K logix

BE CONFIDENT.

AUGUST 2023 | THREAT INTEL NEWSLETTER

WormGPT and SCARLETEEL

C-Suite level threat review by applicable business area addressing active threats.

Cyber defenders will seek to reduce potential entry vectors into their organization. To appropriately allocate resources that account for the existing threat landscape, it is recommended to take notice of the ways in which attackers gain initial access into an organization. The MITRE ATT&CK framework has identified 9 techniques attackers use to gain initial access into a victim's network. This report highlights two of those techniques, phishing, and exploitation of a vulnerability in a public-facing application.

WormGPT:

Threat actors have released a malicious version of OpenAI's ChatGPT called WormGPT. Adversaries can utilize it for nefarious activity without needing to circumvent the safeguards other generative AI tools have in place to prevent such activity. WormGPT makes it easier for attackers to send phishing emails, generate malicious code and conduct reconnaissance, to name a few applications.

SCARLETEEL:

SCARLETEEL is a financially motivated threat actor knowledgeable in AWS, which aided them in their latest campaign to steal data and resources from organizations' AWS environment. This threat actor was first discovered in February by Sisdig and has since improved its capabilities to evade detection, establish persistence, and amplify impact. A trend of targeting specific industries has not yet emerged.

WormGPT

Threat Level: Medium

Attack:

There are a number of ways threat actors can make use of WormGPT for malicious goals, one of which is phishing emails to gain initial access into an organization (MITRE T1566) and / or steal funds. WormGPT can help attackers efficiently create compelling, personalized and grammatically correct phishing emails. Using WormGPT for this purpose, threat actors can scale operations and reduce the likelihood of an email security tool flagging it as suspicious.

Remediation:

- Set your email security tool to flags keywords typically associated with email phishing such as "urgent." This may encourage the recipient to take a second look at the email to verify it is not malicious.
- Conduct phishing simulations on all users, including executives, and follow-up with users who fail the simulation.
- Connect with your email security vendor to learn how they are utilizing generative AI to detect and quarantine suspicious emails.

SCARLETEEL

Threat Level: Low

Attack:

In a recent successful intrusion, SCARLETEEL gained access to an organization's AWS environment by exploiting a vulnerability in a public facing service (MITRE T1190). Once inside, the adversary conducted discovery (MITRE TA007) and launched a cryptominer (MITRE T1496). In its discovery process, the attackers ran a bash script to find and exfiltrate information, such as user credentials. The threat actor then utilized compromised credentials to move laterally across the environment to find and exfiltrate proprietary data. To evade defenses, SCARLETEEL disabled cloud logs (MITRE T1562.008).

Remediation:

- Consider acquiring a Cloud Security Posture Management (CSPM) solution to identify and remediate misconfigurations across your organization's cloud environment.
- Considering acquiring a Cloud Infrastructure Entitlement Management solution to manage identities and privileges in the cloud.
- Implement a process to patch public facing applications in a timely fashion.
- Ensure the principle of least privilege is implemented and maintained in your organization's cloud environment.

WormGPT Details:

- **Examination of WormGPT by the organization that discovered it: https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/**
- **Additional information on WormGPT:** https://www.csoonline.com/article/646441/wormgpt-a-generative-ai-tool-to-compromise-business-emails.html

SCARLETEEL Details:

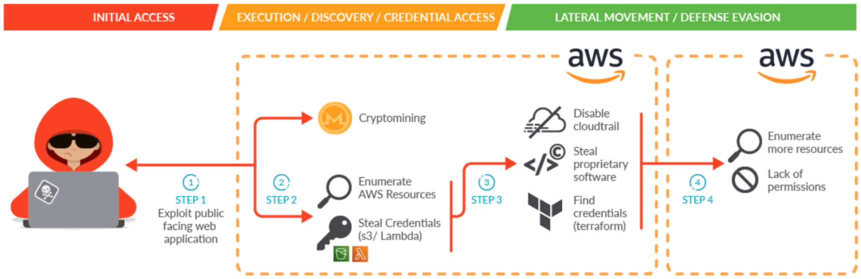
- **Overview of the adversary's kill chain:** https://sysdig.com/blog/cloud-breach-terraform-data-theft/
- **Coverage on how SCARLETEEL is evolving its capabilities:** https://www.csoonline.com/article/645489/cryptominer-scarleteel-evolves-tact-to-steal-container-credentials.html

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)

- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
  - Penetration testing
  - Tabletop exercises
  - Threat Intelligence Program Maturity
  - Develop playbooks of adversary TTPs

SCARLETEEL's Kill Chain


INITIAL ACCESS
EXECUTION / DISCOVERY / CREDENTIAL ACCESS
LATERAL MOVEMENT / DEFENSE EVASION
aws
aws
1 STEP 1
Exploit public facing web application
2 STEP 2
Cryptomining
Enumerate AWS Resources
Steal Credentials (s3/ Lambda)
3 STEP 3
Disable cloudtrail
Steal proprietary software
Find credentials (terraform)
4 STEP 4
Enumerate more resources
Lack of permissions

Source: https://sysdig.com/blog/cloud-breach-terraform-data-theft/

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs to strategically align with the business to reduce risk.