Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

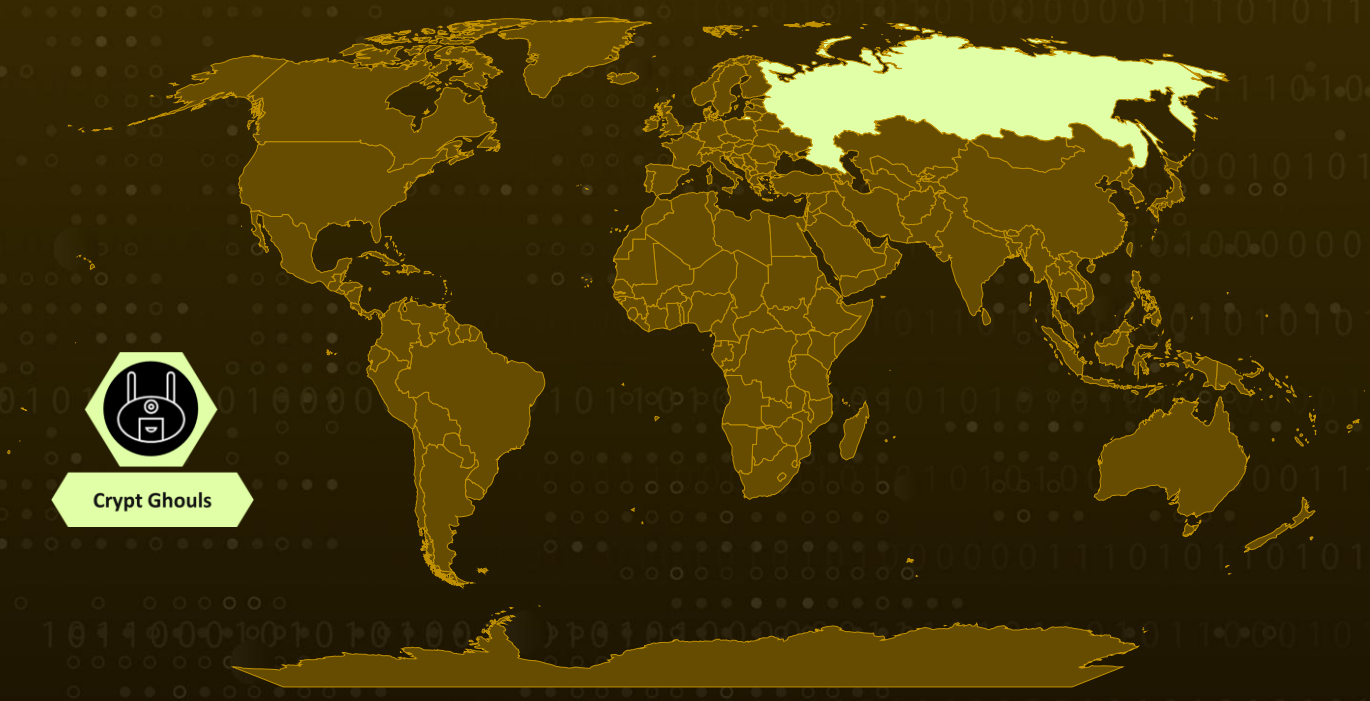
Crypt Ghouls Deployed LockBit and Babuk to Paralyze Russian Firms

Date of Publication	Admiralty Code	TA Number
October 22, 2024	A1	TA2024404

Summary

Attack Commenced: December 2023
Threat Actor: Crypt Ghouls
Ransomware: LockBit 3.0, Babuk
Targeted Region: Russia
Targeted Industries: Business, Government, Mining, Energy, Finance, Retail
Attack: Crypt Ghouls, a rising cybercrime group, launched a wave of ransomware attacks in December 2023, specifically targeting Russian businesses and government agencies. Leveraging powerful ransomware strains like LockBit 3.0 and Babuk, their objective was to cripple operations and demand hefty ransom payments.

Attack Regions



Attack Details

#1 Crypt Ghouls has been tied to a series of cyberattacks that started in December 2023, targeting Russian businesses and government entities. The group deployed ransomware variants LockBit 3.0 and Babuk as their final payloads, intending to disrupt operations and extort payments.

#2 The group gained initial access by exploiting a contractor's login credentials, allowing them to infiltrate internal systems through VPN connections. These VPN sessions were traced to IP addresses linked to a Russian hosting provider and the contractor’s network.

#3 After gaining entry, the attackers used NSSM and Localtonet utilities to maintain persistent remote access. Their toolkit included widely-used tools like Mimikatz, XenAllPasswordPro, PingCastle, resocks, AnyDesk, and PsExec, enabling further compromise of the systems.

#4 In one case, Crypt Ghouls deployed CobInt, a C-based backdoor malware previously associated with the Cobalt Group. CobInt works in three stages: an initial downloader, the core malware component, and additional modules to extend its functionality.

#5 The attacks culminated in the encryption of system data using publicly available versions of LockBit 3.0 for Windows and Babuk for Linux/ESXi. The attackers also encrypted files in the Recycle Bin to make recovery more difficult. A ransom note was left, instructing victims to contact them via a link in the Session messaging service.

#6 Crypt Ghouls' operations share significant infrastructure and tools with other groups targeting Russia, such as MorLock, BlackJack, Twelve, and Shedding Zmiy (also known as ExCobalt).

Recommendations

Adopt the 3-2-1 Backup Strategy: Keep three copies of your data, storing two on different storage devices and one securely offsite or in the cloud. This approach provides robust redundancy and safeguards against data loss, especially in the event of ransomware attacks.

Regularly Update and Patch Systems: Ensure all software, especially VPN services and remote access utilities, are updated to the latest versions. Attackers often exploit unpatched vulnerabilities to maintain access or escalate privileges, so regular patch management is critical.

Strengthen Contractor and Third-Party Access Controls: Limit access rights for contractors and third-party vendors to only what is necessary, and ensure that their accounts are regularly audited. Segment contractor access from critical systems to minimize potential exposure in case of a breach.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**TA0040** Impact
T1199 Trusted Relationship	**T1543** Create or Modify System Process	**T1070** Indicator Removal	**T1070.004** File Deletion
T1055 Process Injection	**T1083** File and Directory Discovery	**T1040** Network Sniffing	**T1057** Process Discovery
T1105 Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel	**T1486** Data Encrypted for Impact	**T1490** Inhibit System Recovery
T1053 Scheduled Task/Job	**T1047** Windows Management Instrumentation	**T1059** Command and Scripting Interpreter	

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[:]//localtonet[.]com/nssm-2[.]24[.]zip, hxxp[:]//localtonet[.]com/download/localtonet-win-64[.]zip
Domain	netstaticpoints[.]com
IPv4	91[.]142[.]73[.]178, 45[.]11[.]181[.]152, 169[.]150[.]197[.]10, 169[.]150[.]197[.]18, 91[.]142[.]74[.]87, 95[.]142[.]47[.]157, 185[.]231[.]155[.]124
File Path	C:\programdata\allinone2023\xenallpasswordpro.exe, C:\programdata\dbg\allinone2023\xenallpasswordpro.exe, C:\programdata\1c\allinone2023\xenallpasswordpro.exe, $user\desktop\allinone2023\xenallpasswordpro.exe, C:\intel\xenallpasswordpro.exe, C:\Windows\System32\wbem\wmiprvse.exe, C:\Windows\Temp\localtonet.exe, C:\ProgramData\oracle\dismcore.dll, C:\Users\User\Downloads\dumper.ps1, C:\Users\User\Desktop\x86\x64\mimikatz.exe, C:\programdata\allinone2023\xenallpasswordpro.exe, C:\programdata\dbg\allinone2023\xenallpasswordpro.exe, C:\programdata\1c\allinone2023\xenallpasswordpro.exe, C:\Windows\Temp\nssm-2.24\win64\nssm.exe, C:\Users\[redacted]\Downloads\AnyDesk.exe, C:\ProgramData\t.exe, C:\Users\User\AppData\Local\Temp\kxxxxxxx.sys, C:\Windows\Temp\kxxxxxxx.sys, /tmp/lock.out, /usr/sbin/xfs-healthcheck, /usr/sbin/xfs-modules, C:\programdata\intell\intellpui.vbs
File Name	dismcore.dll, dumper.ps1, kxxxxxxx.sys, odbcconf.xml
SHA256	01fba22c3e6cf11805afe4ba2f7c303813c83486e07b2b418bf1b3fabfd2544e, 3edb6fb033cc00c016520e2590e2888e393ad5ed725e853eea3bc86cee3b28b8,

TYPE	VALUE
SHA256	5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32, 92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50, dec147d7628d4e3479bc0ff31413621fb4b1b64a618469a9402a42816650f92b, a54519b7530039b9fba9a4143bf549b67048f441bbebf9f8d5cff1e539752189, 56682344aa1dc0a0a5b0d26bd3a8dfe8ceb8772d6cd9e3f8cbd78ca78fe3c2ab, a27d900b1f94cb9e970c5d3b2dcf6686b02fb722eda30c85acc05ba55fdabfbc, eb59a4b1925fdf36dbe41091cb7378291a9116d8150118e4f449cbd1147e204e
SHA1	abd5be341934b315c9b81bb76bb29a80e1c965c2, 32fd4b1abdb027cdd2d99f5cc1e5567b508a2a1c, 57e46697761aa19423765497e9e6a8abbd3f94a9, d1f7832035c3e8a73cc78afd28cfd7f4cece6d20, 583f34dd59d30be4a10dc7021984df0225cef147, 4dec26dfcd3fd938886c9586a8eb62d7a2495be4, 8a1673d5821d306209b1f540741598bbc90ed1d3, 2850dc0447d9512a264b60beb4c804880481a690, b8f699195d575747bba9020dc333861436baa832
MD5	f4a84d6f1caf0875b50135423d04139f, 42bbb6c631644de96c89f17b4ec222d1, 24847ce1f9044e464e50226c5c95a158, 8ea891a3b4049aa059f9bce52574be5c, e930b05efe23891d19bc354a4209be3e, 6e3e5d703ed9bed4b7327a73bc585c04, 8770189ed3ee558819fd6ddf677b0c28, 87667327439292f5d2b2c68d4b88c0ad, c817c3b0dc10d54e780982c18c531260, 19633c025f6e9d9fc65b240c5aa082e0

References

https://securelist.com/crypt-ghouls-hacktivists-tools-overlap-analysis/114217/

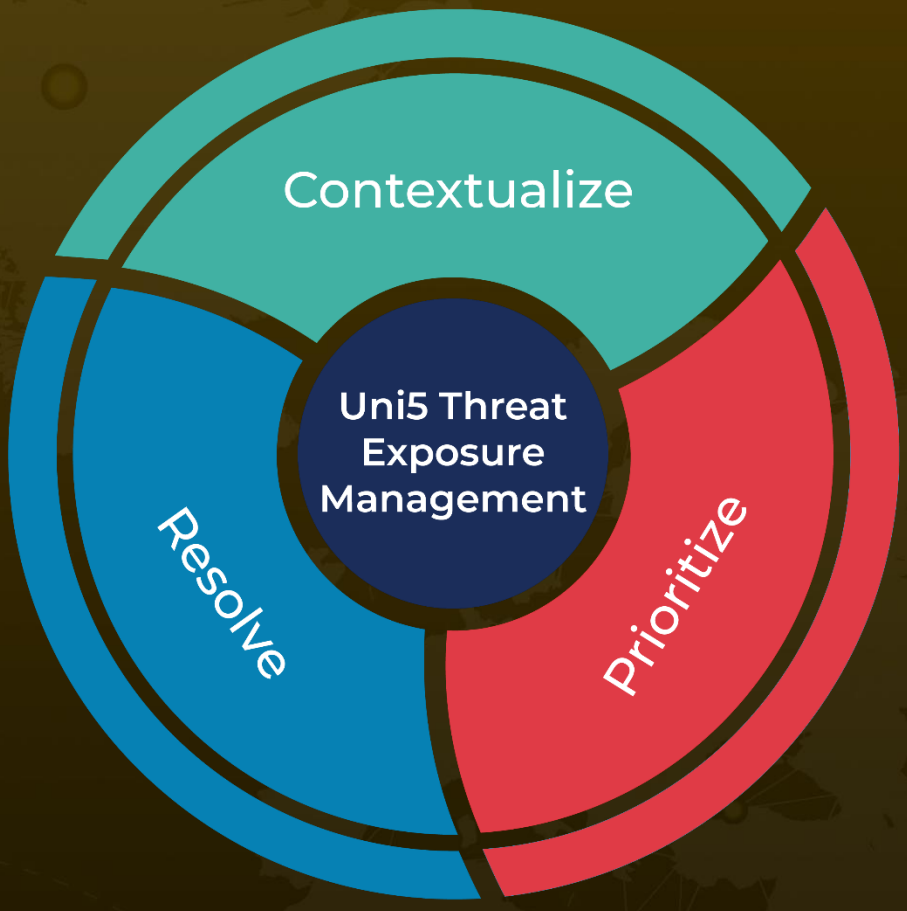
https://attack.mitre.org/groups/G0080/

https://hivepro.com/threat-advisory/lockbit-3-0-builder-unleashed-custom-ransomware-on-the-rise/

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 22, 2024 . 7:00 AM

More at www.hivepro.com