KPMG

KPMG Cyber Threat Intelligence Platform

Zloader - Targeting Windows Users with Revamped Tactics

Zloader, (aka DELoader, SILENTNIGHT, Terdot) a modular trojan derived from the Zeus source code, surfaced in 2016 targeting German banks. After a hiatus, it resurfaced as "Silent Night" in 2019, reaching version 2.0.0.0 by September 2021. Despite a takedown in April 2022, it returned in September 2023 with versions 2.1.6.0 and 2.1.7.0, boasting updated obfuscation, a revised domain generation algorithm (DGA), RSA encryption, and native 64-bit Windows support. Zloader's attacks have globally affected various countries, notably the US, China, Canada, Australia, Poland, Germany, Western Europe, and Japan.

Initial access involves deceptive tactics, like RIG kit usage, COVID-19 spam, fake invoices, and Google Ads misuse, to trick users into downloading malicious software. Execution proceeds with malicious documents, fake updates, or compromised website downloads deploying the payload. Persistence is established through methods like creating registry entries or auto-start services. The malware initially used evasion tactics like disabling Microsoft Defender, exploiting signature vulnerabilities, and encrypting communications with RC4 and XOR algorithms, but now employs junk code and string obfuscation. ZLoader artifacts require specific filenames for execution, potentially evading sandboxes. Additional modules are downloaded for remote PC control and malicious tasks, employing HTTP/HTTPS communication with updated DGAs for C2 server fallback. Each affiliate uses a unique RC4/RSA encryption key for secure communication. Stolen data is exfiltrated to C2 servers, with tailored payloads potentially including ransomware.

Zloader's resurgence has brought significant enhancements to its loader modules, underscoring the importance for defenders to be vigilant and proactive in their defense measures.

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

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

Zloader - Targeting Windows Users with Revamped Tactics

Indicators of Compromise: Domains	
businessdeep[.]com	adslstickerhi[.]world

Indicators of Compromise: Hashes
71c72ad0da3af2fca53a729ef977f344
2f6fcc4884dfa21ee48e463a7a1963f5
46e6fa1793561b4dda0a1848550aab93
950f284c525f5372997af67e082b0bc2
12647f9694eb9d91a7c95238e8a454d7
261e0bb975aad28f0fc84883225e10ad
f82d3b9409c2f60ab0d7b028fa4ee3e4
850210f63988627c1b314b7ee328fd78
127481a65f45fa0859b5be2c00a39885
75868548a0c45e58e00ec34d304dc837
961a84c3f929074136f54a59810168e6
7e7a6064c5c147c500c703390fe914c4
0d6f060e1bb69c647ccdc42c5b32aa89
6e5e356dbf9165782bc336703a9d9487
e54f72b1de3e97efe28c97470d3b00f3
623320e71aeb5208d72fa2e0bd074f21
7ace68f544299d8195eabc3e3f71e548eca51e47
2090c12960dee091681a7a3d334d54f2dd6d0bf2
7288fba570fbba7576ed21db79241dcbc969392c
9bde5a665f3b4d86aa9267b8f587ace95615fbf6
5279e169e67ac7262772a17c897929ace12de647
06134738f055a4b351ddb369cb3cb4d8223469fe
6a6021185686ab0d7eb75d1fc27b6bee2c9b1931
d55243105f5fb2f9d607de91bbcc009f3c2a1a9f
4077efdf98f5b42256158a882ae33a5c52ce7e58
a86b76d0e8359be5508419e7b71c7f78f0abfa07
94c89c0cf2148ee7524ae430da1172863212f117
97e0d4d5480b7a1dbc19229ceecb39213ccc70f5
36fce1194c59cf7d3f278dab97164f6df526d33b
d697dc650c2c9c42ea2142d7507e4dd95ae07fd8

Indicators of Compromise: Hashes
1eeed3b2fd10ff8f2b61237d23648e086fca677d
edb0a1f429c923abb7eb9c7e254c74fcd31f2585
2aa41013eb9ee260563341eb79a860737e495546
f9db1e42a3a3e35076a371de508136ed167f6ee1
355629dd7b1a25fc12264b530be5c456d30a9ef7
d755bc88892cfb653e6c8fb1b05637af916aa22a
a4c2395af6716e5ff7e8db3b59bbcdef336f015d
9e7d1e8042810ee3b691ee307caed7dd5fd0577d
f68ff24be79b0f5b9f24c15bc65d6ce2149dd5fa
e8b44bdc89d0d01711674e8d29fa2b1c0854d013
16af920dd49010cf297b03a732749bb99cc34996f090cb1e4f16285f5b69ee7d
25c8f98b79cf0bfc00221a33d714fac51490d840d13ab9ba4f6751a58d55c78d
2cdb78330f90b9fb20b8fb1ef9179e2d9edfbbd144d522f541083b08f84cc456
83deff18d50843ee70ca9bfa8d473521fd6af885a6c925b56f63391aad3ee0f3
98dccaaa3d1efd240d201446373c6de09c06781c5c71d0f01f86b7192ec42eb2
adbd0c7096a7373be82dd03df1aae61cb39e0a155c00bbb9c67abc01d48718aa
b206695fb128857012fe280555a32bd389502a1b47c8974f4b405ab19921ac93
b47e4b62b956730815518c691fcd16c48d352fca14c711a8403308de9b7c1378
d92286543a9e04b70525b72885e2983381c6f3c68c5fc64ec1e9695567fb090d
eb4b412b4fc58ce2f134cac7ec30bd5694a3093939d129935fe5c65f27ce9499
f03b9dce7b701d874ba95293c9274782fceb85d55b276fd28a67b9e419114fdb
f6d8306522f26544cd8f73c649e03cce0268466be27fe6cc45c67cc1a4bdc1b8
fa4b2019d7bf5560b88ae9ab3b3deb96162037c2ed8b9e17ea008b0c97611616
fbd60fffb5d161e051daa3e7d65c0ad5f589687e92e43329c5c4c950f58fbb75
b916ee9ac5a31baa984fa1f21caa27f09e4441862a49de9173c5ee69866794c1
34683184956ac22bf8dbc9d3b8cc77961029956ad83b94b10c7d25fc1382dcd8
be79799e584cfeac364c9bdbdcae57e05fb4c94bf59886e3325efd1bdd9302cc
346566a4153a1a31a509ebec84a81e0b1659353771ef48801ae6b86afd895da3
934ebca653ff2a2f5b8d56536e90f90f353bb18c761cc5ca82fb72efe7cd4d93
b91bd79e54b479982cc3dbe9eb1ca22b2c91595e80ffc758c06ba54eb0ee4650
2d925c92357e7b3b64f9bc2e7a3bcf7789954ff0985b85a69ba5994c137c8476
3a27df27123dfe41e25bfbbabd52dc78fd6a7dd9c569dd4464a60eca621623e1
3daf01eebe957c2b6f087b806d24f03f4ed657d503d61eb17f1b14181fb5a8e2
b91b0dd75b082180cbe8635b05a98410233831b5faae5168aee8f9299b5484fd