KPMG Cyber Threat Intelligence Platform

Shuckworm - Another Russian APT Targeting Ukraine

Shuckworm aka (Aqua Blizzard (formerly Actinium), Armageddon, Gamaredon, Iron Tilden, Primitive Bear, Trident Ursa, UNC530, and Winterflounder) is a cyber espionage group that is active since at least 2013, linked to Russia's Federal Security Service (FSB). The group is said to have attacked over 5000 Ukrainian entities to steal information from compromised environments whose recent targets include security services, military, and government organizations. Multiple cyberattacks, employing USB-based malware, have been executed by them to steal huge volumes of data from Ukrainian.

Initial access is achieved by spear-phishing emails to deliver malicious attachments (HTA, DOCX, LNK, SFX, RAR) and exploiting MS Office remote template injection vulnerability. On execution, an obfuscated PowerShell script communicates with C2 & spreads a custom VBS backdoor called Pterodo, which is executed using 'wscript.exe'. Further Pterodo gains persistence using scheduled tasks (shtasks.exe) and downloads more malicious code from C2. The PowerShell script also creates deceptive 'rtk.lnk' shortcuts (such as 'porn_video.rtf.lnk', 'do_not_delete.rtf.lnk', 'evidence.rtf.lnk') to lure users onto execting them. It also scans for USB drives & replicates itself onto them for lateral movement to potentially infect air-gapped machines. It employs Telegram as an intermediate C2 & periodically changes its accounts & IP addresses. Giddome, a recognized Shukworm info stealer is utilized to infiltrate victim networks and extract valuable data.

Shuckworm is one of the many Russia aligned adversaries targeting Ukraine in light of the recent invasion Russia is carrying out. Such adversaries not just target Ukraine but also tend to impact countries & agencies aiding Ukraine. Hence it is important that these groups are considered as serious potential threats by the community at large.

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

Shuckworm - Another Russian APT Targeting Ukraine

Indicators of Compromise: IP Addresses	
159.223.112[.]245	45.32.101[.]6
140.82.56[.]186	140.82.18[.]48
45.76.141[.]166	216.128.140[.]45
159.203.164[.]194	146.190.127[.]238
45.32.94[.]58	207.148.74[.]68
45.95.232[.]33	195.133.88[.]19
139.59.109[.]100	146.190.60[.]230
164.92.245[.]246	84.32.190[.]137

Indicators of Compromise: Domains	
shortcut[.]save	drive[.]name
foto[.]safe	deprive[.]wow

Indicators of Compromise: Hashes
b0d72c957982061fcf88798428136039
de9a87a8dc9eb67b3e54c452f63b2579
05f1a2a30b58eee64681a530d7eabfb7
ec9ce922903371efaa9aaab3ad033faa
6ec4ea2d6353eaafe94dcdea5c834c24
08f279d7bc9d2f35628502204f8c4b32
5001878474bb580531b83dfb56ec1e44
b0909447a3b95650d50f2da3e43038d8
b8d2580936d1ca8805550ba6aa2479a0
bc1f5fbdead23ae9c70fd14ce1edc698
ad14459738979213b396140f84dfa79a
371c4edcbd643e40221d640cf6f86a7a
44d6644ac271c3fbf7a5522f17ecaa49
668ec9956c046dbddbd0014e768c50c5
0007bbfd8f5cb8aaad177a475e91cc5c
bfe2351f2b487c0f357af561792119d5
54c20281d74df35f625925d9c941e25b
21a2e24fc146a7baf47e90651cf397ad
da84f8b5c335deaef354958c62b8dafd

KPMG

KPMG Cyber Threat Intelligence Platform

Shuckworm - Another Russian APT Targeting Ukraine

Indicators of Compromise: Hashes
2e374dab4fb853f7acb6c4868c1d1b60f8607b85
d1a8bc5ac80c50645ba9d4e7e6ca86c6b4a816ac
4d681540cac6b464567fca600381ac3b8c43a638
42de89f8bb3eecd7c4909c2497d1bd20ad876ff1
aa88ff761a95bcf73114f0daf885587d06b1ebf6
c55cd49d66e643a859263df1b410ba32c1da76c9
d0c80bfbcc1acb1ea94dcdedbb4ad7c6fcccaae8
98236d0a6e385451d019c7cd2b43653c1339b583
d5f7da39e9a63129e0703b70e3451de81928fe53
4c7d033fcba7f9363738c237124a11382eb69282
083645afb84069dc31e0df72405c57df510fe36c
9119f32780847d3d8a800fe9b2fa2d5d40c02bfb
fa1f5cf3186661856f2267026f99062eb72a25ed
65565b83dbcba54d231ad53c04c1135f372f3387
fe7b1b80dad4aa5e2bd86a6218d4397b274f9277
affc1f00c2dcc37cc0e3da1c69faaa5355e71514
a57503d23408ac2b8f560d8914a7c7e8b0cd0595
540cae6797aa3925a56cc46c2199173504711682
87b1a24e14b04b3b9f7be47a08a6d592189d50e1
31e60a361509b60e7157756d6899058213140c3b116a7e91207248e5f41a096b
f7a6ae1b3a866b7e031f60d5d22d218f99edfe754ef262f449ed3271d6306192
c62dd5b6036619ced5de3a340c1bb2c9d9564bc5c48e25496466a36ecd00db30
c6f6838afcb177ea9dda624100ce95549cee93d9a7c8a6d131ae2359cabd82c8
3393fbdb0057399a7e04e61236c987176c1498c12cd869dc0676ada859617137
3458cec74391baf583fbc5db3b62f1ce106e6cffeebd0978ec3d51cebf3d6601
acc2b78ce1c0fc806663e3258135cdb4fed60682454ab0646897e3f240690bb8
28358a4a6acdcdfc6d41ea642220ef98c63b9c3ef2268449bb02d2e2e71e7c01
2aee8bb2a953124803bc42e5c42935c92f87030b65448624f51183bf00dd1581
dbd03444964e9fcbd582eb4881a3ff65d9513ccc08bd32ff9a61c89ad9cc9d87
a615c41bcf81dd14b8240a7cafb3c7815b48bb63842f7356731ade5c81054df5
91d42a959c5e4523714cc589b426fa83aaeb9228364218046f36ff10c4834b86
3b46daabaca50c0e36742b35e7be6279daf4d88497cf32586eb945ea9e60a3fd
2d831996a9a719e14d6b700c1324b0a7571aa36638174f10190c2474d16905ea
c0042307439926f9b5c574d03f522356575906fe5e31c6b7c34e906482c5c459

KPMG

KPMG Cyber Threat Intelligence Platform

Shuckworm - Another Russian APT Targeting Ukraine

Indicators of Compromise: Hashes
b5a04e7f45c993f50320bd5beff5f709eb88e5782b0560497653edcff25967d6
9ecf13027af42cec0ed3159b1bc48e265683feaefa331f321507d12651906a91
2d99e762a41abec05e97dd1260775bad361dfa4e8b4120b912ce9c236331dd3f
295654e3284158bdb94b40d7fb98ede8f3eab72171e027360a654f9523ece566