UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0307

LEGION CREDENTIAL HARVESTER

DATE ISSUED: 17th April 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A new hacking tool, Legion, can harvest numerous high-risk credential types and breach web and SMTP services from misconfigured servers. It is written in Python programming language and sold on the Telegram channel that targets online email services for phishing and spam attacks.

BREAKDOWN

Legion malware is sold online via a Telegram channel called 'Forza Tools' with over a thousand members. This tool can harvest credentials from services such as Twilio, Nexmo, Stripe & Paypal (Payment API functions), AWS console credentials, SMTP Credentials, AWS SNS, and database and CMS credentials (PHPmyadmin). It targets unsecured web servers running content management systems (CMS) and PHP-based frameworks and searches for files commonly known to hold secrets, authentication tokens, and API keys. Along with stealing credentials, Legion comes with brute-forcing services to guess AWS credentials. It then uses them to gain access to email services and send out spam or phishing emails. If it can capture valid AWS credentials, it attempts to create an IAM user named 'ses_legion.' It sets the policy to give it administrator rights, giving the rogue user full access to all AWS services and resources. It can also exploit known PHP vulnerabilities to register a webshell on the targeted endpoint or perform remote code execution to give the attacker full access to the server.

REMEDIATION STEPS

- Ensure your organisation has an up-to-date Web Application Firewall (WAF) to prevent unauthorised system access.
- Network monitoring and analysis should be conducted regularly to detect and investigate anomalous network behaviour.
- Set a long and complex password for a web application or public server to mitigate brute-force attacks. Always change default or factory passwords on all devices and applications.
- Please refer to the Importance of Strong Passwords and Practices to create solid organisational password policies.

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/google-chrome-emergency-update-fixes-first-zero-day-of-2023/

Chrome https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html