مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Malware Campaign: BunnyLoader 3.0

Tracking #:432315715

Date:20-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed a rapidly spreading malware campaign utilizing a new variant of the BunnyLoader malware.

TECHNICAL DETAILS:

BunnyLoader is a Malware-as-a-Service (MaaS) that has been steadily evolving since its discovery in September 2023. This new version, BunnyLoader malware, version 3.0 poses a significant threat due to its enhanced capabilities for stealing information, credentials, cryptocurrency, and delivering additional malware payloads.
The new version included:

- Bug fixes
- Additional antivirus evasion and protections
- Multiple data recovery functionalities for the stealer portion
- Additional browser paths
- Keylogger functionality

The malware's infrastructure has evolved with changing C2 servers and delivery methods using various packers like PureCrypter and Themida. The release of BunnyLoader 3.0 in February 2024 marked a major overhaul with improved performance and advanced keylogging capabilities.

Security researchers have closely monitored BunnyLoader's communication protocols, modularization of binaries, and C2 functions to understand its operations better. BunnyLoader 3.0 introduced changes in C2 communication encryption using RC4 encryption for HTTP query parameters. The malware's modular design allows operators to deploy specific functions like custom stealers, clippers, keyloggers, and denial-of-service modules as separate binaries.

INDICATORS OF COMPROMISE(IoCs):

Attached File

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Increase Awareness: Educate users about phishing attempts and suspicious emails that might be used to distribute BunnyLoader.
- Software Updates: Ensure all systems are patched with the latest security updates for operating systems, browsers, and applications.
- Endpoint Security: Implement robust endpoint security solutions that can detect and block malware activity.
- User Training: Conduct regular security awareness training to educate users on identifying phishing attempts and avoiding suspicious links and attachments.
- Regular Backups: Maintain regular backups of critical data to ensure quick recovery in case of malware attack.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

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

REFERENCES:

1. https://unit42.paloaltonetworks.com/analysis-of-bunnyloader-malware/