KPMG Cyber Threat Intelligence Platform

Follina : Another Troublemaker in Cyber Market!

Follina, a newfound zero-day remote code execution vulnerability in the ubiquitous Microsoft suite was identified recently by a Japan based independent security vendor "Nao Sec". Suspectedly, a live sample of the bug has been found in a word document template with the links to an internet protocol (IP) address in the Republic of Belarus. Reportedly, Office versions ranging from 2003 to the current build have the bug. The vulnerability was named based on the area code reference of Follina in Italy found in the malicious code, however Microsoft has of late assigned CVE-2022-30190 to this recent bug.

The said zero-day vulnerability is believed to be abusing the remote template feature in Microsoft word to retrieve a HTML file from remote web server and is suspected to be independent of typical macro-based exploit path usually found within office-based attacks. The attack gets triggered the moment specially crafted malicious word document is opened in the target system which enables the attackers to execute the PowerShell commands via Microsoft Diagnostic Tool (MSDT) URI scheme typically used to load code and execute PowerShell. Once the attacker successfully exploits the vulnerability any arbitrary code can be executed with privileges of the calling application furthermore, programs can be installed in target system, data can be manipulated, and new user accounts can be created.

The vulnerability has been recently leveraged by the Chinese threat actors in attacking the international Tibetan agency. The patch has not been released by Microsoft yet, however as per the advisories published by Microsoft, organizations are recommended to follow Microsoft attack surface reduction measures to mitigate the risk.

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

Follina : Another Troublemaker in Cyber Market!

Indicators of Compromise: IP Addresses	
141.105.65[.]149	141.98.215[.]99
212.138.130[.]8	45.76.53[.]253

Indicators of Compromise: Domains	
sputnikradio[.]net	exchange.oufca[.]com.au
xmlformats[.]com	tibet-gov.web[.]app
tripinindian[.]com	seller-notification[.]live
coolrat[.]xyz	osendata[.]com

Indicators of Compromise: Hashes
f531a7c270d43656e34d578c8e71bc39
6bcee92ab337c9130f27143cc7be5a55
529c8f3d6d02ba996357aba535f688fc
52945af1def85b171870b31fa4782e5
d1fe26b84043ac11fa5ddb90906e6d56
52945af1def85b171870b31fa4782e52
d313002804198b5af1e0b537799be348
8ee8fe6f0226e346e224cd72c728157c
ec4c485bb3adceb439c4a0d3304620b7
91f7a5d805812e0c94952c267655111a
82c61ac03395472a0b631670aff3e6a2
000c10fef5a643bd96da7cf3155e6a38
4e67b66a5087bb7a19d9f1f3d1d90607
594f0dd70377792e8535272adb72d264
5ba705b740e2b8fb47de958375df840d
b0ae49bab6ea9fdc3bf70de0ca08260f
ea730d42c659852ffa0e9ffe9f23f6c5
eac5221693d8294a6f1e4db6f40bcd12
ea483ab89d8b9baf00b953f0636e0520
dbd2b7048b3321c87a768ed7581581db
242d2fa02535599dae793e731b6db5a2
ca322dd565f02d6d8c374e220cf8078e
63d502f3f0771468e72346b6f1112851

KPMG

KPMG Cyber Threat Intelligence Platform

Follina : Another Troublemaker in Cyber Market!

Indicators of Compromise: Hashes
604ade56a10fff08e11018f7f82fc7b6
06727ffda60359236a8029e0b3e8a0fd11c23313
934561173aba69ff4f7b118181f6c8f467b0695d
f5978deec22543a301e7ff4e01db950d8f474a4c
b11edf05b9f5bef2c98a46af5c8646fbf74e4a9f
447139a8cfc9660215bef2230e25885f553ddba8
b22db9ccd50064cbaf5876a4a318ec8eea284585
818803f1bd2d2ac66b2e36ccd9971ba85b8901f0
959a41f799fda0e645e52eef450c5ef45ad67d65
9253df019b02e409ac86f9241781b4d1890d3489
8e6524fa86bc4a34b01166445c1fe90ce1f5c041
719bd19c3561031cb056c896869d0804f6988ad8
016be26e27bf6479d21c0f72358eddb489f44ff5
2e5512264d9aa53ea64574846f63cc46679b3681
4c04281b1ca71df086e00e87c5cb8288901980c6
5eb593e9da2221343a527846abfc6cb9a7bedf07
92661e88ed93b873857741dfae58e08da6c3e312
a3a6c30659cf3537c22c3955654139bd7ce12920
b0b952334f0d0195b06faed532170263f7fad6c2
0646ef9e20628c47c2140c0fc4b51ce3a7ad4c30
0031893be42999b493c3e3c7e88d006db44d425f
e07a5ab133d0e22fbb0a434653bf50a851031001
82b0beb6fff9a90dc40b300ebf1b0ec4977ba8ad
22fa626a3a1eb509a1a14b616d4ec094eb2b8f9a
710370f6142d945e142890eb427a368bfc6c5fe13a963f952fb884c38ef06bfa
fe300467c2714f4962d814a34f8ee631a51e8255b9c07106d44c6a1f1eda7a45
d61d70a4d4c417560652542e54486beb37edce014e34a94b8fd0020796ff1ef7
4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784
8e986c906d0c6213f80d0224833913fa14bc4c15c047766a62f6329bfc0639bd
3db60df73a92b8b15d7885bdcc1cbcf9c740ce29c654375a5c1ce8c2b31488a1
d118f2c99400e773b8cfd3e08a5bcf6ecaa6a644cb58ef8fd5b8aa6c29af4cf1
764a57c926711e448e68917e7db5caba988d3cdbc656b00cd3a6e88922c63837
e8f0a2f79a91587f1d961d6668792e74985624d652c7b47cc87367cb1b451adf
4369f3c729d9bacffab6ec9a8f0e582b4e12b32ed020b5fe0f4c8c0c620931dc

KPMG

KPMG Cyber Threat Intelligence Platform

Follina : Another Troublemaker in Cyber Market!

Indicators of Compromise: Hashes
1f245b9d3247d686937f26f7c0ae36d3c853bda97abd8b95dc0dfd4568ee470b
bf10a54348c2d448afa5d0ba5add70aaccd99506dfcf9d6cf185c0b77c14ace5
c0c5bf6fe1d3b23fc89e0f8b352bd687789b5083ca6d8ec9acce9a9e2942be1f
248296cf75065c7db51a793816d388ad589127c40fddef276e622a160727ca29
4f11f567634b81171a871c804b35c672646a0839485eca0785db71647a1807df
4dda59b51d51f18c9071eb07a730ac4548e36e0d14dbf00e886fc155e705eeef
34dc42f3f486ec282c5e3a16d81a377c2f642d87994ae103742df5ed5804d0f7
ca7e9c65fd2cec62110b50581529198c43b7982820a38c912baa81d0294b8126
5385a798d136365b644199359dc2662de3b0d6c5adc09e4cf9cada074e8a9338
0d7f8698dcb03f879bcf4222852e859e1f8d84e61ee25af12312eda290ccde88
c984867923411b3823a39b98672d1d98d1d093ea669f9b2984c05a0cb3072444
c284dcb06ef882b1b45e11e0a16baa223b4117eca94e243c8e725c4ce3f909b3
965574e97c29813feaa62a0a149731306ee4725e027603b937905375d3121c89
8767f01caa430c5bd4e3b008a8e9dfe022156a4e91a23c394fdcb05c267f1b94
5217c2a1802b0b0fe5592f9437cdfd21f87da1b6ebdc917679ed084e40096bfd
39c15fecc73df9e62e0ffea3ead28b316917886ca06a099a7d825f8495c97e2e
3206fe87e2874db37239d64779c1f504cfca528cef8f5c2214f8434b392aa25a
26896559e0cc85fb441792c86279304693546375f1144040e46cd910362b8e43
14c8c62dc692fd8faa04434e3fed25e7c23d596b732f9db88f6e9f9ff5dfa61c
f3ccf22db2c1060251096fe99464002318baccf598b626f8dbdd5e7fd71fd23f
ed4091700374e007ae478c048734c4bc0b7fe0f41e6d5c611351bf301659eee0
b63fbf80351b3480c62a6a5158334ec8e91fecd057f6c19e4b4dd3febaa9d447
aba9b566dc23169414cb6927ab5368b590529202df41bfd5dded9f7e62b91479
9651e604f972e36333b14a4095d1758b50decda893e8ff8ab52c95ea89bb9f74
87bd2ddff6a90601f67499384290533701f5a5e6cb43de185a8ea858a0604974
7d6d317616d237ba8301707230abbbae64b2f8adb48b878c528a5e42f419133a
33297dc67c12c7876b8052a5f490cc6a4c50a22712ccf36f4f92962463eb744d
0af202af06aef4d36ea151c5a304414a67aee18c3675286275bd01d11a760c04
0477cac3443bb6e46de9b904cba478b778a5c9f82ea411d44a29961f5cc5c842