Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

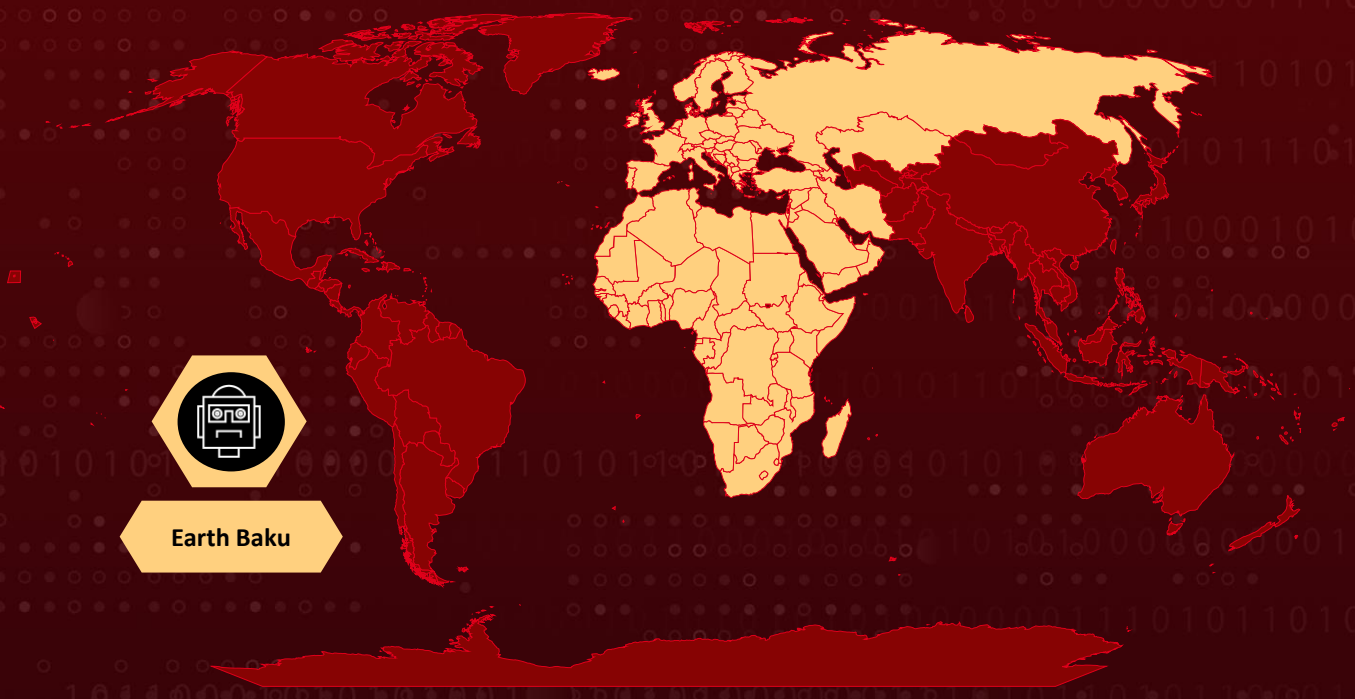
Unmasking Earth Baku: New Tactics and Targets in Cyber Espionage

Date of Publication	Last updated date	Admiralty code	TA Number
August 13, 2024	August 23, 2024	A1	TA2024310

Summary

Attack Began: 2022
Actor Name: Earth Baku (aka APT 41, Double Dragon, TG-2633, Bronze Atlas, Red Kelpie, Blackfly, SparklingGoblin, Grayfly, Redfly)
Targeted Regions: Europe, the Middle East, Africa, Italy, Germany, United Arab Emirates, Qatar, Georgia, and Romania
Malware: StealthVector, StealthReacher (aka DodgeBox), SneakCross (aka MoonWalk), and Cobalt Strike
Targeted Industries: Government, Media and Communications, Telecommunications, Technology, Healthcare, and Education

Actor Map



Actor Details

#1 Earth Baku, an advanced persistent threat (APT) actor, has recently expanded its operations from the Indo-Pacific region to Europe, the Middle East, and Africa (MEA). This shift includes targeting countries such as Italy, Germany, the UAE, and Qatar, with indications of activity in Georgia and Romania as well.

#2 The group's recent campaigns have broadened their focus, now encompassing critical sectors including government, media, telecommunications, technology, healthcare, and education. They exploit public-facing applications, particularly Internet Information Services (IIS) servers, to gain initial access and deploy sophisticated malware, including the Godzilla webshell, which facilitates further control over compromised systems.

#3 Earth Baku's toolkit has evolved to include advanced loaders like StealthVector and StealthReacher, which utilize AES encryption and code obfuscation techniques to evade detection. The newly introduced SneakCross backdoor leverages Google services for command-and-control operations, enhancing its modularity for updates and functionality. After breaching a system, the group employs various tools for persistence and data exfiltration, including a customized tunneling tool, Rakshasa, and MEGAcmd for transferring stolen data to cloud storage.

#4 Earth Baku's advancements in tactics and tools highlight an evolving threat landscape, necessitating robust cybersecurity measures. Organizations are advised to implement best practices such as the principle of least privilege, regular system updates, and proactive incident response strategies to mitigate risks associated with these sophisticated attacks.

Actor Group

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGET REGIONS</th><th>TARGET INDUSTRIES</th></tr>
<tr><td rowspan="3">Earth Baku (aka APT 41, Double Dragon, TG-2633, Bronze Atlas, Red Kelpie, Blackfly, SparklingGoblin, Grayfly, Redfly)</td><td>China</td><td rowspan="3">Europe, the Middle East, Africa, Italy, Germany, United Arab Emirates, Qatar, Georgia, and Romania</td><td rowspan="3">Government, Media and Communications, Telecommunications, Technology, Healthcare, Education</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage and Information theft</td></tr>
</table>

Recommendations

Strengthen Public-Facing Applications: Regularly update and patch public-facing applications like IIS servers to close vulnerabilities that could be exploited for initial access.

Implement Robust Access Controls: Enforce the principle of least privilege, restricting access to critical systems and data, and closely monitor user permissions to prevent lateral movement by attackers.

Enhance Incident Response Capabilities: Develop and regularly test a proactive incident response plan that includes scenarios involving sophisticated malware, persistence mechanisms, and data exfiltration techniques.

Secure Backup Strategies: Follow the 3-2-1 backup rule, ensuring data backups are stored in different formats, with one copy air-gapped and off-site, and regularly test the integrity of these backups to ensure data can be restored in case of an attack.

Advanced Threat Detection and Response: Deploying advanced threat detection and response solutions is essential for identifying and mitigating sophisticated attacks. This includes using Endpoint Detection and Response (EDR) tools, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). These tools can detect unusual activity and provide alerts on potential intrusions, allowing for quicker response times.

Potential MITRE ATT&CK TTPs

TA0011 Command and Control	TA0002 Execution	TA0003 Persistence	TA0010 Exfiltration
TA0005 Defense Evasion	TA0001 Initial Access	TA0004 Privilege Escalation	TA0007 Discovery
TA0040 Impact	TA0008 Lateral Movement	T1027 Obfuscated Files or Information	T1082 System Information Discovery
T1055.012 Process Hollowing	T1055 Process Injection	T1565 Data Manipulation	T1056.001 Keylogging

T1056 Input Capture	T1021.001 Remote Desktop Protocol	T1021 Remote Services	T1071.004 DNS
T1071 Application Layer Protocol	T1133 External Remote Services	T1068 Exploitation for Privilege Escalation	T1059 Command and Scripting Interpreter
T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow	T1480 Execution Guardrails	T1480.001 Environmental Keying
T1027.007 Dynamic API Resolution	T1620 Reflective Code Loading	T1106 Native API	T1562.001 Disable or Modify Tools
T1562 Impair Defenses	T1102.002 Bidirectional Communication	T1102 Web Service	T1573 Encrypted Channel
T1592 Gather Victim Host Information	T1590 Gather Victim Network Information		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	073b35ecbd1833575fbfb1307654fc532fd938482e09426cfb0541ad87a04f75, 07aa971f0791b06dd442d4c7a49c1d3d27a1cbb16602f731e870b5ef50edf69e, 0faddbe1713455e3fc9777ec45adf07b28e24f4c3ddca37586c2aa6b539898c0, 166b6dcdac31f4bf51e4b20a7c3f7d4f7017ca0c30fa123d5591e25c3fa66107, 1c88150ec85a07c3db5f18c5eedcb0b653467b897af01d690ed996e5e07ba8e3, 21fc0f50d545c0a373380934dc61c423c8a31d8c3e6eae4f8a35149ad9962d88, 22a50cea6ad67a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86, 3e52c310c6556367ff9e18448bc41719e603d1cbbdafdcba736c6565529617b6,

TYPE	VALUE
SHA256	773eaba82ef1c502448e533007e92b1afa879b09f85f28b71648668ea62839ff5, 7463700ec5768d4af6549028465f978059611555aa8e22e2b7c664b1cdbfa9ae, 7586e58a569c2a07d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565a, e63c6b9ab3b32beffbc1eb23d6ca7cc59616b0722f0dd4f0d893c0a1724f5d7, 7f24bc080281d250ec88493e5803e488721a17c9382cd54ba8dfbcb785f23a88, 83de8917bf0ac1d670acf27431015215db872b7291979312dd65e30d99806abb, 8405d742405d3a6d3bda6bc49630dd5f3604a3d6ae27cbd533e425f8abbaafdc, a50f85c71b69563ba42bf04c937e1063244ca4957231d3adac76f1c96ab42d3c, ab56501167fe689fe55f6e6ddc3bb91952299bd5c3ef004b02bf1c3b4061c7cf, c02accc26a389397fb172f83258baa8a974986ffd706ba708a3b0a679f61be56, c6a3a1ea84251aed908702a1f2a565496d583239c5f467f5dcd0cfc5bfb1a6db, cdcbd9c25e06ac6da5497fa19459d0007449ec1a3e6bc591334db6fb3598aecb, e4360c0aa995e6e896b22bb7725a6c9b189be8606e7cbbc8b6e80c606358649d, e5f1360d4c299bb32e33e081115f2b520251a983af2ebc649b4b9b70308246fe, ec10a9396dca694fe64366e0dab82d046cf92457f97efd50a68ceb85adef6b74, ec5a96f42aeccdf9a3ae4c3650689606c8539fd65c0b47f30887afecb901be43
IPv4	5[.]182[.]207[.]28, 78[.]108[.]216[.]20, 212[.]87[.]212[.]115
Domains	www[.]mircoupdate[.]https443[.]net, icy-bar-c375[.]microsoft-updates[.]workers[.]dev, www[.]sitennews[.]com, update-chrome[.]realgodad[.]workers[.]dev, track[.]cdn78544[.]ru, www[.]cdn7854[.]workers[.]dev, shrill-tooth-b557[.]vgfjuic[.]workers[.]dev

TYPE	VALUE
MD5	0d068b6d0523f069d1ada59c12891c4a, 294cc02db5a122e3a1bc4f07997956da, 393065ef9754e3f39b24b2d1051eab61, 4141c4b827ff67c180096ff5f2cc1474, 5217b8552321556ea434474377cfcd02, 5b1e8455291d99a1724327b9a7fc2616, 72070b165d1f11bd4d009a81bf28a3e5, 75bfb7d5199bf0c4e62525099b33e14f, b3067f382d70705d4c8f6977a7d7bee4, b69984cbf52b418673bd08279ca845d6, bc85062de0f70afd44bb072b0b71a8cc, bcac2cbda36019776d7861f12d9b59c4, bfd6286bb39a0e24a2af28c63bd8e194, d72f202c1d684c9a19f075290a60920f, f062183da590aba5e911d2392bc29181, f0953ed4a679b987a2da955788737602, f68ef9e40462c9760bf9c829edd9f4a9, 28072e4a3bc3376aba096045824f4c34, c33247bc3e7e8cb72133e47930e6ddad, e9625ce47b87085b66e0ee6e17ecb333, ee7faba27a2c5f7acb5b06e94aa318e0, f42867e74bbc41767bffacc0de7bfa5e
SHA1	13c1c6752006667697cd4f72a2f1b8616af2b60e, 144550355b3dfb67a0ef65dc7f69470b4faf4ca1, 2cc76a0434a1d489c1547c7021a3dd68499141c3, 2fce25afb8a29fcd526f61ba30f14dcc7ecfad3e, 3872c38625ca62de3bcbe29740c1a0b8921fcf48, 54a0dd2003a6dfc5fd035ba3aabb9fd96b5bd09e, 5b46b63e31f307757cedf305005ce9990a07cbf4, 66fb63e6e49c2c201a0b6204e1d0269812a4b662, 8d8161a7fcd835781820e4921039525975f9324d, a555bb5b6b0e9edf49c4f6bfc8638f155dc1986a, ba6d77f358b4fa00dda5d0e2fdd21c761d154f95, d3fdf103e8585192452bb43e902f009c7bc066a3

References

https://www.trendmicro.com/en_us/research/24/h/earth-baku-latest-campaign.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/h/earth-baku/ioc-a-dive-into-earth-baku-latest-campaign.txt

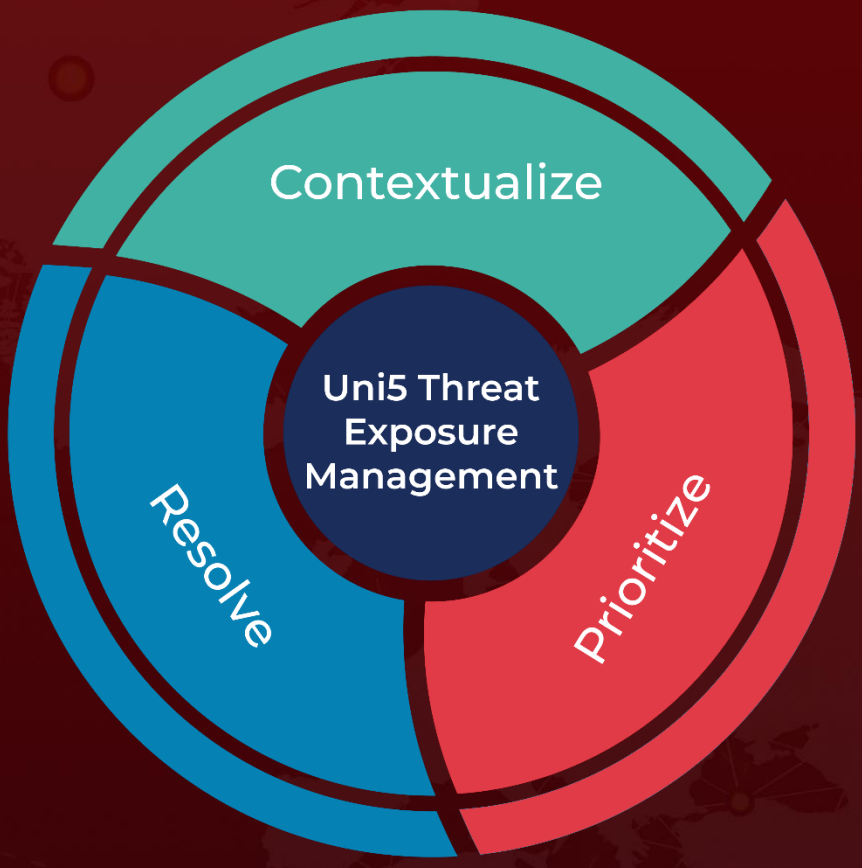
https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1

https://www.zscaler.com/blogs/security-research/moonwalk-deep-dive-updated-arsenal-apt41-part-2

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

August 13, 2024 • 5:30 AM

More at www.hivepro.com