KPMG Cyber Threat Intelligence Platform

Knight Ransomware – Menacing Cross-Platforms Threat

Knight Ransomware, a.k.a. Cyclops 2.0, is an advanced version of the Cyclops ransomware, rebranded in July. It features an updated lite encryptor supporting batch distribution. Operating as a multi-extortion group using a Ransomware-as-a-Service (RaaS) model, Knight targets Windows, Linux, MacOS, and ESXi systems since May 2023. Its impact spans global organizations, particularly in retail and healthcare sectors, affecting the United States, Thailand, Argentina, Canada, and Turkey. They also operate a TOR leak site to extort victims using their stolen data.

Initial access is achieved through phishing emails containing malicious attachments, initially utilizing Zip attachments and later switching to HTML extensions. Upon opening, a script is executed, downloading an archive with multiple files, leveraging "explorer.exe" process to connect to a remote server. It injects a malicious payload into the "explorer.exe" process, creating a new folder named "offlinelsa" and adding various files, including a fake "UXCore.dll." It then downloads a PNG file to a specific user folder, leveraging its data to create additional files in the Temp folder. The injected payload initiates processes like "Dashboard.exe," "cmd.exe," and "explorer.exe" to facilitate encryption. It utilizes advanced encryption algorithms (Curve25519, HC-256, SHA512, CRC32, ChaCha20+AES256) while selectively skipping directories/extensions specified by threat actors. Prior to encryption, it scans for connected devices in the local network, potentially aiming to extend its impact beyond the initial host.

Knight ransomware tries to appeal to affiliates by offering advanced encryption, user-friendly interface and even custom-tailored versions. With Knight already being a rebrand, it is imperative that the operators of Cyclops aren't going to cease operations anytime soon.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

Knight Ransomware – Menacing Cross-Platforms Threat

Indicators of Compromise: IPs
89.23.96[.]203

Indicators of Compromise: Hashes
6a7b78df17ff39bebcfb83d39ae91103
2b6c8901c5b47f9288e5e98a0a0bbbc7
b8d27562296d140867c95749b43425a6
80df8411e2999f8f7acb4cc2b9c1bdc9
ff248a015987e2c2c5f1188054e27d93
11d5b226bbc813687e46864b420ca558
4e894b4a373a21e2b4fc7d9cbcf247e1
1206076502361afe5988ac43853a9c07
a2f4e298756ca440e853d715e050bd67
6b4bd48defde590c99d1fa801d8d55e0
3b01e99c99284c74a90cefdd3bc6e9ff
f5e13d0f83b235179f7715cf8ed0be86
6446b85d60c931de76a2c98112c25309
cd807770398b8f6095807cb696ee04cb
df98e7234665fc69ccb8b34aacbec39d
31146a1095452f8f15ebad9f7e3c6efa
249c28ddd361a48d66723ab39575f81b
24e41e512e15fd5b55c1b617e5bfaa28
53986f4e0fe4301b6a064314ee255500
52026376e76ca95627a04bc765951a34
cbbd3600fdbe6b2cf5dc5552ca3166ba
708650868841943838b905561449d7da
15e1c374e93a364d148f10944792f4c0
ca742c5ddcea20737c6a9d089b756727e1f1ee45
aae050d1deeecfa7396a4ceab7f968ba1fef0431
87090405611573e0679617a9930ed33d6f8b81fa
07eecfd07af0a7a6758d3141e57fbb252364c6b2
981d955ad0f2eee242e774e349fb2ef55a81ca1e
c13581ccbdb7030573778cc89db82591d876e168
dab8ce4dce75b1ab59409f933bb21f269cdd33ad

KPMG

KPMG Cyber Threat Intelligence Platform

Knight Ransomware – Menacing Cross-Platforms Threat

Indicators of Compromise: Hashes
af277577f9cc932686ac0f6b3da44133b26c3188
1cfaf0574aced08c89d01724db2184a894ad109e
45dd48c869d05d6b2db428b26e0349fcddedfce3
93be3c1f4ee7b10660083a5632857d773571c2d0
811cdc61923f2e8ec1449d5be6d82ad4a6ce9159
3cf78ca5b35161a618efadf904abbaa161d7b02c
1960f32c2d62d049012f4deb64ddec341fbe3541
216438b225991716799c0a16de90022bdf13136d
217e1fabce28bae5964d70f747aefa4df0eba4fd
ff51a1c5cab13afe0178163b2b9d60e49c799b74
b872b9a817c2e6cfd507a7a57f1f34b433bbb14a
b64a53ae9dd3f8b8ab5752c3588c934ea63225c3
0ee04f020d4f36ac6c5c2fa7667de7ac897dc41e
20287a02fca852d6713252d18b1a974aea2de649
2c4c0d875a2432d5590f32c64bdcfebddd9ccdd4
66a943dea2cd1c3f440cbebf63f5dad3f04a4aa4
cf0dd52331ce203c723f7be32bd91d7cfb34a988
6adf30be27fe42380ff57caa8bb1c2b955586941
e0e0635c41bbf9450f946e4bb169f26733ee3aaf
1112d8346ee413ac8aecaf5bc0dc5400041669116a5a596c6be2e24c6886849d
2bfababf54992c32afced15b355cf7fcf7c6b0783cfee9086e80893d5f5124ed
3ed381014d25a9796bd6d007573b2abe152ee455738ae5f2288e5146726f3b2e
3f029aee12d43e3c67c4ab07c43bcd0960fa9f6a371f40577004673ac95e870c
40c6896d761595fe190e0fa891462bfb120579b6399bd28f40839c017a367538
4416ba60d11b0e8eafa07f3c3051c2d84ffcb5c860d458b6a1374fdc935e92f2
484414d68e1c3e79e602ed2876e963161916e21ea4e2c920da5cc623ea19731f
50ce3d6e410f0f83c9407a572eb29733084fed94f5dacff59cea350bcccee27d
581c6c58e6ea187e74bc23d8d0fa9feb7dc5cc2db4ca887afee5be229532e8e2
5ec48925f73ea58a27d6306d23d76b5da41e16754f58f26098ed36f0d1f198c8
6ff69b6e0f778aabf521a72a70c34274acfabc59a3472f7cba2372ebb8875d0f
70d2891a1cb3b6172428ea9cdb5a81b0494deac02b7dee91527a17fb9f53509a
712fc089cb028e381e285685519df357fb4102f8bc8de31547a9b98ca7629e49
7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d
7f99540993e2afc351776b85ea22661d3701743521d55d657abdb23e12c93c00

KPMG

KPMG Cyber Threat Intelligence Platform

Knight Ransomware – Menacing Cross-Platforms Threat

Indicators of Compromise: Hashes
a6258d70bc0b5d5c87368c5024d3f23585790b14227b8c59333413082524a956
b586d60beb49b362d4cd9b8d64fc9a3eef3da76b0f494c42c4ac30d6612d8993
b5deec95d1f50229e1361ca47761b9742006f484cf1f2c31ba8a495afb814ae2
cb41bbbe053e7a9b4857bf89c92298e7c0abdf9da157185fcfec5b383fe1e62c
cd92bf9c3349b086eec621de247bbb1bceebffb90863a46496c3b41fb13ec745
ce609604f4deb265ed957540b86ba96b33d26399c8d508110d78b0602f9d9d3a
d256bb30d0609d0e3aa7f1b98077dda6136f2f3604beb71ec982d8125d2858ed
e2af95e7827144a9278fcbb87fe8d9a4cfdb8f69b2f43f63c9e26aa6a33cc2ed
e5f1f8f5b2b4304493f416b54324c0b0e0253ed07ee1f4512bbe184e32e4580a
ecafd694118c4bcd21b4f7a620ed8a1346932f05acefe8cd32a01febec9a92d9
fba8fee602b5c3db46cbbb45ff2f8aa72791f47f8b8c6a556334d3d3358cebba
1341bd6193ea223c05566aaca13fc1152732b67af8344519d6efaaf9ab6ed5f4
14ab9dc515dc22f0bbf5f3e44cc280e35331bf9209b6c4d35b86bfe3f32bcd23
167678eb9daa2376bd805069fac69c42b0ad0c6f70b9d644161970c1770c117f
3bd52cefc9d88c5292275729ca096c131a5db8c77ec142493a066623270cb782
3fbedfb9ae1e9bcef7983491124e3a50937f9c5209b7cfc2614197a2e8045cfb
4f1e46ac9e46f019d3be3173f0541f5ed07bde6389180cd7e8255d35b49f812e
554990b8636baf5af393d52ce85150a8b263b9c5fb214bc0e69a1b032ee8f3ae
5ace35adeb360b9e165e7c55065d12f192a3ec0ca601dd73b332bd8cd68d51fe
5c0f3de1254bcad7f457ad1898df2fdbe44dc964b5e92fba125c19888481da75
5ed4dfb7da504438688d779092a717cb2426ee88bc4f0ee588b3e989b7567dff
61bb91bc554d9b849cbd670669365bc5a58a8c5f9a0f530b8ed9a4b8f0968186
716341671eff8ca18c5f5bbf38095d07225141d02854168f854b168731b4c71c
75e227a3a41dc1c2d4384e877d88f9a06437a49f2c71f8efa7e2cc60bab6cc4a
7ec0d3e3dc4222f34c482926ce1f971b51929e95b9d097140bc1f4b1c84dafd9
9123e42cdd3421e8f276ac711988fb8a8929172fa76674ec4de230e6d528d09a
a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de
b6064f6936f72d1312f40f86f0cb889c6d0477c20f59c6c96c385c6287f701f7
b94e28bc2e23eeff0d8c26334ef6c59d86a45fec37ffc83ab585d34019247355
bb65532e8a52e282d98938031c0d75155082933524924d01de4246e12690cf9c
c42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbccc7d9ab5a
dbf9cc65461c7bc650938156d3751d4ae0ce4312d3899f747e590767c0ef0408
eedda61d02d8bd0e145a07e6048621fc84f420376e6cda2616c2d77d4fd4fe18
f2571431c9d8e87081816d46cda9bde8d98b081056fdc2114e88cbad2d544cec