Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

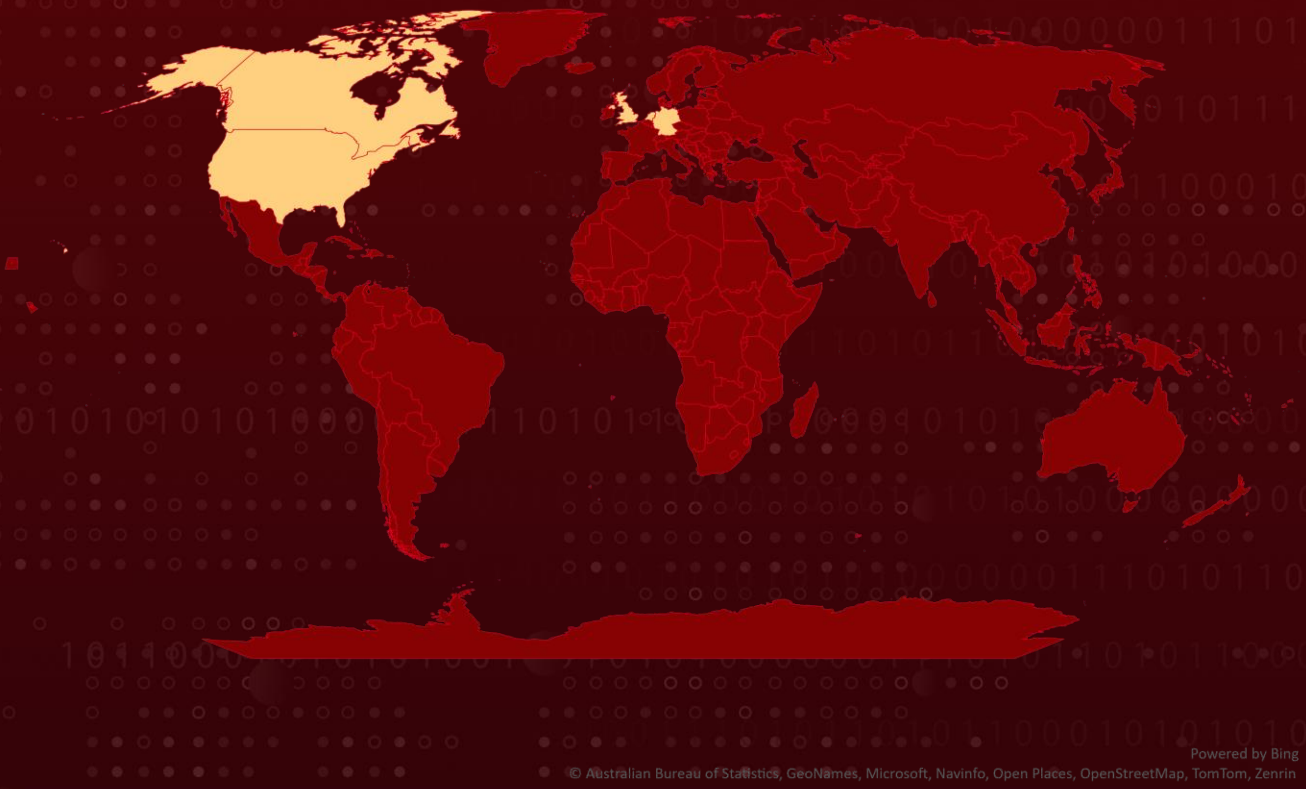
New Linux Variant of Play Ransomware Targeting VMware ESXi Systems

Date of Publication	Admiralty Code	TA Number
July 24, 2024	A1	TA2024282

Summary

First Appearance: January 2024
Malware: Play ransomware, Coroxy backdoor
Targeted Countries: United States, Canada, Germany, United Kingdom, and Netherlands
Affected Platforms: VMWare ESXi
Targeted Industries: Manufacturing, Professional services, Construction, IT, Retail, Financial services, Transportation, Media, Legal Services, and Real Estate
Attack: A new Linux variant of the Play ransomware that targets VMware ESXi environments, marking a shift from its previous focus on Windows systems. This ransomware employs advanced evasion techniques and is linked to the Prolific Puma group, enhancing its operational capabilities. It encrypts critical files and disrupts business operations by leaving ransom notes, prompting organizations to strengthen their security measures, including regular updates, access controls, and offline backups.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 A new Linux variant of the Play ransomware group that specifically targets VMware ESXi environments. This development represents a significant shift in the group's attack strategy, which has primarily focused on Windows systems in the past. By honing in on ESXi, the Play ransomware can exploit critical business infrastructures that host multiple virtual machines and sensitive data, thereby increasing the potential impact of its attacks.

#2 The ransomware employs sophisticated evasion techniques to avoid detection by security measures. Its ability to remain undetected on platforms like VirusTotal indicates that the group has developed advanced methods to bypass traditional security protocols. Additionally, there are indications of a connection between the Play ransomware group and the Prolific Puma group, which is known for providing infrastructure and support to other cybercriminals. This collaboration suggests a shared operational framework that enhances the capabilities of both groups.

#3 Initially, attackers gain access using valid credentials or phishing. They then establish a connection to a command and control (C2) server to deploy necessary tools and payloads. The attackers use network scanning (Netscan) for discovery and PsExec for lateral movement within the network. The Coroxy backdoor maintains persistent access, while tools like WinRAR and WinSCP are used for data exfiltration.

#4 Later, attackers deploy the Play Ransomware payload, which encrypts essential files in the ESXi environment, including virtual machine disk and configuration files, adding a ".PLAY" extension. The ransomware also leaves a ransom note in the root directory of the ESXi host.

#5 To mitigate the risks posed by this new ransomware variant, organizations are encouraged to Regular patching and maintaining regular offline backups of critical data and conducting audits to rectify misconfigurations within ESXi environments are also essential steps in defending against such attacks. The emergence of this variant underscores the evolving nature of ransomware threats, particularly as cybercriminals adapt their tactics to exploit high-value enterprise targets.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Play ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a Play ransomware attack, up-to-date backups enable recovery without paying the ransom.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Network Segmentation: Divide the network into segments to limit the spread of ransomware. This can help contain the damage and protect sensitive data.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0010** Exfiltration	**TA0040** Impact
TA0007 Discovery	**TA0008** Lateral Movement	**TA0005** Defense Evasion	**TA0011** Command and Control
T1566 Phishing	**T1078** Valid Accounts	**T1070.004** File Deletion	**T1070** Indicator Removal
T1046 Network Service Discovery	**T1083** File and Directory Discovery	**T1059.004** Unix Shell	**T1059** Command and Scripting Interpreter

T1570 Lateral Tool Transfer	T1568.002 Domain Generation Algorithms	T1568 Dynamic Resolution	T1105 Ingress Tool Transfer
T1041 Exfiltration Over C2 Channel	T1486 Data Encrypted for Impact	T1491.001 Internal Defacement	T1491 Defacement
T1489 Service Stop			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	2a5e003764180eb3531443946d2f3c80ffcb2c30
URLs	hxxp://108.61.142[.]190/FX300.rar, hxxp://108.61.142[.]190/1.dll.sa, hxxp://108.61.142[.]190/64.zip, hxxp://108.61.142[.]190/winrar-x64-611.exe, hxxp://108.61.142[.]190/PsExec.exe, hxxp://108.61.142[.]190/host1.sa
IPv4	108[.]61[.]142[.]190 , 45[.]76[.]165[.]129, 149[.]248[.]2[.]42
Domains	ztqs[.]info , zfrb[.]info , xzdw[.]info , iing[.]info , mcmb[.]info , lcmr[.]info , thfq[.]info , hibh[.]info , iwqe[.]info , ukwc[.]info , apkh[.]info , vqbl[.]info , vgkb[.]info , znuc[.]info , jhrd[.]me, pkil[.]me, kwfw[.]me,

TYPE	VALUE
Domains	whry[.]me, pxkt[.]me, ylvq[.]me, flbe[.]link, mmhp[.]link, gunq[.]link, ojry[.]link, bltr[.]me

Recent Breaches

https://www.congoleum.com/

https://www.haydenpower.com/

https://www.elyriafoundry.com/

https://fareriassociates.com/

https://hyperice.com/

https://www.inda.org/

https://www.innerspec.com/

https://mips.com/

https://web.prairieathletic.com/

https://texas-ec.org/

https://www.texasrecycling.com/

https://www.21stcenturyenergygroup.com/

References

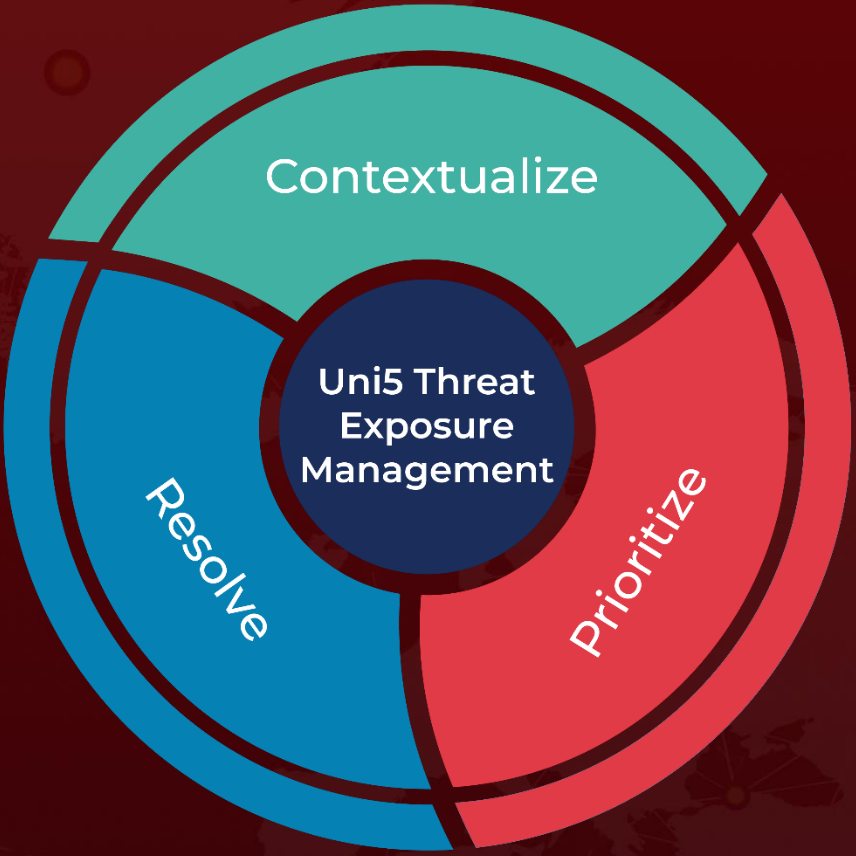
https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html

https://www.hivepro.com/threat-advisory/play-ransomware-a-global-threat-impacting-businesses/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 24, 2024 • 4:30 AM

More at www.hivepro.com