KPMG Cyber Threat Intelligence Platform

Targets high profile firms APT 28: The Infamous Russian Cyber Hazard

Active since 2004, APT 28 a.k.a Fancy Bear, Sofacy, Stronium, is a Russian cyber espionage group suspected to be a GRU Unit i.e., Russia's Intelligence Directorate. The group made its presence felt in 2016 by compromising Democratic National Committee emails to influence the outcome of the United States presidential elections. They have been extensively targeting organizations throughout the globe, across various sectors including aerospace, defense, energy, government, media, and educational sector.

The group targets conventional computers and mobile devices to deploy both phishing messages and harvest credentials using spoofed websites, created by registering domains that closely resemble legitimate domains. Since at least mid-2019 through early 2021, they have used Kubernetes cluster to conduct widespread brute force attempts to gain access to protected and confidential data, such as login credentials, and further use the gathered information to maintain persistence, privilege escalation and defense evasion. The threat actor's next step post gaining access to the network is observed to be a combination of well-known tactics and techniques to move laterally within the victim network.

The widely adopted brute force technique by the group makes Multi Factor Authentication (MFA) as the most popular mitigation technique for defending against the attacks, alongside implementation of zero trust security model. APT 28 is not just persistent but has also been progressively adopting advanced tooling methods resulting into successful attempts of attacking organizations till date making it the most feared hacking group worldwide even after nearly two decades.

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

Targets high profile firms APT 28: The Infamous Russian Cyber Hazard

Indicators of Compromise: IP Addresses	
185.86.149[.]116	185.86.149[.]116
62.113.232[.]197	62.113.232[.]197
86.106.131[.]54	86.106.131[.]54
194.32.78[.]245	194.32.78[.]245
185.77.129[.]106	185.77.129[.]106
23.227.196[.]215	23.227.196[.]215
167.114.153[.]55	167.114.153[.]55
185.183.107[.]40	185.183.107[.]40
103.208.86[.]57	103.208.86[.]57
172.104.21[.]26	172.104.21[.]26
185.217.92[.]119	185.217.92[.]119
193.37.255[.]10	193.37.255[.]10
176.223.111[.]243	176.223.111[.]243
89.34.111[.]107	89.34.111[.]107
185.128.24[.]104	185.128.24[.]104
103.253.41[.]124	103.253.41[.]124
87.120.254[.]106	87.120.254[.]106
169.239.128[.]133	169.239.128[.]133
185.230.124[.]246	185.230.124[.]246
169.239.129[.]31	169.239.129[.]31
169.239.129[.]121	169.239.129[.]121
213.252.247[.]112	213.252.247[.]112

Indicators of Compromise: Domains	
c4csa[.]org	apple-uptoday[.]org
qov.hu[.]com	poczta.mon.q0v[.]pl
nato.nshq[.]in	apple-iclods[.]net
n0vinite[.]com	apple-search[.]info
login-osce[.]org	apple-checker[.]org
apple-iclods[.]org	natoexhibitionff14[.]com

Indicators of Compromise: Hashes
5c3a6978bb960d8fbccd117ddcc3ca10

KPMG

KPMG Cyber Threat Intelligence Platform

Targets high profile firms APT 28: The Infamous Russian Cyber Hazard

Indicators of Compromise: Hashes
da2a657dc69d7320f2ffc87013f257ad
069acbaa44a9a6f9ef5f7fb4a39805e8
272f0fde35dbdfccbca1e33373b3570d
791428601ad12b9230b9ace4f2138713
49a34cfbeed733c24392c9217ef46bb6
c9a43fd6623bf0bc287012b6ee10a98e
34194fd93d93f635e9e27e045d3e7aab
dbf9580947e52ab6421bd18eb0265167
5086989639aed17227b8d6b041ef3163
4fe4b9560e99e33dabca553e2eeee510
8a9a42a9901b80753c12d97ca7bb35af
b1259bebb6ba7061696c03fc17a54b17
df6c6ee05898ce35ce5963ff0ae2344d
71b4b9f105de94090fc36d9226faaa1db6d9f3d1
3e7dfe9a8d5955a825cb51cb6eec0cd07c569b41
0ac1dbb2a732518a1aa044223f4bcae0c73e8754
46e2957e699fae6de1a212dd98ba4e2bb969497d
afbdb13d8f620d0a5599cbc7a7d9ce8001ee32f1
c53930772beb2779d932655d6c3de5548810af3d
b758c7775d9bcdc0473fc2e738b32f05b464b175
046a8adc2ef0f68107e96babc59f41b6f0a57803
80dca565807fa69a75a7dd278cef1daaee34236e
d70db6a6d660aae58ccfc688a2890391fd873bfb
776780cab8371fea0d2103a8c284d3eff9271f4e16042c0734369f1c9e9d939d
f36a0ee7f4ec23765bb28fbfa734e402042278864e246a54b8c4db6f58275662
3ac11a74275725a22c233cd974229d2b167c336da667410f7262b4926dabd31b
5fdc673941ceac84f8f19d550f04a5e1a82c13cbd04771016b68fbf586ff6dc3
ee7cfc55a49b2e9825a393a94b0baad18ef5bfced67531382e572ef8a9ecda4b
6449d0cb1396d6feba7fb9e25fb20e9a0a5ef3e8623332844458d73057cf04a1
3b87bfb837339445987cdf2e97169cb0c63072dc1d5bffa8ffb4af108a410988
a37eda810ca92486bfb0e1f1b27adb7c9df57aafab686c000ae1d6ec5d6f6180
001cf7af29382f4f784fe45df131ca9e14908c6c0717899780f9354b8a5f0090
8c47961181d9929333628af20bdd750021e925f40065374e6b876e3b8afbba57
b40909ac0b70b7bd82465dfc7761a6b4e0df55b894dd42290e3f72cb4280fa44