KPMG Cyber Threat Intelligence Platform

Phobos Ransomware – A Threat to Critical Infrastructure

Phobos ransomware, active since May 2018, operates as Ransomware-as-a-Service, targeting government, healthcare, education, and critical infrastructure sectors. It primarily preys on small to medium-sized businesses with lower ransom demands, using compromised RDP connections and DLL sideloading for stealth. Associated variants include Elking, Eight, Devos, Backmydata, and Faust ransomware. Its targets span across multiple countries, including Japan, Romania, Germany, Indonesia, Brazil, Portugal, Seychelles, USA, and India.

Initial access involves phishing campaigns, exploiting vulnerable RDP ports, and leveraging spoofed email attachments with hidden payloads like SmokeLoader. Phobos actors elevated privileges using executables like 1saas.exe or cmd.exe, controlling compromised systems via the Windows command shell. Persistence is achieved through Windows Startup folders and Run Registry Keys, utilizing built-in Windows API functions for stealing tokens, bypassing access controls, and creating new processes. System firewall configurations are modified to bypass network defenses, and tools like Universal Virus Sniffer, Process Hacker, and PowerTool are used to evade detection. Open-source tools like Bloodhound, Sharphound, Mimikatz, NirSoft, and Remote Desktop Passview aid in credential enumeration and extraction. Remote access tools facilitate network infiltration, while Windows API functions enable lateral movement within compromised networks. Smokeloader decrypts and deploys payloads, while legitimate websites obscure C2 activity. Exfiltration involves WinSCP and Mega.io for transferring archived files containing sensitive documents, and databases.

The utilization of various tools by Phobos ransomware highlights its sophisticated evasion tactics, presenting challenges for security measures to detect and counteract its activities.

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

Phobos Ransomware – A Threat to Critical Infrastructure

Indicators of Compromise: IP Addresses	
45.9.74[.]14	185.112.82[.]235
194.165.16[.]4	185.112.82[.]236
185.202.0[.]111	185.112.82[.]237
147.78.47[.]224	

Indicators of Compromise: Hashes
3b6c915658b74fe1efa43545d59a8a91
e71c0cffb0d9122dca8fc854a55db27c
fe2d1879880466e24e76d8d0963feb93
ecdf7acb35e4268bcafb03b8af12f659
e59ffeaf7acb0c326e452fa30bb71a36
db74cd067d4a0562b26ea4f10e943e3b
b119cdd3d02b60009b9ad39da799ed3b
a567048dd823ff2d395ddd95d1fa5302
9376f223d363e28054676bb6ef2c3e79
69788b170956a5c58ebd77f7680fde7c
62885d0f106569fac3985f72f0ca10cb
2809e15a3a54484e042fe65fffd17409
20d9fa474fa2628a6abe5485d35ee7e0
0900b61febed8da43708f6735ed6c11b
6eff55b9f24c8b276848167c5d64cc9c
4f64165f9dccffe9fb6063f7bdc98276
e4a6b0afc0895a844644ebcc00db7d73
e0fb405aab45ac201e9b7e70fafab068635048db
21f4342e962ab63914a8786343bd2ed36ce86169
cb37b10b209ab38477d2e17f21cae12a1cb2adf0
c88fad293256bfead6962124394de4f8b97765aa
b092a6bf7fb6755e095ed9f35147d1c6710cf2c4
aed68cfa282ec2b0f8a681153beaebe3a17d04ee
a28af73bcfd4ebe2fe29242c07fec15e0578ec8a
93b0d892bd3fbb7d3d9efb69fffdc060159d4536
90b2cebbeb377480e321d8f38ea6de2fa661e437
7332956debc4fb14a54d69b0b858bd5b04becac1

KPMG

KPMG Cyber Threat Intelligence Platform

Phobos Ransomware – A Threat to Critical Infrastructure

Indicators of Compromise: Hashes
66cfc67c4a95129a0e979c1ce025747372d69552
9595bff740d66f8037f7f0346677a70dfef941c4
0c69051c612214ad8f9b57ce99ce60f1d15db453
3482fbb6ab9c43cf7a660528d62c1283e4a058ca
7f59ae781bd4355ea07450d8aca5f68ae18642b70abbf04f0cd8d72743e059c9
fe2b5fb57399cf0c7607d5aa133910a9500d176e0dd6a45a4ff8485ad4e70412
fc4b14250db7f66107820ecc56026e6be3e8e0eb2d428719156cf1c53ae139c6
f3be35f8b8301e39dd3dffc9325553516a085c12dc15494a5e2fce73c77069ed
f1425cff3d28afe5245459afa6d7985081bc6a62f86dce64c63daeb2136d7d2c
c0539fd02ca0184925a932a9e926c681dc9c81b5de4624250f2dd885ca5c4763
a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2
9215550ce3b164972413a329ab697012e909d543e8ac05d9901095016dd3fc6c
7451be9b65b956ee667081e1141531514b1ec348e7081b5a9cd1308a98eec8f0
58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6
518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c
482754d66d01aa3579f007c2b3c3d0591865eb60ba60b9c28c66fe6f4ac53c52
32a674b59c3f9a45efde48368b4de7e0e76c19e06b2f18afb6638d1a080b2eb3
2704e269fb5cf9a02070a0ea07d82dc9d87f2cb95e60cb71d6c6d38b01869f66
0000599cbc6e5b0633c5a6261c79e4d3d81005c77845c6b0679d854884a8e02f
31dba1a23db70ffb952f0e597acf95d16ab60423018a83d0ccb4f57ce0471793
527918fbd218787f202dcfb20024375238aca2dc64c1661bdc71f8833240e7f8
f0d6846da6d45180a695201888edc4f9c512fb0d11ed56394aae9daa874ba88c
255a65d30841ab4082bd9d0eea79d49c5ee88f56136157d8d6156aef11c12309
256984cb62bc879971463ff0ff7567042dc95d8b0fb2bc676f246c2293c77ae8
2f4b78ba820c9692c204995f003f3133661c804b659a367371d2f989492731d5
3924ccabc7bfaeeaded05ffb15855c2cb8ea78ec4f63e1dc66e1d93f9e5b9538
407162437304f05167a4dbd0b7761282165839cadba352ca66fa002781503788
4b298058e1d5fd3f2fa20ead21773912a5dc38da3c0da0bbc7de1adfb6011f1c
6c919c0682ef2d158e40631f06893cefb5a3d09333b3bb3cdd657e779a3be37d
c445a6c61ead94484529fcc923f54ed909228edad3e895b0e8d4e0f777ed5437
fe2b5fb57399cf0c7607d5aa133910a9500d176e0dd6a45a4ff8485ad4e70412
0236468b2fe3354556315d43c7f6b7b23b8a6b664720944bb2f451266e542680
03a9306f8a2011ef00ce28e6d283008ed80589c91bad0d71fbc2e20d63cdb2e2
04fd70875224e622d892910719f30749542867cefd5b53da0727826b2297f820