KPMG Cyber Threat Intelligence Platform

Smokeloader Malware - Targeting Ukrainian Institutions

Smokeloader, also known as Dofoil or Sharik, is a Windows backdoor malware associated with Russian cybercrime. Advertised since 2011, it surged in Ukraine in 2023, targeting financial and government organizations. Geographically, its primary focus lies in Ukraine, where it has been extensively utilized in phishing campaigns targeting a range of sectors. These include financial institutions, government organizations, and private enterprises.

Initial access is gained through phishing emails in Ukrainian, posing as authentic business documents such as invoices. The attackers obfuscate the malicious payload using multiple layers of compression, including ZIP file compressed in 7z. Within the second compressed archive (ZIP), a smokeloader malware file is disguised as a PDF extension. If the PDF fails to execute, smokeloader employs a Self-Extracting Archive (SFX) file within the ZIP for execution. Upon execution, a Batch (BAT) file triggers the smokeloader malware, enabling its malicious activities. Once executed, the malware establishes connections to Command and Control (C&C) servers facilitating communication with the attackers for further instructions or additional payloads downloads. Through C&C communication, additional malware payloads like Lockbit ransomware may be downloaded, further compromising the victim's system and data. Smokeloader injects itself into the explorer.exe process upon execution to maintain persistence on the compromised system. It may also carry out various malicious activities, such as data theft, system reconnaissance, or further propagation within the network.

Smokeloader's use of legitimate processes for malicious activities and its obfuscation tactics highlights its sophistication, emphasizing the need for robust security 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

KPMG

KPMG Cyber Threat Intelligence Platform

Smokeloader Malware - Targeting Ukrainian Institutions

Indicators of Compromise: IP Addresses
85.143.172[.]45

Indicators of Compromise: Domains	
iloveua[.]ir	super777bomba[.]ru
diplombar[.]by	propertyminsk[.]by
zasadacafe[.]by	popuasyfromua[.]ru
restmantra[.]by	specnaznachenie[.]ru
sakentoshi[.]ru	moyabelorussiya[.]by
dublebomber[.]ru	prostosmeritesya[.]ru
zakrylki809[.]ru	tvoyaradostetoya[.]ru
kozachok777[.]ru	ipoluchayteudovolstvie[.]ru
propertyiran[.]ir	nomnetozhedenyuzhkanuzhna[.]ru
yavasponimayu[.]ru	ukr-net-download-files-php-name[.]ru

Indicators of Compromise: Hashes
852ce0cea28e2b7c4deb4e443d38595a
7ccf5bb03e59b8c92ad756862ecb96fd
b6d8f49b3d0f81514e8a40c9a03d8636
54962fc3a843c6b0fc4c2513820d2ad8
65c7d9e822c9f2b8291202128644e825
66d62c348cb3b50d2edd5a9ae6778b51
f9fb94165f54cd0b5b0c00e1880d5363
0728c2a5375b615042020acdf26f4567
b6c134f4f94612f903f6e555af707553
ccbdbaa1f2ba8322554fcfa772d20862
99c11a67c6ab54c5a14dbb0f44edea44
d2534115c697e47fa88ddca72678281b
553cc8aee992da42454595e76d7afb37
89a48a234e13b3dd124dcca372ae6b94
331ddbbd644c1088f56497ea066cf804
a3ca1983e0741d9d5816af3f89570472
f8271574bb8cab3784aef605db83b940

KPMG

KPMG Cyber Threat Intelligence Platform

Smokeloader Malware - Targeting Ukrainian Institutions

Indicators of Compromise: Hashes
fe7c42b5711cdc65af404ef5c299f9ce
45c63b6de683c5bb62cd93ace3c9433a
572cfbf8dad8bdb13d350e0b2da329167b584d68
5fe67d474e01e2e62c8b52c0cdfbccc482fce6ac
0a04e457ebdc5bac15db041d2d461e66bc71c2dc
18f874a4033dd379cf931ec711aa442dbb9df81b
6cb6265721b373df555f0cdbba93dcb7e622344f
f705ca1e807a837a2bb128c7e10f431721aa6efe
00d12aa1686ed2e35d9fe254f64fc899703750f9
d1757a4d08ebcde58e17895b335458d596a334fa
a880a64d2c57b2a3670604868fb31ae2c64913a9
384f1a00a5863559fcde9b69ed945d548b7c31cc
e2f8a1cc9e5d61a70d8dc5b02d64a3460e6ac093
34b6a39629449960796de67a3e84d607788a79ae
47a5850ad4c2b7e6708fa28300f8fdaf54839ebf
8c36816c000181ab8ef94a048695daf003daf2b7
7d507a1bbeca68288a38a0b9f7a89d15bae04974
a41bcad008092841f6672f059a7fdf713ec5e42e
2befdb4f4d864c913a9b42cc74bdbb0b5e6ccd88
db0f4a1f266634bdc466a20374fc433be0b73cd7
1697ce8fc31dfa03b0a9799c77e6fb86510dd062
6525994e3c24b3b6f698f4a62a26e9f3ae96de7c647392f15eff13b0dc26a0c4
c221c376c591db1adf19c53d10e05f602f080e890a64e29831a745b6cbdc28a3
ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4
b24c99ca816f7ac8ca87a352ed4f44be9d8a21519dd1f408739da958b580be0c
9a528b2b31d9d59018878fdf3b9d8db235df606500c67a4b8be3075701b014fc
40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533
41b74077e7707dfce2752668a3201e3bc596ade5594535c266e3249c2e697cb2
d895f40a994cb90416881b88fadd2de5af165eec1cd41b0ddd08fa1d6b3262bb
493f708129bf25ff4bb734c179d336f223d9d21ea53b7e5e52f9535a72415bfd
6999f5f3c6824f27b5a1fb436c59d369f6f1ec08365d48cd1c8d21d1058eaafc
739e735aa73cfdbfc08c696e0426434aa78139110b416313d2a39d93915ee318
7d7262ab5298abd0e91b6831e37ef0156ded4fdceeaf8f8841c9a80d31f33f8e
a8a3130c779904e23b50d69b4e73a714b345e296feebb9f64a732d5c73e7973b

KPMG

KPMG Cyber Threat Intelligence Platform

Smokeloader Malware - Targeting Ukrainian Institutions

Indicators of Compromise: Hashes
cfc44f1399e3d28e55c32bcc73539358e5ac88c0d6a19188a52b161b506bea91
ebbf474d69519b7ded60c1dab807dab492c33d9caf76e6495c2ee92be573011e
fdf8a89e8c90ed0653780acc77c180185b8971e62d2a02dcaabcfc456d05bd96
0a83fcb0b40f35bf6020ad35cedf56b72a6f650a46dc781b2ea1c9647e0f76cc
0f93344347469ebef7b0d6768f6f50928b8e6df7bc84a4293b7c4a7bb5b98072
2c44c9b445d2efc2f46e463d933da2ffc1d3ba6718bd67d3957c3f916b7c79fe