مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RansomHouse targets VMware ESXi with new MrAgent tool

Tracking #:432315622
Date:16-02-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the RansomHouse ransomware group has created a new tool named "MrAgent," which targets VMware ESXi hypervisors.

TECHNICAL DETAILS:

The RansomHouse ransomware gang has developed a new tool called MrAgent, specifically designed to automate and streamline attacks against VMware ESXi hypervisors. This tool allows attackers to deploy ransomware across multiple ESXi servers simultaneously, potentially encrypting all virtual machines managed by the compromised ESXi server, and causing significant data loss and operational disruption.

The RansomHouse group, a Ransomware-as-a-Service (RaaS) operation that emerged in late 2021, has been actively deploying ransomware variants to exploit corporate networks. The group uses double extortion tactics, first by encrypting victims' files and demanding a ransom, and second by naming and shaming non-paying victims on their blog, along with publishing the stolen data from the victim. The group's tactics, techniques, and procedures (TTPs) show a mature and sophisticated level of execution, leveraging content delivery network (CDN) servers for exfiltration and utilizing a Tor-based chat room for victim negotiations. The group tries to differentiate itself from typical ransomware operators by cultivating an image of a "professional mediator community." The group has been identified for using a unique ransomware variant, dubbed Mario ESXi, along with MrAgent, to target both Windows and Linux-based systems

Technical Details:

- MrAgent identifies the host system, disables the firewall, and automates ransomware deployment across multiple hypervisors.
- It receives custom configurations and commands from the RansomHouse command and control server.
- These configurations include setting passwords on the hypervisor, configuring the encrypter command and its arguments, scheduling an encryption event, and changing the welcome message displayed on the hypervisor's monitor (to display a ransom notice)

host.startIn	Number of seconds to wait before starting
host.pass	Password to set on the ESXi host
host.command	Encrypter command
host.args	Arguments to provide to encrypter
host.welcomeMsg	Message to configure in the ESXi /etc/motd file

MrAgent Tool Configurations

- MrAgent can also delete files, drop active SSH sessions, and gather information about running VMs.

INDICATORS OF COMPROMISE(IoCs):

- Attached in Excel 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.
- Update VMware ESXi to the latest version
- Isolate ESXi servers from other systems to limit the spread of ransomware.
- Regularly back up the data and store it in a secure location
- Ensure that all software, operating systems, and security applications are up to date with the latest patches and updates.
- Monitor the network for suspicious activity.
- Change the passwords regularly and Use strong passwords with multi-factor authentication (MFA).
- Educate employees about the risks of ransomware/malware, how to identify phishing attempts, and safe online behaviour.

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://www.trellix.com/blogs/research/ransomhouse-am-see/