KPMG Cyber Threat Intelligence Platform

SocGholish – Hiding Behind the Masks

SocGholish, (aka "Fake Updates") is a Jscript malware that was discovered in early 2017. Allegedly operated by TA569 and historically associated with the Russian cybercrime group Evil Corp, this malware has gained notoriety for its widespread drive-by-download attacks. It has infected numerous victims across the globe, including those in Poland, Italy, France, Spain, Germany, and the United Kingdom. The framework spreads through advertisement and social engineering themes that mimic browser updates, such as Chrome/Firefox and flash player updates, and more recently, as Microsoft Teams updates. It has been observed to establish a preliminary foothold as a pre-cursor to ransomware attack.

SocGholish is a sophisticated threat actor that leverages traffic distribution system (TDS) to redirect visitors to malicious attacker-controlled sites or to legitimate sites containing malicious content in an iframe. SocGholish employs domain shadowing by creating campaign-specific domains and occasionally uses AWS as a temporary substitute. These pages often masquerade as legitimate browser/software updates to lure the victim to download and execute the malicious '.zip' or '.js' payload. Once executed, the threat actor exfiltrates data via POST commands to their C2 domain, enabling post-exploitation activities. Second stage payloads like 'NetSupport Manager', 'Blister Loader', etc. are used for pre-ransomware activity.

To defend against the threat posed by SocGholish, It is important for the defenders to stay alert. Organizations must prioritize educating their users about the tactics employed by SocGholish, and to remain cautious in case of any suspicious activity.

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

SocGholish – Hiding Behind the Masks

Indicators of Compromise: IP Addresses	
45.10.43[.]78	185.185.87[.]24
45.9.190[.]217	195.133.88[.]19
5.42.199[.]146	91.228.56[.]183
77.91.127[.]52	87.249.50[.]201
84.32.188[.]27	91.208.197[.]151
91.213.50[.]65	91.219.238[.]223
77.223.98[.]12	31.184.254[.]115
5.53.125[.]173	91.219.236[.]202

Indicators of Compromise: Domains	
jquery0[.]com	sikescomposites[.]com
pastorq[.]com	friscomusicgroup[.]com
soendorg[.]top	asset.tradingvein[.]xyz
neashell1[.]com	apps.weightlossihp[.]com
pastukhova[.]com	widget.windsorbongvape[.]com
taxes.rpacx[.]com	platform.windsorbongvape[.]ca
skambio-porte[.]com	signing.unitynotarypublic[.]com
xen.hill-family[.]us	host.integrativehealthpartners[.]com

Indicators of Compromise: Hashes
098307aff90f076625a1616bd87d906d
35c34967d389c069ea5a70aaa4dad290
574329a75d815cbd5a7331a02399dc9e
801c13ee34009aa00a195fe75a577b85
93a4fdd473320d37ae59ed875632e4ef
c531d61231e1bbded5a5f773973ab05a
263263e0c4e35af815d2f7054d5e96b4
3881b6d0bf55e91c2a731c0552a5e607
3f2ff9eba9f57075741451b869ad0b8b
417b37b0a324200ea9157f51d7fbd7d6
4f1b5c3aa34f557c86aaee0412a6b626
5128c69077384524b4311ba8b8d96ca8
73b65d1668976db8ada3fd9e0718f0ee

KPMG

KPMG Cyber Threat Intelligence Platform

SocGholish – Hiding Behind the Masks

Indicators of Compromise: Hashes
7a286d02dc8da557b740eaea28235cac
7b573b1159d7d19f9233f324857fe14e
196724d6f8cf530280013afb969554b8802a6c00
2223aea5f9433d94d0dfb0cd4d5ecd0bbb613454
24f608455eacddcb2cc221576f595450ef3ae8e0
2cf87107aaf9441053a7526762a9c6fc19c9e4e2
2f64087ebbd1c7633a183c3ed110e5d9f0bac342
4524894a91f6de4262784162a0a2c1f774734dc4
68ffe19e318a1ff588bfedf1cd994f80c6e8d935
71ee84e62646f2dbf3a9e36587a7fde7e7b1998d
75a4690028051f5eb8df5195a5bec283066b8420
7d5833e5da7119efdd2f73663bf79ca515113fe2
7f10dc72be06fcd7ce0accb0cd90ca9974761f76
81b8f10eba80a891dd4c661157e62b0701f17e0f
8693c1ec31b1f6047661786b007603fdad268975
8cd530750cb036daf4ebee569e6e44d0d4842b50
9c931c0f935820b1e19533b4bf47531b4c0425b9
aa64ce83b0c7e0b2083325a916da0c9f1e4a32a2
befa0e642a57c8a114ad3aaba3b6df6253913d24
0d357a2440537e073c4eeb16a7d109d5eb367557674e8d16615fdb06fb9a2089
13d576dde555a93f8e5ec567e61a44cae663c83b9878bbed7f1e37ee47fb9ee8
18aeff0a97dfd33b6f0664f43ecafd18511af559002072f680a4e5929a9c7e4f
202853bdbebfce4d5c86493abd168d25f5557be039af8fce58eeda47250083ce
23bea4bb6c911fa0d655a4fc2f13d237b19a2dc165b79e00f98919fd1a21b04f
31d7d798d1cde0d978be8aece150160aa2e4da4ce9e5e85972dc2e15e8c8d03b
36dbd2428d6ee76af1e5a4719058c28637963241579dd5aba716d79d26bd0543
388bbd8b592cebe4a0a32351969fe2e19e454af24ff6683524c71f74e0320ac0
3d0bc49f6a4dc55286119be8ec8e24fd1a18f8e817fc4c7809ec018112349699
3dd172bf8a7e2985f8387ffc4b6f2fc3ee05435b69a43d714d3137d9a5147127
52b43d0f11bca924e2ef8d7863309c337910f6a542bf990446b8cd3f87b0800e
681ac78369f4d3688f67c3a363337e3eb855db248e92cff8a35e8abe6028ade5
76b3d17196dd9e99eadd46e8bc760ec8809a0c723f66fb687ab8576dd1299e34
7a1fd70d092ebad80ba298e80147eddcd115194848591c2c23ded266a4881b6e
83cea606cc5d6c671b6b100b6dc3b93786a103b1faf106ce21b4ace02a8369fc

KPMG

KPMG Cyber Threat Intelligence Platform

SocGholish – Hiding Behind the Masks

Indicators of Compromise: Hashes
8f3bb770ad8cafcabe4eba9f67ba79f353ddee4caf30532e724bdeb15489df64
9322965adfa126aa09811ed703da19f588688a65a29bc8cf31612c7b2217fd47
a82a9e1f6667350808a19219d586d10bcea85cf73b67024d8c58366981fe4993
a848e30ce1de8bb52766938f09c90a5c192096820e0890c787b7a352c59ec95b
bad534540ed575c213bd34fe1f21c6ffca58169e9c9c83669749c3f6e398ea4b