مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

DinodasRAT malware targets Linux systems

Tracking #:432315746

Date:02-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that DinodasRAT, also known as XDealer, is a multi-platform backdoor actively targeting Linux systems worldwide.

TECHNICAL DETAILS:

DinodasRAT, also known as XDealer, is a multi-platform backdoor targeting Linux systems. It is written in C++ and offers a range of malicious capabilities, allowing attackers to establish persistence, steal sensitive data, and manipulate the infected system. This variant has been active since at least 2022 and targets systems running Red Hat or Ubuntu 16/18. DinodasRAT grants attackers complete control over infected machines, enabling data theft and other malicious activities.

DinodasRAT primarily targets Red Hat and Ubuntu-based Linux systems. However, due to its multi-platform nature, other Linux distributions might also be vulnerable.

Technical Details

- **Implantation:** DinodasRAT employs various methods to establish persistence on a system. It can create hidden files to ensure only one instance runs and leverages SystemV or SystemD startup scripts to launch automatically during system boot.
- **Information Gathering:** The malware gathers information about the infected machine, including infection time, to generate a unique identifier for the victim. It's important to note that DinodasRAT avoids collecting user-specific data.
- **Command and Control (C2) Communication:** DinodasRAT communicates with its C2 server using TCP or UDP protocols. This allows threat actors to issue various commands remotely.
- **Functionality:** DinodasRAT offers a wide range of capabilities, including:
  - File manipulation (upload, download, delete)
  - Service control (start, stop, restart)
  - Process enumeration
  - Remote shell execution
- **Encryption:** The Linux version of DinodasRAT reportedly utilizes the libqq library from Pidgin to encrypt communication with the C2 server.

INDICATORS OF COMPROMISE(IOCs):

IP	199[.]231[.]211[.]19
Domain	update[.]centos-yum[.]com
MD5	8138f1af1dc51cde924aa2360f12d650
MD5	decd6b94792a22119e1b5a1ed99e8961
SHA256	15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45
SHA256	bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff

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.

- Regularly update all software, including operating systems and applications, to patch vulnerabilities.
- Implement strong authentication methods, such as multi-factor authentication (MFA), for all critical systems and applications.
- Implement endpoint detection and response (EDR) solutions for ongoing threat monitoring.
- Monitor network traffic for suspicious activity that might indicate C2 server communication.
- Educate users about cybersecurity best practices, including identifying phishing attempts and avoiding suspicious attachments or links.
- Regular Backups: Implement a robust backup routine with backups stored offline and regularly tested for recoverability.

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:

https://securelist.com/dinodasrat-linux-implant/112284/