Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

PlayBoy Locker Made Cybercrime More Accessible

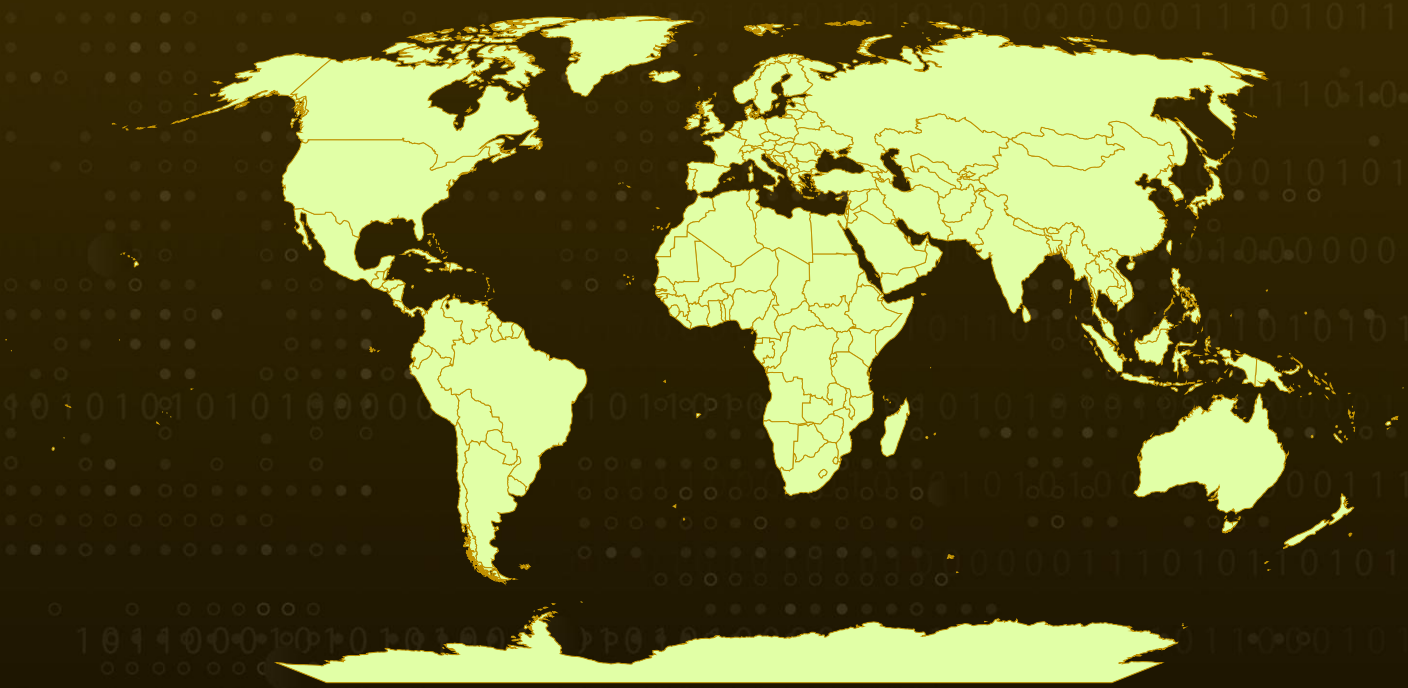
Date of Publication	Admiralty Code	TA Number
April 14, 2025	A1	TA2025113

Summary

Active Since: September 2024
Malware: PlayBoy Locker Ransomware
Affected Platforms: Windows, NAS, and ESXi
Targeted Region: Worldwide

Attack: PlayBoy Locker burst onto the cybercrime scene as a sleek, professional-grade Ransomware-as-a-Service platform, arming even amateur hackers with powerful tools to launch devastating attacks. With its polished affiliate program, tailored payloads, and dark web “customer support,” it quickly gained notoriety.

Attack Regions



Attack Details

#1 Since its emergence in September 2024, PlayBoy Locker has operated as a Ransomware-as-a-Service (RaaS) platform, enabling even low-skilled cybercriminals to execute sophisticated attacks. The service offers a complete suite of tools, including customizable ransomware payloads, web-based management dashboards, and dark web-based customer support.

#2 Like many RaaS operations, PlayBoy Locker functions on an affiliate model, in which profits from successful attacks are split between the operators and the affiliates who distribute the malware. In this case, affiliates agreed to an 85/15 revenue share in favor of the malware creators.

#3 The platform supports attacks against a wide range of targets, offering the ability to tailor ransomware binaries for Windows, Network-Attached Storage (NAS), and ESXi systems. Affiliates were drawn to its versatility and were promised frequent updates, anti-detection improvements, and technical support, making the operation resemble a legitimate business in structure and services.

#4 PlayBoy Locker is written in C++ and uses a hybrid encryption scheme involving the HC-128 stream cipher and the Curve25519 elliptic curve algorithm. Once inside a network typically via phishing emails or vulnerable Remote Desktop Protocol (RDP) services the malware conducts LDAP scans to locate other machines.

#5 It then attempts to replicate itself across the network, terminating active processes and services to unlock in-use files before encrypting them. As part of its standard routine, the ransomware deletes Volume Shadow Copies to prevent victims from recovering data through Windows' built-in backup features. Infected files are renamed with a ".PLBOY" extension, and victims are left with a ransom note titled INSTRUCTIONS.txt, which contains directions for payment and communication.

Recommendations

Implement Email Security and Phishing Awareness Training: Given phishing remains a common infection vector, deploy advanced email filtering solutions and conduct regular employee training to identify and report phishing attempts. Simulated phishing campaigns can significantly improve resilience.

Harden RDP and Other Remote Access Protocols: Since PlayBoy Locker often gains initial access through compromised Remote Desktop Protocol (RDP) services, disable RDP where not needed, enforce strong passwords, enable multi-factor authentication (MFA), and restrict access via VPN or firewall rules.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Implement Strict Privilege Management: Enforce least-privilege access policies to limit user permissions and minimize attack surfaces. Monitor and log all administrative actions to detect and prevent privilege escalation attempts by malware.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
TA0009 Collection	TA0040 Impact	TA0010 Exfiltration	T1566 Phishing
T1543 Create or Modify System Process	T1543.003 Windows Service	T1083 File and Directory Discovery	T1078 Valid Accounts
T1078.001 Default Accounts	T1078.002 Domain Accounts	T1135 Network Share Discovery	T1016 System Network Configuration Discovery

T1027.002 Software Packing	T1027 Obfuscated Files or Information	T1620 Reflective Code Loading	T1119 Automated Collection
T1486 Data Encrypted for Impact	T1489 Service Stop	T1490 Inhibit System Recovery	T1070.004 File Deletion
T1047 Windows Management Instrumentation	T1106 Native API	T1133 External Remote Services	T1070 Indicator Removal
T1547 Boot or Logon Autostart Execution			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3030a048f05146b85c458bcabe97968e5efdd81b224b96c30c83b74365839e7b, a9e1bd8f9cbeeec64da558027f380195f7ed572f03830a890dd0494e64d98556, a9e1bd8f9cbeeec64da558027f380195f7ed572f03830a890dd0494e64d98556
TOR Address	vlofmq2u3f5amxmnblvxaghy73aedwta74fyceywr6eeguw3cn6h6uad[.]onion
Tox	22177C7E7675A2178DE3ADCFC613469D868E5F32996B411CC9AE45848A666E30543BF692E1B7
File Name	INSTRUCTIONS.txt

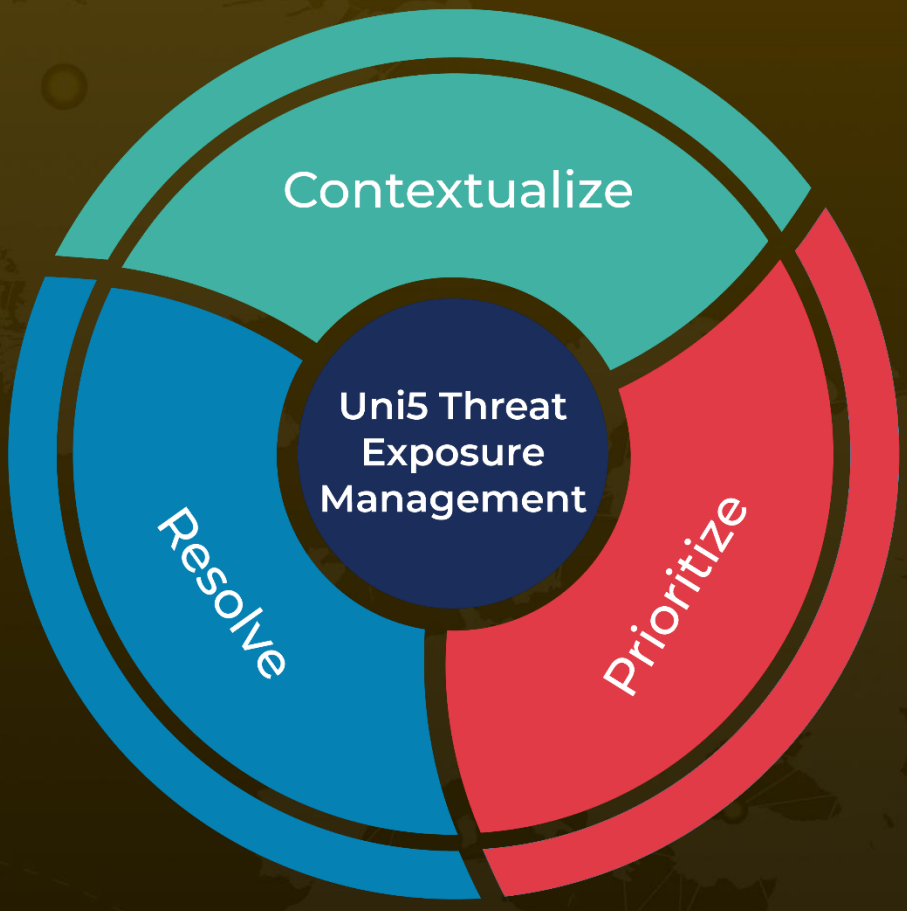
References

https://www.cybereason.com/blog/threat-analysis-playboy-locker

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

April 14, 2025 • 6:00 AM

More at www.hivepro.com