KPMG

Threat Intelligence+

White Rabbit: FIN8 Group's New Pet ?

White Rabbit ransomware, with possible ties to long-time financial crime group, FIN8, was recently discovered during an attack against a local US bank. Although the real-world attacks have gained attention only recently, researchers have pieced together a string a malicious activities dating back to July 2021. White Rabbit's payload binary requires a special command-line password to decrypt its contents and proceed with its ransomware routine, this method of concealing malicious activity is a strategy used by the Egregor ransomware family to mask malware techniques from detection.

White Rabbit's binary appears to be uninteresting at first, with its small size of around 100 KB and lack of remarkable strings or activity, although the inclusion of strings for logging gives away its malicious nature but without the correct password, the fundamental ransomware behavior is difficult to unearth. The ransomware is believed to utilize Cobalt Strike, a post-exploitation framework for reconnaissance, penetration, and dumping malicious payloads into impacted systems.

The ransomware creates a note for each file it encrypts and appends the .scrypt extension to each file name, then drops a second instance with the .scrypt.txt extension for each encrypted file. The ransom note that appears after the encryption procedure warns the victim that their data will be published or sold if they do not meet their demands within the four-day period. The note also states that if victims do not make the payment, their data will be sent to the data protection authorities, generating fines for violations. The link between the White Rabbit operation with FIN8 operations is based on the use of the same malicious URL and a previously unseen version of BADHATCH, a backdoor used by the known threat actor group FIN8,a financially motivated group active since 2016.

What should you do?

- 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.
- Implement well-documented and tested DRP and BCP procedures.

What is KPMG Threat Intelligence+?

The KPMG Threat Intelligence+ approach is an industry defining, research-based capability for enhanced visibility into cyber threats. Our machine ingestible feeds are the result of automated, sensor-based intelligence metrics with dedicated, expert analysis of each threat to provide you the right context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP. These feeds are additionally co-related with out industry partners and independent researchers to ensure you have the most accurate and contextual data. The intelligence is then curated from Strategic, Tactical and Operational perspective to give you 360 degree 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.

Range of services
Strategic Threat Intelligence Report
Machine Ingestible Threat Intelligence feeds
Threat Intelligence driven pre-emptive Threat Hunting Exercise
Cyber Incident Response Services

Contact us

KPMG Cyber Response Hotline : +91 9176 471 471

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

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

Sony Anthony
Partner, KPMG India
+91 98455 65222
santhony@kpmg.com

Chandra Prakash
Partner, KPMG India
+91 99000 20190
chandraprakash@kpmg.com

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

Rishabh Dangwal
Associate Director, Cyber Security
+91 78277 54752
rishabhd@kpmg.com

KPMG

Threat Intelligence+

White Rabbit: FIN8 Group's New Pet ?

Indicators of Compromise

IP Addresses		
5.2.83[.]23	185.167.121[.]3	93.189.144[.]238
185.8.33[.]74	88.198.13[.]114	91.238.228[.]137
195.24.68[.]7	185.167.121[.]7	178.248.233[.]48
195.19.220[.]6	185.167.121[.]4	91.238.228[.]136
94.19.124[.]66	185.233.43[.]13	91.238.228[.]131
89.184.64[.]88	91.203.144[.]46	91.238.228[.]130
89.184.64[.]96	77.88.202[.]228	91.238.228[.]132
78.109.29[.]87	89.184.64[.]108	185.104.45[.]156
185.80.1[.]146	135.181.9[.]149	91.203.146[.]214
178.62.63[.]49	135.181.9[.]156	157.90.133[.]197
5.189.239[.]12	148.251.31[.]51	91.194.251[.]204
80.93.176[.]34	94.130.119[.]36	91.194.251[.]197
185.149.120[.]3	192.95.32[.]151	91.194.250[.]241
195.19.220[.]18	185.53.177[.]12	164.132.16[.]163
217.16.16[.]111	77.244.222[.]74	91.218.212[.]147
195.19.220[.]22	37.139.21[.]107	178.62.202[.]171
185.167.121[.]9	170.130.55[.]120	46.101.210[.]112
82.140.67[.]173	195.19.220[.]238	164.138.218[.]155
195.19.220[.]28	195.93.186[.]191	109.234.158[.]163

Domains	
otbrana[.]com	t[.]ks[.]ua
online812[.]ru	imer[.]ro
mediaport[.]ua	i24[.]com[.]ua
argumenti[.]ru	grupovo[.]bg
an-crimea[.]ru	aica[.]co[.]jp
spbvoditel[.]ru	fontanka[.]ru
sinematurk[.]com	adblibri[.]ro
1dnscontrol[.]com	novayagazeta[.]spb[.]ru
pensionhotel[.]cz	bg[.]pensionhotel[.]com
most-dnepr[.]info	osvitaportal[.]com[.]ua
argumentiru[.]com	calendar[.]fontanka[.]ru
blog[.]fontanka[.]ru	104-168-132-128[.]nip[.]io
ankerch-crimea[.]ru	caforssztxqzf2nm[.]onion
www[.]sinematurk[.]com	va5vkfdihi5forrzsnmins436z3cbvf3sqqkl4lf6l6kn3t5kc5efrad[.]onion

KPMG

Threat Intelligence+

White Rabbit: FIN8 Group's New Pet ?

Indicators of Compromise

Hashes
655c3c304a2fe76d178f7878d6748439
6ffa106ac8d923ca32bc6162374f488b
fb3de0512d1ee5f615edee5ef3206a95
4a03238e31e3e90b38870ffc0a3ceb3b
beffdd959b1f7e11e1c2b31af2804a07
d9f5a846726f11ae2f785f55842c630f
087f82581b65e3d4af6f74c8400be00e
1d724f95c61f1055f0d02c2154bbccd3
fbbdc39af1139aebba4da004475e8839
b14d8faf7f0cbcfad051cefe5f39645f
b4e6d97dafd9224ed9a547d52c26ce02
edb72f4a46c39452d1a5414f7d26454a
ea2033e3c6190a2a025c288cdf429894dc86721b
ec35eeb8afaf0d7521ac098c20acfbb1680fd3d8
fbc28371b9675dbb188f362b11ae407529caf448
d7e1937bc9471e8de0b703b5888c2715d8445773
886f1831f4560d32595a1d0b964835c9c86fbb4b
5409fb14a49115eac8119b76be5afebbf8c52049
37341c6cc2c4913fcc2e33c0de0a49c4741eca15
03e8b29ad5055f1dda1b0e9353dc2c1421974eb3d0a115d0bb35c7d76f50de20
4ee21b5fd8597e494ae9510f440a1d5bbcdb01bc653226e938df4610ee691f3a
8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93
682adcb55fe4649f7b22505a54a9dbc454b4090fc2bb84af7db5b0908f3b7806
630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da
579fd8a0385482fb4c789561a30b09f25671e86422f40ef5cca2036b28f99648
301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c
2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035
0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
b0844458aaa2eaf3e0d70a5ce41fc2540b7e46bdc402c798dbdfe12b59ab32c3

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.