Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

ScarCruft Unleashes Tailored Attacks on Cybersecurity Frontlines

Date of Publication	Admiralty Code	TA Number
January 23, 2024	A1	TA2024028

Summary

Attack Commenced: December 13, 2023
Threat Actor: ScarCruft (aka Reaper, TEMP.Reaper, APT 37, Ricochet Chollima, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet)
Malware: RokRAT backdoor
Targeted Industries: Media, Cybersecurity Professionals, Defense, Education
Attack Region: South Korea
Attack: The ScarCruft APT group is actively targeting attacks on media organizations and individuals in the realm of threat intelligence. ScarCruft employs persistent tactics, using phishing emails to deliver RokRAT, a custom-designed backdoor.

Attack Regions

Attack Details

#1 The state-sponsored advanced persistent threat (APT) group known as ScarCruft is actively preparing for targeted attacks on media organizations, educational institutions, and individuals involved in threat intelligence, particularly cybersecurity professionals.

#2 Employing persistent tactics since December 2023, ScarCruft uses phishing emails that pose as presentation materials related to fictitious events tailored to specific targets. ScarCruft utilizes large Windows Shortcut (LNK) files to initiate complex infection chains, delivering RokRAT, a custom-designed backdoor associated with the threat group.

#3 RokRAT is a comprehensive backdoor equipped with features that empower its operators to effectively surveil the targeted entities. Notably, RokRAT leverages public Cloud services for command-and-control purposes, employing platforms like pCloud and Yandex Cloud to camouflage malicious communications within seemingly legitimate network traffic.

#4 A recurring pattern in ScarCruft's activities is the registration of domains through Namecheap, followed by parking the domain on a Namecheap IP address before transitioning to Cherry Servers. The adversary's commitment to innovation is evident in ScarCruft's malware testing activities, indicating a strategic focus on enhancing its arsenal and broadening its target spectrum, potentially impersonating cybersecurity professionals or businesses.

Recommendations

Enhance Email Security Measures: Strengthen email security protocols to mitigate the risk of falling victim to ScarCruft's phishing attacks, which often involve emails posing as presentation materials.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect any suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Heighten Employee Awareness: Educate employees on cybersecurity best practices, emphasizing the importance of vigilance against phishing attempts. Encourage reporting of any suspicious emails or activities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**T1566** Phishing	**T1598.002** Spearphishing Attachment	**T1204.002** Malicious File
T1105 Ingress Tool Transfer	**T1005** Data from Local System	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1204 User Execution	**T1562** Impair Defenses	**T1083** File and Directory Discovery	**T1041** Exfiltration Over C2 Channel
T1537 Transfer Data to Cloud Account			

Indicators of Compromise (IOCs)

TYPE	VALUE
Email	c039911[@]daum[.]net, kirnchi122[@]hanmail[.]net
IPv4	84.32.129[.]32, 84.32.131[.]104, 84.32.131[.]30, 84.32.131[.]50, 84.32.131[.]59, 84.32.131[.]66, 84.32.131[.]87

TYPE	VALUE
URLs	hxxp[://]app[.]documentoffice[.]club/salt_view_doc_words?user=8B86CA616964A84Y7A75B950, hxxp[://]app[.]documentoffice[.]club/salt_view_doc_words?user=H11I75PFF0ZG53NDG00H64OE, hxxp[://]app[.]documentoffice[.]club/salt_view_doc_words?user=MZ9IUNQ7KX7GSLO5LY8HTMP6, hxxp[://]app[.]documentoffice[.]club/voltage_group_intels?user=HE16AJHVFCZ48HFTGD059IGU, hxxp[://]nav[.]offlinedocument[.]site/capture/parts/you?view=5JV0FAGA6KW1GBHB7LX2HCIC, hxxp[://]nav[.]offlinedocument[.]site/capture/parts/you?view=GV6BQLRKHW7CRMSLIX8DSNTM, hxxp[://]nav[.]offlinedocument[.]site/capture/parts/you?view=IV3D9YMNJW4EAZNOKX5FB0OP
Domains	app[.]documentoffice[.]club, benefitinfo[.]live, benefitinfo[.]pro, benefiturl[.]pro, careagency[.]online, cra-receivenow[.]online, crareceive[.]site, depositurl[.]co, depositurl[.]lat, direct.traderfree[.]online, forex.traderfree[.]online, groceryrebate[.]online, groceryrebate[.]site, gstcreceive[.]online, instantreceive[.]org, nav[.]offlinedocument[.]site, receive[.]bio, receiveinstant[.]online, rentsubsidy[.]help, rentsubsidy[.]online, tinyurlinstant[.]co, urldepost[.]co, verifyca[.]online, visiononline[.]store
SHA1	0ed884a3fc5c28cdb8562cd28993b30991681b0a, 2f78abc001534e28eb208a73245ce5389c40ddbe, 39c97ca820f31e7903ccb190fee02035ffdb37b9, 4024a9b0c0f19a33a3c557c7e220b812ee6fdd17, 46c3f9de79d85165e3749824804235aca818ba09, 483b84f973528b23e5c14bc95fbc7031a4b291f1, 4c74e227190634a6125b2703b05cb16ad69ac051, 577c3a0ac66ff71d9541d983e37530500cb9f2a5,

TYPE	VALUE
SHA1	7c4e37e0a733b5e8f0f723cca2a9675901527dc4, 88db1e2efbb888a97a530c8bef8ca104ceaab80c, 8951f3eb2845c0060e2697b7f6b25abe8ade8737, 9dd8aa1d66cc4e765e63dc5121216d95e62a0e1c, 9e0c6a067aab113e6a4b68299ab3b9d4c36fc330, 9eaaab9d4f65e3738bb31cdf71462e614ffbd2ba, b23a3738b6174f62e4696080f2d8a5f258799ce5, b91b318a9fbb153409a846bf173e9d1bd0cc4dbf, c4b58ca12f7b16b6d39ce4222a5a2e054cd77b4e, d457d6bdcfa6d31934fb1e277fa0de7119e9c2a5, d9ac0cc6d7bdc24f52878d3d5ac07696940062d0, e46907cfaf96d2fde8da8a0281e4e16958a968ed, e9df1f28cfbc831b89a404816a0242ead5bb142c, Fbf4d8c7418b021305317a185b1b3534a2e25cc8

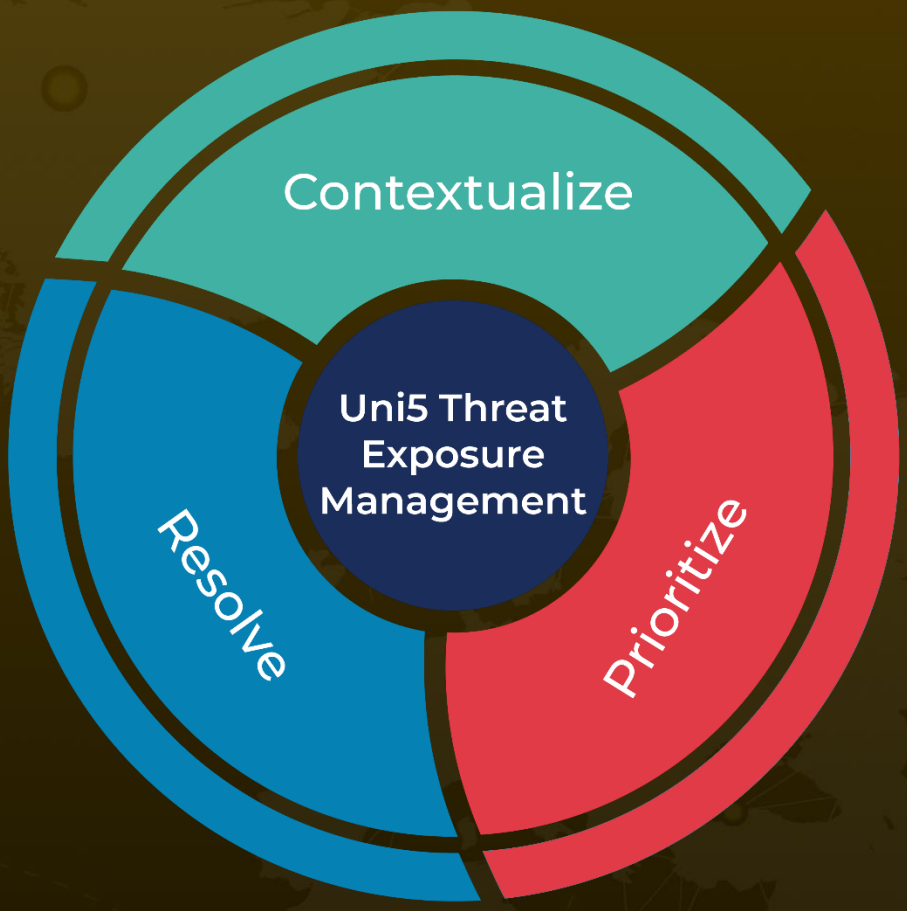
References

https://www.sentinelone.com/labs/a-glimpse-into-future-scarcruft-campaigns-attackers-gather-strategic-intelligence-and-target-cybersecurity-professionals/

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

January 23, 2024 • 3:00 AM

More at www.hivepro.com