KPMG Cyber Threat Intelligence Platform

RedLine Stealer – A cheap and versatile malware

First observed in March 2021, RedLine is an extremely versatile information stealer malware distributed in various forms of Trojanised services, games, tools, etc. The C# written malware is being distributed as Malware-as-a-Service (MaaS) with a monthly subscription as low as $150. The malware is also being constantly evolved leading to multiple variants which are being spread via a variety of social engineering campaigns, posing threat to both enterprise and personal systems.

RedLine stealer is spread in a multitude of campaigns including disguising the malware as fake windows 11 installer, fake Binance Mystery Box NFT bots, by exploiting vulnerabilities such as RIG EK and extensive phishing. As a fake windows 11 installer, an encoded PowerShell command initiates the malicious process, and after some delay, a DLL is downloaded from C2 masqueraded as a jpg file. The DLL is executed by the initial process and then executes itself again with a different thread i.e actual RedLine malware. The new DLL acts as a stealer collecting all the system information and exfiltrating sensitive data to C2 through SOAP API messages. RedLine gathers a wide range of critical information like windows credentials, autofill data like card details, cookies & stored passwords from browsers, along with application specific data like FTP & VPN credentials, chatlogs & tokens of instant messaging platforms, popular cryptocurrency files and wallet information.

Primarily distributed via Telegram and in Russian-speaking forums, the threat actors leverage prominent and current announcements to lure the victims into downloading the payload. Since the attack vector depends largely on fake and cracked tools, organizations must be cautious to download only verified tools along with updating their software and security solutions at regular intervals.

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

RedLine Stealer – A cheap and versatile malware

Indicators of Compromise: IP Addresses	
37.0.8[.]88	193.43.146[.]17
77.91.74[.]67	45.146.166[.]38
146.19.75[.]8	193.38.54[.]101
45.84.0[.]152	66.206.18[.]186
46.8.19[.]196	188.227.106[.]3
51.89.155[.]45	193.203.203[.]82
94.158.247[.]24	94.158.244[.]213
85.239.34[.]235	45.140.146[.]169
74.119.193[.]57	135.181.105[.]89
146.19.247[.]28	185.215.113[.]15
77.91.102[.]115	185.197.74[.]223
45.159.251[.]21	136.144.41[.]201
146.19.247[.]52	194.180.174[.]180
45.150.67[.]175	194.180.174[.]187
193.43.146[.]22	194.180.174[.]186
193.43.146[.]26	176.111.174[.]254
146.70.124[.]71	185.215.113[.]121

Indicators of Compromise: Domains	
viper-air[.]xyz	main-soft[.]site
oyaliecem[.]xyz	fill-empty[.]xyz
idanwaval[.]xyz	cover-you[.]site
load-brain[.]xyz	fall-hire[.]site
just-trust[.]xyz	brain-lover[.]xyz
feel-quite[.]xyz	use-freedom[.]xyz
polar-gift[.]xyz	soft-viper[.]site
retro-rave[.]xyz	jasafodidei[.]xyz
cool-story[.]xyz	broke-bridge[.]xyz
fall2sleep[.]xyz	software-load[.]xyz
heal-brain[.]xyz	violance-heck[.]site
tech-lover[.]xyz	violance-rave[.]site
love-light[.]xyz	really-software[.]xyz
side-soft[.]site	interactive-soft[.]xyz
both-those[.]xyz	windows-upgraded[.]com

KPMG

KPMG Cyber Threat Intelligence Platform

RedLine Stealer – A cheap and versatile malware

Indicators of Compromise: Hashes
c827633ffacf2424112957e2ba523909
771a4fea6f33eac0771b108e8933703a
7f6de92ece5a366cc15af5574701fe98
06f65e5d32f58944fe0a50f12d8eb5c4
5acd1037872f39b9034707ae3618f3a3
154bda18ddf65e3d79caa9abeb7c4468
1c8112b8e1f13ca4129cae22f3387d47
57bf626239b8db6e1434dbc8ee7cef86
9b85cd189f7b8f6ba4213470523a0f59
c79bb6ecc930cb9a6aba43de47e02013
5545a2ff42f03e95661aba7eb080ce17
7e16c22ecc22113854b247f5886c98f5
45cf0a81dc1a3b75b0f3cf598566d315
8a6ce4ad539d027b4cbbdd147158af4d
cd39fa7364d13fe521aad91b8e99760f
0d9ac7274be792796eeebed217cc6e58
b8312c8e83bab1f003d03eacc10c8054
3f6ec963e276603ece3af20d5a3075cc
92d939fabae206a9e5df8ba2e8a10877
63fdd2a00dc456a3189a2c4fd3d499d1
d3ca123f9e81ad8f8e8ae4cc3803f590
7aeac72fd0ef3b77e8c6bf0212bc99dd
bd0592b2c25c38a7cf353095cc97bdc8
701f36ba3ecdc890710413ed7a26861d
dc815147f7fe11d08d7d64213f9032e7
bf285233dc836f62bc82a209c5dab48b
6dfa84ac778aa418adcb649651d17ccd
332790b27d3492dbcfb053213be95aa6
2d355ad6f26126ab10939bc68818df20
bc1d075b6bd88430bd6ba076a31a75db
4ef6f8d71a4855a4a6c87a1d09d91924
4a2c4c69b3ff3ced4b5f32621e4afb1e
ece994c1a16e969a20e859bbcc3300c2
0f8b9dddaf33692f797af885053458c0

KPMG

KPMG Cyber Threat Intelligence Platform

RedLine Stealer – A cheap and versatile malware

Indicators of Compromise: Hashes
7be34ab79073cac431a53f9f59ef4cac
8bc8f4d898ab59c8b938c8a72944c25d
9e2b723fc9fa77e5de1224e22d94ed2f
b72d86cd242c96d8e773706fb692818c
b90bbda56242264873a3ebd259a9acc1
d44d0362c0b11852c9dd3407d45f868b
eb6cfd95a4fa3490591c95f014e1f6f2
efd3e9de6b0dfb1b5c2f666f727f47d5
4d77e265722624b5d4d1841d45c7c677
500a62b980fe1089beb63e14d61b244a
8c24b7746d006c63db615dd43187651b
d3f749cc20369e215d59f9d8bfde1a41
f0d65470988478921ff40b6fb3def616
26fe666edc2c8715e6c349b9ee025bf1
75778b2b0c7f89306b662b4fe3218f1a
deb95cae4ba26dfba536402318154405
ff30196b3713229fa31a8db05ac1c411
4293d3f57543a41005be740db7c957d03af1a35c51515585773cedee03708e54
b50b392ccb07ed7a5da6d2f29a870f8e947ee36c43334c46c1a8bb21dac5992c
7d5ed583d7efe318fdb397efc51fd0ca7c05fc2e297977efc190a5820b3ee316
c7bcdc6aecd2f7922140af840ac9695b1d1a04124f1b3ab1450062169edd8e48
6b089a4f4fde031164f3467541e0183be91eee21478d1dfe4e95c4a0bb6a6578
76ca4a8afe19ab46e2f7f364fb76a166ce62efc7cf191f0f1be5ffff7f443f1b
258445b5c086f67d1157c2998968bad83a64ca3bab88bfd9d73654819bb46463
1741984cc5f9a62d34d180943658637523ac102db4a544bb6812be1e0507a348
ee4608483ebb8615dfe71924c5a6bc4b0f1a5d0eb8b453923b3f2ce5cd00784b
9dc934f7f22e493a1c1d97107edc85ccce4e1be155b2cc038be8d9a57b2e430f
0ddd7d646dfb1a2220c5b3827c8190f7ab8d7398bbc2c612a34846a0d38fb32b
5df956f08d6ad0559efcdb7b7a59b2f3b95dee9e2aa6b76602c46e2aba855eff
95f79fdcfb83a5035a2e3fa8621a653a0022925a9d1cb8729b8956db202fc3d8
9072f90e16a2357f2d7e34713fe7458e65aae6e77eeb2c67177cf87d145eb1a6
f224b56301de1b40dd9929e88dacc5f0519723570c822f8ed5971da3e2b88200
ffee20e0c17936875243ac105258abcf77e70001a0e8adc80aedbc5cfa9a7660
88ff40bd93793556764e79cbf7606d4448e935ad5ba53eb9ee6849550d4cba7f