مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

New Mallox Ransomware Linux Variant

Tracking #:432316034

Date:09-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a ransomware called Mallox that primarily targets Microsoft Windows systems has released a Linux variant.

TECHNICAL DETAILS:

Mallox is a ransomware strain that primarily targets Microsoft Windows systems. It has been active since June 2021 and is notable for exploiting unsecured MS-SQL servers as a penetration vector to compromise victims' networks. Recently, a Linux variant of Mallox has been discovered, targeting VMWare ESXi environments with high-level user privileges.

The Linux variant includes a Flask-based web panel that allows attackers to create customizable ransomware for Linux systems. Admins can manage users, view logs, and create ransomware builds using this panel. The ransomware encryptor and decryptor are generated for any registered user.

Features:

- **Custom Python Scripts:** The attackers use custom Python scripts for payload delivery and victim information exfiltration.
- **Encryption:** Mallox encrypts user data and appends the .locked extension to the encrypted files, rendering them inaccessible

Targeted Platform:

- VMWare ESXi environments

Propagation Methods:

- **Worm-Like Spread:** Mallox spreads like a worm through file sharing, rapidly retrieving and encrypting files.
- **Similar to Search Artifact:** It uses a similar file retrieval technology as Search Artifact.

Impact:

- The Mallox ransomware group claims hundreds of victims across multiple industries, including manufacturing, professional services, legal services, and retail.

INDICATORS OF COMPROMISE:

Indicator Type	Indicators	File name
IP	185[.]73[.]125[.]6	
IP	91[.]215[.]85[.]142	
IP	91[.]215[.]85[.]135	
MD5	3dde1507996cf8c3dd53a726501be33b	Webserver.py
MD5	b0770b7f24a436d256f2d58fc8581a18	decryptor
MD5	231478ff24055d5cdb5fbec36060c8ff	encryptor
MD5	51d51696c7f3a0e3fba4b8ceab210bac	decryptor
MD5	8d0fd41d35df82d3e7e2ff5c1747b87c	encryptor
MD5	e9e087c52b97c7a3e343642379829e0a	decryptor
MD5	68785d476573955d50a3908dc18bf73b	encryptor
MD5	cb60ad37c9a632c697fb2da7add7ccb5	decryptor
MD5	6bb2752ea73b4d6a5c33f543b5c29461	encryptor
MD5	1448ce8abc2f0184ec898d55f9c338b4	decryptor
MD5	5b0c1958a875c205951b88fd1c885900	encryptor
MD5	7f099845d8e6849d6ab4d64b546477d6	decryptor
MD5	4825f3a92780be4a285583b0f24fed99	encryptor
MD5	be08c3e95df5992903a69e04cbab22e3	decryptor
MD5	779aa15cd6a8d416e7f722331d87f47b	encryptor

RECOMMENDATIONS:

- **Block the IOCs** on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- **Patch Systems:** Ensure all systems are up-to-date with the latest security patches from operating system and software vendors.
- **Enforce Strong Passwords:** Implement strong and unique passwords for all administrative accounts and enforce multi-factor authentication (MFA) wherever possible.
- **Segment Networks:** Segment network to limit the lateral movement of attackers in case of a breach.
- **Endpoint Detection and Response (EDR):** Deploy EDR solutions to detect and respond to malicious activity on endpoints.
- **Regular Backups:** Maintain regular backups of critical data with offline storage isolated from the production network.

- **Employee Training:** Train employees on cybersecurity best practices, including phishing awareness and social engineering techniques
- **Securing Microsoft SQL Server:** Utilize a firewall to restrict access to SQL servers. Allow incoming traffic only from trusted networks and IPs.

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://www.uptycs.com/blog/mallox-ransomware-linux-variant-decryptor-discovered