



AL2024_23 New Play ransomware Linux version targets VMware ESXi VMs (23rd July 2024)

Summary

In a recent development, the Play ransomware gang has expanded its malicious activities by targeting Linux systems, specifically focusing on VMware ESXi virtual machines. This marks the first time Play ransomware has been observed attacking ESXi environments, a strategic move that could lead to significant disruptions for affected organizations. Cybersecurity company Trend Micro identified the new variant, which demonstrates advanced capabilities to evade detection on Linux systems and efficiently encrypt critical data stored on virtual machines.

Details

Play ransomware's new Linux variant is engineered to identify and target ESXi environments. The attack flow involves several sophisticated steps to maximize impact:

1. **Environment Check:** The ransomware first determines if it is running in an ESXi environment.
2. **Powering Off VMs:** Once confirmed, the ransomware scans for all VMs in the compromised environment and powers them off using the following shell command:

```
/bin/sh -c "for vmid in $(vim-cmd vmsvc/getallvms | grep -v Vmid | awk '{print $1}'); do vim-cmd vmsvc/power.off $vmid; done"
```

3. **Encryption Process:** After shutting down the VMs, the ransomware encrypts VM disk files, configuration files, and metadata files, appending the .PLAY extension to each encrypted file.
4. **Ransom Note:** A ransom note is dropped in the root directory of the VM, which is displayed in the ESXi client's login portal and console after the VM is rebooted.

Indicators of Compromise (IoCs):

- Presence of files with the .PLAY extension.



- Unusual VM shutdowns followed by encryption activities.
- Ransom notes appearing in VM root directories or ESXi client login portals.
- Network traffic involving URL-shortening services provided by a threat actor known as Prolific Puma.

Remediation

To protect against Play ransomware and similar threats, organizations should implement the following remediation steps:

1. **Activate Multi-Factor Authentication (MFA):** Ensure MFA is enabled for all critical systems to prevent unauthorized access.
2. **Maintain Offline Backups:** Regularly backup important data and store backups offline to prevent them from being encrypted during an attack.
3. **Implement a Recovery Plan:** Develop and test a comprehensive recovery plan to quickly restore operations in the event of a ransomware attack.
4. **Keep Software Up to Date:** Regularly update all software, including ESXi environments, to patch vulnerabilities that could be exploited by ransomware.
5. **Monitor Network Traffic:** Be vigilant for unusual network traffic patterns, particularly those involving known threat actors like Prolific Puma.
6. **Educate Employees:** Train employees on the importance of cybersecurity practices, including recognizing phishing attempts and other common attack vectors.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2024, July 22). New Play ransomware Linux version targets VMware ESXi VMs. Retrieved from *BleepingComputer*.
<https://www.bleepingcomputer.com/news/security/new-play-ransomware-linux-version-targets-vmware-esxi-vm/>
- *New Play Ransomware Linux variant targets ESXI shows ties with prolific Puma*. (2024, July 19). Retrieved from Trend Micro.



CIRT.GY

Guyana National Computer Incident Response Team

https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html