KPMG

KPMG Cyber Threat Intelligence Platform

Exela Stealer – Rise of Open-source Info-Stealers

Exela Stealer is a Python-based open-source InfoStealer that was introduced in 2023 with paid customization options, excels in discreetly extracting sensitive data. Its dependence on Discord webhook URLs for data exfiltration adds an intriguing layer to its operations. Targeting Windows systems, the stealer adeptly harvests a range of data including credentials, cookies, credit card details, and more. Its attacks have been notably directed at organizations in Russia, Saudi Arabia, Vietnam, Brazil, Romania, the U.S., India, Morocco, and Greece, underscoring the global threat Exela Stealer poses.

While initial access is largely unclear, is it likely that Exela is being distributed at scale by social engineering techniques like phishing. Post initial access and gaining a foothold, the attacker configures features in the builder file, including a Discord remote server, Discord Injector, keylogger, and obfuscation layers. Sensitive information is gathered using various command line utilities. The stealer creates a mutex, "Exela | Stealer | on | Top“, to prevent multiple instances, terminating if the mutex exists; otherwise, it proceeds with data theft. For persistence, it replicates itself into a new directory under “\appdata\local” and adds a startup entry. On execution, it modifies Windows Discord client files for unauthorized acquisition and monitoring. Stolen data is organized & compressed into a ZIP file, sent discreetly to the attacker's Discord webhook and traces of execution are removed. Exela packs various defense evasion & anti-analysis techniques such as binary padding & process termination of debuggers & virtual machines.

Exela Stealer highlights how Discord webhooks can collect sensitive data from compromised systems, emphasizing risks with open-source repositories when exploited by threat actors.

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

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

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

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

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

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.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Exela Stealer – Rise of Open-source Info-Stealers

Indicators of Compromise: IP Addresses
209.197.3[.]8

Indicators of Compromise: Hashes
a774e1965dea429e097e4a3e1bef0943
5429328937ed51076df9f8c4e5edc93a
0758c56672f29aa493d955ced3682239
5c7805f87a6e396231a360a4f350378f
8b594b44addb55ebac34806dd0935181
11a3fdf887b8fbf0a3dc46f5619519ea
676c3f8f3daf104b4257b04f3f091c02
a747e9e56dd7a92451da36229be6dd6b
8af34955435bd8f44f54ce25b4a5d649
da3b095055145d5914ea33842c143eed
fd46c648f250a78c28d981bea8fc5474
08859f9e14d2e67913b8596e6b04123a
f93d6c1941d16431a6bc9181dab758fe
7e163f0a39e95e1cba705949e5974b06
8a98406e32ed6139bd9e75342d452948
2693497c7728b574fd73d5a21ccad6ec
e4e82d1ac3c209ff47e1ccc88bc1bffd
08b34a77c80cf1bc645d5b0fc9ed1f49
562cfdd2aea820c6721e6e1c6de927eb
328c18d3eb510ceeaff731154d4e76a7
d5cca10a28fd3be2093e6c3a260515cb085f5e10
3419c3731df1df2bef00e997e7ac398324b14a4a
05540875a7a44d5fd9688a9d33b6c36b3d4cd611
f0851f29d60447690cd19ac3200d521669ad941b
7b3dc2dbb081f502099a8117f03758fdc8e23c2f
9a7b46aad319c2a3ed04d576164e4e0a6afe3cf0
9702246eb55580219c1f01f30ff4deb94a4f5d58
0d971fcf6250f5972852dad42a0e1e9062f0f9ce
df790ced744a967c87e40171f974d385351afb8e
4db17bdf5c27ce33599fc3b128c569870b6d917c

KPMG

KPMG Cyber Threat Intelligence Platform

Exela Stealer – Rise of Open-source Info-Stealers

Indicators of Compromise: Hashes
9895a3def0ccefd717ee85befb7c3b314191b0bf
52fbf26ca315f5fdfc576a20e8aa829dd546a85a
a7cb93d1d399dc41f5f2021035cc0bc06a98960d
89ee0ae7bde03eab1cdbdf9329f10cbfb50df385
ed77737b88a7351d0bc5f542ddb7ce84f8f95588
0115d56f65869c76f3033b623cdaefd6ee159dfc
68ccd9885408230ddd1805dc05b36f5c1e434d64
7513fc7319da86caa0b54c174a5c70eadf9244e6
bdbf3f8b92a2eb12b8134be08a2fcd795a32ef25
3d202363660ec1c03db5911a77cb16f992e31aa1
a525cdc3b96ff5e440902d7fd770fa096303f958
bc05938d4ffcc5703d65d64eda903797f9136bb0
f96bc306a0e3bc63092a04475dd4a1bac75224df242fa9fca36388a1978ce048
95d860570b2777d7af213f9b48747d528251facada54842d7a07a5798fcbfe51
5aff2c5e65d8e4e7fa0b0c310fbaef1e1da351de34fa5f1b83bfe17eeabac7ef
34dca3c80cd5125091e6e4de02e86dcc6a2a6f9900e058111e457c9bce6117c0
c56b23602949597352d99aff03411d620b7a5996da2cab91368de275dcfbaa44
b9bc445af6729a95599f1a39e37f559f3ca18dbbc8ae4e60263af565ef4f4db3
882484b56ad4418786852f401b1b81f31030bec8566b6b07c9798d4ea3033516
ccb1337383351bb6889eb8478c18c0142cb99cbb523acc85d0d626d323f5d7ad
d8488f93b8c096838b3d9b335091216667ce4ffc7ae2cf3c8925271f0f190c11
b6ca47065e68aebb007657ff0e6b0dfa0fc4e19823f336ab73f42b25dd5cfc22
206278545b897a7e2ebb1ec4687e6ec31d7ca8f1828792a34f4fca745db8e3d4
53b1b3c6f73312cdae7be69d16a42d298fae0cb3721c7fc11252f65b10f5a323
2db54628a877ab40463a128496cb94523ccae6186d1648c6f372c719f6ed8152
34b84fa312cedc7d3529b12ed3a4e739e4ff0d3ade7c62cc3d0368cc5bee7d27
a4240ea0e8a916d15f8391edef9705ab4de1f516dd360f0a336c5358686d434b
d37da75cbc53e03f2e1509932999948d4b6204935d4c86360176c3837b1e808e
1dd65d314aacdfb9198ed4165cd9a5bd846514a6fda0723f844b86c8d5a454fb
54489dfd48ea989cda44b58542ecac4f83b338c1705b65600ec7e19459bd1945
250b2e7962e2533bdc112346bbc5c5f66a574af0b87e18f261f48ef8cee3f1a5
2c59be6d217f8d500771f006a3f9c4ee02d23d88541e3f6920bed2061a5d8efe
0cc6ad840b2002b018d4e4338bb48703bfb62ee38e795abea27788e293cc8c20
11d05841e73020067234a2845ee7fb6fda4d8603665f7be319c11581fb828333