Date of Publication
April 3, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

27 MARCH to 2 APRIL 2023

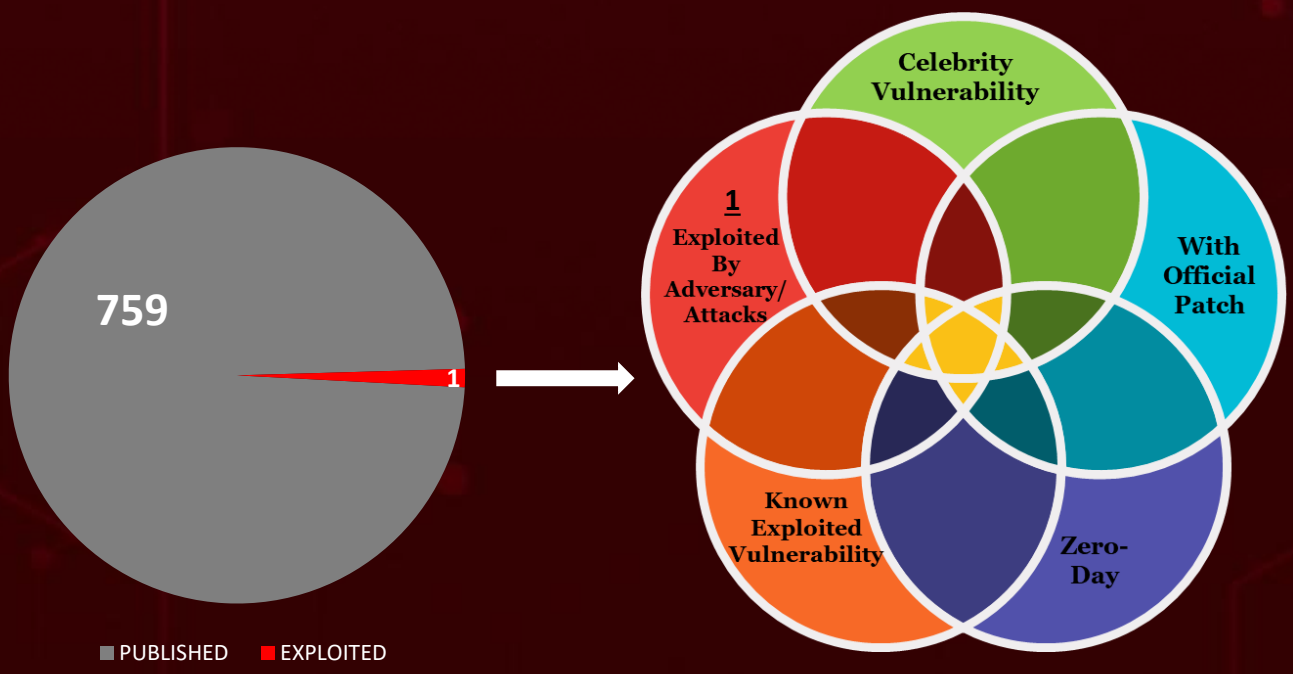
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, they identified a total of **Nine attacks** that were executed. Additionally, HiveForce Labs identified **seven** different **adversaries** that were actively carrying out these attacks.

Interestingly, **one** of the vulnerability exploited in the **SmoothOperator** campaign to get access to 3CXdesktopapp trojanized via a multi-stage supply attack chain had not yet been patched.

Apart from these threats, the number of strikes by Chinese espionage groups has increased. **ChinaZ**, **Gallium**, and **APT 41** were among these actors. All these attacks were observed to be on the rise, posing a significant threat.



High Level Statistics

9
Attacks Executed

1
Vulnerabilities Exploited

7
Adversaries in Action

- Dark Power ransomware
- ChinaZ DDoSClient
- mim221
- donot
- DBatLoader
- Formbook
- Remcos RAT
- Creal Stealer
- ICONIC Stealer

- CVE-2023-29059

- Dark Power ransomware
- ChinaZ
- Bitter APT
- Gallium
- APT 41
- Donot group
- LABYRINTH CHOLLIMA

Insights

9 Years later, ChinaZ a Chinese threat actor resurfaces

Gallium & APT41 the Chinese cyber duo behind Operation Soft Cell

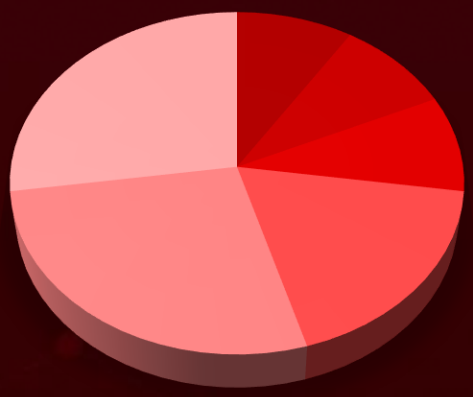
Creal Stealer the predator of cryptocurrency users

Dark Power ruthless ransomware reigns over all major industries.

SmoothOperator Campaign Trojanizing the 3CXDesktopApp

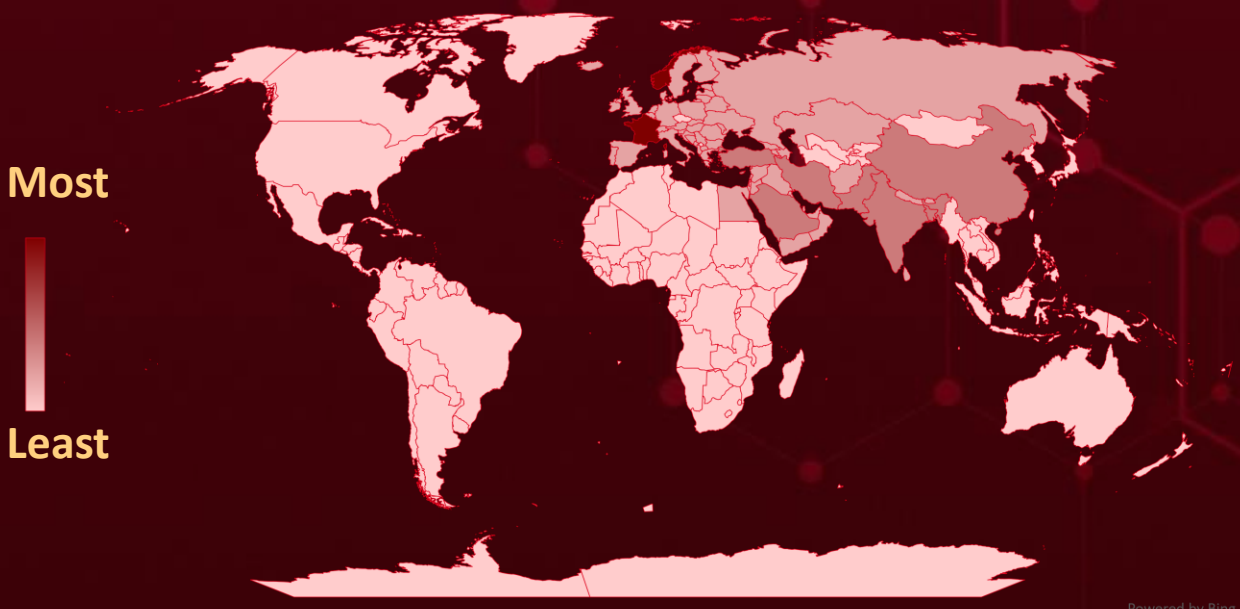
1 Vulnerability has no patch available

Threat Distribution



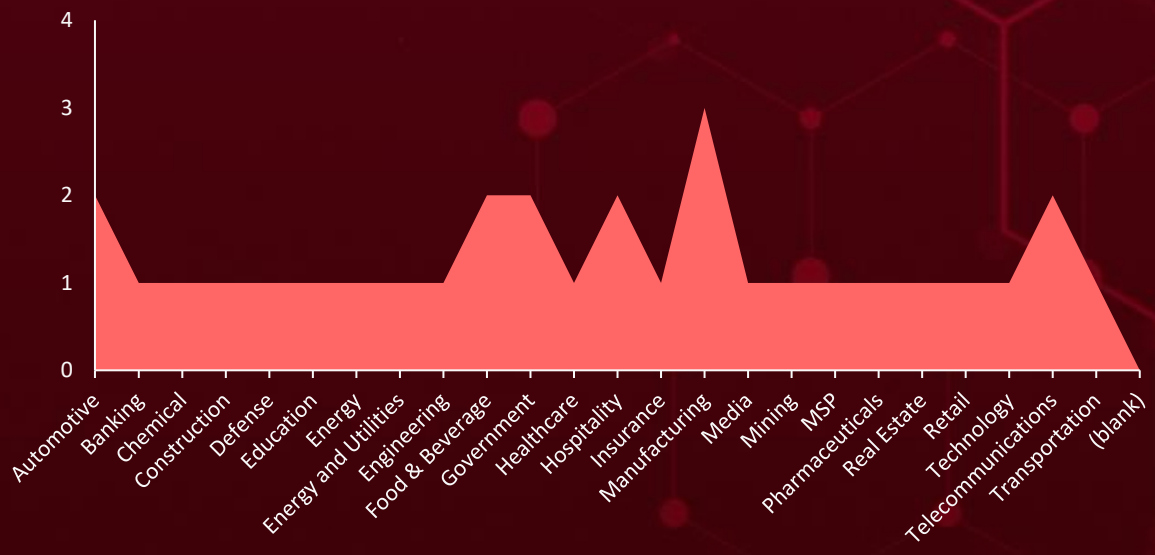
Donot APT target South Asia's government and military

Targeted Countries



Countries	Countries	Countries	Countries	Countries
Norway	Liechtenstein	Montenegro	Syria	Japan
France	Croatia	Iceland	Italy	Chile
China	Malta	Netherlands	UAE	Kenya
Turkey	Albania	Armenia	Jordan	Colombia
Saudi Arabia	Nepal	Bahrain	Ukraine	Brazil
Cyprus	Denmark	Austria	Kazakhstan	Zimbabwe
Bangladesh	Oman	Afghanistan	Yemen	Singapore
Pakistan	Egypt	Serbia	Kuwait	Malaysia
India	Portugal	Poland	Thailand	South Africa
Iran	Estonia	Slovenia	El Salvador	South Korea
Luxembourg	San Marino	Qatar	Equatorial Guinea	Cambodia
Romania	Finland	Sri Lanka	Australia	Taiwan
North Macedonia	Vatican City	Russia	Dominican Republic	Canada
Belgium	Andorra	Switzerland	Nigeria	Dominica
Latvia	Lebanon	Belarus	Philippines	Morocco
Bhutan	Georgia	Azerbaijan	Hong Kong	Myanmar
Monaco	Lithuania	Slovakia	Czech Republic	Vietnam
Bosnia and Herzegovina	Germany	Iraq	Indonesia	New Zealand
Palestine	Maldives	Spain	Argentina	Kyrgyzstan
Bulgaria	Greece	Ireland	USA	Mexico
UK	Moldova	Sweden	Jamaica	Myanmar
Akrotiri and Dhekelia	Hungary	Israel	North Korea	Zambia

Targeted Industries



TOP MITRE ATT&CK TTPS

T1547 Boot or Logon Autostart Execution

T1059 Command and Scripting Interpreter

T1071 Application Layer Protocol

T1027 Obfuscated Files or Information

T1547.001 Registry Run Keys / Startup Folder

T1057 Process Discovery

T1082 System Information Discovery

T1566 Phishing

T1574 Hijack Execution Flow

T1070 Indicator Removal

T1021 Remote Services

T1055 Process Injection

T1518 Software Discovery

T1059.001 PowerShell

T1560 Archive Collected Data

T1036 Masquerading

T1497 Virtualization/ Sandbox Evasion

T1041 Exfiltration Over C2 Channel

T1546 Event Triggered Execution

T1053 Scheduled Task/Job

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Dark Power Ransomware	Dark Power ransomware uses Nim programming language to create malware that encrypts specific services and processes, excludes crucial system files, clears logs, and generates a ransom note in every folder.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Compromise of Sensitive Information, and Potential Financial Losses	-
ASSOCIATED ACTOR			**PATCH LINK**
Dark Power Ransomware			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ChinaZ DDoSClient (or ChinaZ)	ChinaZ DDoSClient is an infamous DDoS botnet used by a Chinese threat group to target Windows and Linux systems, likely by using stolen account credentials from scanners and SSH Brute Force malware.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
DDoS botnets		Gain unauthorized access sensitive business data	-
ASSOCIATED ACTOR			**PATCH LINK**
ChinaZ			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
mim221	A Chinese cyber espionage group attributed to the Operation Soft Cell campaign has been observed infiltrating Microsoft Exchange servers to deploy web shells for command execution.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Credential theft tool		Data Theft, Compromise of Sensitive Information, and Potential Financial Losses	-
ASSOCIATED ACTOR			**PATCH LINK**
Gallium and APT 41			-

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
Donot	Donot samples use different malicious code implantation methods and change the code details of attack components. Donot executes shellcode to download subsequent DLL components by carrying macros in documents.	Using macro documents, self-extracting RAR archives, and EXE components	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Espionage and Theft of sensitive data	-
ASSOCIATED ACTOR			**PATCH LINK**
Donot group (APT-Q-38)			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DBatLoader (aka ModiLoader and NatsoLoader)	DBatLoader is used to deliver the payload, the attackers use multilayer obfuscation techniques and various file formats, such as PDF, HTML, ZIP, and OneNote.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Theft of sensitive business data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Formbook	The FormBook stealer can search for, viewing, interact with files, and take screenshots. The malware has advanced stealing and evasion functions including the ability to pull stored and recorded victim input.	DBatLoader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information stealer		Theft of sensitive business data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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
Remcos RAT	Remcos is a RAT that attackers use to perform actions on infected machines remotely and control PCs with any Windows OS, including XP and newer. The RAT captures screenshots, record keystrokes, and send the collected information.	DBatLoader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote Access Trojan		Theft of sensitive business data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Creal Stealer	The Creal stealer binary is compiled with PyInstaller, indicating that it was written in Python. There are 50 samples in the wild, demonstrating that threat actors were actively using the open-source code to infect unwitting victims.	Phishing site impersonating a cryptocurrency mining platform	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		data-stealing, compromise of sensitive data, and potential financial loss.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ICONIC Stealer (aka SUDDENICON)	The SmoothOperator campaign conducted a supply chain attack targeting downstream customers via rigged installers. The ICO file containing URLs hosting the final-stage payload ICONIC Stealer is capable of harvesting system information and sensitive data stored in web browsers.	Compromised 3CX DesktopApp	CVE-2023-29059
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		data theft, financial loss, and damage	3CX DesktopApp for Windows Versions: 18.12.407, 18.12.416 & 3CX DesktopApp for macOS Versions: 18.11.1213
ASSOCIATED ACTOR			**PATCH LINK**
LABYRINTH CHOLLIMA			No Patch Available

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

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-29059</td><td>  </td><td rowspan="2">3CX DesktopApp for Windows Versions: 18.12.407, 18.12.416 & 3CX DesktopApp for macOS Versions: 18.11.1213</td><td rowspan="2">LABYRINTH CHOLLIMA</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:3cx:desktop_app_windows:*:*:*:*:*:*:*:*
cpe:2.3:a:3cx:desktop_app_maOS:*:*:*:*:*:*:*:*</td><td rowspan="2">ICONIC Stealer (aka SUDDENICON)</td></tr>
<tr><td rowspan="2">Arbitrary code execution in 3CXDesktopApp</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-506</td><td>T1059: Command and Scripting Interpreter</td><td>No Patch Available</td></tr>
</table>

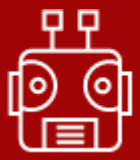
Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	Unknown	All industries	Worldwide
	MOTIVE		
	Information theft and espionage		
Dark Power ransomware	**TARGETED CVEs**	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Dark Power ransomware	-
TTPs			
T1047:Windows Management:Instrumentation;T1070:Indicator Removal;T1070.001:Clear Windows Event:Logs;T1027:Obfuscated Files or:Information;T1082:System Information:Discovery;T1486:Data Encrypted for:Impact;T1490:Inhibit System Recovery:T1489:Service Stop;T1623:Command and Scripting:Interpreter;T1057:Process Discovery;T1140:Deobfuscate/Decode:Files or Information			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	China	-	Worldwide
	MOTIVE		
	Information theft and espionage		
ChinaZ	**TARGETED CVEs**	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ChinaZ DDoSClient Botnet	-
TTPs			
T1110:Brute Force;T1498:Network Denial of:Service;T1057:Process Discovery;T1546:Event Triggered:Execution;T1021:Remote Services;T1499:Endpoint Denial of:Service;T1027:Obfuscated Files or:Information;T1027.005:Indicator Removal from:Tools;T1129:Shared Modules;T1547:Bootor Logon Autostart:Execution;T1547.001:Registry Run Keys/StartupFolder;T1497:Virtualization/Sandbox Evasion;T1497.001:System Checks			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	South Asia	Energy, Engineering, Government	Bangladesh, China, India, Pakistan, and Saudi Arabia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Bitter APT	-	-	-
TTPs			
T1589.002:Email Addresses;T1566.001:Spearphishing Attachment;T1059:Command and Scripting Interpreter;T1059.001:PowerShell;T1203:Exploitation for Client Execution; T1036:Masquerading;T1053.005:ScheduledTask;T1218.007:Msiexec; T1218.001:Compiled HTML File;T1082:System Information:Discovery;T1071.001:Web Protocols;T1041:Exfiltration Over C2:Channel;T1566:Phishing;T1218:System Binary Proxy:Execution;T1071:Application Layer Protocol;T1053:Scheduled Task/Job			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	China	Telecommunications	Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, UAE, Yemen.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Gallium(aka Phantom Panda)	-	mim221	-
TTPs			
T1055:Process Injection;T1059:Command and Scripting:Interpreter;T1049:System Network:Connections Discovery;T1003:OS Credential Dumping;T1547:Boot or Logon Autostart:Execution;T1106:Native API;T1021:Remote Services;T1074:Data Staged;T1033:System Owner/User Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	China	Telecommunications	Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, UAE, Yemen.
	MOTIVE		
	Financial crime, Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
APT 41	-	mim221	-
TTPs			
T1055:Process Injection;T1059:Command and Scripting:Interpreter;T1049:System Network:Connections Discovery;T1003:OS Credential Dumping;T1547:Boot or Logon Autostart:Execution;T1106:Native API;T1021:Remote Services;T1074:Data Staged;T1033:System Owner/User Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	South Asia	Government agencies, Defense military	Afghanistan, China, Bangladesh, Bhutan, India, Iran, Maldives, Nepal, Pakistan, and Sri Lanka.
	MOTIVE		
	Espionage and Information theft		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Donot group (APT-Q-38)	-	Donot	-
TTPs			
T1059:Command and Scripting Interpreter;T1053:Scheduled Task/Job;T1137:Office Application:Startup;T1027:Obfuscated Files or Information;T1056:Input Capture;T1562:Impair Defenses;T1560:Archive Collected Data;T1113:Screen Capture;T1033:System Owner/User Discovery;T1546:Event Triggered Execution;T1574:Hijack Execution Flow;T1105:Ingress Tool Transfer;T1566:Phishing;T1070:Indicator Removal;T1204:User Execution;T1204.002:Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	North Korea	Automotive, Food & Beverage, Hospitality, Managed Information Technology Service Provider (MSP), Manufacturing	Worldwide
	MOTIVE		
	Financial gain and Information Theft		
LABYRINTH CHOLLIMA (aka HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Lazarus Group)	**TARGETED CVEs**	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-29059	ICONIC Stealer or SUDDENICON	3CX DesktopApp for Windows Versions: 18.12.407, 18.12.416 & 3CX DesktopApp for macOS Versions: 18.11.1213
TTPs			
T1091:Replication Through Removable Media;T1059:Command and Scripting Interpreter;T1543:Create or Modify System Process;T1543.003:Windows Service;T1547:Boot or Logon Autostart Execution;T1547.001:Registry Run Keys / Startup Folder;T1574:Hijack Execution Flow;T1574.002:DLL Side-Loading;T1056:Input Capture;T1071:Application Layer Protocol			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **1 exploited vulnerability** and block the indicators related to the threat actor **Dark Power ransomware, ChinaZ, Bitter APT, Gallium, APT 41, Donot group, LABYRINTH CHOLLIMA** and malware **Dark Power ransomware, ChinaZ DDoSClient, mim221, donot, DBatLoader, Formbook, Remcos RAT, Creal Stealer,** and **ICONIC Stealer.**

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 **1 exploited vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Dark Power ransomware, ChinaZ, Bitter APT, Gallium, APT 41, Donot group, LABYRINTH CHOLLIMA** and malware **Dark Power ransomware, ChinaZ DDoSClient, mim221, donot, DBatLoader, Formbook, Remcos RAT, Creal Stealer,** and **ICONIC Stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

New Dark Power Nim-based Ransomware Targeted Attacks Globally

Unveiling ChinaZ DDoS Threat Landscape

Bitter APT Group Targets Chinese Energy Sector with New phishing Campaign

Chinese Cyber Espionage Targets Middle Eastern Telecoms

Donot APT Group Targets Government and Military Orgs in South Asia

New DBatLoader Malware Campaign Targets European Countries

Creal Stealer Preys on Cryptocurrency Users

SmoothOperator Campaign Trojanizes 3CXDesktopApp

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
Dark Power Ransomware	SHA256	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde 9a389 11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea46736 7394
	SHA1	9bddcce91756469051f2385ef36ba8171d99686d
	MD5	df134a54ae5dca7963e49d97dd104660
ChinaZ DDoSClient	MD5	c69f5eb555cc10f050375353c205d5fa c9eb0815129c135db5bbb8ac79686b9a 2ec7348e6b6b32d50a01c3ffe480ef70
	URLs	hxxp[:]//45.113.163[.]219/linux32 hxxp[:]//45.113.163[.]219/linux64 hxxp[:]//45.113.163[.]219/win32
	IPV4:PORT	45.113.163[.]219:29134
	Domains	www[.]911ddos[.]com
mim221	SHA1	f54a41145b732d47d4a2b0a1c6e811ddcba48558 1c405ba0dd99d9333173a8b44a98c6d029db8178 df4bd177b40dd66f3efb8d6ea39459648ffd5c0e 814f980877649bc67107d9e27e36fba677cad4e3 508408edda49359247edc7008762079c5ba725d9 97a7f1a36294e5525310f121e1b98e364a22e64d

Attack Name	TYPE	VALUE
donot	MD5	06adbb4ba31a52cc5c9258bf6d99812c,d98e2d7c8e91a9d8e87abe744f6d43f9,c839d8a01c97407526b3407022823c8a,1c4fb7c41e7928bfb74784d910522771,e1d235c95a7c06b1203048972cf179fa,6de75b200652eefa4a6a3bb84da7f798,0ec8911f9764ea7b254ea19cd171535e,171c011571f94ea2f5c928bdf5d560dc,79cff3bc3cbe51e1b3fecd131b949930,dcac3a03c0c58b90cd4cbcc814d12847,e46cd1c4b32355cad39b41ef3b66b659,c231254ced08ca556bf35e587469628f,5557b32672ee9ad6be20395d447a3e52,3feb4de4375dcc3ffb4144e2fc61dd94,4c0dadc4b6938dcc9ca8951d34cb2a09,d30631ba67a28a6e4ab0c4e9584e26c2,2abc60fa1e042612e723360ccd8220c6,3c6ad03f0ab284350d8b0d3d4cf22196,07a3c19bc67c5f44c888ce75d4147ecf,d7e123fe7fb8a5f56ec9d89f7787340d,20c581284cccadd8b6193c2e1c84a900,5e464d04b35a83d28c4e26c06eec28f5,9946df6c429b83009535dca8d1a5d321,ee24afbe471b5e63b06a759fa0eba0cc,7750cac1cab5e6fd9e5cadecbc3c51f6,0844b582c202dca08083d04d10bdf36e,4eaa63dd65fc699260306c743b46303b,a84d7a5b8831d7494ee20b939e37e56f,3b730afd4ed953a9031a3facf111a64e,cf646416025a84c5ef25b99dc999da9d
	Domains	one[.]localsurfer[.]buzz orangevisitorss[.]buzz morphylogz[.]buzz crezdlack[.]buzz crushter[.]info monitoriing[.]buzz m[.]seasurfer[.]buzz bloggerboy[.]buzz sky[.]ydnmovers[.]buzz itygreyhound[.]buzz balancelogs[.]buzz mayosasa[.]buzz goldliney[.]buzz briefdeal[.]buzz repidyard[.]buzz salcomp[.]buzz grapehister[.]buzz orangeholister[.]buzz blogs[.]firelive[.]pics records[.]libutires[.]info forum[.]winidowtech[.]info
	URLs	hxxp://one[.]localsurfer[.]buzz/jl60UwJBkaWEkCSS/MU3gLGSnHhfDH RnwhlILSB27KZaK2doaq8s9V5M2RIgpeaD8[[.]ico|[.]png|[.]mp3|[.]mp 4]

Attack Name	TYPE	VALUE
donot	URLs	hxxp://orangevisitorss[.]buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1t RyF47ZXLIdqNGRqiHQQHL6DJIjl2IoxUA[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://morphylogz[.]buzz/Ik3EIidq3fc2GGig/aFwrDmHIiBWh62kZPVb4 bmV0waydPv0WtgqM0QTte5iAFzF0[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://crezdlack[.]buzz/icsJOzJVtdTcGPB3/PT0w3akYLzLtd5AGs3PVEj MKJ1aO5xtfGvWbFmc4ubgXBvJO[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://crushter[.]info/m4k1doWVqrvvbjsc/AOg9AQ2SVeHsiL61tkS53q 02NnMToZuOb8s5yUe8jEcBxAs0[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://monitoriing[.]buzz/3fHYKahOXhkVV3Uj/dqyWpAfXBcyQkTkzoa mk25hn3cbTbeuhImfJO08uTOFCkhIa[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://m[.]seasurfer[.]buzz/33IhGEeiVe57s8gY/nmEVLghL0B5dMtBiZ MAgeIVniuP4bVFETWfsZqQ2jZ1bMJYd[[.]ico|[.]png|[.]mp3|[.]mp4] hxxps://bloggerboy[.]buzz/zapterserty512wer/plekobakarester hxxps://bloggerboy[.]buzz/zapterserty512wer/xcvderioneytr hxxps://sky[.]ydnmovers[.]buzz/Kolpt523ytcserstrew/torel hxxps://sky[.]ydnmovers[.]buzz/Kolpt523ytcserstrew/meoko/P/sa hxxps://itygreyhound[.]buzz/Kolpt523ytcserstrew/torel hxxps://itygreyhound[.]buzz/Kolpt523ytcserstrew/meoko/P/sa hxxps://balancelogs[.]buzz/Kolpt523ytcserstrew/torel hxxps://balancelogs[.]buzz/Kolpt523ytcserstrew/meoko/P/sa hxxps://mayosasa[.]buzz/Testoresisty/kolimekatares hxxps://mayosasa[.]buzz/Testoresisty/bekolopexar hxxps://goldliney[.]buzz/Lomiapekaso/texadikkomanapel hxxps://goldliney[.]buzz/Lomiapekaso/ertopikana hxxps://briefdeal[.]buzz/Treolekomana/recopereta hxxps://briefdeal[.]buzz/Likorecasta/mikachar hxxps://repidyard[.]buzz/Romexicarto/terokanama hxxps://repidyard[.]buzz/xoexapolicreate/ertyprmekabiops hxxps://salcomp[.]buzz/Terolekaremos/romeosata hxxps://grapehister[.]buzz/DoPstRgh512nexcvv[.]php hxxps://orangeholister[.]buzz/kolexretriya78ertdcxmega895200[.]php

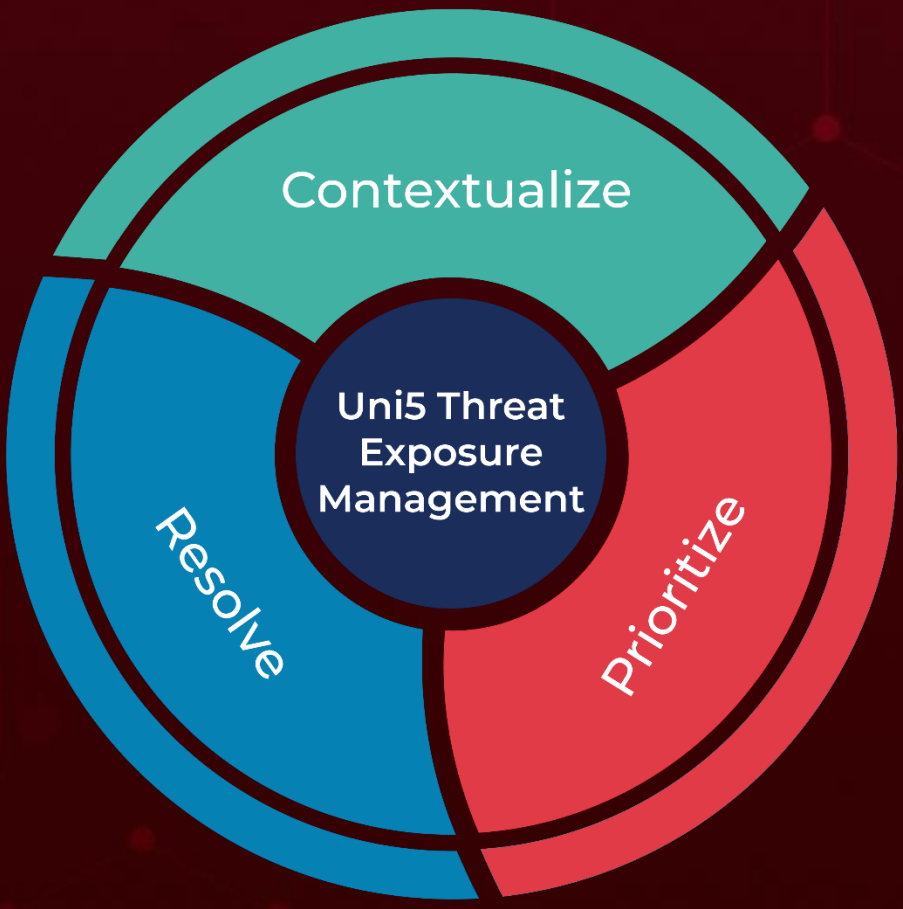
Attack Name	TYPE	VALUE
DBatLoader	MD5	55aba243e88f6a6813c117ffe1fa5979 213c60adf1c9ef88dc3c9b2d579959d2 231ce1e1d7d98b44371ffff407d68b59 b375e74a145c45d07190212e9157e5f8
Formbook	MD5	d9844515b7d09d74de188856b60c88c0 10904cb6103086d04ba0d76bcf7a65dc 1978b12cacb91b0d0f77a9979db9e671 3dde7b13d4736c11a67bc8fbad976d37 fb7dbeea12e4729cf11d6de8588f2b7e
	URLs	hxxps://sleda[.]sleda[.]eu/wp-content/themes/A0034372876RFQ021423.cab hxxps://sleda[.]sleda[.]eu/wp-content/themes/A0034372876RFQ021423.cab hxxps://sleda[.]sleda[.]eu/wp-content/themes/A0034372876RFQ021423.cab hxxps://thesquirrelgame[.]net hxxps://b-yy[.]xyz
Remcos RAT	MD5	d51576e2e216292a72ce16821f9696d3 0e8aefd1dade4f059c2881c6e05f689f ef02ba99d974787a70085537918117c4 4c39cdd2bfb2c7dde761a6e5b8c01321 85b2a41e98412f2867715c9ae5ad27ac c1d19535ded9e0ff8e293f6852b24b91 1d1f8534ee6dbe1dbeade30e912a9136 f0b7bad0eb081c6b7d3df74e733efd1c 00c168883239c13aa213a5337aca3dae aa8836fa3879074748f6dca63476aba9 b2d368435d5896419751add4cc338fc4 be889f4ab5ce7e99c131463c58205ba0
	URLs	hxxps://silverline[.]com[.]sg/new/Revised_Order_Document.cab hxxps://silverline[.]com[.]sg/admin/Xdfiifagcwrbrg.exe hxxps://silverline[.]com[.]sg/private/SZ59020_JF_KOREA_Co_Ltd_Sales_Order.cab hxxps[://]silverline[.]com[.]sg/admin/Fsofwcqmhvvgna.exe hxxps://silverline[.]com[.]sg/new/Dvicvwxfouxvgm.exe hxxps://hallowed247[.]duckdns[.]org:9150 hxxps://silverline[.]com[.]sg/new/Eyeqkzxtfeyxwr.exe
	IPV4	185[.]246[.]220[.]63
Creal Stealer	URLs	hxxps[:]//www.dropbox[.]com/s/dl/x4vgcaac6hcdgla/kryptex-setup-4.25.7[.]zip

Attack Name	TYPE	VALUE
Creal Stealer	Domain	kryptex[.]software
	SHA256	4ee417cbefa1673d088a32df48b8182bdad244541e8dc02faf540b9aa483fdcb,f3197e998822bc45cb9f42c8b153c59573aad409da01ac139b7edd8877600511
	MD5	bb2ca78ffff72d58599d66bf9b2f0ae6 929e6f2c8896059c72368915abcaefa2
	SHA1	20dcb84660e5f79a98c190d3d455fce368d96f35 7122f0b88607061806fd62282e8b175ae28b7e29
ICONIC Stealer	URLs	github[.]com/IconStorages/images https[://]www.3cx[.]com/blog/event-trainings/ https[://]akamaitechcloudservices[.]com/v2/storage https[://]azureonlinestorage[.]com/azure/storage https[://]msedgepackageinfo[.]com/microsoft-edge https[://]glcloudservice[.]com/v1/console https[://]pbxsources[.]com/exchange https[://]msstorageazure[.]com/window https[://]officestoragebox[.]com/api/session https[://]visualstudiofactory[.]com/workload https[://]azuredeploystore[.]com/cloud/services https[://]msstorageboxes[.]com/office https[://]officeaddons[.]com/technologies https[://]sourceslabs[.]com/downloads https[://]zacharryblogs[.]com/feed https[://]pbxcloudeservices[.]com/phonesystem https[://]pbxphonenetwork[.]com/voip https[://]msedgeupdate[.]net/Windows https[://]sbmsa[.]wiki/blog/_insert
	Emails	cliego.garcia@proton[.]me philip.je@proton[.]me
	SHA1	cad1120d91b812acafef7175f949dd1b09c6c21a bf939c9c261d27ee7bb92325cc588624fca75429 20d554a80d759c50d6537dd7097fed84dd258b3e 769383fc65d1386dd141c960c9970114547da0c2 3dc840d32ce86cebf657b17cef62814646ba8e98 9e9a5f8d86356796162cee881c843cde9eaedfb3
	SHA256	dde033480755127962413 89dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc,fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405,92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61,b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb,aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868,59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983,5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290

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

April 3, 2023 . 7:01 AM

More at www.hivepro.com