KPMG Cyber Threat Intelligence Platform

RedCurl – Exploiting Mail Transfer Service and PCA

RedCurl, also known as Earth Kapre and Red Wolf, is a Russian-speaking cybercrime group operating since at least 2018. The group is seen employing the Program Compatibility Assistant (PCA), a legitimate Microsoft Windows component, to execute malicious commands. Known for corporate cyber espionage, the group has conducted approximately 40 attacks, with half targeting entities in Russia and the remainder in the UK, Germany, Canada, Norway, and Ukraine, etc.

RedCurl initiates its attacks by distributing emails containing malicious attachments, such as SVG files or RAR archives containing SVG files, to employees of targeted companies. These SVG files contain links to RedCurl.ISO, initiating the malware's first stage. In recent instances, SVG files are utilized to mimic legitimate secure mail transfer services. The ISO includes an LNK file that executes RedCurl.SimpleDownloader. This downloader component fetches malware components & displays a decoy site, using rundll32.exe to execute commands & communicate with remote servers for payload retrieval. It utilizes pcalua.exe (PCA) to execute an executable file, potentially launching the next malware stage called RedCurl.Downloader. RedCurl.Downloader, upon execution conducts system checks, gathers system information, and transmits it to Command and Control (C2) servers. RedCurl.FSABIN provides remote control capabilities, executing commands, running BAT scripts, and communicating with C2 servers for instructions and payload delivery. While earlier attacks employed RedCurl.Extractor for persistence, recent instances show RedCurl.FSABIN present without corresponding extraction stages.

RedCurl's utilization of its own unique and updated tools necessitates vigilance and adaptability from cybersecurity professionals to detect, mitigate, and counteract their evolving tactics.

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 josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

RedCurl – Exploiting Mail Transfer Service and PCA

Indicators of Compromise: IP Addresses	
23.254.224[.]79	198.252.101[.]86

Indicators of Compromise: Hashes
b0084e505663a05425eaaae058ebc48c
ff8772484a6798ce270a3b4eed3dedae
57f087cc375f04f27a99e31d9006b12f
78f69d4ff80b57747ca0a1e5a4305514
9d7d79c17dab6ff01c5804866eb4c81d
46a7d14e899171a136f69782a5cbbe35
6ece95df231083c37ecf9a39c324e2bb
a7b515678444d3590acf45bfc508b784
6afc831b325efed29f4e513abc3239b1
a4dfe407a33358224a521f51611a4b5c
bdfa38042099cf24128d2daf13ae5ecb
10dac2d8fdbf056c0de6e3a47197889c
d6cf3f26ab8c25a49a4a6025b0099906
6a36f3ba849adc65831bf709586e63b5
4bda4bb698294eb2c8d233a6901e6d17
78859b00cf6fafe4326c7ef3ef4e14ef
bb87a994e6049160a3bdce56caf7f2bf
cea0a824d357d43a2bbd2fb34d2cd70d
b1538b3e057146ae6e0317c31f777750
e31d4c157711f0de9b291576541984cc
6642fb75031ac58800beb288518ec186
dcabab59c3a49e0ae345051350c6f415
e257d29201892816b9934ad7989eed45
7fad9e25d69e3d07882c0fa7a91e1067
99681e4c6951d4bc015f2fd94afc4306
6c87f917e074e750d3cd5bb6e41663ca
1cf5d081dcc474eefb710ce11f67ab2a9d5f829a
28ef33b00c9c347f35405ff0b35c499acd71573e
2003d2de9c155799fea82663245add57d59813aa
240e037af8964388d8ca92385528bece5e0c6546

KPMG

KPMG Cyber Threat Intelligence Platform

RedCurl – Exploiting Mail Transfer Service and PCA

Indicators of Compromise: Hashes
5f0fea19115fea2596a6db636736ff96510b79fb
67dae474eb9eb8c2f7b8d315d84ca9b5de31d5da
732aa4679a372696b67c0666cd8c0279049d7a92
819c480f31650773a8e3de3ffb8f89a8ce062368
8a8f1dcdc301036fae02269da2d26f321886444b
8e5bacc6773843bac2f52c63bd0f6e4a868eb4da
ae5496ce5295a11957d7bb19c903c8128d0e73c1
df4099baa679fca159a301fb1b9aaa9d4ef4648c
f3cfbf02099830ce9492d231b4a00dbcb46facd4
7d01c27e827e02f32f12ada25da929fa911e965c
a1cb733708debb4c51967bf56ca0a0f750156cfa
1d1a59b1a3a9e5477ff6763ff97f90b52613932d
1004309c4567b45f3ecc7219765a1584aff6deec
7f765d69c089a0a983ce10c8d38fa21f1691bdaa
7ed830b915d118f5145b3e941e23fd0e12b5537c
c139b126a1714a32794d1213008d1526f46cdd44
301397c557c7d4aa995e6757a04dd81e2b2b59a5
c4f5be65b66cf5904eb1ec3d33ef92ae8dc7c2be
4e9d477a2abe3b7bfbf0e77ec98887276bd8849a
c90445f26f66aec87d9a2069427c622bde90766c
931fc81ce07db7b67041c49e430b3f88ac7cb521
73fa77816e27a3c42e8dea3d4ed5225dcb2402d6
cd90fa6b3f260b5763444d5bb4a64dbc2fb5c872
3b0223e0f4b52e2e7907a12bdf3672c0bd365d38
ea8ac97007879094ee5948e6c8fa3dab2e9cd894
a5e04d2e61478a632a93507a65e470fe3fdb40d1
e1f39bd3d4015d93dc2d274d574b9b8dc0d74e53
e31a9c0e86474255a2a13bb93c2c02d91ada5caee35bae9b2d142d8cad9e4c37
04f58fce886d80501fca5f9ea1f05a524a5604000ef828331eba9ca15a904232
34d81142467b937ef190175cb399579c96dbe2fcf40ad4418ced8c804fa8d985
5c09f38829d659f47239513f1825c41a419f04630ffb455862b6274a7adbfeae
e7b881cd106aefa6100d0e5f361e46e557e8f2372bd36cefe863607d19471a04
3bd054a5095806cd7e8392b749efa283735616ae8a0e707cdcc25654059bfe6b
4188c953d784049dbd5be209e655d6d73f37435d9def71fd1edb4ed74a2f9e17

KPMG

KPMG Cyber Threat Intelligence Platform

RedCurl – Exploiting Mail Transfer Service and PCA

Indicators of Compromise: Hashes
ca03ec0e4a3ba3678ca7560e95f00b838d2fcf5424560b23b4e9fc108b86fd86
92ffd2197a9af2721d42826ab17fdabc3c8f9d48b17f2405f890a40763a28c78
1feb42273e01c9d619de1204793bba704b83ad59ba4b3a12ff32e3513b9c8947
d45cad4fd575b0329b4c565231172012b0e690b9c325398833d738bf75308935
dadf00f36cc9ebe3895855aa18188bd5c9773f1b563d64daae03b57061e19dbb
01d34a341e2bd165c25c5010ac0ca320e7039162dd853496dd884f48f5bc9589
10cd18114397f1b87e9a5f87bbd378e6095febf7364e3b8858f7348152812dc8
b58bb1e1c96f4709ea737cafd84cf50c65f5ca1d177bb5d25b7e96d310f5c5d9
53e084c908285cb201fff38f6a5ff648ff8e8b00283948f6674ad248152fa12d
fa6e7cddb425923ee9b5930754ad960c1d35808871450f77ce49844a0f60d340
8803d1787a69af82bc34b9d8b8190c253daf86b9a5b6fac8d07c206af2a70798
2e8cc3dbb1aff91bdc462d57f84eaea3d00dd0b4ec1171c7a7a84ff30085a1bb
8d9aaa5cf9c7b442917a8f8542d020b221e9de595d78ef88b82ee696880491ef
f6e6491737d443af221855bbf35a430b271c7f0e234863a560d9304409a1bacc
2347e3b48c717399b001209442b4a23d39ecf5e22aa728951a0328983b17308f
61ca00df551f138d3f8602c19936c4a70b1da581183b8d1264fbd2bc416361cf
88edd697a50ef6bc1fb6cecd6867227c090cd6072cbfc5e01fcf7ccf2e11ee04
d921866d7adf0e0537c1506b878664008d7c7eeb778dab9459de1098ffc7d9d0
3dd6940a45ef6a5398f3d293c07ec9b6f2301bf5ff8835750039ea62853e2c7a
a34feabaeaacb4c96104a3939286f06f71724fdc7af52b5f2be9fccd9525c8df
d7a18103817b24b84ec4cea4c0758791ec1138791f73b123fc2855a8381f7b1c
37fc60bea66420a847408bf34a9702be7861aa262898d5f214ca1cd2c91f6c25
e060c4d7bb2dff383f08f26b8851cb291da5c145ed2fc0c0ec166768ef2122aa
2766fa91594ba04c3c27b9ec39865a8d13fe62d79da8516c1c36d1ba607eddd7
0f02a77ecc502db1b4041d4607881ed390c06633de9281affc86a5ace8faee76
c218f8bbb8197b3c18f168e9cc688e5c6feed944703a157f6b28420739de7860
37bdf68c4903bf20e0702d383c647400b71760d2a6745223e860be163b384c9a
21adf42e13397fc219b4b1564ecf0462e6a94379cd02bebcd033c8fb77f281a2
10977be90b3a4d373a562136c11d37e189381f1cbbea0d4c7ffb31953e881ec2
570d68678fa9e05cb22a85ac5fbccd7d56894045f6e0ea83660bb3781f47f8ff
935c4350dc6d184b627c672f12a9a9a061288acedb32ff50c2bb72cce0b686e7
51b17872e1401b8ae48015eec7da85a099660b53eaeac9c57b61aaabc9fdb31d
22989624772790307be9d6cedeed0a4ab322743b1729d28c3b0f0c0f0c02c08d
8878b4308f9b09f76ad1d1d53fce91aae59b081fee94c2baf19cb8ac3baeadd7