Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

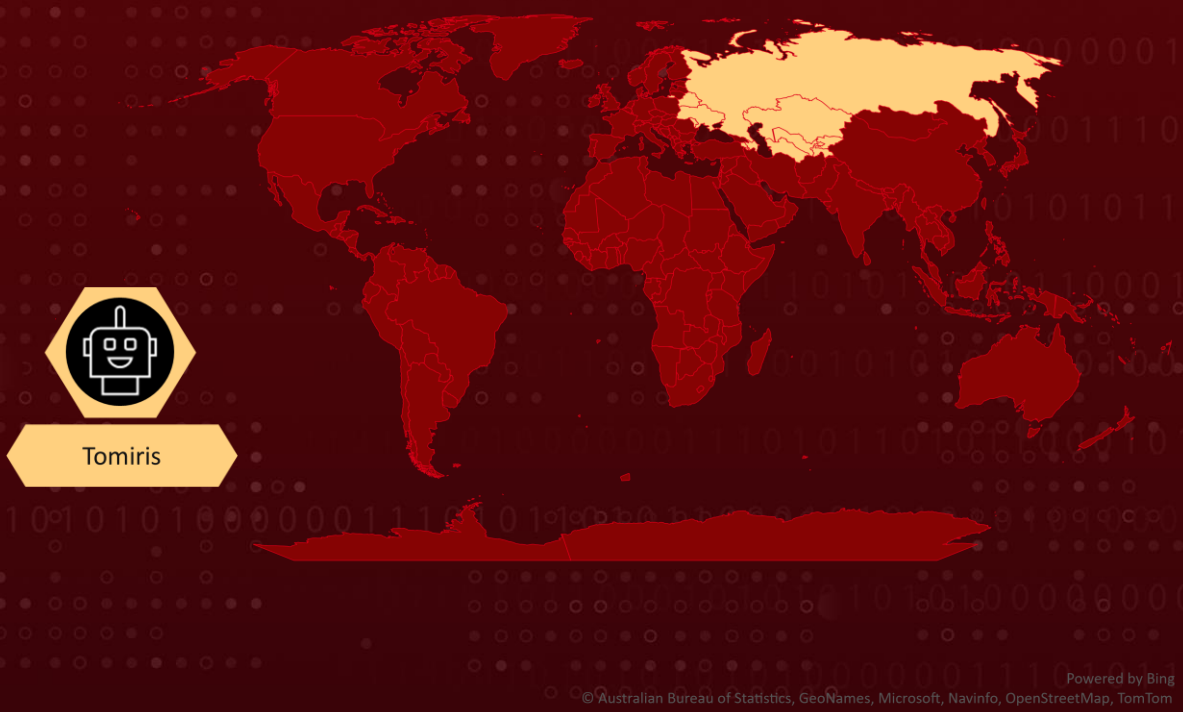
New Tomiris APT Group Targets Governments

Date of Publication	Admiralty code	TA Number
April 25, 2023	A1	TA2023198

Summary

First Appearance: September 2021
Actor Name: Tomiris
Target Countries: Commonwealth of Independent States (CIS)
Target Sectors: Government and Diplomatic Entities

Actor Map



Actor Details

#1 Tomiris is a Russian-speaking advanced persistent threat (APT) group that has been active since at least 2021. Tomiris is known for its use of sophisticated tactics and tools, including zero-day exploits and custom malware implants. The group has been observed using a range of malware, including the Tomiris implant, which is a Golang-based backdoor that allows the group to execute commands on infected systems and exfiltrate sensitive data.

#2 Tomiris is also known for its use of supply chain attacks and domain hijacking tactics, which involve taking over legitimate websites and using them to distribute malware to unsuspecting victims. In one notable incident, the group was observed taking over the website of the Ministry of Foreign Affairs of Kyrgyzstan to distribute malware to visitors.

#3 Despite some initial speculation that Tomiris may be linked to the Turla APT group, we have concluded that the two groups are likely separate entities, although they may share some tools and techniques. Tomiris is thought to be a relatively new and emerging threat actor, and its activities are likely to continue to be closely monitored by cybersecurity researchers and government agencies.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Tomiris	Russia	Commonwealth of Independent States (CIS)	Government and Diplomatic Entities
	MOTIVE		
	Information theft & Espionage		

Recommendations

- Keep all software and systems up-to-date with the latest security patches and updates to mitigate against known vulnerabilities that may be exploited by Tomiris.
- Implement strong authentication and access controls, including two-factor authentication and privileged account management, to reduce the risk of unauthorized access to sensitive systems and data.
- Educate employees on how to recognize and report suspicious activity, including phishing emails and other social engineering tactics used by Tomiris and other APT groups. Regular security awareness training can help improve overall cybersecurity posture.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0011** Command and Control	**TA0010** Exfiltration
T1059 Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation	**T1566** Phishing	**T1027** Obfuscated Files or Information
T1189 Drive-by Compromise	**T1041** Exfiltration Over C2 Channel	**T1127** Trusted Developer Utilities Proxy Execution	**T1110** Brute Force
T1105 Ingress Tool Transfer	**T1049** System Network Connections Discovery		

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	edb0c08f8b6bb179b4395d8a95619d07 c49dbf390e876e926a338ea07ac5d4a7 485a08c6ff6a8b05fab42facc0225035 6b567779bbc95b9e151c6a6132606dfe 51aa89452a9e57f646ab64be6217788e 20c9ca66d2844edb94a623e77accaa5f 5d6b920fd8f3b5a3a8c9dead25e3a255 4452290e674ab521fa0941d45cc6b22f e59752ffc116388dd863fc2e30e4aaea 47870ff98164155f088062c95c448783 a80bbd753c07512b31ab04bd5e3324c2 9be1cccd8e6ff0bd2ad7868a7c1308c0 66357e47bbc2ec5694e2c5de9cc3b9c6 d3e1043cf5382e97685340760c9d3d61 0f092bfc9f9adaf93750df4ae3cdc0f7 8674100d43231294b6562717a9ab3a07 d09f792e5ea9f1239f3454fd1ce7893c fd59dd7bb54210a99c1ed677bbfc03a8 bcd52718195416b47c3538a89b62c305 daf4f59224cc7c5e94c924f43a76f300 d1986646b9be824414845f8e98c7961b 45a857603e0e72174452fd073ad373de 11ed3f8c1a8fce3794b650bbdf09c265 92c6d7fb1118d2e276dd4ad878db37f6 796c232286743b95fed38d9d5c74f879 956cefc9a1759078ccf75b192db10ced 67340dba1c379a84df88e639608de310 d83b31fe5f0144468aad4619c2418ac8 447cf4a077f17096ca16a29333b7a046 10b315fb7d8ba8d69337f04ed3891e75 322837acdcedc952587e7be9886ddffd 778d491e9742199b558e84a27c559612
SHA1	66271b2536481a6b2a3ae21412ce5ef50a692cfa 19357154ff3e43c968fd09f61db1e6e8084384fa c56991857a9c09e25f3dd56066b4a322cc5c03d9 4a572e67a799ebbb2b9d7260aedb780e3005be51 23f388aced4b1732744cbd5fca1a24b8a82c01a9 aa494696a413b652e667cbbb7ccee35a68b45c87 245b78c615c57abaf46235f184a727587c882b69 cac58134db8bb3c6b0d8f21957cadb9110fa3727 53baccf15963dc85447cc822ec95ef8ed0326ac6 4040bb7e4ebc98c22bda98680b207ec89767b759 c1b7547da13b7c78cd6c5c354af945b2eff767c9 98f1a215cd87e08d33f0d2ba13020661e629c6b8

TYPE	VALUE
SHA1	6161aa9d9888472647a9792eead944bfc678c920 5a368354696d06319a050071f48bc6767d92b49a 292c3602eb0213c9a0123fdaae522830de3fad95 9902917a3af585e695141caf347a2f19a065a7df f918e5f50bb3b73a732bc9cb3595bff2ea7b761f e2f191b251ba5c57cdbb5a6d3bfab57957900fcf 90f1e9fb5845f985cd0995c75e0746a8e47cf8e9 ce9db7dbf3368757c232aa960bbfa7b83278618d 0be035e2d7180a908566a6bdaa907ed74b08b790 7bb6e4a1ede35867ce5c57b5668f6aacae025b81 15e710a107830b193124a6d2bbc785b9383262a9 98059a86b681b0b8a09a95def3ef874c531b1d66 459b17c42017cfdfc7eb804b5c0ee52aa6035d78 902b27a5fd2e5f17e5340e350afa037549ce9faa 752678274224bf9fef83843e44820f6bcd738758 0b6e1df37ba89d3d35b4b18afc0ffeb46644ff76 a0de69ab52dc997ff19a18b7a6827e2beeac63bc da6635def86b50a5de25f148426f68d3d8ab450a bc9314760071a4aef12e503104478059808e7047 f8d87d5b251671af624c3eaf7ac5cc42a0acadd0
SHA256	00466d76832193b3f8be186d00e48005b460d6895798a67bc1c21e 4655cb2e62 df75defc7bde078faefcb2c1c32f16c141337a1583bd0bc14f6d93c13 5d34289 fd7fe71185a70f281545a815fce9837453450bb29031954dd2301fe 4da99250d 80721e6b2d6168cf17b41d2f1ab0f1e6e3bf4db585754109f3b7ff99 31ae9e5b cb78495bee37e768ef4566aa1c2cfb5478bae779127430f90c3da75 e407350b8 0767806f5734dca1553cae6a835c24a6d92abd678928b64f70dbd8 811ed44aca 0fc624aa9656a8bc21731bfc47fd7780da38a7e8ad7baf1529ccd70a 5bb07852 3f94b20cb7f4ff55207660649ebbb02679c991fe03efbcb0bd3840fc 7f0bd527 29314f3cd73b81eda7bd90c66f659235e6bb900e499c9cc7057d10a 9083a0b94 009406c1c7c0b289a25d44dfaa8364633d9b71df5f3c7a65deec1ef0 0a8c2ebb 046f11a6c561e46e6bf199ab7f50e74a4d2aaead68cdbd6ce44b37b 5b4964758 85295ab44d0903a2cf4cbdcae55129a40cf5f7fb7210a304fa91a869 29fd2cd9 0dfbc54a5a88f27e52807873c20872bc6bf92b822de90545492081c 4e4f96778

TYPE	VALUE
SHA256	9c086f242120be7a9e57e06b75d8ef6f051a77c6339deaeb574e80ee69590111 a4ea3462bd5aedccc783d18d24589018c257b2a6e092164c01de067a8e3cd649 296599df29f4ffa9bf753ff9440032d912969d0bab6e3208ab88b350f9a83605 69bb729ff354cd9651f99a05f74f3ea20d483dc8e6e5838e4dd48858fd500d29 c9db4f661a86286ad47ad92dfb544b702dca8ffe1641e276b42bec4cde7ba9b4 8391c182588b79697337e401a6424c12b3d707c00c15a17ec59059deedb0e2c4 8ec159179d49b44849febe7ed522c8fb836d5658ef868db41d2181fb4b1cbd3f b144229fb62799aa23537eaf0ce267b1445a182c28f4679e8f8234eeb5e603f3 e2d4d030542a44a8d4cc8b97da7b26487570dda432a736766dd2ab6d57a3b787 4f237b5aa3ff4fc4e3014f693c27a1cba94fc24f3a6054c28d090592343c06a2 358411a3b4a327805d629612b1b64357efe5389e56ddae9128ababbc8a2357a1 65da1696d36da254779a028b881a1890b0b037e7eee8ea0a9446c8bb0729c1cf c5a9be4055e5f00bf3f2e6c57ba1b796157a74406657fd554d69491868cd5925 5e66256adbf973f6ab2252c14d6f0d8da2d326f52f6433bcf3a7cd7c60ae8f01 e152322530819d196fb411a0cb12cf4bcc94975b400a17b95f0fc2e28f6493e5 352f9cd4c14c1002d6c8d902cbca4e96d03a8bb243b33dd192a2260fe66091a1 4c8eddeab2d40178712685d09da5187b996389fba62c7f9b9635b07060b1e013 98275bfe968d5998230bdf18de1be795b5ad42bd82b5ecb1405b00afba6f533d 9cd10a2d9db9cf1c5b3454c323fd148f5a322b4100f35e0a73ed4632038631cc

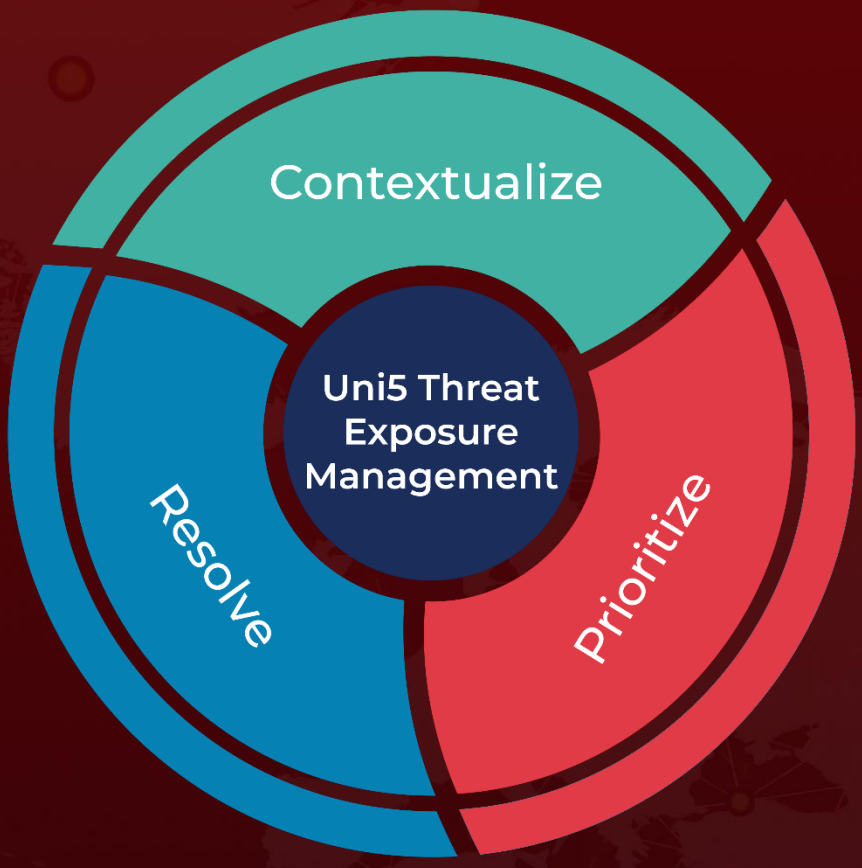
References

https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

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 25, 2023 • 4:30 AM

More at www.hivepro.com