مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Ghost Network Spreading Malware on GitHub

Tracking #:432316099

Date:29-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the discovery of "Stargazers Ghost Network", a network used to facilitate the distribution of malware and malicious links.

TECHNICAL DETAILS:

The Stargazers Ghost Network is a sophisticated cyber threat network recently discovered by Check Point Research. Operating on GitHub, it facilitates the distribution of malware and malicious links through a network of fake accounts.

Features:

- **Ghost Accounts**: The network comprises over 3,000 active Ghost accounts that manage various roles, including starring, forking, and creating malicious repositories.
- **Distribution as a Service (DaaS)**: Threat actors can share malware or links via this network, making it a convenient platform for cybercriminals.
- **Malware Families**: The network distributes various malware families, including **Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer, and RedLine**.

Targeted Platform:

- The Stargazers Ghost Network primarily targets GitHub repositories. Its focus on a developer platform allows it to infiltrate software projects and potentially compromise codebases.

Operational Tactics:

- **Phishing Repositories**: The network creates fake repositories containing malicious code or links. Unsuspecting developers may unknowingly include these repositories in their projects.
- **Ghost Accounts**: The Ghost accounts follow legitimate repositories, giving them an appearance of authenticity. When developers follow back, they inadvertently expose themselves to the network's malicious content.
- Employs password-protected archives to evade detection by standard scanning solutions.
- Other campaigns utilized tactics such as shortened links and deceptive README.md templates.

Impact:

- **Malware Distribution**: It facilitates the widespread distribution of malware, potentially compromising sensitive data.
- **Developer Risk**: Innocent developers may inadvertently interact with malicious repositories, leading to codebase compromise.
- **GitHub Reputation**: The network tarnishes GitHub's reputation as a secure collaboration platform.

INDICATORS OF COMPROMISE(IOCs):

Description	Value
Atlantida – HTA	2B6C8AA2AC917D978DFEC53CEF70EACA36764A93D01D93786CC0D84DA47CE8E6
Atlantida – MHTML	385EBE3D5BD22B6A5AE6314F33A7FA6AA24814005284C79EDAA5BDCF98E28492
Atlantida – Powershell	2EBF051F6A61FA825C684F1D640BFB3BD79ADD0AFCFF698660F83F22E6544CBA
Atlantida – .NET Injector	AB59A8412E4F8BF3A7E20CD656EDACF72E484246DFB6B7766D467C2A1E4CDAB0
Atlantida – C&C	185.172.128[.]95
Rhadamanthys – GO downloader	060DE3B4CF3056F24DE882B4408020CEE0510CB1FF0E5007C621BC98E5B4BDF3
Rhadamanthys – GO downloader – C&Cs	147.45.44[.]73[:]1488
	89.23.98[.]116[:]1444
Rhadamanthys – GO Loader	64A49FF6862B2C924280D5E906BC36168112C85D9ACC2EB778B72EA1D4C17895
Rhadamanthys – C&C	147.78.103[.]199[:]2529
Lumma Stealer	148C456E83E746A63E54EC5ABDA801731C42F3778E8EB0BF5A5C731B9A48C45D
	2F5624DCDA1D58A45491028ACC63FF3F1F89F564015813C52EEBD80F51220383
	98B7488B1A18CB0C5E360C06F0C94D19A5230B7B15D0616856354FB64929B388
	A484FA09BE45608E23D8E67CD28675FA3E3C4111AF396501385256CE34FF1D95
Lumma – C&Cs	hxxps://considerrycurrentyws[.]shop
	hxxps://deprivedrinkyfaiir[.]shop
	hxxps://detailbaconroollyws[.]shop
	hxxps://distincttangyflippan[.]shop
	hxxps://greentastellesqwm[.]shop
	hxxps://horsedwollfedrwos[.]shop
	hxxps://innerverdanytiresw[.]shop
	hxxps://lamentablegapingkwaq[.]shop
	hxxps://macabrecondfucews[.]shop
	hxxps://messtimetabledkolvk[.]shop
	hxxps://patternapplauderw[.]shop
	hxxps://relaxtionflouwerwi[.]shop
	hxxps://sideindexfollowragelrew[.]pw

Description	Value
Lumma – C&Cs	hxxps://slamcopynammeks[.]shop
	hxxps://standingcomperewhitwo[.]shop
	hxxps://stickyyummyskiwffe[.]shop
	hxxps://sturdyregularrmsnhw[.]shop hxxps://understanndtytonyguw[.]shop
	hxxps://vivaciousdqugilew[.]shop
RedLine Stealer	8D8D7EB1180C13ED629DCEAC6C399C656692A6476C49047E0822BEC6156A253A
RedLine – C&C	147.45.47[.]64[:]11837

RECOMMENDATIONS:

- Patch Management: Prioritize regular updates for operating systems, applications, and security software to address vulnerabilities.
- Block the IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Email Filtering and Gateway Security: Deploy robust email filtering solutions that can detect and block phishing emails.
- Network Monitoring and Threat Intelligence: Continuously monitor network traffic for signs of communication with known malicious domains or IP addresses.
- Layered Security: Combine endpoint security with robust antivirus/anti-malware for advanced threat detection, prevention, and removal.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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