a sophisticated botnet that hijacks Linux servers by exploiting vulnerabilities and installs malicious code to carry out DDoS attacks, spread malware, and engage in cryptocurrency mining	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet			-
ASSOCIATED ACTOR		Disruption	PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	c5142b41947f5d1853785020d9350de4 2cd8157ba0171ca5d8b50499f4440d96		
URLs	Hxxp://ddoser[.]org/siwen/bot / Hxxp://ddoser[.]org/logo		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>FadeStealer</u>	FadeStealer features various information theft capabilities, including screenshot capturing, keylogging, microphone wiretapping, and exfiltration from removable media devices and smartphones.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
InfoStealer			
ASSOCIATED ACTOR		Privacy intrusion	PATCH LINK
Red Eyes			
IOC TYPE	VALUE		
MD5	f44bf949abead4af0966436168610bcc		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>CHM malware</u>	CHM malware disguises itself as legitimate files, exploiting users' trust to execute malicious scripts and gain unauthorized access to systems.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
-			
ASSOCIATED ACTOR		Compromised systems, Data breaches	PATCH LINK
Red Eyes			
IOC TYPE	VALUE		
MD5	1352abf9de97a0faf8645547211c3be7		




The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>AblyGo backdoor</u>	AblyGo backdoor is a malicious tool that utilizes the Ably platform to enable real-time command and control communication with infected systems, allowing threat actors to issue commands and receive results stealthily.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR			
Red Eyes			
IOC TYPE	VALUE		
MD5	3277e0232ed6715f2bae526686232e06 3c475d80f5f6272234da821cc418a6f7		
URLs	hxxp://172.93.181[.]249/file/		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Backdoor.Graphical</u>	Backdoor.Graphican is a new backdoor used by the Flea APT group, leveraging the Microsoft Graph API and OneDrive for C&C communication in their recent attack campaign targeting foreign ministries in the Americas.	Unknown	CVE-2020-1472
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR			
Flea APT group		Microsoft Netlogon https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472	
IOC TYPE	VALUE		
SHA256	4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa802e8ea9a58c13f216bdae478f9f007e20b45217742d0f4e47f66173f1b195ef5617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253		




The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.




Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-1389		TP-Link Archer AX21 versions before 1.1.4 Build 20230219	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:tp-link:archer_ax21_firmware:*:*:*:*:*:*	Condi Botnet
TP-Link Archer AX-21 Command Injection Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://www.tp-link.com/us/support/download/archer_ax21/v3/#Firmware
	CWE-77		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472		Microsoft Netlogon	Flea (APT15, Playful Taurus, BackdoorDiplomacy, Vixen Panda, Ke3Chang, Playful Dragon, Bronze Palace, and NICKEL)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64.*	Backdoor.Graphical
Microsoft Netlogon Privilege Escalation Vulnerability			
	CWE ID	T1068: Exploitation for Privilege Escalation	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
	CWE-330		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-17621</u>		D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir-859_firmware:*:*:*:*:*	Mirai botnet
D-Link DIR-859 Remote Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10146 ; https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10147




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-12725</u>		Zeroshell versions: 3.9.0 - 3.9.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:zeroshell:zeroshell:3.9.0:*:*:*:*:*	Mirai botnet
Zeroshell Remote Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1203: Exploitation for Client Execution	https://www.zeroshell.org/download/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-20500</u>		D-Link DWL-2600AP 4.2.0.15	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:dlink:dwl-2600ap_firmware:*:*:*:*:*:*:*	Mirai botnet
D-Link Remote Command Execution Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113
	CWE-78		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-25296</u>		Nagios XI version xi-5.7.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:nagios:nagios_xi:5.7.5:*:*:*:*:*:*	Mirai botnet
Nagios OS Command Injection			
	CWE ID	T1059: Command and Scripting Interpreter	-
	CWE-78		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-46422</u>		Telesquare SDT-CW3B1 1.1.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV		
Telesquare Router Command Injection Vulnerability		cpe:2.3:o:telesquare:sdt cs3b1_firmware:1.1.0:*: *:*:*:*:*	Mirai botnet
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	-




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-27002</u>		Arris TR3300 v1.0.13	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV		
Arris Remote Command Injection Vulnerability		cpe:2.3:o:commscope:a rris_tr3300_firmware:1. 0.13:*:*:*:*:*	Mirai botnet
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	-




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-29303</u>		SolarView Compact version: 6.00	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:contec:sv-cpt-mc310_firmware:6.00:*:*:*:*:*	Mirai botnet
SolarView Compact Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	-




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-30023</u>		Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:tenda:hg9_firmware:1.0.1:*:*:*:*:*	Mirai botnet
Tenda Router Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	-




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30525		Zyxel Multiple Firewalls	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:zyxel:usg_flex_100w_firmware:*:*:*:*:*:*:*:*	Mirai botnet
Zyxel Command Injection Vulnerability			ASSOCIATED TTPs
	CWE ID	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls
	CWE-78		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-31499		Nortek Linear eMerge E3-Series devices before 0.32-08f	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:nortekcontrol:emerge_e3_firmware:*:*:*:*:*:*	Mirai botnet
Nortek Linear eMerge Command Injection Vulnerability			ASSOCIATED TTPs
	CWE ID	T1059: Command and Scripting Interpreter	-
	CWE-78		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-37061</u>		All FLIR AX8 version up to and including 1.46.16	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:o:flir:flir_ax8_firmware:*:*:*:*:*:*	Mirai botnet
FLIR Unauthenticated OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.flir.com/products/ax8-automation/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-40005</u>		Intelbras WiFiber 120AC inMesh before 1-1-220826	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:o:intelbras:wifiber_120ac_inmesh_firmware:*:*:*:*:*:*	Mirai botnet
Intelbras Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://seclists.org/fulldisclosure/2022/Dec/13

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-45699</u>		APSystems ECU-R version 5203	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:apsystems:ecu_r_firmware:5203:*:*:*:*:*:*	Mirai botnet
APsystems Remote Command Execution Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://github.com/Oxst4n/APSystems-ECU-R-RCE-Timezone
	CWE-77		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-25280</u>		D-Link DIR820LA1_F W105B03	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir820la1_firmware:105b03:*:*:*:*:*	Mirai botnet
D-link Command injection vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://github.com/migraine-sudo/D_Link_Vuln/tree/main/cmd%20inject%20in%20pingV4Msg
	CWE-78		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-27240</u>	 ZERO-DAY	Tenda AX3 Version: 16.03.12.11	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
	NAME	CISA KEV	cpe:2.3:o:tenda:ax3_fir mware:16.03.12.11:*:*: *.*.*.*.*
Tenda Command Injection Vulnerability		ASSOCIATED TTPs	PATCH LINK
	CWE ID	CWE-77	T1059: Command and Scripting Interpreter

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 STORM-1359 (Anonymous Sudan)	Unknown	Technology Companies, Government Organisation, Aviation	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMW ARE	AFFECTED PRODUCTS
	-	-	-

TTPs

T1526 - Cloud Service Discovery; T1590 - Gather Victim Network Information; T1498 - Network Denial of Service; T1583 - Acquire Infrastructure; T1190 - Exploit Public-Facing Application

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Diicot (aka Mexals)	Unknown	Technology Companies, Government Organisation, Aviation	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMW ARE	AFFECTED PRODUCTS
	-	Mirai, Cayosin, XMRig	-


TTPs

T1027 - Obfuscated Files or Information; T1110 - Brute Force; T1027 - Obfuscated Files or Information; T1106 - Native API; T1102 - Web Service; T1082 - System Information Discovery; T1496 - Resource Hijacking; T1059 - Command and Scripting Interpreter; T1056 - Input Capture

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Flea (APT15, Playful Taurus, BackdoorDiplomacy, Vixen Panda, Ke3Chang, Playful Dragon, Bronze Palace, and NICKEL)</u></p>	China	Foreign Affairs, Government, Diplomatic, Finance, Political, Foreign	North, Central, and South America
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
CVE-2020-1472	Backdoor.Graphical	Microsoft Netlogon	

TTPs

T1550: Use Alternate Authentication Material; T1027: Obfuscated Files or Information; T1204: User Execution; T1140: Deobfuscate/Decode Files or Information; T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1083: File and Directory Discovery; T1550.001: Application Access Token; T1059.001: PowerShell; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1082: System Information Discovery

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Red Eyes (APT 37, Reaper, Ricochet Chollima, ScarCruft, Thallium, Group 123, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)</u></p>	North Korean	Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation.	China, Czech, Hong Kong, India, Japan, Kuwait, Nepal, Poland, Romania, Russia, South Korea, UK, USA, Vietnam.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	FadeStealer, CHM malware, AblyGo backdoor	-	
TTPs			
<p>T1068:Exploitation for Privilege Escalation; T1204:User Execution; T1140:Deobfuscate/Decode Files or Information; T1059:Command and Scripting Interpreter; T1059.001:PowerShell; T1056:Input Capture ; T1560:Archive Collected Data; T1176:Browser Extensions; T1218:System Binary Proxy Execution; T1547:Boot or Logon Autostart Execution; T1106:Native API; T1566.001:Spearphishing Attachment; T1566:Phishing ; T1036:Masquerading ; T1218.005:Mshta; T1547.001:Registry Run Keys /Startup Folder; T1546.015:Component Object Model Hijacking; T1546:Event Triggered Execution; T1574.002:DLL Side-Loading ; T1574:Hijack Execution Flow ; T1056.001:Keylogging ; T1025:Data from Removable Media; T1027:Obfuscated Files or Information</p>			



Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seventeen exploited vulnerabilities** and block the indicators related to the threat actor **STORM-1359, Diicot, Flea, Red Eyes** and malware **Mystic Stealer, XMRig, Cayosin, Shampoo, Condi, Tsunami, Mirai, Shellbot, FadeStealer, CHM malware, AblyGo backdoor, Backdoor.Graphical**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **seventeen exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **STORM-1359, Diicot, Flea, Red Eyes** and malware **Mystic Stealer, XMRig, Cayosin, Shampoo, Condi, Tsunami, Mirai, Shellbot, FadeStealer, CHM malware, AblyGo backdoor, Backdoor.Graphical** in Breach and Attack Simulation(BAS).



Threat Advisories

[Mystic Stealer Malware Targeting Browsers, Wallets, and Messaging Platforms](#)

[STORM-1359 DDoS triggered outage of Microsoft Services](#)

[The Rising Diicot Threat Group with Diverse Attack Capabilities](#)

[State-Sponsored Hackers Target Middle Eastern and African Governments](#)

[New Chromeloder Shampoo Campaign Infecting Chrome and Stealing Data](#)

[Condi Malware Strikes TP-Link Routers for DDoS Rampage](#)

[Tsunami Botnet Preying on Insufficiently Shielded Linux SSH Servers](#)

[Flea APT Targets Foreign Ministries with New Backdoor.Graphican](#)

[Mirai Botnet Exploits Multiple Flaws in the Latest Campaign](#)

[RedEyes Exploiting Aply Platform Using FadeStealer and Wiretapping Capabilities](#)

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>Mystic Stealer</u>	SHA256	7c185697d3d3a544ca0cef987c27e46b20997c7ef69959c720a8d2e8a03cd5dc 5c0987d0ee43f2d149a38fc7320d9ffd02542b2b71ac6b5ea5975f907f9b9bf8 8592e7e7b89cac6bf4fd675f10cc9ba319abd4aa6eaa00fb0b1c42fb645d3410 45d29afc212f2d0be4e198759c3c152bb8d0730ba20d46764a08503eab0b454f ce56e45ad63065bf16bf736dccb452c48327803b434e20d58a6fed04f1ce2da9 fc4aa58229b6b2b948325f6630fe640c2527345ecb0e675592885a5fa6d26f03
<u>XMRig</u>	MD5	0014403121eeaebaeede796e4b6e5dbe 125951260a0cb473ce9b7acc406e83e1
<u>Condi</u>	SHA256	091d1aca4fcd399102610265a57f5a6016f06b1947f86382a2bf2a668912554f 291e6383284d38f958fb90d56780536b03bcc321f1177713d3834495f64a3144 449ad6e25b703b85fb0849a234cbb62770653e6518cf1584a94a52cca31b1190 4e3fa5fa2dcc6328c71fed84c9d18dfdbd34f8688c6bee1526fd22ee1d749e5a

Attack Name	TYPE	VALUE
<u>Condi</u>	SHA256	509f5bb6bcc0f2da762847364f7c433d1179fb2b2f4828eefb30828c485a3084 593e75b5809591469dbf57a7f76f93cb256471d89267c3800f855cabefe49315 5e841db73f5faefe97e38c131433689cb2df6f024466081f26c07c4901fdf612 cbff9c7b5eea051188cfd0c47bd7f5fe51983fba0b237f400522f22ab91d2772 ccda8a68a412eb1bc468e82dda12eb9a7c9d186fabf0bbdc3f24cd0fb20458cc e7a4aae413d4742d9c0e25066997153b844789a1409fd0aacc e8cc6868729a15 f7fb5f3dc06aebcb56f7a9550b005c2c4fc6b2e2a50430d64389914f882d67cf
<u>Tsunami</u>	MD5	822b6f619e642cc76881ae90fb1f8e8e
	C2	ircx.us[.]to:53 ircxx.us[.]to:53
<u>Mirai</u>	SHA256	b43a8a56c10ba17ddd6fa9a8ce10ab264c6495b82a38620e9d54d66ec8677b0c b45142a2d59d16991a38ea0a112078a6ce42c9e2ee28a74fb2ce7e1edf15dce3 366ddbbaa36791cdb99cf7104b0914a258f0c373a94f6cf869f946c7799d5e2c6 413e977ae7d359e2ea7fe32db73fa007ee97ee1e9e3c3f0b4163b100b3ec87c2 2d0c8ab6c71743af8667c7318a6d8e16c144ace8df59a681a0a7d48affc05599 4cb8c90d1e1b2d725c2c1366700f11584f5697c9ef50d79e00f7dd2008e989a0 461f59a84ccb4805c4bbd37093df6e8791cdf1151b2746c46678dfe9f89ac79d aed078d3e65b5ff4dd4067ae30da5f3a96c87ec23ec5be44fc85b543c179b777 0d404a27c2f511ea7f4adb8aa150f787b2b1ff36c1b67923d6d1c90179033915 eca42235a41dbd60615d91d564c91933b9903af2ef3f8356ec4cfff2880a2f19 3f427eda4d4e18fb192d585fca1490389a1b5f796f88e7ebf3ec eec51018ef4d aaf446e4e7bfc05a33c8d9e5acf56b1c7e95f2d919b98151ff2db327c333f089 4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b

Attack Name	TYPE	VALUE
<u>Shellbot</u>	URLs	ddoser[.]org/logo ddoser[.]org/siwen/bot
	MD5	c5142b41947f5d1853785020d9350de4 2cd8157ba0171ca5d8b50499f4440d96
<u>Backdoor.Grap hical</u>	SHA256	4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13a c302a84553e2d5 a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f 12a3a9e9bfa8 02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f6 6173f1b195ef5 617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e 50fb31a9a98bcd 858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf890 26d3c2732c253 fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5 d094b1f1476 177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e5 6d4e0c0063eecf 8d2af0e2e755ffb2be1ea3eca41eebfc6341fb440a1b6a02bfc 965fe79ad56b f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777 da8c6dcf578286 865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b 7dce1f66cf48 d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9 380e534aaf5e30
<u>FadeStealer</u>	MD5	f44bf949abead4af0966436168610bcc
<u>CHM malware</u>	MD5	1352abf9de97a0faf8645547211c3be7
<u>AblyGo backdoor</u>	MD5	3277e0232ed6715f2bae526686232e06 3c475d80f5f6272234da821cc418a6f7
	URL	hxxp://172.93.181[.]249/file/

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5:Threat Exposure Management Platform.



REPORT GENERATED ON

June 26, 2023 • 9:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com