Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

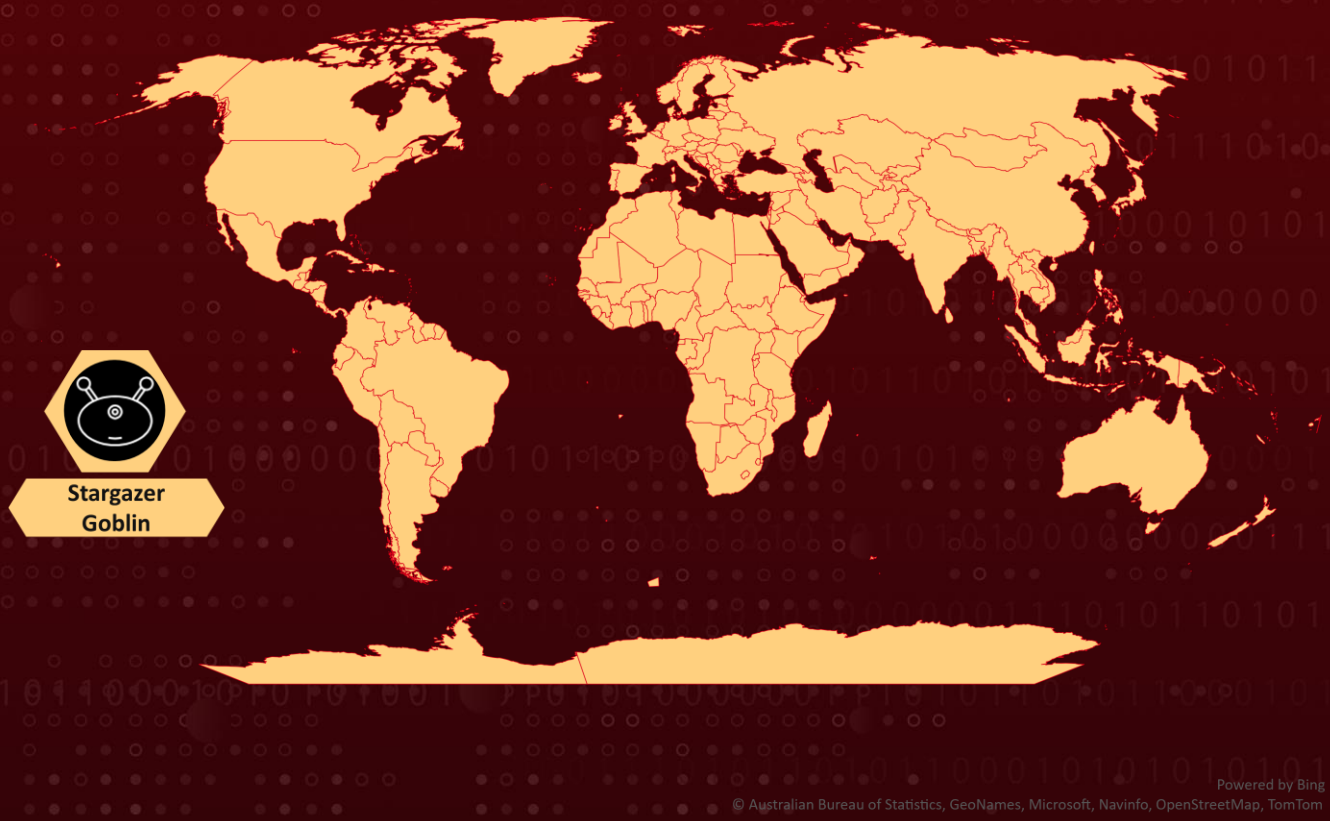
Stargazers Ghost Network: 3,000 Rogue GitHub Accounts Fuel Malware Spread

Date of Publication	Admiralty Code	TA Number
July 31, 2024	A1	TA2024289

Summary

Active Since: August 2022
Threat Actor: Stargazer Goblin
Malware: Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer, and RedLine
Targeted Region: Worldwide
Attack: Stargazer Goblin, a highly sophisticated cybercriminal group, operates the 'Stargazers Ghost Network' on GitHub. This advanced Distribution as a Service (DaaS) platform utilizes over 3,000 fraudulent accounts to spread various types of information-stealing malware.

Attack Regions



Attack Details

#1 Stargazer Goblin is a sophisticated threat actor group responsible for operating the "Stargazers Ghost Network" on GitHub. This advanced network functions as a Distribution as a Service (DaaS) platform, utilizing over 3,000 fraudulent accounts to disseminate information-stealing malware, including Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer, and RedLine.

#2 Since June 2023, Stargazer Goblin has been actively promoting this malware distribution service on the dark web. The development or testing of the Stargazers Ghost Network initially began on a smaller scale around August 2022. Stargazer Goblin's early earnings were approximately $8,000.

#3 However, this is a mere fraction of the revenue generated during their more extensive campaigns from mid-May to mid-June 2024, with total estimated earnings of around $100,000 throughout the operation's lifespan. The Stargazer Goblin group employs "ghost accounts" within the Stargazers Ghost Network to engage in activities such as starring, forking, and subscribing to malicious repositories, thereby lending them an appearance of legitimacy.

#4 GitHub's reputation as a trusted service reduces users' suspicion, making them more likely to click on links within these repositories. The malicious repositories are cleverly named and tagged to attract users with interests in cryptocurrency, gaming, and social media. Different categories of GitHub accounts manage distinct aspects of the scheme to enhance the network's resilience against takedown efforts.

#5 These include accounts responsible for the phishing repository template, accounts providing images for the phishing template, and accounts pushing malware disguised as password-protected archives of cracked software and game cheats.

#6 If any accounts in the third category are detected and banned by GitHub, Stargazer Goblin swiftly updates the phishing repository with a new link to an active malicious release, ensuring minimal disruption to their operations. The Stargazers Ghost Network is just one part of a larger DaaS ecosystem, with other ghost accounts operating across platforms like Discord, Facebook, Instagram, X, and YouTube, further expanding their reach and impact.

Recommendations

Exercise Caution with File Downloads and URLs: When accessing GitHub repositories via Google Search results, YouTube videos, Telegram, or social media, be extremely vigilant about the files you download and the URLs you click.

Handle Password-Protected Archives with Care: Since antivirus software cannot scan password-protected archives, take extra precautions by extracting these files on a Virtual Machine (VM) to isolate potential threats and then scan the contents with antivirus software. If a VM is unavailable, use VirusTotal to upload and scan the archive, provided it contains only a single file.

Verify Repository Authenticity: Check the legitimacy of GitHub repositories by examining the account activity and history. Suspicious accounts may have recently created repositories with little to no genuine development history.

User Education and Awareness: Educate users about the risks of suspicious GitHub repositories and the importance of cautious behavior when receiving files and links. Promote awareness of the steps needed to enable the installation of unknown apps, highlighting the associated risks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0042 Resource Development	T1204 User Execution
T1566 Phishing	T1189 Drive-by Compromise	T1059 Command and Scripting Interpreter	T1071 Application Layer Protocol
T1027 Obfuscated Files or Information	T1036 Masquerading	T1212 Exploitation for Credential Access	T1083 File and Directory Discovery
T1585 Establish Accounts	T1585.001 Social Media Accounts	T1608 Stage Capabilities	T1608.001 Upload Malware

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxps[:]//vivaciousdqugilew[.]shop, hxxps[:]//sturdyregularrmsnhw[.]shop , hxxps[:]//understanndtytonyguw[.]shop, hxxps[:]//stickyyummyskiwffe[.]shop, hxxps[:]//standingcomperewhitwo[.]shop, hxxps[:]//slamcopynammeks[.]shop, hxxps[:]//sideindexfollowragelrew[.]pw, hxxps[:]//relaxtionflouwerwi[.]shop, hxxps[:]//patternapplauderw[.]shop, hxxps[:]//messtimetabledkolvk[.]shop, hxxps[:]//macabrecondfucews[.]shop, hxxps[:]//lamentablegapingkwaq[.]shop, hxxps[:]//innerverdanytiresw[.]shop, hxxps[:]//horsedwollfedrwos[.]shop, hxxps[:]//greentastellesqwm[.]shop, hxxps[:]//distincttangyflippan[.]shop, hxxps[:]//detailbaconroollyws[.]shop, hxxps[:]//deprivedrinkyfaiir[.]shop, hxxps[:]//considerrycurrentyws[.]shop, hxxps[:]//github[.]com/bludmooncutie2/bludmooncutie2/releases/tag/latest, hxxps[:]//github[.]com/witch12138/test/releases/tag/lat, hxxps[:]//github[.]com/soulkeeper500/soulkeeper500/releases/tag/lat, hxxps[:]//github[.]com/xumuk71discoatoh/xumuk71discoatoh/releases/tag/new, hxxps[:]//goo[.]su/gisof1sda, hxxps[:]//github[.]com/zigzagcharming643/zigzagcharming643/releases/tag/lat
SHA256	ab59a8412e4f8bf3a7e20cd656edacf72e484246dfb6b7766d467c2a1e4cdab0, a484fa09be45608e23d8e67cd28675fa3e3c4111af396501385256ce34ff1d95, 98b7488b1a18cb0c5e360c06f0c94d19a5230b7b15d0616856354fb64929b388, 8d8d7eb1180c13ed629dceac6c399c656692a6476c49047e0822bec6156a253a, 64a49ff6862b2c924280d5e906bc36168112c85d9acc2eb778b72ea1d4c17895, 385ebe3d5bd22b6a5ae6314f33a7fa6aa24814005284c79edaa5bdcf98e28492,

TYPE	VALUE
SHA256	2f5624dcda1d58a45491028acc63ff3f1f89f564015813c52eebd80f51220383, 2ebf051f6a61fa825c684f1d640bfb3bd79add0afcff698660f83f22e6544cba, 2b6c8aa2ac917d978dfec53cef70eaca36764a93d01d93786cc0d84da47ce8e6, 148c456e83e746a63e54ec5abda801731c42f3778e8eb0bf5a5c731b9a48c45d, 060de3b4cf3056f24de882b4408020cee0510cb1ff0e5007c621bc98e5b4bdf3
IPv4	185[.]172[.]128[.]95
IPv4:Port	147[.]45[.]44[.]73[:]1488, 147[.]45[.]47[.]64[:]11837, 147[.]78[.]103[.]199[:]2529, 89[.]23[.]98[.]116[:]1444

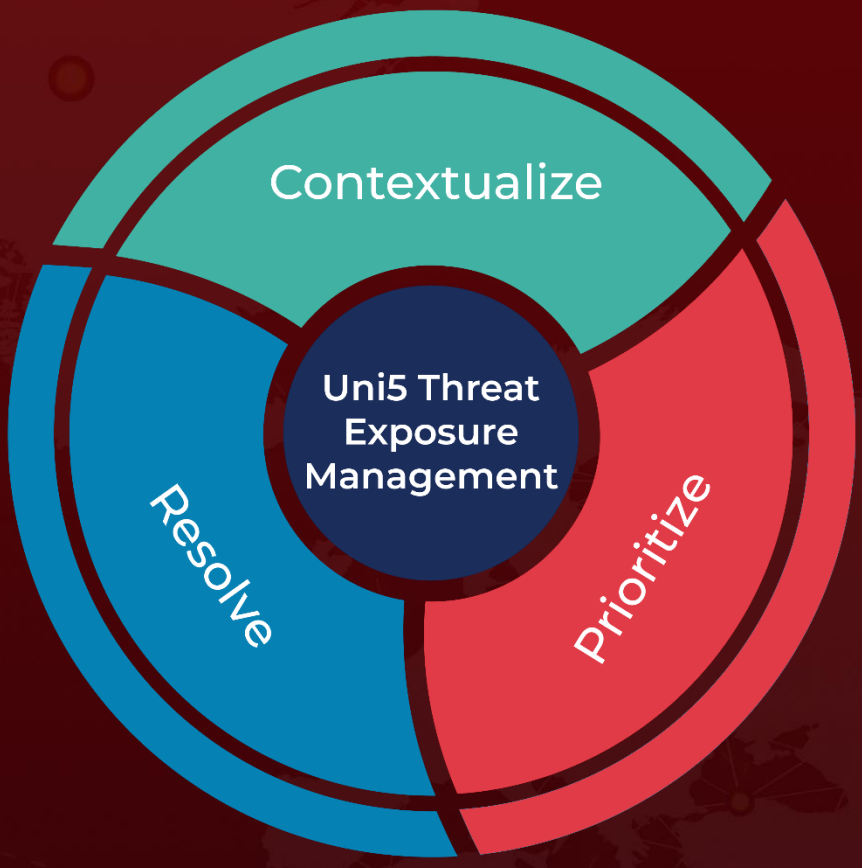
References

https://research.checkpoint.com/2024/stargazers-ghost-network/

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

July 31, 2024 • 1:00 AM

More at www.hivepro.com