THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

RansomHub

Threat Actor
Ransomware

CATEGORY

Malware | Ransomware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Financial Losses
- Data Loss and Disruption
- Reputational Damage
- Legal and Regulatory Issues
- Psychological Impact

Description

RansomHub

RansomHub's criminal activity in 2024 has spanned across a vast geographic area, impacting organizations in at least 17 countries.RansomHub, a recently identified cyber-crime operation, appears to be a rebrand of the Knight Ransomware gang. Their activities involve data theft from institutions such as Christie’s auction house, US broadband telco Frontier Communications, and Change Healthcare. RansomHub exploits the ZeroLogon vulnerability (CVE-2020-1472) to gain unauthorized access to victims’ IT environments. Notably, their code exhibits significant overlap with Knight’s, making differentiation challenging. If you encounter RansomHub, I recommend seeking professional assistance for removal and decryption options.

Indicator of compromise

SHA-256

02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292

34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087

7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a

8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7

ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00

104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2

2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad

36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e

595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb

7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2

e654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23

fb9f9734d7966d6bc15cce5150abb63aadd4223924800f0b90dc07a311fb0a7e

f1a6e08a5fd013f96facc4bb0d8dfb6940683f5bdfc161bd3a1de8189dea26d3

a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2

SHA-1

eec3a55b1599eee16a47954e1bb230ec99db5f96
bd886d47719d0881fcd7001713169215996f530f
a7ca950c6dadd02ab8fafdba8f984266fc2f9b7c
06156f7e42dc18f36c64855edb8adbb892cac0c0
63c31bcda20194821d142a0ed131eb32649aa32e
82793d93d987abb357809f069420d17a25a59f26
261535c91df592071adb5cdbf255566c9ce019dc
ada3a90f022fbdaee50245ecdaab6e5756d18d0d
63c31bcda20194821d142a0ed131eb32649aa32e
5f27d44bfdd918e17605cdef3883c8070325cdfb
b67b17b8930c872da4347be931fb9b27c624f0cb
ee682488fe843d8bb826854d23b2cea73fad4969
c2f6ce083fe3850f082719026486160ea266e6a8
e9aa4e6c514ee951665a7cd6f0b4a4c49146241d

MD-5

3034b61a52ddc30eabdb96f49334453b
a1dd2dff2859b22bcf6a3a4d868a2dbc
0cd4b7a48220b565eb7bd59f172ea278
392880023da7df0f504056be9e58d141
bd1efe953875f35cc8b787c0980e8a75
cfb2286b45544fdb23569f59c02e3d58
19209b41db4a3d67e2c2c1962d91bd25
8c8916d8ea8c44e383d55e919a9f989f
bd1efe953875f35cc8b787c0980e8a75
19ebefbb1e4cb0fc5ce21b954f52e1bc
eaa6160cf4ed6b7d8d68eeb42c0362d5
ba8763fc59d73b28b070cb6eb393aa83
bbdcda77bfb86e861474617cc5c828f9
477293f80461713d51a98a24023d45e8

Remediation

1. Isolate **Infected Systems:** Disconnect affected systems from the network immediately.
2. Identify **and Contain:** Use threat detection tools to identify and contain the infection.
3. Restore **from Backups:** Recover data from clean, verified backups.
4. Update **and Patch:** Ensure all systems and software are fully updated.
5. Enhance **Security:** Implement robust firewalls, anti-malware, and intrusion detection/prevention systems.
6. Employee **Training:** Educate employees on phishing and safe cyber practices.
7. Incident **Response Plan:** Develop and regularly update an incident response plan.
8. Consult **Experts:** Engage cybersecurity professionals for thorough remediation.
9. Compliance**:** Report incidents to relevant authorities and ensure regulatory compliance.
10. Continuous **Monitoring:** Monitor systems for reinfection and review security policies.
11. Block all IOCs on your XDR, EDR and other security tools.


THREAT
CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE
Cyber Threat Advisory
Secure your byte world
+1 (832) 271 2738
info@threatcure.net
https://threatcure.net/