CYSIV
A FORESCOUT COMPANY

Threat Report: Rise in Linux Ransomware

March 2022

Table of Contents

1 EXECUTIVE SUMMARY

Ransomware is a huge money-maker for cybercriminals, and it has been around for decades now. Through a combination of advanced encryption and effective extortion mechanisms, a ransomware attack is usually devastating, resulting in data loss, reputation harm, recovery costs and significant downtime. Ransomware has been rapidly evolving, and it is now targeting Linux users.

More than 70% of webservers are Linux-based. Organizations run Linux servers to administer enterprise and government networks, web services and massive databases. Since most of the critical infrastructure is Linux based, Cybercriminals are dramatically expanding their scope to target Linux-based operating systems. As endpoint security hardening has improved over the past years, it is becoming more difficult to navigate to higher value targets after infecting an endpoint.

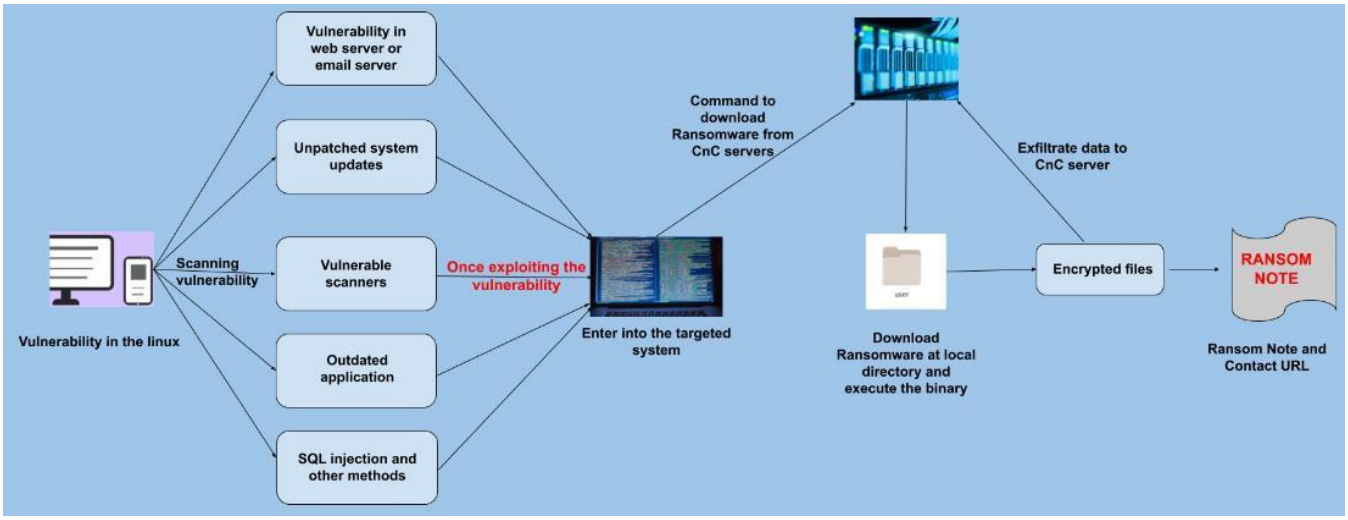
Cybercriminals have noticed that compromising a single Linux server can be comparatively easy and deliver a massive payoff. In recent times we have seen multiple ransomware attacks targeting Linux users by exploiting loopholes. The main vectors are phishing, stolen credentials, exfiltrate data, brute force attack, and vulnerability exploitation such as misconfiguration or incomplete patch management.

The following Linux ransomware variants have been prominent in the past few months:

- **Sneaky/lockbit**: One of the most inventive families of ransomware now has additional Linux and VMware ESXi variants.
- **REvil**: Attempts to target VMware's ESXi virtual machine management software and network attached storage (NAS) devices that run on the Linux operating system (OS).
- **Hive**: Ability to encrypt Linux and FreeBSD using new malware variants specifically developed to target these platforms.
- **HelloKitty**: Targeting ESXi servers and the virtual machines running on them.
- **KillDisk**: Ability to encrypt files, demand a bitcoin ransom and leave Linux systems unbootable, with the ability to target specific locales.

2. ATTACK CHAIN

In the case of Linux ransomware variants, the infection mechanism is quite different as compared to Windows ransomware. Linux ransomware infection relies on vulnerability exploitation. Linux ransomware exploits either unpatched system vulnerabilities or flaws in a service, outdated applications, the targeting of VMware's ESXi virtual machine and NAS devices, and SQL injection vulnerabilities.



Upon exploitation, the infected machine connects to the CnC to download a malicious executable and executes it in the target environment. At this stage of the attack, the ransomware communicates with the C2 server to negotiate its public key post, at which point data is exfiltrated.

This is followed by the encryption of target files using a random symmetric key that the ransomware generates. This symmetric key is then encrypted using a public key. The ransomware then deletes the original version of the files it has encrypted.

Ransom notes containing the contact URLs and email addresses, typically TOR sites, are added to various directory locations.

3. REVIL RANSOMWARE

REvil was first observed as a Ransomware-as-service (RaaS) operation in mid-2019 and became the most successful and damaging threat group that year. In the primary stage, REvil targets Windows Operation Systems with a variety of infection methods. The REvil group has now evolved to target VMware's ESXi virtual machine management software and network attached storage (NAS) devices that run on the Linux operating system (OS).

VMware ESXi, formerly known as ESX, is a bare-metal hypervisor that installs easily on to your server and partitions it into multiple virtual machines (VM) to share the same hard drive storage. Targeting these important servers for encryption and ransom presents a huge opportunity for the bad actors and an equally large threat to potential victim organizations considering the enormous cost involved in recovering the data.

While analyzing the ELF binary for the REvil ransomware, we were able to see the esxcli commands being used in the code.

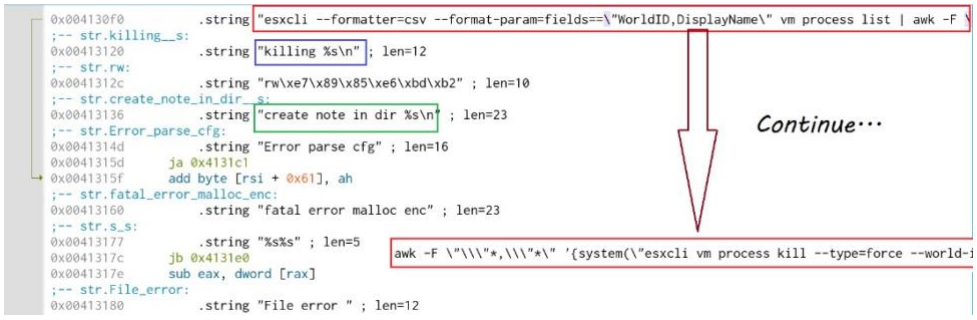


Fig 1. Esxcli command killing VM process.

By using this tool, attackers can get the process list using the command "vm process list", allowing them to kill running vm process using the command "esxcli vm process kill –type=force --", to make sure that the VMs are forced to terminate.

To encrypt files, the number of threads is specified with the path to encrypt "BY DEFAULT THIS SOFTWARE USE 50 THREADS". Silent mode is also used while stopping the VMs.

Fig 2. Uses 50 threads.

Before encrypting the files, the ransomware gets the details of the host, then checks the debug for victim

specific information. Here “nbody” specifies the base64 encoded content in the ransom note and “nname” denotes the filename of the ransom-note.

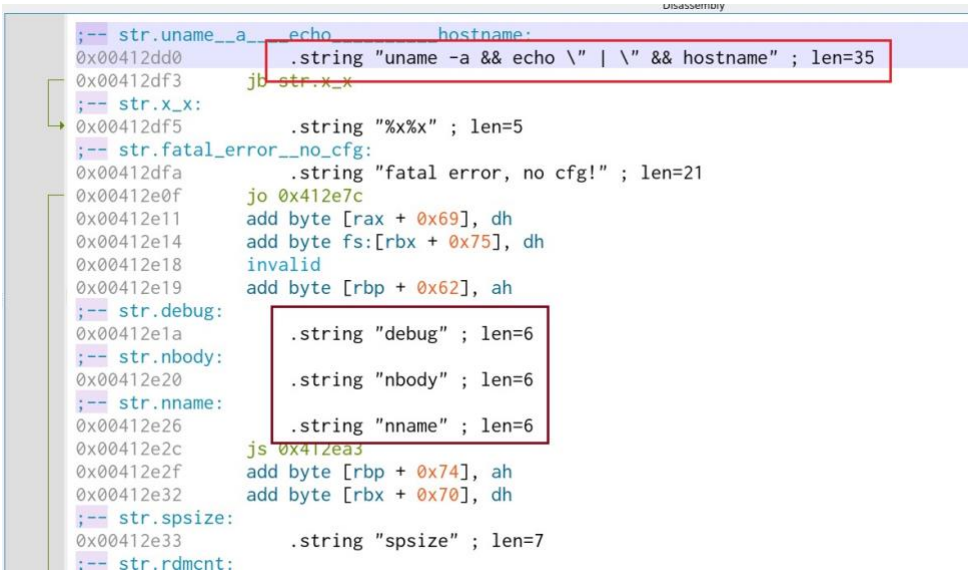


Fig 3. Get hostname.

At the execution of ransomware, the usual configuration will check with the Pkkey, pid, verand the OS specific to the UID, KEYand EXT. This pk key is used to generate a XOR key used in the encryption of files.

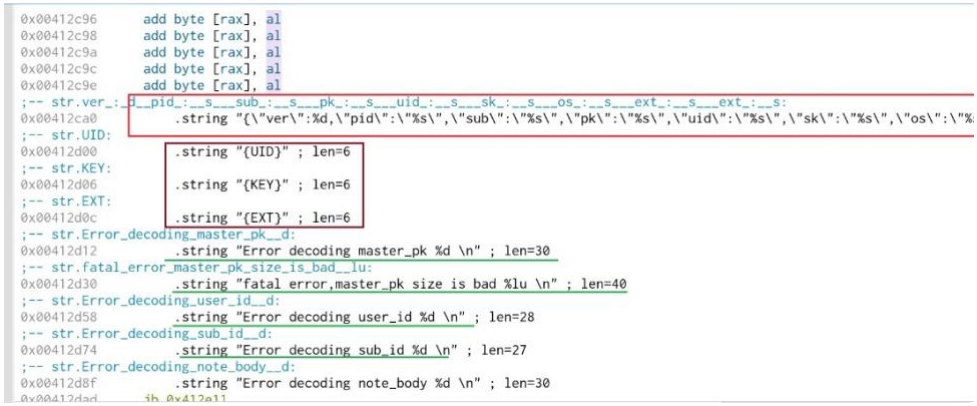


Fig 4. REvil ransomware usual configuration.

Fig 5. Pk key, Pid and Extension.

During execution, the ransomware checks to ensure the “vmx-*” and “pkill –9 %s” commands are executed to ensure that processes terminate promptly.

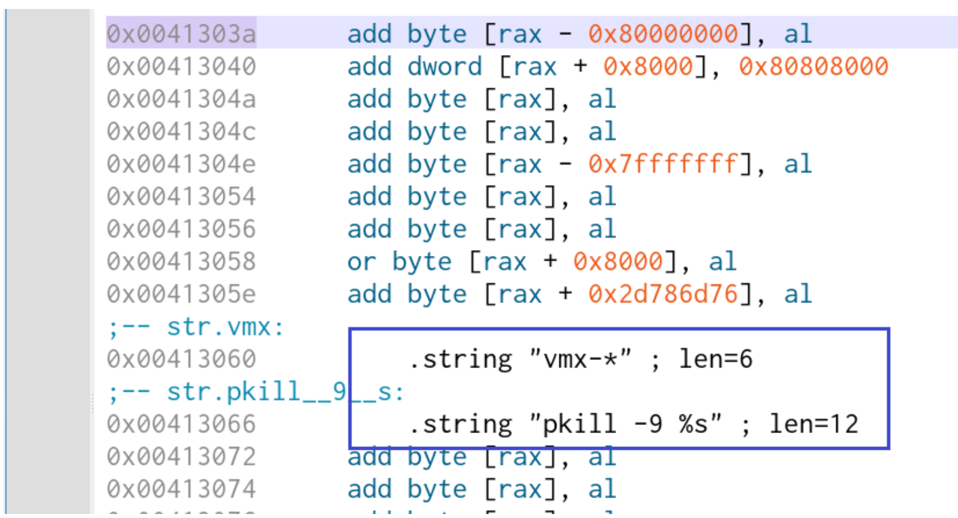


Fig 6. Pkill for vmx.

Mutexhas been initialized in the code, and mallocand pthreadare employed to perform persistence in the execution.

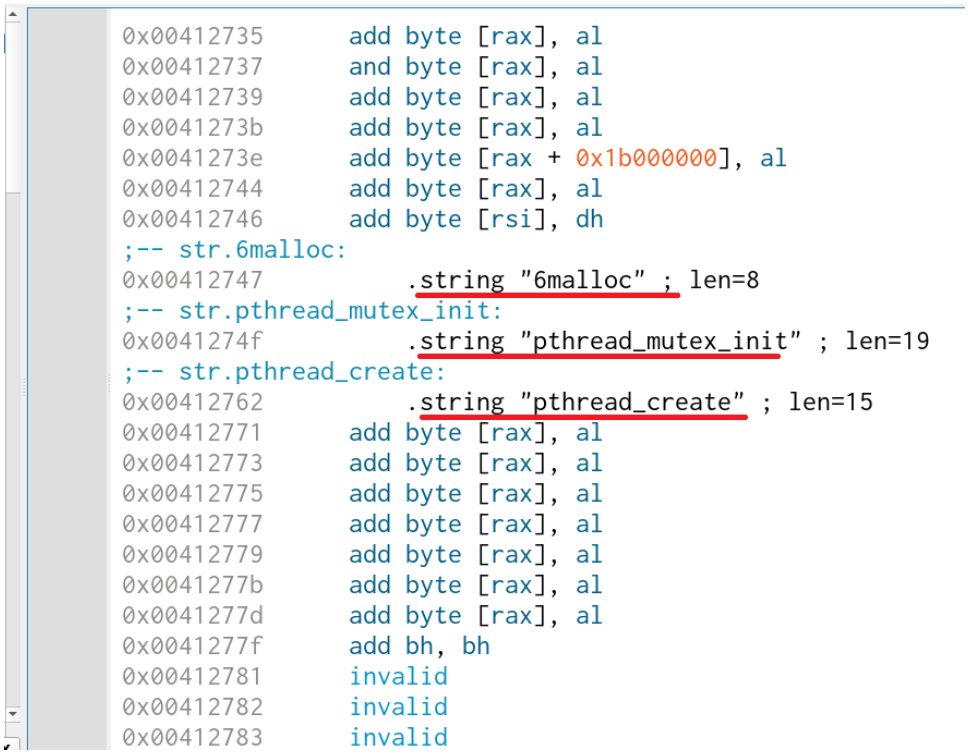


Fig 7. Mutex initialization and thread creation.

Before encrypting directory files, the ransomware first checks if the files are already encrypted and which files are protected by the OS. Then it will encrypt the files and, when this is complete, display the encrypted and non-encrypted files.

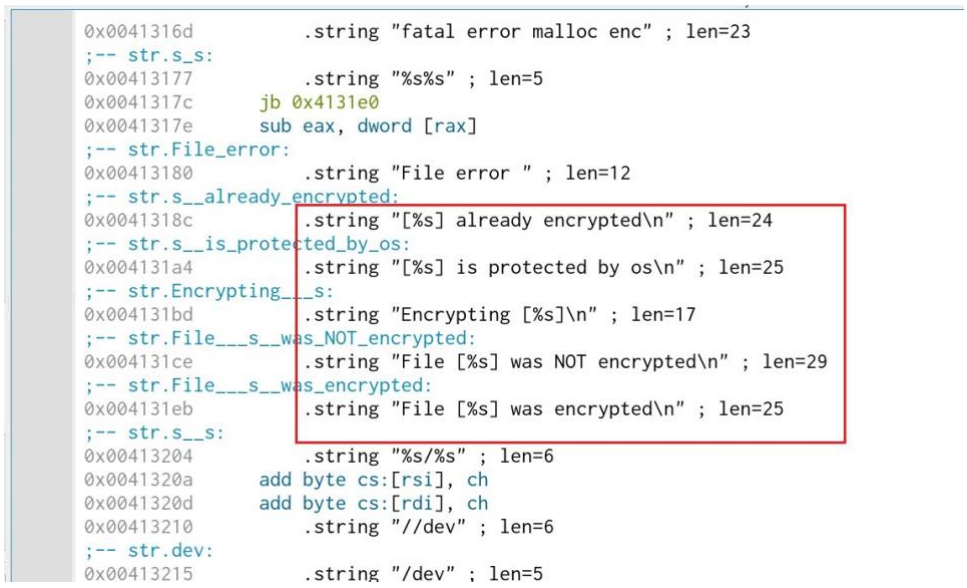


Fig 8. Checking encrypted and not encrypted files.

After successful encryption of files, a random five-character extension is added to the encrypted file. The following is an example of encrypted files with the extention “qoxaq”:

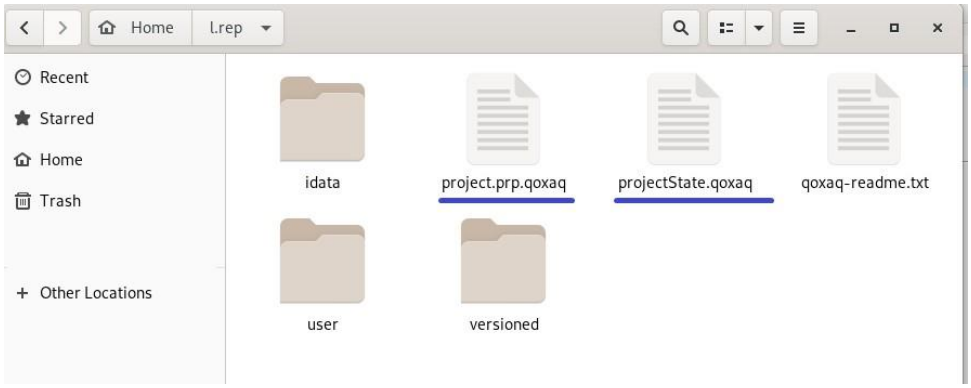


Fig 9. Files encrypted with **qoxaq** extension.

Finally, the ransom note is added to directories and sub directories with name “qoxaq-readme.txt”.

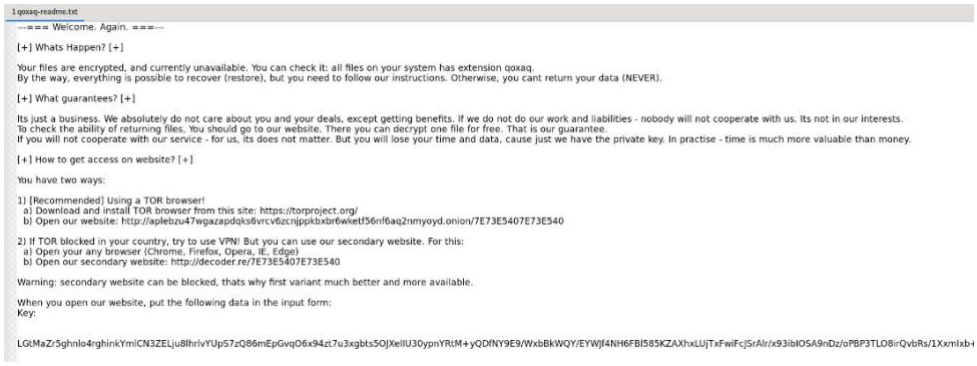


Fig 10. Ransom note.

Commands observed in REvil:

Commands	Description
esxcli --formatter=csv --format-param=fields== "WorldID,DisplayName" vm process list	Get list of running VMs
esxcli vm process kill --type=force --world-id= [ID]	Terminate processes the VM from the list
pkill –9 %s	The process terminates promptly.

Cysiv’s Rule Engine covers TTPs like Impairing Defenses, Inhibiting System Recovery, Date Encrypted for Impact and also defends against Victim Host Information & Identity information Gathering, Active Scanning etc.

4. INDICATOR OF COMPROMISE

SHA256
ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4
3d375d0ead2b63168de86ca2649360d9dcff75b3e0ffa2cf1e50816ec92b3b7d
796800face046765bd79f267c56a6c93ee2800b76d7f38ad96e5acb92599fcd4
d6762eff16452434ac1acc127f082906cc1ae5b0ff026d0d4fe725711db47763

5. MITRE ATT&CK TECHNIQUES

Tactics	Technique ID	Technique name
Reconnaissance	T1591	Gather Victim Host Information
	T1595	Active Scanning
	T1589	Gather Victim Identity Information
Initial Access	T1190	Exploit Public-Facing Application
Resource Development	T1583	Acquire Infrastructure
	T1588	Obtain Capabilities
	T1587	Develop Capabilities
Defense Evasion	T1027	Obfuscated Files or Information
Discovery	T1083	File and Directory Discovery
Collection	T1005	Data from Local System
Command and control	T1573	Encrypted Channel
Exfiltration	T1020	Automated Exfiltration
Impact	T1486	Data Encrypted for Impact