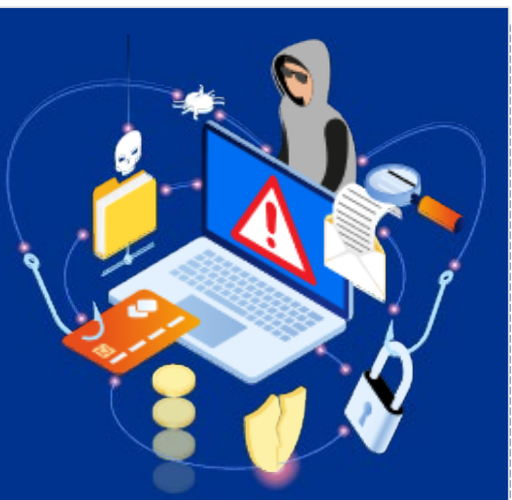
KPMG Cyber Threat Intelligence Platform

New FiveSys Rootkit – A Microsoft-Signed Malicious Kernel Driver



FiveSys, a Chinese cybersecurity threat that emerged in October 2021, abused Windows Hardware Quality Labs (WHQL) to obtain a valid digital signature, camouflaging it as a genuine Microsoft driver file. It is known to target victims in the Chinese gaming sector & focusses on proxying traffic through attacker-controlled proxy servers. Recently in 2023, a new rootkit with similarities to FiveSys surfaced, in terms of functionality, code similarity, infrastructure, and victimology. This new signed rootkit comes with expanded capabilities, allowing it to deploy any second stage unsigned driver that might be of interest to the attacker.

With few samples packed with VMProtect, the new rootkit comes as a generic standalone kernel driver signed directly by Microsoft. It disables User Account Control (UAC) and Secure Desktop Mode by modifying registry entries. It utilizes Winsock Kernel (WSK) for communication with C2. It uses DGA along with hardcoded fallback IP addresses to connect to C2 via TCP port 80. The second-stage driver payloads are fetched from the C2, decoded, decrypted and loaded directly into memory, bypassing Windows native driver loader to evade detection. Second-stage driver, then reads, encodes & writes the first stage driver, deleting the original file to remain undetected. Persistence is achieved through customized second-stage plug-ins that are deployed on victim's machine, some containing custom compiled drivers for each machine. During shutdown/reboot, the first-stage driver copies itself back to disc from memory. These plug-ins are used to disarm Microsoft Defender, deploy proxies on machine & redirect web browsing traffic to a remote server.

Increasing number of threats using legitimate digital signatures is becoming a challenge for defenders. Vigilant cybersecurity measures are vital to detect and counter the presence of such threats.

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

New FiveSys Rootkit – A Microsoft-Signed Malicious Kernel Driver

Indicators of Compromise: IP Addresses	
45.248.11[.]7	103.53.124[.]199
110.42.5[.]55	115.230.124[.]18
110.42.11[.]6	103.91.209[.]141
36.99.113[.]51	125.77.158[.]136
103.88.32[.]158	180.188.17[.]204
103.85.85[.]103	103.45.162[.]204
60.217.248[.]67	221.229.210[.]107
162.14.178[.]70	103.107.190[.]116

Indicators of Compromise: Domains	
68chuanqi[.]com	20mussw4c9pfhea.mpydj[.]xyz
gj2oydber4xfa6c[.]com	gdaszt6be.ady4111523[.]com
ywmmmm.bairimen[.]com	2afybptuag7bi94c.fodvtlyn[.]xyz
4cjhmtf.gg-mmfpz79[.]xyz	19gq0tjscglhzduwy8h.atqvx69f1[.]xyz
ybqjb6.ady4111523[.]com	1bwbosmlqqp3gf.vhld53sxiosqjm[.]xyz
30ku9efzdtj.oq873mn[.]xyz	31mewt-iugrsmty5f4hk.ftrnoxld[.]xyz
0dt7fmri.n7vzlm2tfdz4[.]xyz	08tayhl9pzog5l.7hgum3mdrp1y6h4unvp[.]xyz

Indicators of Compromise: Hashes
7bff10a3978efb400d6101bb3c7ef280
41e64591ddb6030a11ac1fc338a15b23
3f295401fa59a32ff7a11551551ec607
b4ea213fb1dd7dfdd9dee4231e365b47
b518aef1535874b128f47bfebb3a87ce
f0f0e0a106b050f174533e0216de6f8c
191fad43ef6cc3ca1557e033bc4c64b8
218d0dbfcadb17bd17b71bc7a44f40c8
2c84f47290e5757da268e6a6260bbfee
3718a1d067029dd11b60f9737332dcee
65c9a6cc173945a6e8b5efc8403d7fac
7613e0ca3ed198660e2f5445b00b4ecb
9d41afbd7eb51de7a349cac5dbf4ec55

KPMG

KPMG Cyber Threat Intelligence Platform

New FiveSys Rootkit – A Microsoft-Signed Malicious Kernel Driver

Indicators of Compromise: Hashes
03199cb353eebe25c5ce44552db94408
0b4a0fe7db8400ef65ce7618177351cf
0e1fef330a4b6e3260fb819ae3e48ebe
0ed68e212253907dc48b0dc41238fe7a
1244ab729219d741a890ec368266bc5f
212b3c513789474c50013692940f8d45
2970f371d154604ce98e2c5f73c04dd6
37d4ba16136986bfded2b6fc698abf02
466fa3ee3faa900fd89261f291640e8b
4ea977e4f3bda41ce7aed78fb5747817
609c57b2202f9c06511b3cbf09533d8f
1fa8471bf22d9867f349b35276b72440c9d9bde4
ea9c4026b0415e3a35dc51f49d7597ee07de1ccc
2e1f1c03ee126297a64ea285c195f0864e91e824
072c7e3939012eb0c862fae9ff7c5db336f9b69b
10178d14962697fb2911e562bead41d8abbe1044
15061adf38446fcff8e4a214a055a3f6158f3ad6
092b7494afeae45662f5ce416b93a6583556cb37
c36ec8fd5c2501eb82832bedb9a906fdd8d750fa
71ae8824395463b08eda228492b3ce9ccd3aa03b
a879dd29cd6dfb289fc29680923a8ad0107203b6
18ac3a69d495be634873fa4869d0f31de8b10914
f5da9d2603f5457a8a96db076eff193e78f072df
07c5a6568caf372b55e17d7fae88ac474bbadbee
ac131518b2cdfbaf772a4bfbcb520851f1b85db8
7c04c4567b77981d0d97d8c2eb4ebd1a24053f48
4ac6eb0c34158ce9fb49fb4ceb836d45eb87feeb
a47aaf0f5513a90a5efb7134c7a8f12f53c17667
a3b9809f847f273df6f42badd726ca601baf3c9c
a44ef0e53c9440c17335ff4c71f87feb40445f33
e301b89634eb6b95b2dc86d8b00fbbc5c8698b36
7c60d629a8620e7d8edc45e173dd300b745a6bec
9eeae55832174cd5efbfd41725ca933cf9eb9540
f8c19d70e065b5babdc44df60ca883e7ba78e4f8

KPMG

KPMG Cyber Threat Intelligence Platform

New FiveSys Rootkit – A Microsoft-Signed Malicious Kernel Driver

Indicators of Compromise: Hashes
1ac7f8d7db9685ac0746a02c25a489f14395b5ec
b848e7dfa039d9af252332cef03c96123987bc51
3109acd74a8299c45daece07b1c7adcce43ecd3c
a952e90ddd9c3688f46fec2c8a035920caf5b1ab
3ba223669177a2ef06742e8cc00c60ab56bf8b36
36e0710e14ff21d9464bfb9ecfcbe3f7ae5da969
9dc1b844b18ec415718894ce38b9cbbfae53ad0b
c72abd49c0db7d1493fd3548d9a864c7cad9e916
5be4c1f32ead78e643a27832f155803b3b0d4775
e9ef1355c9a983286a8c6bea0a8899b0c2b0afd48955abaf0cc0fc12e14c944e
e39c007ca1a25ae5169f650e1842c33c0ae2d2982085e57258a43930e4ab8bd9
52809533edcd92a143dacf0a46870abe0357422bff7485970ec21061594e4e96
86924ac0b1f93cd70dd5103f17776bc9b70326dc9ee2ed5421b9b548c2833e08
b0c41d9534fe32becaa0613f389c731cc3bd9581711bb6458e87496fc6a01b96
c17651e6953c0a83abb95bd5226fc2ccff4a3cb68499412b2f61d15a5c0a6579
2979c5fd17152164e5e71fd5d4dc17ee46d6e6880e00a47bd69100c7b1102381
465ba20a93abb0d9fded8a55faa5551dacbcad02e026657945e00e9fd9a26c47
05e6b093d34a684647b35b502babe7e5ff1a087ceea1c4a964be662a3a0afc94
8e1a116cb416a0e0614404c7a052dc2ac5f1e847eef2431e9a42276d09079595
15a30214723fe2a98e86c6f542aa6c2394c73eab93d464fa75c4c833df7b8509
9933f40bc304b335b3393959301ba341c165cb13069d88e477510af06d776ea7
0ab9404dedd63c218fa9be416a33988254c350e66aa511e887c9acca94eba5d1
021688ed3ba5966a1ea9ad8e186bc1a073fd73a8148f36a734624a7aece801aa
53213ac12ce2906a2347b500f30c70c42cb4f991c9725d6ff183431133059f0c
802c3ec59c050c3aaee45b66314d8fc865b5e3cae82645b425cf586402115839
Dc4aa34636da31dda0edd841a2753021cc31016ba7e5910f5a7a79bc2429f3b0
ced8b282d86a727fc4b70a50abc9c23235576d1f55baeb740e0a51dd54514e28
2d4c2c621bbfbca1ad6c55d7b12e9ae90aab97df75271d8b53752638da2c6331
f35d490b4995cd6b177b9e9080afd6bdcf74efa6a89ea0f0db257696cb8dd6fc
3dfb9bee5caf96a716ab9ca560db670e28591f76ac71f7bf87a78b18a50bc662
a9ba3540269f524edf29378c35dba510b81fdbea0bb4374466a5cf8cbd0075a6
13943cc96a7d9cfdc6699e2409b14c9ddf8d13e15bcfcc021b9ed99d694ab94b
0378949d3fe9d6f0d965267cfcb68f5ac20404ddb496289f62367601026c47c2
89d52ff0c26d373fff35473d6a6fc12378ad3a7b4313550d1c3ba4f9b86c35df

KPMG

KPMG Cyber Threat Intelligence Platform

New FiveSys Rootkit – A Microsoft-Signed Malicious Kernel Driver

Indicators of Compromise: Hashes
6a10dad205800396b54c4b428cbca161e9aaa0397355db3a25ff5eb629a13abd
109699bc500301a194e9775913f632113eba5805b9b29a558bbcadced170b6e1
315854ec602d0a9cd570189e1133482d510661979ebe4833b1420c764da4f591
5977d7e2e225a522de2dd3d5b0698816c3b962932c074e425d8d0463e5ce5cb0
3b3dcd3d16032dd4c83fe830cb5de1d073b9bd4c43e8e35d09b2026d5ec1e4b0
b42077e0f81fa2f531e0978f2bd77555b6c441446e58049ab52e2001960b1d69
8e2a8d4ef83c8d6dd3682c6292784aea76aa19b0742169aeb88110d31e12ed42
2303b69f630d35d7eae22d30c5efeb76d6d89e80c7be9365b90db44e5ce5e94a
62c32c371d1d812adaf24a8cd3c695dcc6d811eaefd7a81562419363ee56cfa2
176f32495298619ac26ed52a7554f5b4c85c72a29363c5b89df678ad438e9b94
fd765103cd948bd0099cc05782348f2b425441a87a7f38f1bfcdb185aecca84d
0e3cb859370fe0c936424a45beca707fa1f27106e30f34725f97ce51dbfbd482
233421c1e7210fe1c669057038ae122ae02fe0d8ec97970bfc1e26ab26a03376