Hacker Groups impacting the Region

Date: 20/09/2023
Version: 2.0

NATIONAL AUTHORITY FOR ELECTRONIC CERTIFICATION AND CYBER SECURITY

Table of Content:

This document is written by the Directorate of Cyber Security Analysis, National Authority for Electronic Certification and Cyber Security.

Creating a profile on several threat actors impacting Albania and the Region involves a methodical and careful process to gather and analyze information from hidden Internet sources. The goal is to discover and document the activities related to the hacker groups "State Sponsored Attackers" and "Advanced Persistent Threat" (APT) related to the targeting that these groups have towards Albania and the Region. The following are the steps for making this report:

The first phase:
Identification and Detection: Identifying potential indicators of a state threat actor's presence on the DarkWeb. These indicators include URLs, forum names, or other sources that suggest a state's involvement in cyber activities.

Second phase:
Evidence Collection: Documenting and storing relevant evidence from the DarkWeb. Recording of screenshots, recording of communication details and threat actor tactics, techniques and procedures (TTP).

The third stage:
Analysis and Verification: Analyzing the information collected to determine the trustworthiness and authenticity of the DarkWeb profile. Data verification with additional sources, threat intelligence platforms to reduce the risk of misinformation.

The fourth stage:
Impact Assessment: Assessing the potential impact of malicious actor activities on target entities or industries. Understanding the objectives behind their actions, whether they involve espionage, data theft, sabotage or other cyber operations.

Fifth stage:
Technical details: Documentation of technical information, such as IP addresses, malware hashes, and domain names used by the state threat actor. These details help identify and track their activities.

Sixth stage:
Continuous Monitoring: Continuous monitoring for any updates or new activity related to the threat actor, as their tactics may evolve over time.

The findings of the report are based on the information available at the time of the investigation and analysis. There are no guarantees regarding possible changes or updates to the information reported during the following period.

Gamaredon Group

The State Sponsored Gamaredon group is of Russian origin. Gamaredon targets Ukrainian entities. It first appeared in 2013. Some of the other target countries are: Albania, Austria, Australia, Bangladesh, Brazil, Canada, Chile, China, Colombia, Croatia, Denmark, Georgia, Germany, Guatemala, Honduras, India, Indonesia, Iran, Israel, Italy, Japan, Kazakhstan, Latvia, Malaysia, Netherlands, Nigeria, Norway, Pakistan, New Guinea, Poland, Portugal, Romania, Russia, South Africa, South Korea, Spain, Sweden, Turkey, United Kingdom, Ukraine, USA and Vietnam. The main target sectors are: the defence sector, governments, law enforcement and non-governmental organizations. This group is a persistent risk that poses a significant threat, and an increased level of covert tactics is evident. The attackers use some malware such as "7ZSfxModx86.exe" (dropper) and "myfile.exe". Techniques used: TA0043, TA0001, TA0002, TA0003, TA0005, TA0006, TA0009, TA0011, T1047, T1036, T1027, T1102, T1140, T1547, T1557, T1559, T1566 etc.

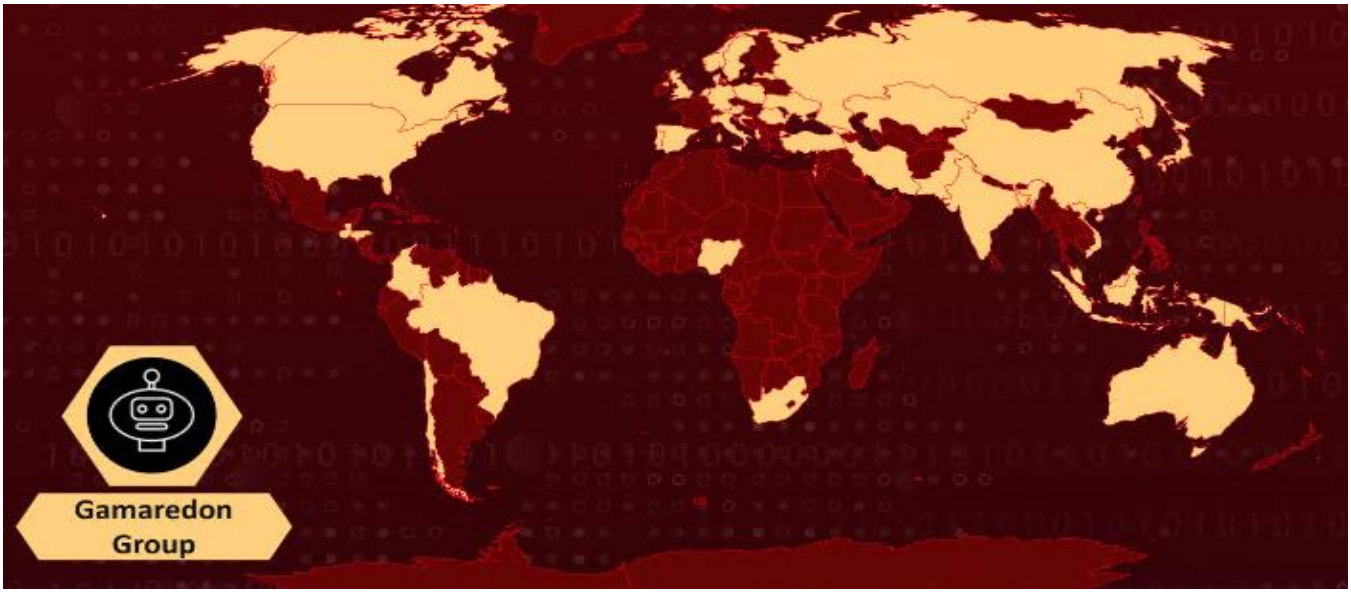


Figura 1: The extent of the Gamaredon Group

Recommendations:

Simulate phishing attacks in your organization, implement training and apply awareness of the use of Multifactor Authentication (MFA).

Use priorities and block all indicators attributed to the risk actor through your monitoring centre. Do your own testing by simulating similar attacks.

Refer to and act upon the MITER ATT&CKS Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IoC) presented below.

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0009** Collection	**TA0011** Command and Control
T1047 Windows Management Instrumentation	**T1036** Masquerading	**T1027** Obfuscated Files or Information	**T1053** Scheduled Task/Job
T1102 Web Service	**T1140** Deobfuscate/Decode Files or Information	**T1547** Boot or Logon Autostart Execution	**T1557** Adversary-in-the-Middle
T1559 Inter-Process Communication	**T1566** Phishing	**T1204** User Execution	

Figure 2: Techniques, Tactics, Procedures of the Gamaredon group

Indicators of compromise:

HASH
007483ad49d90ac2cabe907eb5b3d7eef6a5473217c83b0fe99d087ee7b3f6b3
00ca57feac8695e915664398e82131d9c70a45a68f741b78f13c88ad61c49cda
019e0910c6d62d6948ea6f2c83c62491b24cefa4dedc830b93b3c6176a7d9c76
01bead955437c198ddd134236a9fbe0442bb0e6170a59b039352929028972384
01da7d2722477522bf5cb0a757d922cfe07575984e15df56cd3658722a907f1b
02ed10858a777d2cf2c6cd22dfeccb338aa7ce381273de4eebaf6894334c7a34
0608ae0f28510591798a1603adabde86a9dbd67e1bfb1713c3f397d0d1a306d1
0720a9b5ecd98163208ad5d6d041679c0a6954d80685695df55b0e105dca7b09
07661128749c960ea28126cf6b76f9a223d6523c0df917e3ece46bfce2d0d3e9
08ff31342b174a2e07d6f81d9c2844f90b44b03f6a531fc06cd131b838d3e571
09472d6bfb1c142a3b02f73175254a5e961f91e792dc9b347b099944bcfeab6f

DOMAIN
kyoungo[.]org
labutens[.]ru
muscarias[.]ru
ovinuso[.]ru
pafamar[.]ru
quyenzo[.]ru
radiumo[.]ru
a0662337.xsph[.]ru
abbasa[.]ru

bahadurdo[.]ru
caccabius[.]ru

IP
104.248.36.191
140.82.29.65
141.164.45.200
155.138.138.195
155.138.252.221
159.89.31.49
162.33.178.129
167.99.138.16
188.166.43.183
194.180.191.105
199.247.14.64
206.81.0.182
45.77.11.107
45.77.229.187
45.77.237.252
82.146.39.104
91.188.222.50
95.179.216.77

LockBit Ransomware:

LockBit

LockBit first appeared in January 2020. The feature of this group is that it has attacked countries all over the world. The Lockbit Ransomware group (version 2.0 and version 3.0), originates from Taiwan. It operates using "Ransomware-as-a-Service". The group exploits CVE-2023-0669, CVE-2023-27350, CVE-2021-44228, CVE-2021-22986, CVE-2020-1472, CVE-2019-0708, CVE-2018-13379. The sectors primarily targeted are critical infrastructure sectors, including financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing and transportation. The platforms that can be infected are Windows, Linux and MacOS. The malware used is LockBit Ransomware. The LockBit ransomware is a variant that targets critical sectors around the world. As of 2020, victims in the US alone have paid about $91 million in settlements. LockBit continues to pose an ongoing threat, with multiple cases reported in May 2023.

The LockBit Ransomware group announced on DarkWeb that the Air Albania airline was targeted by LockBit ransomware cybercriminals, trying to extract a ransom.
Air Albania did not report any cyber incident that could have impacted their system.

Attack Type: Ransomware Data Breached.

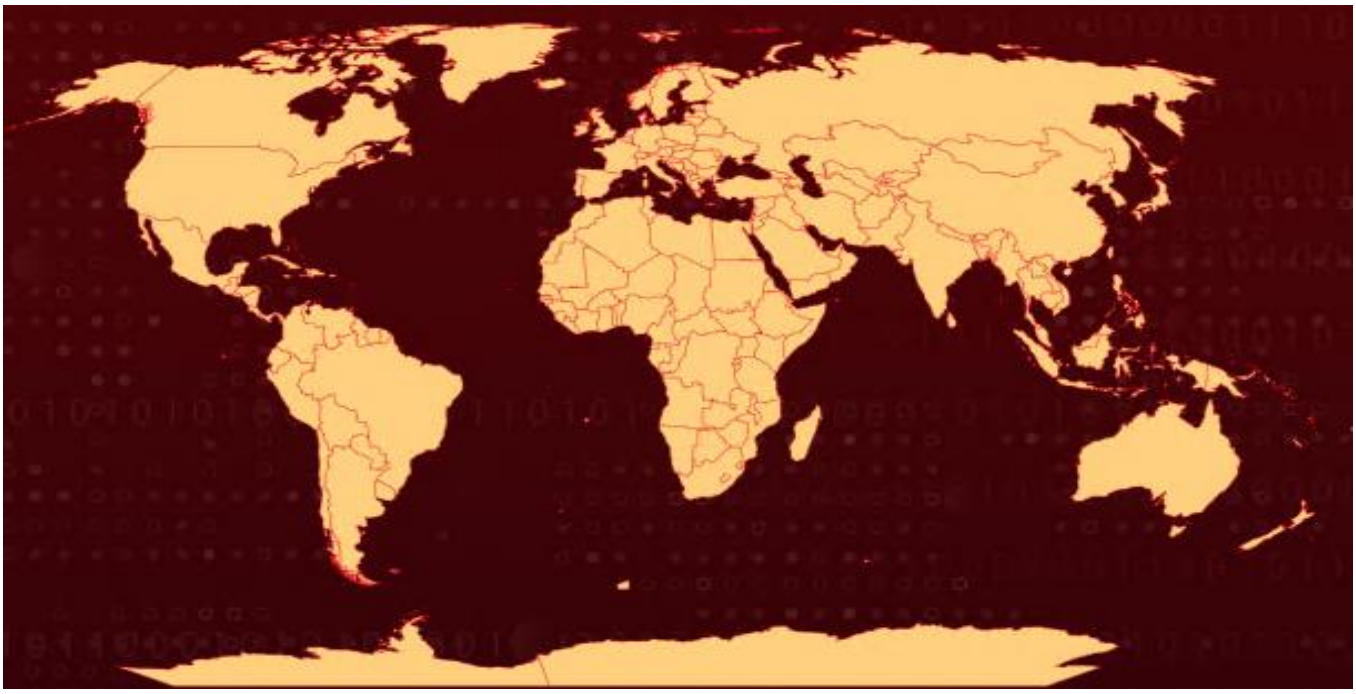


Figure 3: Scope of the Lockbit Ransomware Group

CVE	Name	Affected Products
CVE-2023-0669	Fortra GoAnywhere MFT Remote Code Execution Vulnerability	Fortinet FortiOS SSL VPN Path Traversal Vulnerability
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF/NG
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2
CVE-2021-22986	F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability	F5 BIG-IP and BIG-IQ Centralized Management
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability	Microsoft Netlogon
CVE-2019-0708	Microsoft Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Remote Desktop Services
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS

Details:

1. LockBit Ransomware has been one of the most widespread and active variants in the world, with collaborators targeting organizations across various critical infrastructure sectors. LockBit operates as a Ransomware-as-a-Service (RaaS) model, where collaborators are recruited to carry out attacks using LockBit's tools and infrastructure. The tactics, techniques, and procedures (TTPs) used by LockBit's collaborators vary significantly, presenting a challenge for organizations attempting to protect against ransomware.
2. Ransomware has gone through several stages, including LockBit 2.0, LockBit 3.0 and LockBit Green, each with its own improvements and features.
3. LockBit has gained popularity among affiliates by providing multiple payouts. They have also engaged in activities to generate publicity and developed an easy user interface for their ransomware, making it accessible to individuals who do not have much knowledge about this technique.
4. LockBit is responsible for a significant percentage of ransomware incidents in various countries, such as Australia, Canada, New Zealand, and the United States. Payments made to LockBit by victims in the US alone have reached approximately $91 million as of 2020. LockBit activity has been reported since 2020 in various countries, and the latest cases were reported in May 2023. LockBit Associates have used legitimate freeware and open source tools for malicious purposes.
5. They also exploited old and new security vulnerabilities, such as CVE-2021-22986, CVE-2023-0669, CVE-2023-27350, CVE-2021-44228, CVE-2020-1472, CVE-2019 -0708 and CVE-2018-13379. After successfully attacking an organization, LockBit associates attempt to carry out extortion with Ransomware targeting the organization's customers or other networks connected to it.

Recommendations:

Implement Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with LockBit ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against threats.

Software Update: Keep all operating systems, applications and firmware up to date with security patches. LockBit collaborators often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can reduce the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Back Up Data and Test Recovery: Implement a data backup strategy that includes regular backups of critical data and systems. Ensure that copies are stored offline or in a secure and isolated environment to prevent them from being compromised in the event of an attack. Test the restore process regularly to verify the integrity and availability of the copies. In the event of a ransomware attack by LockBit, if you have a copy of your data you will be able to recover your systems and data without paying a ransom.

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1219 Remote Access Software	T1562.001 Disable or Modify Tools
T1562 Impair Defenses	T1482 Domain Trust Discovery	T1072 Software Deployment Tools	T1003 OS Credential Dumping
T1071 Application Layer Protocol	T1071.002 File Transfer Protocols	T1567.002 Exfiltration to Cloud Storage	T1567 Exfiltration Over Web Service
T1095 Non-Application Layer Protocol	T1003.001 LSASS Memory	T1555.003 Credentials from Web Browsers	T1555 Credentials from Password Stores
T1572 Protocol Tunneling	T1082 System Information Discovery	T1219 Remote Access Software	T1046 Network Service Discovery
T1021.001 Remote Desktop Protocol	T1021 Remote Services	T1219 Remote Access Software	T1071.001 Web Protocols
T1048 Exfiltration Over Alternative Protocol	T1189 Drive-by Compromise	T1190 Exploit Public-Facing Application	T1133 External Remote Services
T1566 Phishing	T1078 Valid Accounts	T1059.003 Windows Command Shell	T1059 Command and Scripting Interpreter
T1072 Software Deployment Tools	T1569.002 Service Execution	T1569 System Services	T1547 Boot or Logon Autostart Execution
T1548 Abuse Elevation Control Mechanism	T1484 Domain Policy Modification	T1484.001 Group Policy Modification	T1480.001 Environmental Keying
T1480 Execution Guardrails	T1070.004 File Deletion	T1027 Obfuscated Files or Information	T1027.002 Software Packing
T1562 Impair Defenses	T1046 Network Service Discovery		

Figure 4: Lockbit Group Techniques, Tactics, Procedures

Indicators of compromise:

HASH	VALUE
SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194 498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f af4c28fb1c65ebe93181b67d279733e864cafab5919a7aa7eced93fc8113df16 984d96730ae19d4532325c6fcbd34580fb02fbe454781b589d2eea6090ea2b6d 2cee882bd0dc4267bacf099ac4571c319ac547be12b955f7ccb2f0144ae40876 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c 5a13ac97ce91d5b095c7154fe756615fa0730c17ddf432ae4af6c42d2c29946d 9aa5bcee06109d52fade97ad21317ff951abc656ba4c800441bacfec00328fd8 379c4620d6f482e153d7033bba21da5d8027387c0e60e3497b63d778dcafd888 0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194 b964a5253c25465633ef8c2e7f77703d27227bfc0b13a7ca49d187dadc4d38ae ba0eefdfbd1421d37d47f3feaae8e768a4679d6b544bb97f5237319e8ab0b122 f9dbdb825067616070c64565b6b27dc872c4a7219856eb5f8eb3eb1eb1463423 2e218735fa53e036659ea721bfd7b97e2af67b7eda648e9e2579356eb20899d9 1f0e4cbc1a4b52b6d7e4188e4a835a904cf783c75db9a066df4201452bd9647d de7f501e4a17898e85229b962e2f43b9a20d995c8a9fe0cad4536adc8fbd9f48 8989a9aec8d2c4d61fa399a97807f8e62814b1a55fecbd38d11d4d35fdf4a7d1 01bf78841b63bcdd8280157c486b45ad74811c0251140a054de81a925ce7f716 ab4d20b73c7358f1e3a60145d5debc791a17416e2a88eb39f80ec1f53985fad5 9366a5b8021d0283156986bbf020c99ae5e2a3dcbbaa03db934e94bfa7088b86 4bdda7dd3bbe1f9cb0a7d42f6947ba0f6442e52758bd2638541f9409b573d5c9 6b4502d8ba3cff1a3139f72cdad863d53551b65b8c38d7b838d64212822e4630 4d0f95028bb6a04e64550872ddeef6b0c6fa4a5bd368736da47401420df2bee7 cfc45c36b4c731f2308e19a087c3dc3fb7b12eef93e171e8e86e2134ead325ee 4134d5d8f7b038e23e7887db56bb3ad295341a1aaf0bebe6be21d901d06dd662 153fc9e90b955e2cfaf91b86888a29fdd8685144a3802f5e90b95b64116cdd33 00accc2c186201607d3e36c1b013872ac51d4f805f23e625dc70154fb58fd4f4 48a0366841e2f59b533510f532b220458d3fd489efc4b71d00d2b9429b292fb9 149d691411f10f8ec7af43f0237ccfab5b65a9ae73718acf1e0cc0dbdea36ebd cb83eb6f5fd42f59b1c1a34826df48e5a5882c45e4a7f34c80c0830c26cb30dd 4d4bc9d78db93c25548a679de06e267363a31a400e2e37caf9d1fce91b65fe8d b9872ad6ec82d3f2f9a8c6af7e5838f91712e52ece265cd04f4452378bd5bcfd a8939a43feb8cc258507ffd0be564d56a2874c220729e00da8ad204c3b4012c5

	fef1f9664fde9b23754c691b15a05fdc35a51a0ceb8a18fb9a5a0166e6377c69 fef1f9664fde9b23754c691b15a05fdc35a51a0ceb8a18fb9a5a0166e6377c69 734955fdb84b29fa1aa87aa0af2ebf155125917a6b61ffe4b4dc7030dd212309 e47b928d0fc16348b828abeb3c2106a6d752512f60ef4583d6532cc0dbebebbf 239c9969fd07e1701a129cfd033a11a93ee9e88e4df4f79b7c5c0dd5bba86390 a439c5093801d3b12e2f79b64c0b65bdf148eb6eca8c1e3d179af5ab4995034d 54ac7ac6db6fcec5234454430513d1d2787ee8a48aa60fbf95c1af27534fdb4a A9abab8ab44ccec6321da83d9960a1f30ba783e02b6e0ba3f2e9d19cee76b39b 286726ecca68f8c2752116258aba0cd35c051a6342043ee1add84b890654276f

DNSpionage Group

State Sponsored DNSpionage group from **Iran,** uses DNS Hijacking, and injects "remote access trojan", phishing emails with Excel document attached. This group also collaborates with OilRig, APT34, Helix Kitten, Chrysene. Tools used: DNSpionage, Karkoff.

DNSpionage, the set of risk activities attributed to **APT34**, has been observed using an updated version of the Karkoff backdoor, using Microsoft Exchange servers in compromised environments to communicate with C2. This version of Karkoff mainly relies on the victim's Exchange Server to gather important information from the targeted inbox.

Indicators of compromise:

HASH
1f47770cc42ac8805060004f203a5f537b7473a36ff41eabb746900b2fa24cc8
27e03b98ae0f6f2650f378e9292384f1350f95ee4f3ac009e0113a8d9e2e14ed
82285b6743cc5e3545d8e67740a4d04c5aed138d9f31d7c16bd11188a2042969
097e5c804b16974c6b8442c4ab0bee5a4f492e2ab98080c9e3f64e1f596c3165
559d9d8bf66fdcfed078d636c1e5e94a
b1d621091740e62c84fc8c62bcdad07873c8b61b83faba36097ef150fd6ec768
ba2ed97dd5673e07dfc4b1ab8153d4fb25fafc04
d6b876d72dba94fc0bacbe1cb45aba493e4b71572a7713a1a0ae844609a72504
f91c5250b33fc5f95495c5e3d63b5fde7ca538178feb253322808b383a26599d
2943e69e6c34232dee3236ced38d41d378784a317eeaf6b90482014210fcd459
07e791d18ea8f2f7ede2962522626b43f28cb242873a7bd55fff4feb91299741

Malware	Karkoff
	DNSpionage
organizations	APT34 OilRig (Cobalt Gypsy, Helix Kitten, Timberworm, Twisted Kitten)
Hash	d6b876d72dba94fc0bacbe1cb45aba493e4b71572a7713a1a0ae844609a72504

	f91c5250b33fc5f95495c5e3d63b5fde7ca538178feb253322808b383a26599d
	1f47770cc42ac8805060004f203a5f537b7473a36ff41eabb746900b2fa24cc8
Attack vectors	C&C Server
Malware category	Backdoor

BackDoor Diplomacy (BackDip)

The BackdoorDiplomacy group, otherwise known as BackDip, Quarian, CloudComputation exploits CVE-2020-5902, CVE-2021-26855 (Microsoft Exchange Server Remote Code Execution Vulnerability, to infect with "backdoor: – malicious programs inside servers.
BackdoorDiplomacy targets the telecommunications industry in the Middle East. For the first time it appeared in 2017.

Some of the other target countries are: Albania, Croatia, Georgia, Germany, Ghana, India, Libya, Namibia, Nigeria, Poland, Saudi Arabia, South Africa, Sri Lanka, United Arab Emirates and Uzbekistan. The main target sectors are governments and telecommunications.

Figure 5: Backdoor Diplomacy Group's geographic reach.

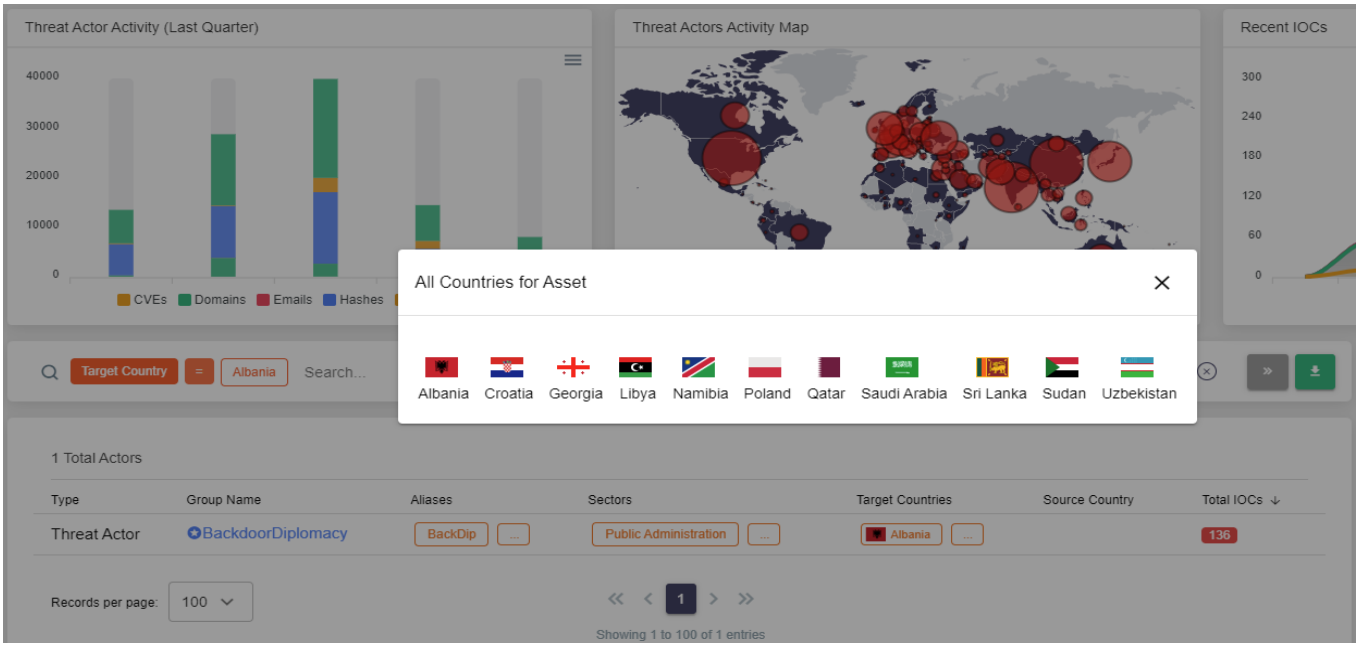


Figure 6: Countries targeted by this group.

The details:

Origin	Motive	Target regions	Target industries
China	Information Theft and Espionage	Albania, Croatia, Georgia, Germany, Ghana, India, Libya, Namibia, Nigeria, Poland, Saudi Arabia, South Africa, Sri Lanka, United Arab Emirates and Uzbekistan	Governments and Telecommunications

Recommendations:

Develop simulations of phishing attacks, implement training and raise awareness of the use of Multifactor Authentication (MFA).

Use priorities and block all indicators attributed to the risk actor through your monitoring center. Do your testing by simulating the attack.

Refer to and act upon the MITER ATT&CK Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IoC) presented below.

TA0042 Resource Development	**TA0001** Initial Access	**TA0005** Defense Evasion	**TA0007** Discovery
TA0009 Collection	**TA0010** Exfiltration	**TA0011** Command and Control	**TA0040** Impact
T1190 Exploit Public-Facing Application	**T1574** Hijack Execution Flow	**T1574.001** DLL Search Order Hijacking	**T1105** Ingress Tool Transfer
T1074 Data Staged	**T1074.001** Local Data Staging	**T1036** Masquerading	**T1036.004** Masquerade Task or Service
T1588 Obtain Capabilities	**T1588.001** Malware	**T1082** System Information Discovery	**T1560** Archive Collected Data

Figure 7: Backdoor Diplomacy Group Techniques, Tactics, Procedures

Indicators of compromise:

HASH
06faa40b967de7168d16fec0519b77c5e319c6dc021578ed1eb8b337879018fe
eff22d43a0e66e4df60ab9355fa41b73481faea4b3aa6905eac3888bc1a62ffa
bbcd7dc60406a9fa439d183a10ad253426bae59424a0a1b91051d83d26bb0964
9d167adc290de378071c31cfd8f2059523e978c6f14a7079157d564f976c544b
e2589f9942e9ec6b9c385fec897ffc3a71fcd8d7e440e3302efc78760c40f926
c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e
ec6fcff9ff738b6336b37aaa22e8afa7d66d9f71411430942aed05e98b3f4cd5
a43a4cd9c2561a4213011de36ac24ee1bf587663ed2f2ae1b1eac94aa2d48824
7ed44a0e548ba9a3adc1eb4fbf49e773bd9c932f95efc13a092af5bed30d3595
f293ab13a04ff32ebfbe925b42eca80a57604d231ae36e22834bea0dbdcf26e2
d1948085fc662f7aed592af2eab9f367b3040bba873fec24b939395515f54a83
99f31526fa18dc8c5f09b212909a9df889ea0bc3da979e4892666d626cc4aaf0
07e8b2c8cf5fcdbd29cf864cda3c5c2df3999c35a5da28a18af5dedd5f1db60a
6373ee72c811cf77a46e0cffd3c8f83d02173946b714d946e4c4c91cef41685f
d583189d66b0aa09405a0ed2440c72f741caedb250525be2b17a1f9616fab9e6
99e62952f66b487349493657d6aec8456afef0fb72aad084c388677912210bf9
b87580211c1748c7f223d6bfc96cd8eca5a19022758d964b40612639dfbe147d
363a2006c8faff9e533093d1562028c4b53d5be52028bb91259debc472399c9b

7c92d3754c6278636ff980a3b3ef6bd9b817eeeb7fc8524034858e1148acf116 132d9ce88304ec29c10c7744c81746de8be7a205b9c8dbdfb42b058bcc34ccd1
e52028bb91259debc472399c9b,7c92d3754c6278636ff980a3b3ef6bd9
b817eeeb7fc8524034858e1148acf116,132d9ce88304ec29c10c7744c81
746de8be7a205b9c8dbdfb42b058bcc34ccd1

IP
185.80.201[.]87
140.82.38[.]177
103.152.14[.]162
152.32.181[.]55
192.155.86[.]128
199.247.19[.]24
208.85.23[.]64
70.34.248[.]149
136.244.112[.]39
43.251.105[.]139

DOMAIN
cloud.microsoftshop[.]org
info.fazlollah[.]net
info.payamradio[.]com
mail.irir[.]org
news.alberto2011[.]com
picture.efanshion[.]com
plastic.delldrivers[.]in
proxy.oracleapps[.]org
srv.fazlollah[.]net
srv.payamradio[.]com
uc.ejalase[.]org

Evilnum Group

Evilnum is also known by the names *Jointworm, Knockout Spider, TA4563 and DeathStalker*. It targets cryptocurrency exchange and forums. In recent campaigns, the Evilnum actor group has targeted the Finance sector using the Evilnum malware. One of Evilnum's backdoor tactics uses a variety of *ISO, Microsoft Word, and Shortcut (.LNK*) files. Also, malware is used for espionage, data theft and the placement of further malicious files. The espionage group uses spearphishing campaigns by attaching OneDrive URLs and .LNK files inside emails.

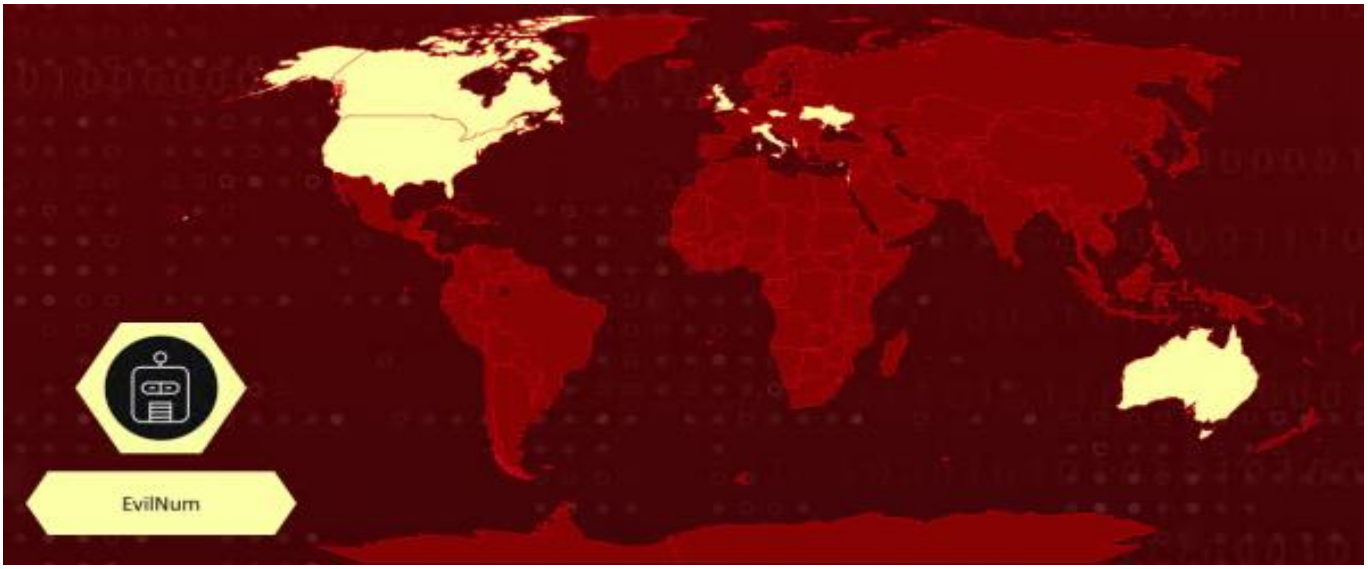


Figure 8: Geographical scope of the Evilnum Group

General details

Origin	Motive	Target regions	Target industries
Unidentified	Information Theft and Espionage	Albania, Australia, Belgium, Canada, Cyprus, Czech Republic, Israel, Italy, United Kingdom, Ukraine and United States of America	Financial Sector, Governments, Sales Sector and Media

Technical Details:

1. The Evilnum actor group targets victims with spear phishing emails that include a link to a ZIP file. The actor uses monetary incentives to convince the recipient to share EvilNum's file.
2. The payload is used to decrypt and restart the infection chain. Once the antivirus on the target endpoint is compromised, it dynamically loads the C# code and sends the screenshot to the Command and Control server (C2).

TA0003 Persistence	**T1547** Boot or Logon Autostart Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
T1140 Deobfuscate/Decode Files or Information	**T1027** Obfuscated Files or Information	**TA0001** Initial Access	**T1566** Phishing
TA0002 Execution	**T1059** Command and Scripting Interpreter	**TA0007** Discovery	**T1057** Process Discovery

Figure 9: Evilnum Group Techniques, Tactics, Procedures

IOCs:

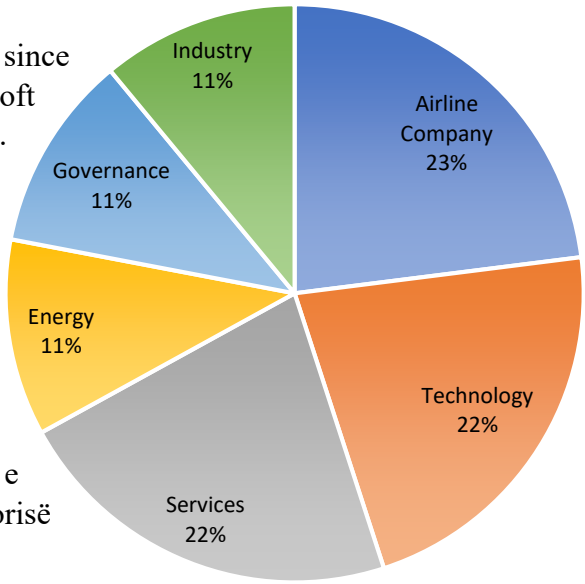
Type	Value
SHA256	ef1a660ee8b11bbcf681e8934c5f16e4a249ba214d743bbf8b1f804 3296b6ffc da642cc233ea3595d8aaf8daf6129c59682b19462d5d5abb1f4940 42d4c044f4 53ade63ba9938fd97542a0a725d82045f362766f24f0b1f414f4693 d9919f631 f0a002c7d2174f2a022d0dfdb0d83973c1dd96c4db86a2b687d145 61ab564daa 53ade63ba9938fd97542a0a725d82045f362766f24f0b1f414f4693 d9919f631 649183519d59ea332d687a01c37040b91da69232aadb0c1215c36 a5b87ad2ec7
Domain	bookingitnow[.]org bookaustriavisit[.]com moretraveladv[.]com estoniaforall[.]com
Email	viktoria.helle79@zingamail[.]uk paul@christiesrealestate[.]uk sherry@schalapartners[.]com arfeuille19@gmail[.]com arole@delaware-north[.]com
URL	hxxp://officelivecloud[.]com hxxp://mailgunltd[.]com hxxp://officelivecloud[.]com hxxp://visitaustriaislands[.]com hxxp://outlookfnd[.]com hxxp://infntio[.]com/save/user.php hxxp://advflat[.]com/save/user.php hxxp://pngdoma[.]com/admin/index.php hxxp://goalrom[.]com/admin/settings.php hxxp://elitefocuc[.]com/save/user.php hxxp://hubflash[.]co/configuration.php hxxps://onedrive.live[.]com/download?resid= 680BC877518B4D11%21388&authkey=!AMMjaIOZSltiS_Q hxxps://onedrive.live[.]com/download?resid= 680BC877518B4D11!531&authkey=!ADr0ziYEPBJJK9w hxxps://onedrive.live[.]com/download?resid= 680BC877518B4D11!426&authkey=!AB60IPFY2E-XMXs

Ke3Chang,Vixen Panda, Gref, Playful, Dragon Groups

Also known as VIXEN PANDA, APT 15, Playful Dragon, Metushy, Lurid, Social Network Team, Royal APT, BRONZE PALACE, BRONZE DAVENPORT, BRONZE IDLEWOOD, NICKEL, G0004, Red Vulture, are State-Sponsored groups of Chinese origin whereas the main technique uses phishing attacks to compromise the financial networks of European governments or foreign ministries for espionage purposes.

Ke3chang is a group that has been operating since 2004, and over time the tools they use have come and gotten more sophisticated. Despite their Chinese origins, they are suspected of operating outside of China since 2010.

A backdoor called ***Backdoor.Graphican*** has been identified since late 2022 to early 2023 by this group leveraging the Microsoft Graph API for Command and Control (C&C) communication.



Percentage of attacks on industries by the Ke3chang group.

Fillimisht synimi i tyre ishin organizatat qeveritare, misionet diplomatike dhe organizatat joqeveritare për të marrë sa më shumë informacione.

Nga analizimet e bëra nuk shihet të ketë IP C2 të implementuar në kodin e saj, por në vend të IP ajo lidhet me *OneDrive* përmes Microsoft Graph API nga ku merr adresën e enkriptuar të serverit C2 dhe e dekripton brenda direktorisë "Person".

After accessing the computer, Graphican behaves as follows:

1) Disables Internet Explorer 10 launch page through registry switches.
2) Checks if the iexplorer.exe process is running.
3) Creates an IWebBrowser2 COM object to access the Internet
4) Authenticates to the Microsoft Graph API to receive an access token.
5) Using the Graph API it analyzes all subdirectories of the 'Person' directory in OneDrive.
6) Gets the folder names and decrypts them so that C2 can be accessed.
7) Generates a BOT ID based on the hostname, and local IP, Windows version and language the system uses, as well as other data whether the system is 32 or 64 bit.
8) Logs the data to the C2 server, in the format 'f@@@%s###%s###%s###%d###%ld###%s' based on the data collected above.

Some of the commands that the C2 server can execute:

1) 'C' - Creates an interactive command shell commanded by C2.
2) 'U' – Creates a file on the victim's computer.
3) 'D' - Downloads files from the victim's computer to C2
4) 'N' - Creates a new background process.
5) 'P' – Creates a new Powershell process in the background and saves the results to a file in the TEMP directory from where it then sends them to the C2 server.

Backdoor.Graphican is a more sophisticated version of **Ketrican,** another tool used by Ke3chang**.**

Other tools:

EWSTEW – a backdoor used to extract emails sent or received on an infected Microsoft Exchange server.

Mimikatz,Pypykatz, Safetykatz – tools that are used to steal credentials.

Lazagne – An Open Source tool used to steal passwords from programs.

Quarks PwDump – Another Open Source tool that uses different ways to get credentials from the local user, or from domain users.

SharpSecDump – Serves to get SAM and LSA Secrets.

K8Tools – Widely used to escalate privileges.

Ehole – Tool which is used to identify vulnerabilities in the system.

Exploitation of vulnerability **CVE-2020-1472** – otherwise known as *ZeroLogion*, which is about privilege escalation which allows the hacker to compromise the Domain Controller.

TA0003 Persistence	**TA0011** Command and Control	**TA0005** Defense Evasion	**TA0002** Execution
TA0007 Discovery	**TA0001** Initial Access	**TA0009** Collection	**TA0008** Lateral Movement
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	**T1547.001** Registry Run Keys / Startup Folder	**T1547** Boot or Logon Autostart Execution	**T1082** System Information Discovery

Figure 9: : Techniques, Tactics, Procedures of groups Ke3Chang, Vixen Panda, Gref, Playful, Dragon

IOCs:

Type	Value
IP	172.104.244[.]187 50.116.3[.]164
DOMAIN	www.beltsymd[.]org www.cyclophilit[.]com www.cyprus-villas[.]org www.perusmartcity[.]com www.verisims[.]com
SHA256	4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5 a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8 02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5 617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd 858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253 fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476 177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf 8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286 865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48 d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30 bf4ed3b9a0339ef80a1af557d0f4e031fb4106a04b0f72c85f7f0ff0176ebb64 5600a7f57e79acdf711b106ee1c360fc898ed914e6d1af3c267067c158a41db6

	f06692b482d39c432791acabb236f7d21895df6f76e0b83992552ab5f1b43c8d af4a10cbe8c773d6b1cfb34be2455eb023fb1b0d6f0225396920808fefb11523 548ce27996e9309e93bf0bd29c7871977530761b2c20fc7dc3e2c16c025eb7bc 9829c86fab4cbccb5168f98dcb076672dc6d069ddb693496b463ad704f31722e 18560596e61eae328e75f4696a3d620b95db929bc461e0b29955df06bc114051 f6f57fc82399ef3759dcbc16b7a25343dea0b539332dacdf0ed289cc82e900db df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f c559eb7e2068e39bd26167dd4dca3eea48e51ad0b2c7631f2ed6ffcba01fb819 7d93862c021d56b4920cab5e6cb30a2d5fb21478e7158f104e520cc739a1678d 17a63ccd749def0417981c42b0765f7d56e6be3092a1f282b81619ca819f82ef b42f9571d486a8aef5b36d72c1c8fff83f29cac2f9c61aece3ad70537d49b222 bff65d615d1003bd22f17493efd65eb9ffbfe9a63668deebe09879982e5c6aa8 ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56 e7a6997e32ca09e78682fc9152455edaa1f9ea674ec51aecd7707b1bbda37c2f 07fc745c29db1e2db61089d8d46299078794d7127120d04c07e0a1ea6933a6df 42379bb392751f6a94d08168835b67986c820490a6867c28a324a807c49eda3b a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86 e25cc57793f0226ff31568be1fce1e279d35746016fc086a6f67734d26e305a0 617af8e063979fe9ca43479f199cb17c7abeab7bfe904a2baf65708df8461f6d dc2423e21752f431ce3ad010ce41f56914e414f5a88fd3169e78d4cc08082f7b f653e93adf00cf2145d4bfa00153ae86905fe2c2d3c1f63e8f579e43b7069d51 65436d5646c2dbb61607ed466132302f8c87dab82251f9e3f20443d5370b7806 44c1c5c92771c0384182f72e9866d5fed4fda896d90c931fe8de363ed81106cf 7fa350350fc1735a9b6f162923df8d960daffb73d6f5470df3c3317ae237a4e6 9a94483a4563228cb698173c1991c7cf90726c2c126a3ce74c66ba226040f760 f4575af8f42a1830519895a294c98009ffbb44b20baa170a6b5e4a71fd9ba663 2da9a09a14c52e3f3d8468af24607602cca13bc579af958be9e918d736418660 d21797e95b0003d5f1b41a155cced54a45cd22eec3f997e867c11f6173ee7337 31529b8b86d4b6a99d8f3b5f4b1f1b67f3c713c11b83b71d8df7d963275c5203 7d3f6188bfdde612acb17487da1b0b1aaaeb422adc9e13fd7eb61044bac7ae08 2b60e49e85b21a439855b5cb43cf799c1fb3cc0860076d52e41d48d88487e6d8 819d0b70a905ae5f8bef6c47423964359c2a90a168414f5350328f568e1c7301 7aa10e5c59775bfde81d27e63dfca26a1ec38065ddc87fe971c30d2b2b72d978

RECOMMENDATIONS

Implement the latest system and endpoint updates. Use anti-malware programs to protect yourself from malicious programs. Monitor traffic in real time to detect anomalies.

Fortify your network with devices such as Firewalls, IPS, and Secure Web Gateways to reduce the risk of being threatened by malicious actors.

MuddyWater Group

MuddyWater Group, Iranian state-sponsored group, also known as *Static Kitten, Earth Vetala, Mercury, Seedworm, and Temp.Zagros,* which started in 2017 with espionage and information theft, aims to attack state organizations of telecommunications, defence, local governments, hydrocarbon, gas industries or critical infrastructure.

Usually, **MuddyWater** uses a number of malware variants such as PowGoop, Small Sieve, Canopy or Starwhale, Mori and Powerstats.

Geographical extent of the Muddy Water Group

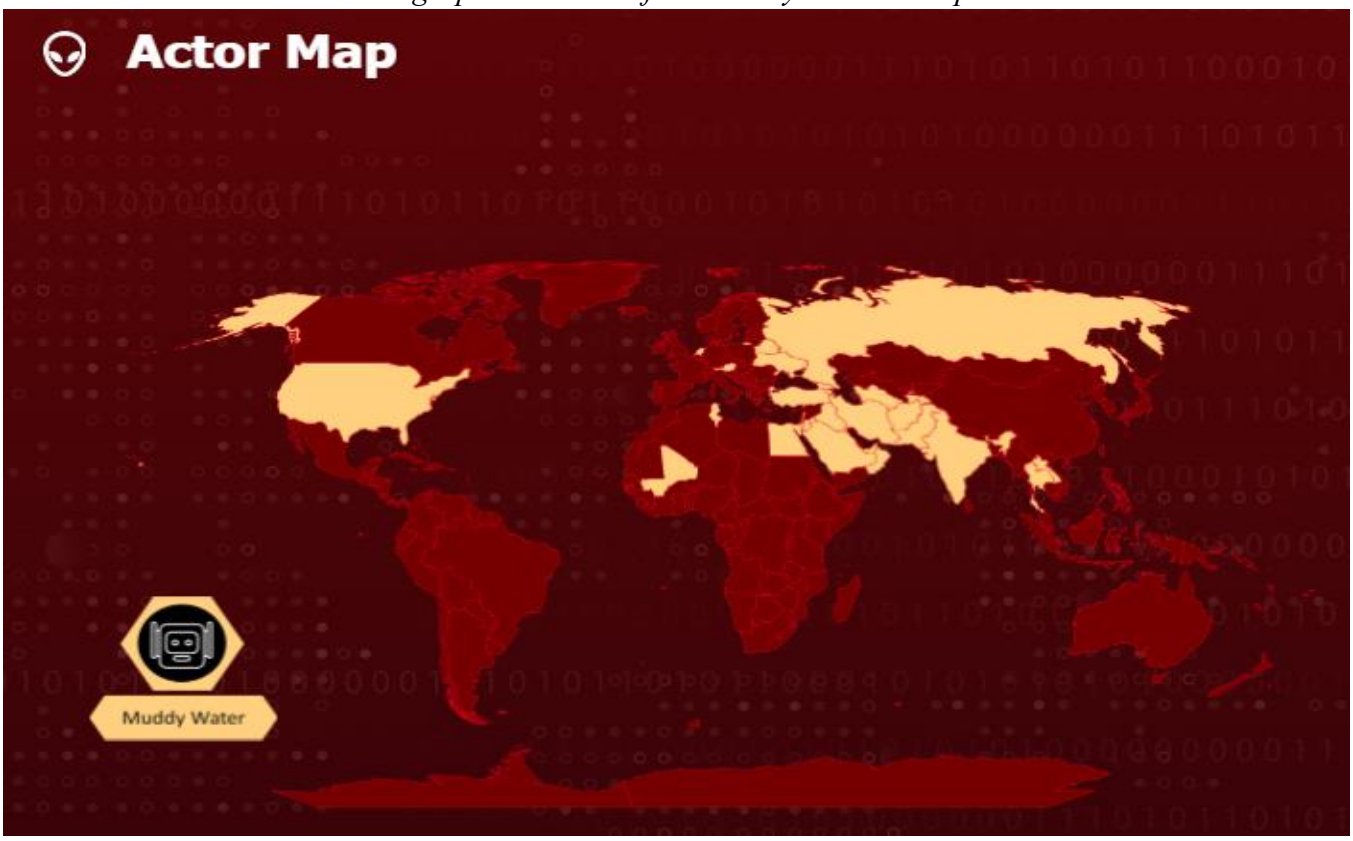


Figure 10: Geographical extent of the Muddy Water Group

Name	Origine	The regions where they attack	Industries it attacks
MuddyWater (Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, ATK 51, Cobalt Ulster, T-APT-14,)	Iran Motive Information theft and espionage	Albania, United States, Libya, Egypt, Armenia, Syria, Sweden, United Arab Emirates, Lebanon, India, Russia Netherlands, Saudi Arabia, Iraq etc.	State Industries, Media, Transport Organizations, Hydrocarbon Industries Critical infrastructures etc.

TA0042 Resource Development	TA0001 Initial Access	TA0011 Command and Control	T1566 Phishing
T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1219 Remote Access Software	T1588 Obtain Capabilities
T1588.002 Tool	T1583 Acquire Infrastructure	T1583.006 Web Services	

Figure 11: Muddywater Group Techniques, Tactics, Procedures

Other Techniques:

T1589.002 Gather Victim Identity Information: Email Addresses
T1583.006 Acquire Infrastructure: Web Services
T1588.002 Obtain Capabilities: Tool
T1566.001 Phishing: Spearphishing Attachment
T1566.002 Phishing: Spearphishing Link
T1047 Windows Management Instrumentation
T1059.001 Command and Scripting Interpreter: PowerShell
T1059.003 Command and Scripting Interpreter: Windows Command Shell
T1059.005 Command and Scripting Interpreter: Visual Basic
T1059.006 Command and Scripting Interpreter: Python
T1059.007 Command and Scripting Interpreter: JavaScript
T1203 Exploitation for Client Execution
T1204.001 User Execution: Malicious Link
T1204.002 User Execution: Malicious File
T1559.001 Inter-Process Communication: Component Object Model
T1559.002 Inter-Process Communication: Dynamic Data Exchange
T1053.005 Scheduled Task/Job: Scheduled Task
T1137.001 Office Application Startup: Office Template Macros
T1543.003 Create or Modify System Process: Windows Service
T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1547.005 Boot or Logon Autostart Execution: Security Support Provider
T1134 Access Token Manipulation
T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control
T1555 Credentials from Password Stores
T1555.003 Credentials from Web Browsers

T1027 Obfuscated Files or Information
T1027.003 Steganography
T1027.004 Compile After Delivery
T1027.005 Obfuscated Files or Information: Indicator Removal from Tools
T1036.005 Masquerading: Match Legitimate Name or Location
T1055.001 Process Injection: Dynamic-link Library Injection
T1055.002 Process Injection: Portable Executable Injection
T1140 Deobfuscate/Decode Files or Information
T1218.003 Signed Binary Proxy Execution: CMSTP
T1218.005 Signed Binary Proxy Execution: Mshta
T1218.011 Signed Binary Proxy Execution: Rundll32
T1480 Execution Guardrails
T1562.001 Impair Defenses: Disable or Modify Tools
T1574.001 Hijack Execution Flow: DLL Search Order Hijacking
T1574.002 Hijack Execution Flow: DLL Side-Loading
T1574.007 Hijack Execution Flow: Path Interception by PATH Environment Variable
T1574.008 Hijack Execution Flow: Path Interception by Search Order Hijacking
T1574.009 Hijack Execution Flow: Path Interception by Unquoted Path
T1003.001 OS Credential Dumping: LSASS Memory
T1003.004 OS Credential Dumping: LSA Secrets
T1003.005 OS Credential Dumping: Cached Domain Credentials
T1552.001 Unsecured Credentials: Credentials In Files
T1552.002 Unsecured Credentials: Credentials in Registry
T1552.006 Unsecured Credentials: Group Policy Preferences
T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting
T1005 Data from Local System
T1012 Query Registry
T1016 System Network Configuration Discovery
T1033 System Owner/User Discovery
T1049 System Network Connections Discovery
T1057 Process Discovery
T1082 System Information Discovery
T1083 File and Directory Discovery
T1087.002 Account Discovery: Domain Account
T1482 Domain Trust Discovery
T1518 Software Discovery
T1518.001 Security Software Discovery
T1056.001 Input Capture: Keylogging
T1113 Screen Capture
T1123 Audio Capture
T1560.001 Archive Collected Data: Archive via Utility

T1071.001 Application Layer Protocol: Web Protocols
T1090.002 Proxy: External Proxy
T1102.002 Web Service: Bidirectional Communication
T1104 Multi-Stage Channels
T1105 Ingress Tool Transfer
T1132.001 Data Encoding: Standard Encoding
T1132.002 Data Encoding: Non-Standard Encoding
T1219 Remote Access Software
T1572 Protocol Tunneling
T1041 Exfiltration Over C2 Channely

Exploitation of vulnerabilities

CVE-2021-44228 - SysAidCloud versions prior to version 22.1.10
CVE-2021-45046 - SysAidOn-premises versions before 21.4.45
CVE-2021-44228 - Apache Log4j2 Vulnerability
CVE-2021-45046 - Apache Log4j2 Vulnerability
CVE-2020-1472 - Microsoft Window Netlogon privilege escalation
CVE-2021-34527 - Microsoft Exchange Memory Corruption Vulnerability

RECOMMENDATIONS

To counter this group's attacks or to avoid attacks, IoC blocking measures should be taken, as well as updating where the aforementioned CVEs may be affected. Also have continuous traffic monitoring against the above **IoC** factors as they may change as the case may be.

IOCs:

MD5
b0ab12a5a4c232c902cdeba421872c37
e182a861616a9f12bc79988e6a4186af
cb84c6b5816504c993c33360aeec4705
e1f97c819b1d26748ed91777084c828e
0431445d6d6e5802c207c8bc6a6402ea
15fa3b32539d7453a9a85958b77d4c95
5763530f25ed0ec08fb26a30c04009f1
f21371716c281e38b31c03f28d9cc7c0
817ab97c5be4f97a3b66d3293e46adc7
366910fc6c707b5a760413dd4ab0c8e9
fbacc4e15a4c17daac06d180c6db370e
59629ec48fec4c8480a9b09471815ad5

325493b99c01f442200316332b1d0b4c
218d4151b39e4ece13d3bf5ff4d1121b
a65696d6b65f7159c9ffcd4119f60195
a27655d14b0aabec8db70ae08a623317
cec48bcdedebc962ce45b63e201c0624
c0c2cd5cc018e575816c08b36969c4a6
37fa9e6b9be7242984a39a024cade2d5
64fc017a451ef273dcacdf6c099031f3
3c2a436c73eeb398cfc0923d9b08dcfe
2ec61c8b7e57126025ebfdf2438418fc
d632c8444aab1b43a663401e80c0bac4
ff46053ad16728062c6e7235bc7e8deb
d15aee026074fbd18f780fb51ec0632a
fbe65cd962fc97192d95c40402eee594
ee2d1e570be5d53a5c970339991e2fd7
2c3d8366b6ed1aa5f1710d88b3adb77d
1d6f241798818e6fdc03015d01e1e680ü
b07d9eca8af870722939fd87e928e603
b44ccd6939bdbc8f61c9e71a128b2613
692815cce754b02fe5085375cab1f7b2
851f083d29c5f8f411a7ad0392c4496c
8b3da6c97a53188e4af2d404dea654b6
6c303f68b97b72100637735cd2150393
cf5c526d50a385ba289c08affbdc85ed
d4259eb8e3b90ac08c9337df84468e87
6f44e57c81414355e3d0d0dafdf1d80e
1dae271ffc1841009104521e9c37e993
ed490e756b349443694d9a14952a0816
eed599981c097944fa143e7d7f7e17b1
21aebece73549b3c4355a6060df410e9
5c6148619abb10bb3789dcfb32f759a6
ddba713c20c232bcd60daf0ffabeffb8
e2ed0be977ab9e50055337ec8eb0ddf4
54982c616098f6c6fbc48703922f15f4
e6e7661efb60b9aea7969a30e17ace19
488723b8e56dbaac8ccdc79499037d5f
fa200e715e856550c76f729604ebaf57
837eaad1187fe9fbf91f9bc7c054f5d9
989e9dcc2182e2b5903b9acea03be11d
a750e2885ed3c294de148864723f73e3
ca9230a54f40a6a0fe52d7379459189c
5935522717aee842433a5de9d228a715
0cf25597343240f88358c694d7ae7e0a
44c900bd374ebce1aac1f1e45958f0fe

9533003c5f7c718951a3171da03844fb
3b6b74bf57746a31b7c8bdbb22282290
127bd5e7f11977a07428837a2d2fa9f1
b897fa2a9a3067dfd919cc27c269b203
8fbb83e448095d1c73ee1431abc15c80
24e1bd221ba3813ed7b6056136237587
37f7e6e5f073508e1ee552ebea5d200e
ffb8ea0347a3af3dd2ab1b4e5a1be18a
fdb4b4520034be269a65cfaee555c52e
7a2ff07283ddc69d9f34cfa0d3c936d4
9486593e4fb5a4d440093d54a3519187
b8939fa58fad8aa1ec271f6dae0b7255
665947cf7037a6772687b69279753cdf
801f34abbf90ac2b4fb4b6289830cd16
68e89d88b7cca6f12707d5a463c9d1d8
5bd61a94e7698574eaf82ef277316463
bf310319d6ef95f69a45fc4f2d237ed4
1de684f66a87cdf8485f95693d188596
3e6e37b381bf968c7718cb2323f275f8
ccb6108b7d29e8f3af6275c1256dd82e
c90e22b6579a3447836e299cbc5d0af0
a86249a392b394c803ddbd5bbaa0b4bb
ebc529b32422b6385b6ba3416c7afe13
9f00ac3bef01d2e3d8ebc48c3468d5c0
0873ddb4df8320b493a719bdddd7d182
b0a365d0648612dfc33d88183ff7b0f0
0e53da32937cb3718988026d9e96a5f0
135238bc43fddd0867676aef1e9aaf83
65c64c5aa55d3d78f08456cb20012fcf
2ded75ea4e55ed1dad579b9ce0eb01b2
d1b4ca2933f49494b4400d5bf5ab502e
aaa9db79b5d6ba319e24e6180a7935d6
2ed6ebaa28a9bfccc59c6e89a8990631
9486593e4fb5a4d440093d54a3519187
b8939fa58fad8aa1ec271f6dae0b7255
665947cf7037a6772687b69279753cdf
801f34abbf90ac2b4fb4b6289830cd16
68e89d88b7cca6f12707d5a463c9d1d8
5bd61a94e7698574eaf82ef277316463
bf310319d6ef95f69a45fc4f2d237ed4
1de684f66a87cdf8485f95693d188596
3e6e37b381bf968c7718cb2323f275f8
ccb6108b7d29e8f3af6275c1256dd82e
c90e22b6579a3447836e299cbc5d0af0

a86249a392b394c803ddbd5bbaa0b4bb
ebc529b32422b6385b6ba3416c7afe13
9f00ac3bef01d2e3d8ebc48c3468d5c0
0873ddb4df8320b493a719bdddd7d182
b0a365d0648612dfc33d88183ff7b0f0
0e53da32937cb3718988026d9e96a5f0
135238bc43fddd0867676aef1e9aaf83
65c64c5aa55d3d78f08456cb20012fcf
2ded75ea4e55ed1dad579b9ce0eb01b2
d1b4ca2933f49494b4400d5bf5ab502e
aaa9db79b5d6ba319e24e6180a7935d6
2ed6ebaa28a9bfccc59c6e89a8990631

SHA-256
026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141
c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e
d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0
ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418
3098dd53da40947a82e59265a47059e69b2925bc49c679e6555d102d1c6cbbc8
b75208393fa17c0bcbc1a07857686b8c0d7e0471d00a167a07fd0d52e1fc9054
bf090cf7078414c9e157da7002ca727f06053b39fa4e377f9a0050f2af37d3a2
f6569039513e261ba9c70640e6eb8f59a0c72471889d3c0eaba51bdebb91d285
7dc49601fa6485c3a2cb1d519794bee004fb7fc0f3b37394a1aef6fceefec0c8
450302fb71d8e0e30c80f19cfe7fb7801b223754698cac0997eb3a3c8e440a48
5cdc7dd6162a8c791d50f5b2c5136d7ba3bf417104e6096bd4a2b76ea499a2f4
fcdd38ff378605c66333429d9df2242fbce25a5f69f4d6d4c11d9613bcb409b0
a69fee382cf86f9e457e0688932cbd00671d0d5218f8043f1ee385278ee19c8c
2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82
b5b1e26312e0574464ddef92c51d5f597e07dba90617c0528ec9f494af7e8504
12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa
dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92
b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c
42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986
70cab18770795ea23e15851fa49be03314dc081fc44cdf76e8f0c9b889515c1b
468e331fd3f9c41399e3e90f6fe033379ab69ced5e11b35665790d4a4b7cf254
ccdddd1ebf3c5de2e68b4dcb8fbc7d4ed32e8f39f6fdf71ac022a7b4d0aa4131
3da24cd3af9a383b731ce178b03c68a813ab30f4c7c8dfbc823a32816b9406fb
6edc067fc2301d7a972a654b3a07398d9c8cbe7bb38d1165b80ba4a13805e5ac
af5f102f0597db9f5e98068724e31d68b8f7c23baeea536790c50db587421102
61072ae06a5e25194e7bf6297026b54ae52fcfc14787ead8866866d8098a1fa3
92bbd427ad2daf5644c5671b6dc369e02c00d03e4a13eadc2bb3025c0cdf3ec2

6d065532daab06c0b15c73d808c03b8497bb80fdd19c012bfc8771905f1f4066
b154d3fd88767776b1e36113c479ef3487ceda0f6e4fc80cef85ba539a589555
19ec3f16a42ae58ab6feddc66d7eeecf91d7c61a0ac9cdc231da479088486169
503b2b01bb58fc433774e41a539ae9b06004c7557ac60e7d8a6823f5da428eb8
6be18e3afeec482c79c9dea119d11d9c1598f59a260156ee54f12c4d914aed8f
484f78eb4a3bb69d62491fdb84f2c81b7ae131ec8452a04d6018a634e961cd6a
3deaa4072da43185d4213a38403383b7cefe92524b69ce4e7884a3ddc0903f6b
4ba618c04cbdc47de2ab5f2c91f466bc42163fd541de80ab8b5e50f687bbb91c
e241b152e3f672434636c527ae0ebbd08c777f488020c98efce8b324486335c5
6ee79815f71e2eb4094455993472c7fb185cde484c8b5326e4754adcb1faf78e
81c7787040ed5ecf21b6f80dc84bc147cec518986bf25aa933dd44c414b5f498
999e4753749228a60d4d20cc5c5e27ca4275fe63e6083053a5b01b5225c8d53a
4bd93e4a9826a65ade60117f6136cb4ed0e17beae8668a7c7981d15c0bed705a
a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
0d3e0c26f7f53dff444a37758b414720286f92da55e33ca0e69edc3c7f040ce2
bef9051bb6e85d94c4cfc4e03359b31584be027e87758483e3b1e65d389483e6
1205f5845035e3ee30f5a1ced5500d8345246ef4900bcb4ba67ef72c0f79966c
51121dd5fbdfe8db7d3a5311e3e9c904d644ff7221b60284c03347938577eecf
51ac160f7d60a9ce642080af0425a446fb25b7067e06b3a9a8ec2f777836efd3
5723f425e0c55c22c6b8bb74afb6b506943012c33b9ec1c928a71307a8c5889a
884e991d2066163e02472ea82d89b64e252537b28c58ad57d9d648b969de6a63
bf696397784b22f8e891dd0627dce731f288d14d4791ac5d0a906bc1cbe10de6
bf8f30031769aa880cdbe22bc0be32691d9f7913af75a5b68f8426d4f0c7be50
c92e70515d594c582e4433f2aca6c8f2aa60f1af0aa21a08173ff2feb7d34359
f1f11830b60e6530b680291509ddd9b5a1e5f425550444ec964a08f5f0c1a44e
294a907c27d622380727496cd7c53bf908af7a88657302ebd0a9ecdd30d2ec9d
65bd49d9f6d9b92478e3653362c0031919607302db6cfb3a7c1994d20be18bcc
b6c483536379840e89444523d27ac7828b3eb50342b992d2c8f608450cd7bb53
e5c56c5b9620fb542eab82bdf75237d179bc996584b5c5f7a1c34ef5ae521c7d
43080479eb1b00ba80c34272c5595e6ebdc6b0ffabcdc2c40ea2af49fcc43db4
0acd10b14d38a4ac469819dfa9070106e7289ecf7360e248b7f10f868c2f373d
888a6f205ac9fc40d4898d8068b56b32f9692cb75f0dd813f96a7bd8426f8652
4f509354d8b3152a40c64ce61f7594d592c1256ad6c0829760b8dbdcb10579a2
41ee0ab77b474b0c84a1c25591029533f058e4454d9f83ba30159cc6309c65d1
3d96811de7419a8c090a671d001a85f2b1875243e5b38e6f927d9877d0ff9b0c
d07d4e71927cab4f251bcc216f560674c5fb783add9c9f956d3fc457153be025
fbbda9d8d9bcaaf9a7af84d08af3f5140f5f75778461e48253dc761cc9dc027c
240b7d2825183226af634d3801713b0e0f409eb3e1e48e1d36c96d2b03d8836b
18cf5795c2208d330bd297c18445a9e25238dd7f28a1a6ef55e2a9239f5748cd
707d2128a0c326626adef0d3a4cab78562abd82c2bd8ede8cc82f86c01f1e024
76e9988dad0278998861717c774227bf94112db548946ef617bfaa262cb5e338

94625dd8151814dd6186735a6a6a87b2a4c71c04b8402caf314fb6f98434eaad
b7b8faac19a58548b28506415f9ece479055e9af0557911ca8bbaa82b483ffb8
2727bf97d7e2a5e7e5e41ccbfd7237c59023d70914834400da1d762d96424fde
c87799cce6d65158da97aa31a5160a0a6b6dd5a89dea312604cc66ed5e976cc9
009cc0f34f60467552ef79c3892c501043c972be55fe936efb30584975d45ec0
40a6b4c6746e37d0c5ecb801e7656c9941f4839f94d8f4cd61eaf2b812feaabe
16bcb6cc38347a722bb7682799e9d9da40788e3ca15f29e46b475efe869d0a04
b2c10621c9c901f0f692cae0306baa840105231f35e6ec36e41b88eebd46df4c
58282917a024ac252966650361ac4cbbbed48a0df7cab7b9a6329d4a04551c0d
588cd0fe3ae6fbd2fa4cf8de8db8ae2069ea62c9eaa6854caedf45045780661f
97f9a83bc6bb1b3f5cb7ac9401f95265597bff796bb4901631d6fa2c79a48bdc
1b60b7f9b0faf25288f1057b154413921a6cb373dcee43e831b9263c5b3077ce
2c8d18f03b6624fa38cae0141b91932ba9dc1221ec5cf7f841a2f7e31685e6a1
a3c1fd46177a078c4b95c744a24103df7d0a58cee1a3be92bc4cdd7dec1b1aa5
367021beedb3ad415c69c9a0e657dc3ed82b1b24a41a71537d889f5e2b7ca433
de6ce9b75f4523a5b235f90fa00027be5920c97a972ad6cb2311953446c81e1d
16985600c959f6267476da614243a585b1b222213ec938351ef6a26560c992db
cf87a2ac51503d645e827913dd69f3d80b66a58195e5a0044af23ea6ba46b823
f511bdd471096fc81dc8dad6806624a73837710f99b76b69c6501cb90 e37c311
efd5271bdb57f52b4852bfda05122b9ff85991c0600befcbd045f81d7a7 8eac5
d65d80ab0ccdc7ff0a72e71104de2b4c289c02348816dce9996ba3e2a 4c1dd62
1670a59f573037142f417fb8c448a9022c8d31a6b2bf93ad77a9db292 4b502af
dedc593acc72c352feef4cc2b051001bfe22a79a3a7852f0daf95e2d10e 58b84
eae0acba9c9e6a93ce2d5b30a5f21515e8ccca0975fbd0e7d8862964fd fa1468
7e7292b5029882602fe31f15e25b5c59e01277abaab86b29843ded4aa 0dcbdd1
c7a2a9e020b4bcbfa53b37dea7ebf6943af203b94c24a35c098b774f79 d532ac
887c09e24923258e2e2c28f369fba3e44e52ce8a603fa3aee8c3fb0f1ca 660e1
01dfa94e11b60f92449445a9660843f7bea0d6aad62f1c339e8825200 8e3b494
d550f0f9c4554e63b6e6d0a95a20a16abe44fa6f0de62b6615b5fdcdb8 2fe8e1
61dcf1eeb616104742dd892b89365751df9bb8c5b6a2b4080ac7cf342 94d7675
653046fa62d3c9325dbff5cb7961965a8bf5f96fa4e815b494c8d3e165 b9c94a
76ab046de18e20fd5cddbb90678389001361a430a0dc6297363ff10ef bcb0fa8
c6cfd23282c9ff9d0d4c72ee13797a898b01cd5fd256d347e399e7528d ad3bfd
32339f7ac043042e6361225b594047dd4398da489a2af17a9f74a51593 b14951
dab77aea8bf4f78628dcf45be6e2e79440c38a86e830846ec2bddc74ff0 a36e4
b5c7acf08d3fd68ddc92169d23709e36e45cb65689880e30cb8f376b5c 91be57
2a5f74e8268ad2d38c18f57a19d723b72b2dadd11b3ab993507dd2863 d18008d
e87fe81352ebda0cfc0ae785ebfc51a8965917235ee5d6dc6ca6b730eda 494cf
aa282daa9da3d6fc2dc6d54d453f4c23b746ada5b295472e7883ee6e63 53b671
4e80bd62d02f312b06a0c96e1b5d1c6fd5a8af4e051f3f7f90e29765808 42515
697580cf4266fa7d50fd5f690eee1f3033d3a706eb61fc1fca25471dbc36 e684

dc7e102a2c68f7e3e15908eb6174548ce3d13a94caadf76e1a4ee834dc 17a271
f24ce8e6679893049ce4e5a03bc2d8c7e44bf5b918bf8bf1c2e45c5de4d 11e56
433b47f40f47bea0889423ab96deb1776f47e9faa946e7c5089494ed00 c6cc29
011cb37733cdf01c689d12fedc4a3eda8b0f6c4dcdeef1719004c32ee33 1198e
e217c48c435a04855cf0c439259a95392122064002d4881cf093cc59f81 3aba8
331b513cf17568329c7d5f1bac1d14f38c77f8d4adba40c48dab6baf988 54f92
4d24b326d0335e122c7f6adaa22e8237895bdf4c6d85863cf8e84cfcc05 03e69
a35a1c92c001b59605efd318655d912f2bcd4e745da2b4a1e385d289e1 2ee905
4550b4fa89ff70d8ea59d350ad8fc537ceaad13779877f2761d91d69a2c 445b2
5578b7d126ebae78635613685d0cd07f4fb86f2e5b08e799bdc67d6d60 53ede2

APT34 (OilRig)

Sectors targeted: This threat actor has carried out extensive targeting of a variety of industries, including finance, government, energy, chemical industries and telecommunications, and has mainly focused its operations within the Middle East.

Overview: We believe that APT34 is engaged in a long-term cyberespionage operation, focused primarily on reconnaissance efforts to benefit the interests of the Iranian state, and has been operational since at least 2014. We estimate that APT34 works on behalf of to the Iranian government based on infrastructure details containing references to Iran, the use of the Iranian nation's infrastructure, and the targeting of the country's state interests.

Actor-related malware: *Pupy RAT, Liderc, LittleLooter, BONDUPDATER, Saitama, DNSpionage, Helminth, Jason, Marlin Backdoor, OopsIE, PowerExchange, SideTwist, TriFive, ZeroCleare, Aleta Ransomware, AnubisSpy, Atmos, BankBot, Catelites Bot, Cryptolocker, DanBot, Disdain Exploit Kit, Dustman, DustySky, ELVENDOOR, Executioner Ransomware, FastPOS, GozNym, Gugi Botnet, Infy, Ismdoor, ISMInjector, Ixeshe, Jaku, Karkoff, Kronos, LokiBot (Android), LYCEUM malware, MegalodonHTTP, Mingloa, Mordor Ransomware, NANHAISHU, NemeS1S, njRAT, Petya, POWRUNER, QUADAGENT, ROADSWEEP, Shamoon 2, Sigma Ransomware, SmokeLoader, StuxnetTidePool, TRISISTVSPY, UnransXKEYSCORE, Zemra, ZEROCLEAR, Zeus.*

The tools used by these malicious actors: *Glimpse, Helminth, Jason, MacDownloader, PoisonFrog, RGDoor, ThreeDollars, TinyZbot, Toxocara, Trichuris, TwoFace etj.*

Figure 12: Malicious Group Description

The attack vectors that are made by this group are: ***C&C Server, DDoS, Data Exfiltration, Phishing, Social Engineering, Spear Phishing.***

Mittre Att&ck TTPs commonly used by OilRig are:

TA0001: Initial Access
TA0002: Exécution
TA0005: Defense Evasion
TA0003: Persistence
TA0011: Command and Control
T1059.001: PowerShell
T1059.003: Windows Command Shell
T1053.005: Scheduled Task
T1204.002: Malicious File
T1047: Windows Management Instrumentation
T1480: Execution Guardrails
T1087.001: Local Account
T1083: File and Directory Discovery
T1049: System Network Connections Discovery
T1071.004: DNS
T1132.002: Non-Standard Encoding
T1568.002: Domain Generation Algorithms
T1041: Exfiltration Over C2 Channel

IOCs:

Organisations
Federal Security Service (Russia)
Islamic Republic of Iran's Ministry of Intelligence
Jordanian Ministry of Foreign Affairs and Expatriates
Islamic Revolutionary Guard Corps (Iran) (Iranian Revolutionary Guard Corps)
IRGC Basij
IRGC Cyber (IRGC Electronic Warfare and Cyber Defense Organization) (ISLAMIC REVOLUTIONARY GUARD CORPS ELECTRONIC WARFARE AND CYBER DEFENSE ORGANIZATION)
Middle Eastern government
Kvant Scientific Research I

Vulnerabilities used:
CVE-2015-2545

CVE-2017-11882

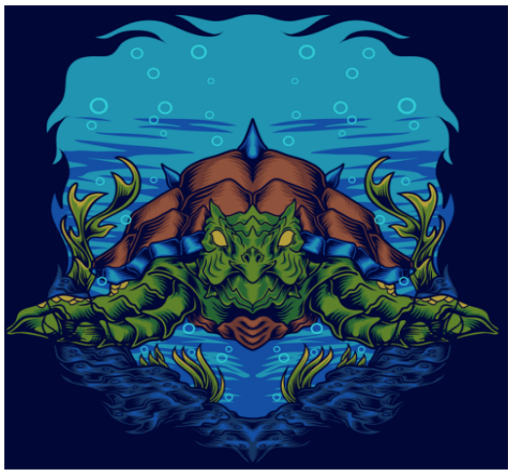
Domains
mastertape.org
myleftheart.com
offsetweb.com
sarmsoftware.com
update-microsoft.space
apigoogle-accounts.biz
mycrossweb.com
asiaworldremit.com
dropboxengine.com
joexpediagroup.com
kizlarsoroyur.com
lebworld.us
ns1.mastertape.org
ns2.mastertape.org
rdmsi.com
redjewelry.biz
requestbin.net
tv7476tvan000002a61.mastertape.org
uber-asia.com joexpediagroup[.]com, asiaworldremit[.]com, uber-asia[.]com

HASH:
SHA-256: 1f47770cc42ac8805060004f203a5f537b7473a36ff41eabb746900b2fa24cc8
SHA-256: 26884f872f4fae13da21fa2a24c24e963ee1eb66da47e270246d6d9dc7204c2b
SHA-256: e0872958b8d3824089e5e1cfab03d9d98d22b9bcb294463818d721380075a52d
SHA-256: 27e03b98ae0f6f2650f378e9292384f1350f95ee4f3ac009e0113a8d9e2e14ed
SHA-256: 0cab88bb37fee06cf354d257ec5f27b0714e914b8199c03ae87987f6fa807efc
SHA-256: b1d621091740e62c84fc8c62bcdad07873c8b61b83faba36097ef150fd6ec768
SHA-256: e00655d06a07f6eb8e1a4b1bd82eefe310cde10ca11af4688e32c11d7b193d95
SHA-256: 73cb7452fc167765a53a4beed3bda7c1fd54e0f8c4aa5c71e1b48fbbfb971127
SHA-256: a4aea112321df21651918c3096a870bc748557c8b3eb5398c675025bd6d0ec83
SHA-256: d6b876d72dba94fc0bacbe1cb45aba493e4b71572a7713a1a0ae844609a72504
SHA-256: f91c5250b33fc5f95495c5e3d63b5fde7ca538178feb253322808b383a26599d
SHA-1: 273488416b5d6f1297501825fa07a5a9325e9b56
SHA-256: 47d3e6c389cfdbc9cf7eb61f3051c9f4e50e30cf2d97499144e023ae87d68d5a
MD5: 94004648630739c154f78a0bae0bec0a
SHA-256: 2943e69e6c34232dee3236ced38d41d378784a317eeaf6b90482014210fcd459

SHA-256: 06cb3f69ba0dd3a2a7fa21cdc1d8b36b36c2a32187013598d3d51cfddc829f49
SHA-256: 0714b516ac824a324726550b45684ca1f4396aa7f372db6cc51b06c97ea24dfd
SHA-256: 07e791d18ea8f2f7ede2962522626b43f28cb242873a7bd55fff4feb91299741
SHA-256: 7eeadfe1aa5f6bb827f9cb921c63571e263e5c6b20b2e27ccc64a04eba51ca7a
SHA-256: ad5babecf3a21dd51eee455031ab96f326a9dd43a456ce6e8b351d7c4347330f SHA-256: 82A0F2B93C5BCCF3EF920BAE425DD768371248CDA9948D5A8E70F3C34E9F7CCA SHA-256: 7EBBEB2A25DA1B09A98E1A373C78486ED2C5A7F2A16EEC63E576C99EFE0C7A49 SHA-256: C744DA99FE19917E09CD1ECC48B563F9525DAD3916E1902F61B79BDA35298D87 SHA-256: E0872958B8D3824089E5E1CFAB03D9D98D22B9BCB294463818D721380075A52D

Malicious IP:
204.11.56.48
209.99.40.222
209.99.40.223
58.158.177.102
142.93.110.250
209.99.40.227
208.115.211.88
45.86.162.34
160.20.147.198
185.141.63.8
185.243.115.157
46.21.147.83
54.36.12.175
160.20.147.100
185.188.206.185
23.19.227.117
79.137.2.125
193.29.59.28
23.106.123.206
80.209.253.114

Sea Turtle (UNC1326)



Suspected Origin: Turkey	
Name: Sea Turtle	**Last Active:** April 2023
APT Type: State Sponsored	**Aliases:** Cosmic Wolf, UNC1326
Industry Concentrations:	**Geographic Activity:**

Aviation	Telecomm
Oil & Gas	Technology

Lebanon	Greece
Egypt	Albania
Iraq	Jordan
India	UAE

Figure 13: Sea Turtle group details

Details

The Sea Turtle group, otherwise known as **Silicon, UNC1326 or Marbled Dust**, of Turkish origin has its beginnings in 2017 and aims to steal information, espionage and continuous control of critical and sensitive systems.
The attacks are related to campaigns that focus on the **DNS Hijacking** technique, but also **DDOS or Sql Injection.** They usually make it possible to change the parameters of the DNS records for the attacking victims as well as change the traffic for the victims' servers**.**

These techniques to exploit CVE as follows:

CVE-2009-1151: PHP code injection vulnerability affecting phpMyAdmin

CVE-2014-6271: RCE affecting GNU bash system, specific the SMTP (this was part of the Shellshock CVEs)

CVE-2017-3881: RCE for Cisco switches

CVE-2017-6736: Remote Code Exploit (RCE) for Cisco integrated Service Router 2811

CVE-2017-12617: RCE affecting Apache web servers running Tomcat

CVE-2018-0296: Directory traversal to gain unauthorized access to Cisco Adaptive Security Appliances (ASAs) and Firewalls

CVE-2018-7600: RCE for Website built with Drupal aka "Drupalgeddon"

CVE-2021-4034: Red Hat Polkit Out-of-Bounds Read and Write Vulnerability

CVE-2020-2034: OS command injection vulnerability in GlobalProtect portal

CVE-2021-26084: Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability

Name	Origin	The regions where they attack	Industries it attacks
Sea Turtle (Silicon, UNC1326, Marbled Dust)	Turkey MotivE Information theft and espionage	Albania, United States, Libya, Egypt, Armenia, Syria, Sweden, United Arab Emirates, Lebanon	State, Media, Transport Organizations, Critical Infrastructures, etc.

IOCs:

DOMAIN
ns1[.]intersecdns[.]com - 95.179.150.101
s2[.]intersecdns[.]com – 95.179.150.101
ns1[.]lcjcomputing[.]com - 95.179.150.101
ns2[.]lcjcomputing[.]com - 95.179.150.101

IP
199.247.3.191
37.139.11.155
185.15.247.140
206.221.184.133
188.166.119.57
185.42.137.89
82.196.8.43
159.89.101.204
146.185.145.202
178.62.218.244
139.162.144.139
142.54.179.69
193.37.213.61
108.61.123.149
212.32.235.160
198.211.120.186
146.185.143.158
146.185.133.141
185.203.116.116

95.179.150.92
174.138.0.113
128.199.50.175
139.59.134.216
45.77.137.65
142.54.164.189
199.247.17.221

RECOMMENDATIONS

To avoid attacks from this threat group, measures should be taken to block IoCs as well as perform updates where the CVEs may be affected. Frequent checking of DNS records.

Continuous traffic monitoring of the above IoC factors should also prevail as they may change on a case-by-case basis.

Grupi Arid Viper (Martis, APT23)

Figure 14: Arid Viper group details

Details:

The Arid Viper group, otherwise known as the **Desert Falcon (APT-C-23 and Mantis)** of **Palestinian** origin from **Gaza**, has its beginnings in 2011 and aims for espionage. The first infections from this group were reported in 2013, attacking organizations in Israel, further Middle East and other regions.

Their most frequent attacks involve various versions of Arid Gopher and Micropsia Backdoor, to gain access to where they attack. Usually, their most used tactic is spear-phishing emails and fake social networks to install malware on victims' devices. Also, other techniques such as DNS Hijacking or Payloads.

The most used tools are: ***ViperRat, Frozen Cell or VolatileVenom, Micropsia*** where it can operate on different platforms.

In a campaign carried out by them, 3 different versions of the same malware (Micropsia) were distributed, successfully connecting to the C2 server.

Arid Gopher is coded in the Go language, this allows it to bypass detection by antivirus devices, firewalls, etc., and was identified in March 2022.

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1190 Exploit Public-Facing Application	T1566 Phishing
T1059 Command and Scripting Interpreter	T1053 Scheduled Task/Job	T1204 User Execution	T1047 Windows Management Instrumentation
T1543 Create or Modify System Process	T1574 Hijack Execution Flow	T1548 Abuse Elevation Control Mechanism	T1055 Process Injection
T1564 Hide Artifacts	T1562 Impair Defenses	T1070 Indicator Removal	T1036 Masquerading
T1212 Exploitation for Credential Access	T1056 Input Capture	T1083 File and Directory Discovery	T1046 Network Service Discovery
T1057 Process Discovery	T1560 Archive Collected Data	T1071 Application Layer Protocol	T1001 Data Obfuscation
T1105 Ingress Tool Transfer	T1571 Non-Standard Port	T1047 Windows Management Instrumentation	T1566.002 Spearphishing Link

Figure 15: Tactics used by the Arid Viper group

Name	Origin	Rajonet ku sulmojnë	Industritë që sulmon
Desert Falcons (Mantis, APT-C-	Gaza (Palestine) Motive	Algeria, Australia, Bahrain, Central Europe, Russia, the	State, Media, Research Institutes, Transport Organizations, Critical Infrastructures, etc.

23, Two-tailed Scorpion, Arid Viper, ATK 66, TAG-CT1)	Information theft and espionage	Balkans (including Albania), Africa, etc.	

IOCs:

Type	Value
SHA256	4840214a7c4089c18b655bd8a19d38252af21d7dd048591f0af12954232b267f
	4a25ca8c827e6d84079d61bd6eba563136837a0e9774fd73610f60b67dca6c02
	624705483de465ff358ffed8939231e402b0f024794cf3ded9c9fc771b7d3689
	7ae97402ec6d973f6fb0743b47a24254aaa94978806d968455d919ee979c6bb4
	8d1c7d1de4cb42aa5dee3c98c3ac637aebfb0d6 220d406145e6dc459a4c741b2
	b6a71ca21bb5f400ff3346aa5c42ad2faea4ab3f067a4111fd9085d8472c53e3
	bb6fd3f9401ef3d0cc5195c7114764c20a6356c63790b0ced2baceb8b0bdac51
	bc9a4df856a8abde9e06c5d65d3bf34a4fba7b9907e32fb1c04d419cca4b4ff9
	d420b123859f5d902cb51cce992083370bbd9deca8fa106322af1547d94ce842
	0fb4d09a29b9ca50bc98cb1f0d23bfc21cb1ab602050ce786c86bd2bb6050311
	3d649b84df687da1429c2214d6f271cc9c026eb4a248254b9bfd438f4973e529
	82f734f2b1ccc44a93b8f787f5c9b4eca09efd9e8dcd90c80ab355a496208fe4
	85b083b431c6dab2dd4d6484fe0749ab4acba50842591292fdb40e14ce19d097
	cb765467dd9948aa0bfff18214ddec9e993a141a5fdd8750b451fd5b37b16341
	f2168eca27fbee69f0c683d07c2c5051c8f3214f8841c05d48897a1a9e2b31f8
	21708cea44e38d0ef3c608b25933349d54c35e392f7c668c28f3cf253f6f9db8
	58331695280fc94b3e7d31a52c6a567a4508dc7be6bdc200f23f5f1c72a3f724
	5af853164cc444f380a083ed528404495f30d2336ebe0f2d58970449688db39e
	0a6247759679c92e1d2d2907ce374e4d6112a79fe764a6254baff4d14ac55038
	1d1a0f39f339d1ddd506a3c5a69a9bc1e411e057fe9115352482a20b63f609aa
	211f04160aa40c11637782973859f44fd623cb5e9f9c83df704cc21c4e18857d
	d10a2dda29dbf669a32e4198657216698f3e0e3832411e53bd59f067298a9798
	5405ff84473abccc5526310903fcc4f7ad79a03af9f509b6bca61f1db8793ee4
	f38ad4aa79b1b448c4b70e65aecc58d3f3c7eea54feb46bdb5d10fb92d88020 3
	c4b9ad35b92408fa85b92b110fe355b3b996782ceaafce7feca44977c037556b
	f98bc2ccac647b93f7f7654738ce52c13ab477bf0fa981a5bf5b712b97482dfb
	411086a626151dc511ab799106cfa95b1104f4010fe7aec50b9ca81d6a64d299
	5ea6bdae7b867b994511d9c648090068a6f50cb768f90e62f79cd8745f53874d

	6a0686323df1969e947c6537bb404074360f27b56901fa2bac97ae62c399e061
	11b81288e5ed3541498a4f0fd20424ed1d9bd1e4fae5e6b8988df364e8c02c4e
	1b62730d836ba612c3f56fa8c3b0b5a282379869d34e841f4dca411dce465ff6
	220eba0feb946272023c384c8609e9242e5692923f85f348b05d0ec354e7ac3c
URL	hxxp[:]//5.182.39[.]44/esuzmwmrtajj/cmsnvbyawttf/mkxnhqwdywbu
Domain	jumpstartmail[.]com
	paydayloansnew[.]com
	picture-world[.]info
	rnacgroup[.]com
	salimafia[.]net
	seomoi[.]net
	soft-utils[.]com
	chloe-boreman[.]com
	criston-cole[.]com
IPV4:Port	104.194.222[.]50:4444

RECOMMENDATIONS:

To avoid attacks, measures should be taken to block 104.194.222[.]50:4444 as the main C2 (Command&Control Server) where the traffic is generated is found. There should also be continuous traffic monitoring of the above IOC factors as they may change.

BlackCat (ALPHV)

The BlackCat group first appeared in February 2023. Blackcat ransomware is otherwise known as ALPHV, AlphaV, AlphaVM, ALPHV-ng, or Noberus. Its feature is that it has attacked countries all over the world. Damage claims are typically $1.5 – $3 million. The platforms that can be infected are Windows, Linux and VMware ESXi. Operation BlackCat ransomware is a highly advanced and customizable threat that targets corporate environments, including advanced encryption, distribution capabilities, and other tactics**.**

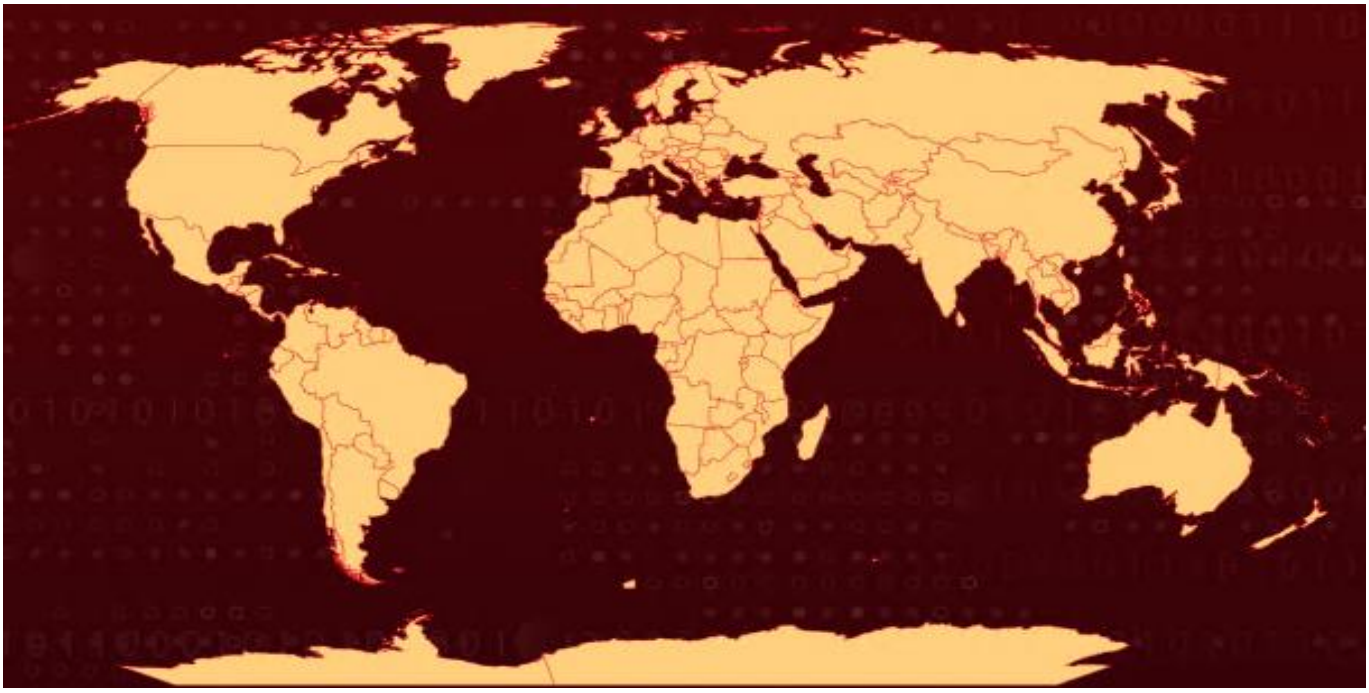


Figure 16: Tactics used by the BlackCat group - ALPHV

1. **Ransomware ALPHV**, also known as BlackCat, is a sophisticated ransomware operation that has come onto the scene recently. It is considered one of the most advanced ransomware variants this year, with a wide range of features customized to target corporate environments. Ransomware is written in Rust, a programming language known for its high performance and memory safety.
2. **ALPHV BlackCat** acts as *a ransomware-as-a-service (RaaS).* Ransomware offers multiple encryption methods and algorithms, allowing flexibility and optimization in the encryption process.
3. **Ransomware** it is designed to be commanded through the command line, configurable and capable of performing various actions such as spreading between computers, damaging virtual machines, deleting ESXi *snapshots*, etc. It also can encrypt files on various operating systems, including Windows, ESXi, Debian, Ubuntu, and ReadyNAS/Synology.
4. **ALPHV BlackCat** includes a complete cross-platform approach, ensuring that files can be decrypted even when they are on different operating systems. Ransomware is known to demand rewards ranging from $400,000 to $3 million, paid in Bitcoin or Monero. Furthermore, it uses a tactic that steals the data before encrypting the devices and threatens to publish the data if the ransom is not paid.
5. A distinctive feature of ALPHV BlackCat is the use of kernel drivers. These drivers are used to gain high-level access and compromise security on target systems.

RECOMMENDATIONS:

- **Keep systems and security measures up to date:** Keep all software, applications and operating systems up to date with the latest security updates. Use popular antivirus suggestions to detect and prevent ALPHV BlackCat ransomware infections**.**

- **Perform regular backups of critical data and test recovery:** Perform regular backups of critical data and verify the integrity of the backups by testing the recovery process. Store copies offline or on a separate and secure network to prevent them from being compromised in the event of a ransomware attack.
- **Implement strong login controls and user awareness:** Implement strong password policies and encourage the use of multifaceted authentication (MFA). Educate employees about phishing attacks, safe web browsing practices, and the importance of not opening suspicious email attachments or clicking on unfamiliar links.

TA0003 Persistence	TA0002 Execution	TA0008 Lateral Movement	TA0004 Privilege Escalation
TA0011 Command and Control	TA0042 Resource Development	TA0005 Defense Evasion	TA0040 Impact
TA0001 Initial Access	TA0006 Credential Access	T1569 System Services	T1027 Obfuscated Files or Information
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1110 Brute Force	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1562.009 Safe Mode Boot	T1489 Service Stop	T1057 Process Discovery
T1649 Steal or Forge Authentication Certificates	T1588.003 Code Signing Certificates	T1529 System Shutdown/Reboot	T1566 Phishing
T1588 Obtain Capabilities	T1564 Hide Artifacts	T1486 Data Encrypted for Impact	T1210 Exploitation of Remote Services
T1078 Valid Accounts	T1505 Server Software Component	T1021 Remote Services	T1068 Exploitation for Privilege Escalation
T1040 Network Sniffing	T1041 Exfiltration Over C2 Channel	T1046 Network Service Scanning	T1047 Windows Management Instrumentation
T1106 Native API	T1119 Automated Collection	T1553 Subvert Trust Controls	T1105 Ingress Tool Transfer

Figure 17: BlackCat Group Techniques, Tactics, Procedures - ALPHV

HASH	VALUE
SHA256	52d5c35325ce701516f8b04380c9fbdb78ec6bcc13b444f758fdb03d545b0677 c8f9e1ad7b8cce62fba349a00bc168c849d42cfb2ca5b2c6cc4b51d054e0c497
MD5	909f3fc221acbe999483c87d9ead024a a837302307dace2a00d07202b661bce2

SHA1	17bd8fda268cbb009508c014b7c0ff9d8284f850 78cd4dfb251b21b53592322570cc32c6678aa468 c2387833f4d2fbb1b54c8f8ec8b5b34f1e8e2d91 91568d7a82cc7677f6b13f11bea5c40cf12d281b 0bec69c1b22603e9a385495fbe94700ac36b28e5 5ed22c0033aed380aa154e672e8db3a2d4c195c4 cb25a5125fb353496b59b910263209f273f3552d 994e3f5dd082f5d82f9cc84108a60d359910ba79 f6793243ad20359d8be40d3accac168a15a327fb b2f955b3e6107f831ebe67997f8586d4fe9f3e98

The most dangerous groups the techniques they use campaign 1:

DATE: 18-09-2023

Threat actors are reusing old proof of concept (PoC) code to create a fake PoC for a newly released vulnerability. The Zero Day Initiative reported a remote code execution (RCE) vulnerability in WinRAR named CVE-2023-40477. Four days after the CVE was reported, an actor using the alias Whalersplonk posted a fake PoC script to the GitHub repository.

This fake PoC to exploit this vulnerability in WinRAR was based on a publicly available PoC script that exploits a SQL injection vulnerability in a GeoServer application, which is named as CVE-2023-25157. According to the analysis, the script and all the links in the infection chain installed a VenomRAT payload. It is discussed that threat actors have created this script to take advantage of other criminals who try to adopt new vulnerabilities in their operations.

Vulnerabilities:

Details of vulnerabilities:

- A fake PoC script based on a public PoC code for a GeoServer vulnerability has been published.
- The fake WinRAR PoC script is classified as CVE-2023-40477 and the GeoServer PoC script is classified as CVE-2023-25157.
- The fake PoC script does not exploit the WinRAR vulnerability but starts an infection chain which after many steps installs a VenomRAT payload.
- CVE-2023-40477 vulnerability allows an attacker to execute code on a system that opens a malicious file.

- The code is contained within a ZIP file named CVE-2023-40477-main.zip, in the poc.py file. Along with the code, inside the zip file was a README.md file, which attempted to trick the user into compromising their system by providing a summary of CVE-2023-40477, instructions for the poc.py script, and a link to of a video hosted on streamable.com, which was set to expire on August 25, 2023.
- According to analytics, the video had over 100 individual views. Two images that were used as video thumbnails, one of them showing the threat actor's desktop, along with the task manager open, showing a process called Windows.Gaming.Preview, which is the same name as the VenomRAT payload , while the second image shows a Burp Suite archive, password 311138 in Notepad and Putty client..
- The fake PoC python script although based on PoC CVE-2023-25157, had the following changes:
    - Uncommented details of vulnerability CVE-2023-25157
    - Removed lines of code that suggest a network-related vulnerability, such as setting the PROXY and PROXY_ENABLED variables
    - The string from geoserver to exploit has been modified
    - Placement of additional code which installs and executes a script with a comment for "Check dependency"
- The vulnerability procedure is as follows:

    - Malicious code in poc.py before the script terminates with an exception creates a script dump in *%TEMP%/ba*t.bat.
    - This script will then grab the URL *http://checkblacklistwords[.]eu/check-u/robot?963421355?Ihead=true* and run the response.
    - The script bundle hosted at the URL above executes an encrypted PowerSell script, which then installs another PowerShell script from *checkblacklistwords[.]eu/c.txt*. This script then saves the file to *%TEMP%\c.ps1* and executes it.
    - The script then installs an executable file from checkblacklistwords[.]eu/words.txt and saves it to *%APPDATA%\Drivers\Windows.Gaming.Preview.exe*. This PowerShell script also creates a scheduled task called *Windows.Gaming.Preview*.

- *Windows.Gaming.Preview.exe* is a variant of **VenomRAT**. This program then communicates with *http://checkblacklistwords[.]eu/list.txt* to get the location of C2. This VenomRAT client starts a keylogger functionality which logs the keystrokes in *%APPDATA%\MyData\DataLogs_keylog_offline.txt*, and then the client starts communicating with the C2 server and processes the server's responses.

IOC:

File	7fc8d002b89fcfeb1c1e6b0ca710d7603e7152f693a14d8c0b7514d911d04234	CVE-2023-40477-main.zip

File	ecf96e8a52d0b7a9ac33a37ac8b2779f4c52a3d7e0cf8da09d562ba0de6b30ff	poc.py
File	c2a2678f6bb0ff5805f0c3d95514ac6eeaeacd8a4b62bcc32a716639f7e62cc4	bat.bat
File	b99161d933f023795afd287915c50a92df244e5041715c3381733e30b666fd3b	c.ps1
File	b77e4af833185c72590d344fd8f555b95de97ae7ca5c6ff5109a2d204a0d2b8e	Windows.Gaming.Preview.exe -VenomRAT
IPv4	94.156.253[.]109	VenomRAT C2
Domain	checkblacklistwords[.]eu	Hosted files in infection chain
URL	http://checkblacklistwords[.]eu/check-u/robot?963421355?Ihead=true	Hosted bat.bat
URL	http://checkblacklistwords[.]eu/c.txt	Hosted c.ps1
URL	http://checkblacklistwords[.]eu/words.txt	Hosted Windows.Gaming.Preview.exe

Attacks occurred during the year on Critical Infrastructures in the Region

As can be seen from the graph below, most of the attacks in Albania have been political - phishing. These attacks make up 50% of all attacks in the territory of the Republic of Albania. 25% of attacks are ransomware, while 25% are unidentified. Albania is the country with the most political attacks until June 2023. In terms of espionage, Bosnia and Herzegovina is the only country in the Balkans and this category accounts for 9.09% of attacks in this country. As for ransomware attacks, they make up the majority of attacks in North Macedonia.

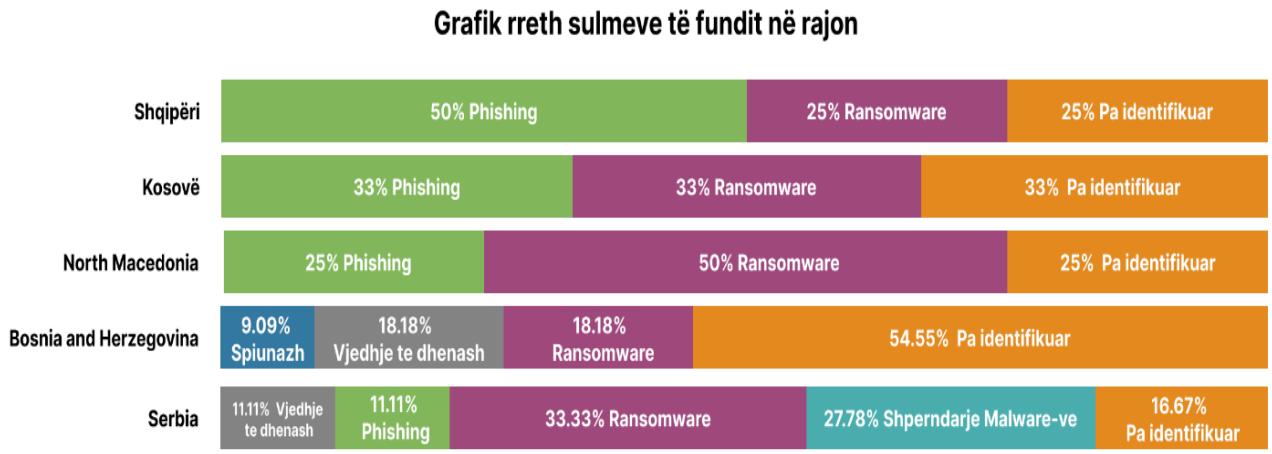


Figure 18: Chart of the latest attacks in the region

The graph below shows that Albania is included in the categories of Ransomware and Exploit attacks. All the Balkan countries have been the target of ransom attacks. Regarding phishing attacks, they have occurred in Bosnia and Herzegovina, Kosovo and a large part in Serbia. DDos attacks were recorded only in Serbia, while malware only in Bosnia and Herzegovina.

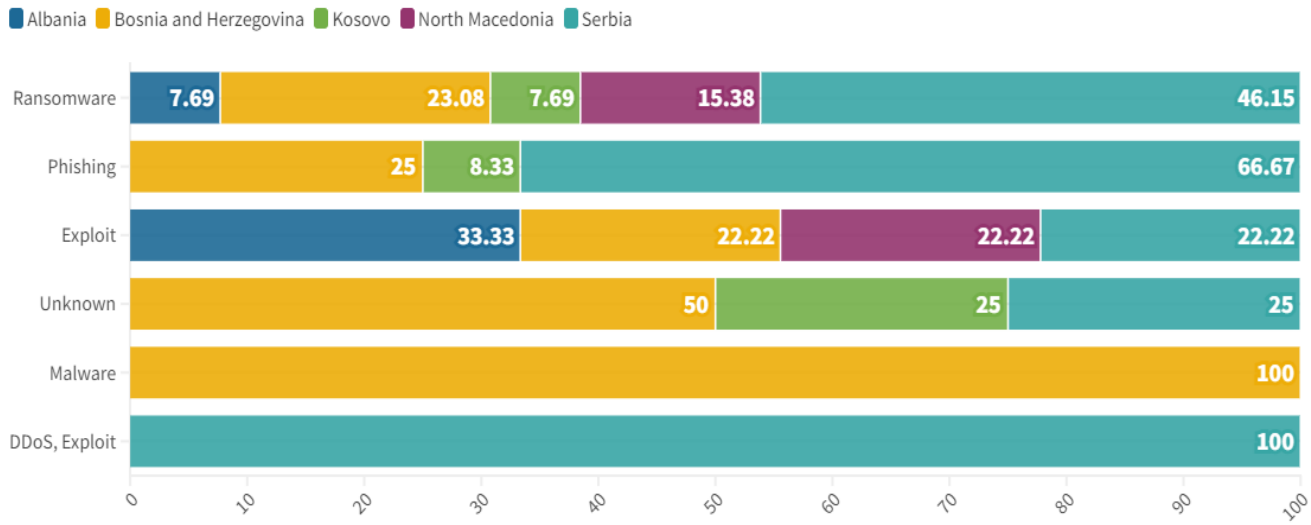


Figure 19: Chart of recent attack categories

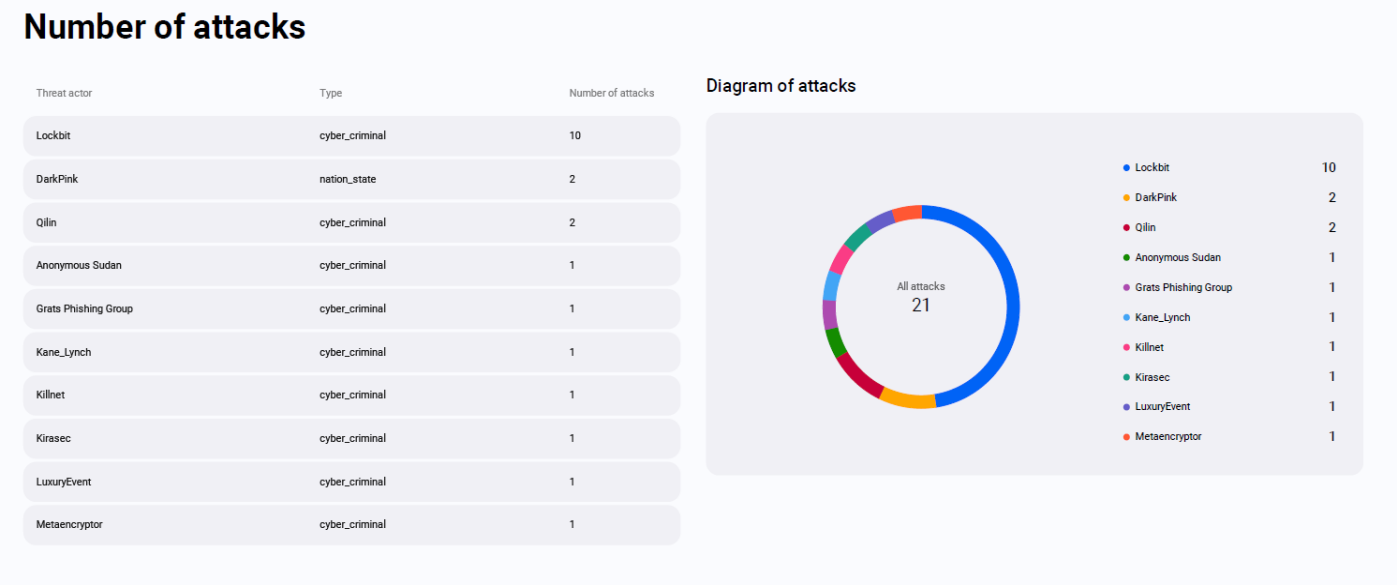


Figure 20: Statistics of incidents occurred by hacking groups

RECOMMENDATIONS

Some of the measures that are recommended for organizations to prevent their systems and networks from cyber attacks:

AKCESK recommends that organizations implement the following best practices to reduce the risk of attacks by these malicious actors.

- Ensure that antivirus and anti-malware software is enabled and signature definitions are updated regularly and in a timely manner. Well-maintained antivirus can prevent the use of commonly deployed cyberattack tools that are distributed through spear-phishing.
- If your organization is using certain types of applications and devices vulnerable to common known vulnerabilities and exposures (CVEs), make sure these vulnerabilities are patched.
- Monitor for large amounts of data (ie several GB) being transferred from a Microsoft Exchange server.
- Check for host-based indications, including webshells on your network.
- Maintain and test an incident response plan.
- Proper configuration of Internet-facing network devices.
- Not exposing management interfaces to the web.
- Disabling unused or unnecessary network ports and protocols.
- Deactivation of network services and devices that are no longer in use.
- Adopting the Zero-Trust principle and architecture, including:

Implement phishing-resistant multi-factor authentication (MFA) for all users and VPN connections. Limiting access to trusted devices and users on networks.

- Continuously identify exposures to attack surfaces that could allow attacks via a compromised network, including unpatched vulnerabilities, misconfigurations, and exposed network ports

- Categorize vulnerabilities according to priorities, from the highest potential first where they are directly related to objects to Ransomware of APT groups, or has a high impact such as impact.
- Sign up for continuous exercises, vulnerability testing (pentest) or connect with a known RedTeam that can test your network for errors or vulnerabilities from which hackers can access your network and system.