Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Cicada3301 The RaaS Predator Preying on Enterprises

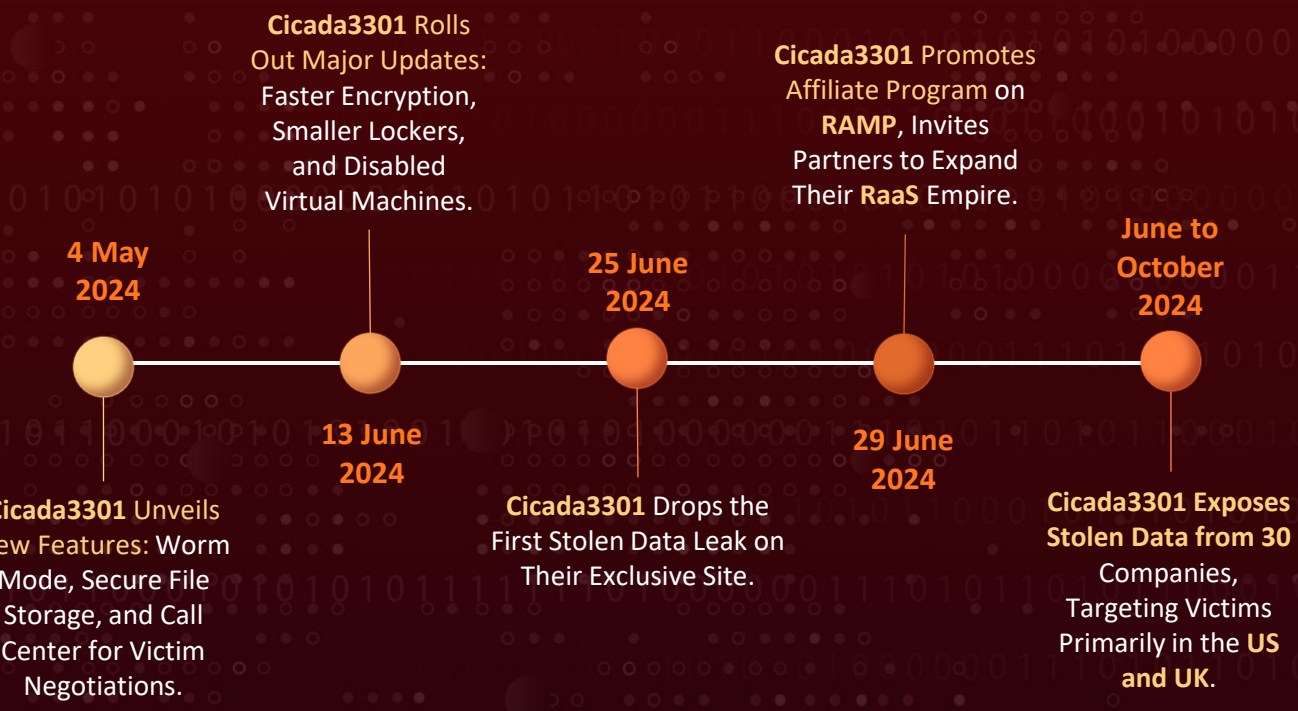
Date of Publication	Admiralty Code	TA Number
October 18, 2024	A1	TA2024401

Summary

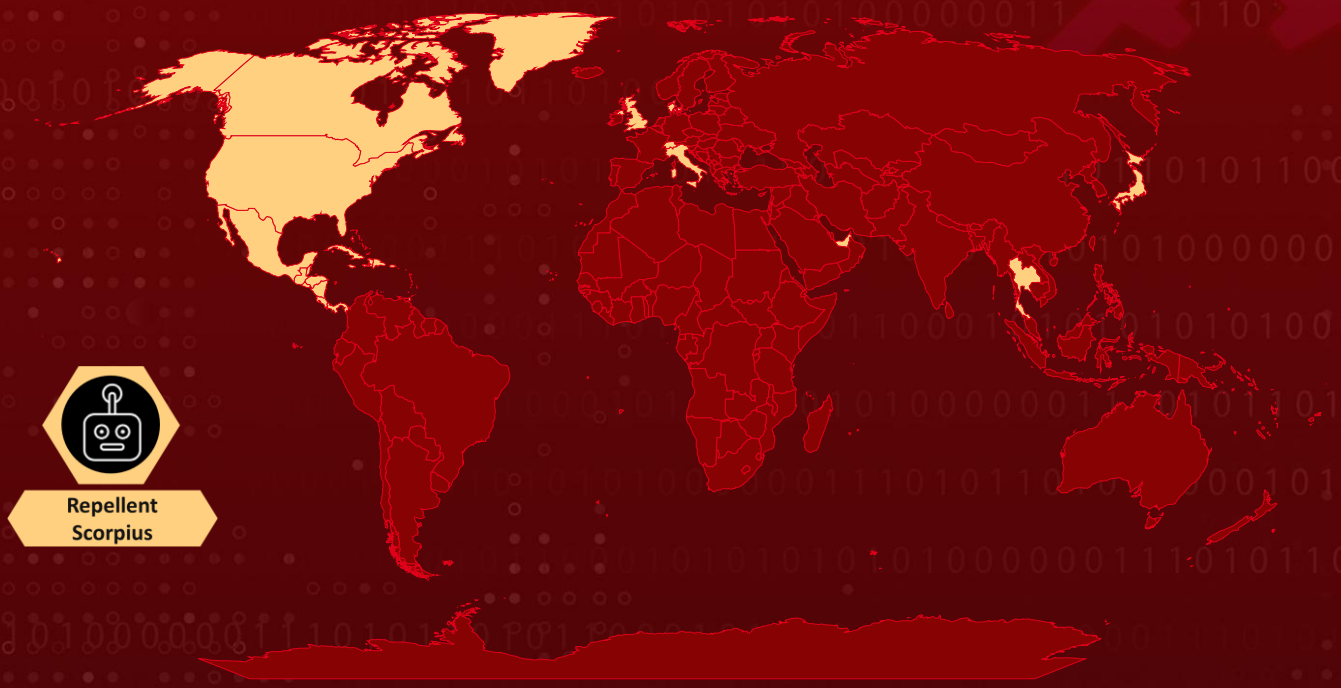
Active Since: May 2024
Threat Actor: Repellent Scorpius
Malware: Cicada3301
Attack Countries: United States, United Kingdom, Denmark, United Arab Emirates, Switzerland, Japan, Italy, England, Thailand, Canada, Greenland, Mexico, Nicaragua, Honduras, Cuba, Guatemala, Panama, Costa Rica, Dominican Republic, Haiti, Belize, El Salvador, Bahamas, Jamaica, Puerto Rico, Trinidad and Tobago, Dominica, Antigua and Barbuda, Barbados, Grenada
Targeted Industries: Advertising, Construction, Consulting & Professional Services, Consumer, E-commerce, Education, Financial Services, Food & Beverage, Gaming, Government, Healthcare, Hospitality, IT, Legal, Manufacturing, Medicine, Military, Real Estate, Retail, Technology, Telecommunications, Transportation, Travel & Tourism

Attack: The Cicada3301 Ransomware-as-a-Service (RaaS), distributed by Repellent Scorpius, has actively targeted businesses in key sectors, mainly in the United States and the United Kingdom, with 24 confirmed attacks. The group endorsed an affiliate program on the dark web forum "RAMP," recruiting partners for its expanding criminal network while strictly banning operations within the Commonwealth of Independent States (CIS).

Attack Timeline



Attack Regions



Attack Details

#1 Since May 2024, the Cicada3301 Ransomware-as-a-Service (RaaS), distributed by Repellent Scorpius, has been targeting businesses across various critical sectors. Their primary focus has been on victims in the United States and the United Kingdom, with a total of 24 confirmed attacks.

#2 On June 29, 2024, Cicada3301 introduced an affiliate program, promoting it on the underground dark web forum “RAMP”. The group maintains strict guidelines, prohibiting affiliates from operating within the Commonwealth of Independent States (CIS).

#3 Cicada3301's roots date back to 2012 when it first emerged as a mysterious cryptographic puzzle group. Renowned for its notorious global scavenger hunt, it captivated participants with intricate ciphers and concealed clues in both digital and physical environments.

#4 To this day, the true motives and identity of the group remain cloaked in speculation, with theories suggesting it could be a secret society or a covert recruitment initiative for intelligence agencies. Cicada3301 ransomware is written in Rust and utilizes ChaCha20 and RSA encryption methods. It is compatible with various platforms, including Windows, Linux, ESXi, NAS, and even less common architectures like PowerPC.

#5 Its capabilities include shutting down virtual machines on ESXi and Hyper-V, terminating processes and services, deleting shadow copies, and encrypting network shares to maximize disruption. For files exceeding 100MB, the ransomware encrypts data in 1MB chunks.

#6 Cicada3301 exhibits notable similarities to **BlackCat** ransomware; however, key distinctions exist. Notably, it features only six command line options, which are fewer than those offered by BlackCat. Additionally, the ransom note is formatted as RECOVER-[encrypted_extension]-DATA.txt, while BlackCat uses RECOVER-[encrypted_extension]-FILES.txt. Cicada3301 accepts ransom payments in Bitcoin and Monero.

Recommendations

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.

Implement Zero Trust Architecture: Adopt a Zero Trust security model that requires verification for every user and device attempting to access network resources, minimizing unauthorized access risks.

Enhance Network Segmentation: Divide your network into smaller segments to limit lateral movement by attackers. This containment strategy helps to restrict the spread of ransomware in the event of an infection.

Limit User Privileges: Apply the principle of least privilege by limiting user access rights to only those necessary for their role. This minimizes the risk of unauthorized access and potential data breaches.

Set Up Automated Alerts for Anomalous Behavior: Configure systems to automatically alert security teams for anomalous activities, such as large file transfers or unexpected process executions, particularly those resembling Cicada3301's tactics.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0008 Lateral Movement	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
T1041 Exfiltration Over C2 Channel	T1574 Hijack Execution Flow	T1543 Create or Modify System Process	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1070 Indicator Removal	T1070.004 File Deletion	T1046 Network Service Discovery
T1016 System Network Configuration Discovery	T1570 Lateral Tool Transfer	T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery
T1489 Service Stop	T1562 Impair Defenses	T1562.002 Disable Windows Event Logging	T1562.001 Disable or Modify Tools
T1562.004 Disable or Modify System Firewall	T1070.001 Clear Windows Event Logs	T1497 Virtualization/Sandbox Evasion	T1030 Data Transfer Size Limits

Indicators of Compromise (IOCs)

TYPE	VALUE
TOR Address	cicadabv7vicyvgz5khl7v2x5yygcgow7ryy6yppwmxii4eoobdaztqd[.]onion
IPv4	103[.]42[.]240[.]37, 91[.]238[.]181[.]238, 91[.]92[.]249[.]203
File Path	C:\Users\Public\psexec0.exe
File Name	csrss.exe, veeam.exe, system32.exe
SHA256	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b, 7b3022437b637c44f42741a92c7f7ed251845fd02dda642c0a47fde179bd984e, 3969e1a88a063155a6f61b0ca1ac33114c1a39151f3c7dd019084abd30553eab, 56e1d092c07322d9dad7d85d773953573cc3294b9e428b3bbbaf935ca4d2f7e7, dd98133b825a1632879b689b864b15a66741208343bc8ba080354e0133181d69, 2d614f088f486f0870b3839ddb361e33efb73526a0a585f691874039f23171cc, 8ec114b29c7f2406809337b6c68ab30b0b7f0d1647829d56125e84662b84ea74, 0260258f6f083aff71c7549a6364cb05d54dd27f40ca1145e064353dd2a9e983, 2d73b3aefcfbb47c1a187ddee7a48a21af7c85eb49cbdcb665db07375e36dc33

Recent Breaches

https://dubingroup.com/
https://corstat.com/
https://hughes-gill.com/
https://crownmortgagecompany.com/
https://designbymodel.com/
https://capitalprintingco.com/
https://www.brooker-cpa.com/
https://www.khoocpa.com/

https://www.blvdresidential.com/
https://www.kashima-coat.com/
https://bayoudesiardcc.com/
https://christen-sanitaer.ch/
https://www.findel.co.uk/
https://www.bfcpas.com/
https://www.hofmann-malerei.ch/
https://www.ebapc.com/
https://ufcw135.com/
https://www.dkgroup.com/
https://www.vvs-eksperten.dk/
https://silipos.com/
https://www.squareonecoatingsystems.com/
https://www.vossbelt.com/
https://tristardisplay.com/
https://www.railworks.com/narstco

References

https://www.group-ib.com/blog/cicada3301/

https://blog.morphisec.com/cicada3301-ransomware-threat-analysis

https://www.truesec.com/hub/blog/dissecting-the-cicada

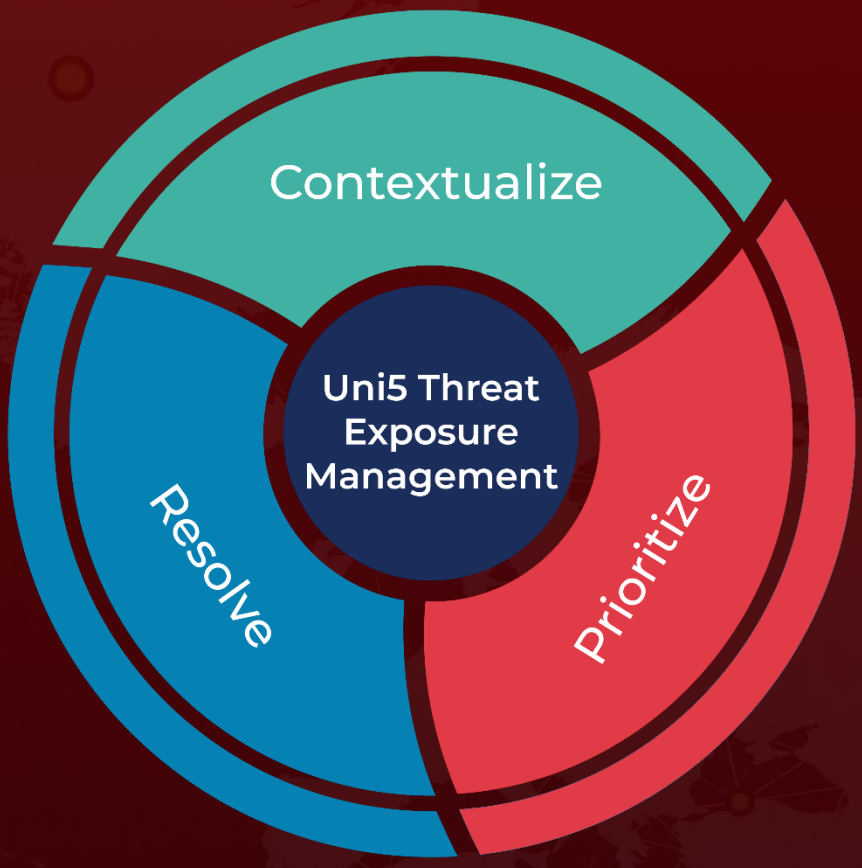
https://unit42.paloaltonetworks.com/repellent-scorpius-cicada3301-ransomware/

https://hivepro.com/threat-advisory/blackcats-resurgence-despite-law-enforcement-disruptions/

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

October 18, 2024 . 7:30 AM

More at www.hivepro.com