Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

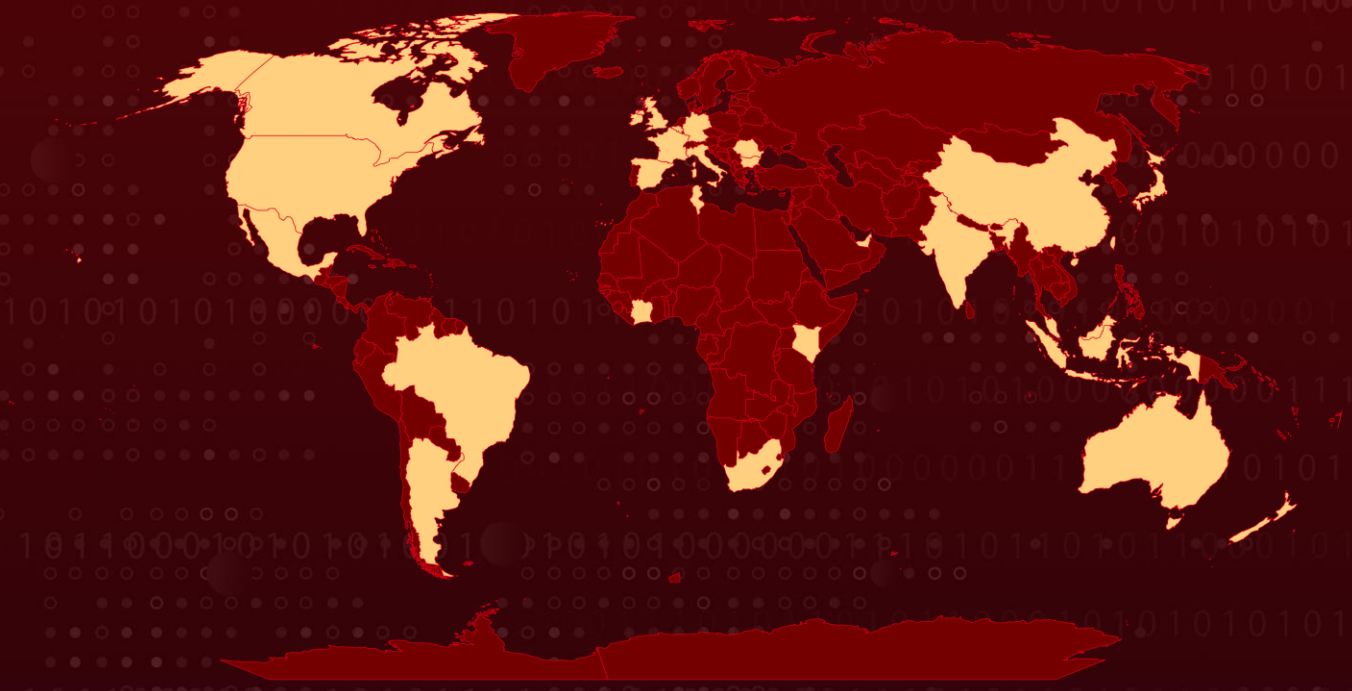
Hunters International is Redefining RaaS Operations

Date of Publication	Admiralty Code	TA Number
August 6, 2024	A1	TA2024296

Summary

First Seen: October 2023
Malware: SharpRhino RAT, Hunters International
Targeted Countries: Argentina, Australia, Belgium, Brazil, Bulgaria, Canada, China, Côte d'Ivoire, France, Germany, India, Indonesia, Ireland, Italy, Japan, Kenya, Malaysia, Mexico, New Zealand, Romania, South Africa, Spain, Taiwan, Tunisia, United Arab Emirates, United Kingdom, United States
Targeted Industries: Aerospace, Defense, Agriculture, Associations, Business Services & Consulting, Education, Energy, Financial Services, Food Service, Government, Healthcare, Hospitality, Insurance, Legal, Manufacturing, Media, Pharmaceutical, Real Estate, Retail, Technology, Telecommunications, Transportation
Attack: Hunters International, a Ransomware-as-a-Service (RaaS) operation suspected to be a rebrand of Hive ransomware, surfaced in October 2023. With around 60% code similarity to Hive, they have claimed responsibility for 134 attacks in early 2024. In recent attacks, they deployed SharpRhino, a new C# remote access trojan distributed via typosquatting domains.

Attack Regions



Attack Details

#1 Hunters International is a Ransomware-as-a-Service (RaaS) operation that surfaced in October 2023. Suspected to be a rebrand of Hive ransomware, approximately 60% of its source code shows similarities. In a recent attack, the Hunters International group deployed SharpRhino, a new C# remote access trojan designed for initial infection and persistence, showcasing the continuous evolution of RaaS threat groups' capabilities.

#2 Hunters International has taken credit for 134 attacks in the first half of 2024. SharpRhino is distributed via a typosquatting domain convincingly mimicking the legitimate network administration tool Angry IP Scanner.

#3 Upon execution, it establishes persistence and grants the attacker remote access to the compromised device, facilitating further progression of the attack. SharpRhino enables Hunters International to achieve initial infection, escalate privileges on compromised systems, execute specific PowerShell commands, and ultimately deploy the ransomware payload.

#4 Before encrypting files, Hunters International exfiltrates data from victim organizations, changes file extensions to .locked, and leaves a README message directing recipients to a chat portal on the TOR network for payment instructions.

Recommendations

Exercise Caution with Malvertising: Be cautious of sponsored search results that may contain malvertising. Activating ad blockers can help hide these potentially harmful results. Additionally, bookmark official project sites are known for safe installers to ensure you download legitimate software. This practice reduces the risk of encountering malicious ads that could lead to ransomware infections.

Handle Password-Protected Archives with Care: Since antivirus software cannot scan password-protected archives, take extra precautions by extracting these files on a Virtual Machine (VM) to isolate potential threats and then scan the contents with antivirus software. If a VM is unavailable, use VirusTotal to upload and scan the archive, provided it contains only a single file.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Implement Network Segmentation: Segment your network to isolate critical systems and sensitive data from general user access and potential malware spread. Use intrusion detection and prevention systems (IDPS) to monitor and analyze network traffic for abnormal behavior.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0040 Impact
TA0042 Resource Development	TA0010 Exfiltration	T1134 Access Token Manipulation	T1497.003 Time Based Evasion
T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks
T1608 Stage Capabilities	T1608.004 Drive-by Target	T1036 Masquerading	T1036.001 Invalid Code Signature
T1027.004 Compile After Delivery	T1480 Execution Guardrails	T1543 Create or Modify System Process	T1543.003 Windows Service

T1135 Network Share Discovery	**T1547.001** Registry Run Keys / Startup Folder	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1071.001 Web Protocols	**T1573** Encrypted Channel	**T1041** Exfiltration Over C2 Channel	**T1486** Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	4bba5b7d3713e8b9d73ff1955211e971
SHA1	9473104a1aefb0daabe41a92d75705be7e2daaf3
SHA256	d2e7729c64c0dac2309916ce95f6a8253ca7f3c7a2b92b452e7cfb69a601fbf6, 3f1443be65525bd71d13341017e469c3e124e6f06b09ae4da67fdeaa6b6c381f, 223aa5d93a00b41bf92935b00cb94bb2970c681fc44c9c75f245a236d617d9bb, 9a8967e9e5ed4ed99874bfed58dea8fa7d12c53f7521370b8476d8783ebe5021, b57ec2ea899a92598e8ea492945f8f834dd9911cff425abf6d48c660e747d722, 09b5e780227caa97a042be17450ead0242fd7f58f513158e26678c811d67e264
File Name	LogUpdate.bat, Wiaphoh7um.t, ipscan-3.9.1-setup.exe, kautix2aeX.t, WindowsUpdate.bat
Domains	cdn-server-1[.]xiren77418[.]workers[.]dev, cdn-server-2[.]wesoc40288[.]workers[.]dev, Angryipo[.]org, Angryipsca[.]com, ec2-3-145-180-193[.]us-east-2[.]compute[.]amazonaws[.]com, ec2-3-145-172-86[.]us-east-2[.]compute[.]amazonaws[.]com
TOR Address	hxxps[:]//hunters55atbdusuladzv7vzv6a423bkh6ksl2uftwrxyuarbzlfh7yd[.]onion, hxxps[:]//hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid[.]onion

Recent Breaches

https://www.lrn.com
https://www.jangho.com
https://www.khandelwallab.com
https://www.enea.it
https://www.durhammfg.com
https://www.klevenconstruction.com
https://www.thegillcorp.com
https://www.crownlea.com
https://www.priefert.com
https://ptot.texas.gov
https://betances.org
https://www.arcmedgroup.com
https://www.santarosa.gob.ar
https://www.northeastrehab.com
https://seamonwhiteside.com
https://www.braums.com
https://www.lantronix.com
https://www.rzo.com
https://ms-industre.de
https://www.comnetcomm.com
https://www.gibbsca.com.au
https://carigalihess.com
https://kura.go.ke
https://www.indikaenergy.co.id
https://www.multisuns.com.tw
https://www.coquitlamconcrete.com
https://wheelership.com
https://bartlettlaw.com

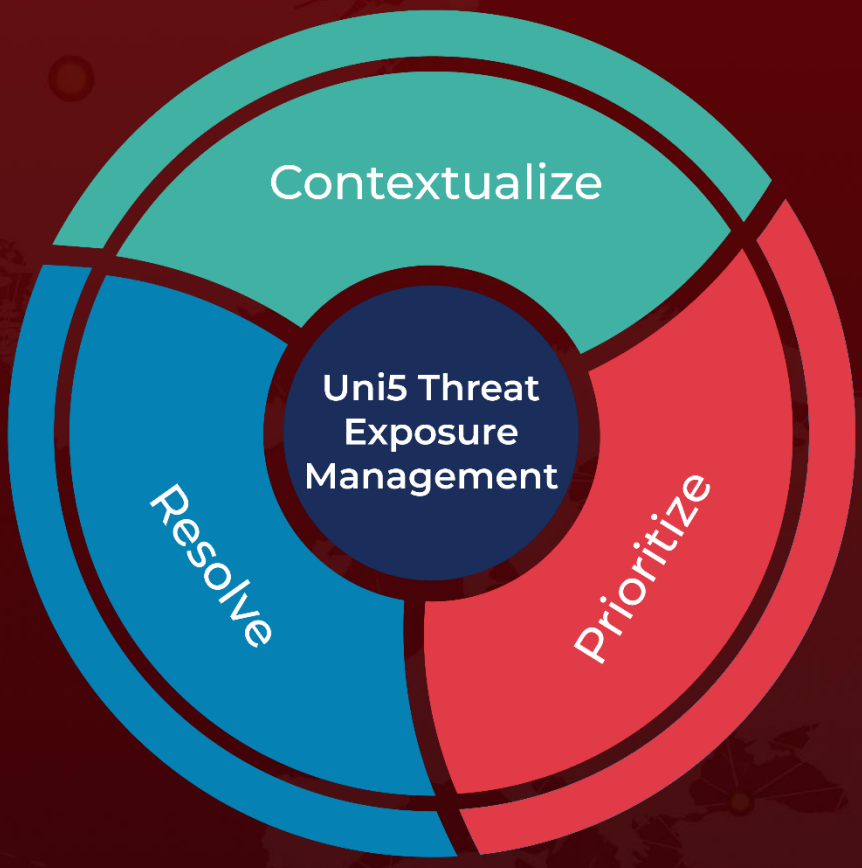
References

https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/

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

August 6, 2024 . 6:00 AM

More at www.hivepro.com