KPMG Cyber Threat Intelligence Platform

Gallium APT – Pulls out a new RAT

The Chinese leaning Gallium APT group (aka Softcell) are back in with a stealthy new tool dubbed "PingPull" which could utilize ICMP, HTTP(S) or raw TCP protocol to communicate with C2. The previously telecom centered cyber-espionage group owing to their geographic and sector-specific nature has now expanded its attack horizon to target financial and government organizations across Africa, Europe, Australia & Southeast Asia.

Back in 2019, when Microsoft brought Gallium's operations to light, the group was limited to modified versions of popular publicly available exploitation tools. Remote Access Trojans (such as Gh0st RAT, Poison Ivy RAT, etc.) and China Chopper webshell were prominent tools and were predominantly delivered through locating & exploiting internet-facing servers and moving laterally through compromised domain credentials. While payload delivery and lateral movement doesn't seem to be reinvented much, the group now leverages its new Visual C++ written PingPull RAT to gain reverse shell. PingPull masquerades itself as "Iph1psvc" trying to mimic the legitimate "iphlpsvc" service and establishes connection with the hardcoded C2. The ICMP variant employs ICMP Echo Request (ping) packets to communicate to C2, with the data being base64 encoded and AES encrypted with a key specific to each sample. The C2 replies with Echo Reply packets that follow similar structure. The HTTPS and raw TCP variants of PingPull also incorporate almost similar message structures with only the protocol being the major difference.

With more than hundreds of IPs being attributed to Gallium through the analysis of various PingPull samples it's certain that the group is evolving towards more stealthy tactics in order to persist in the threat landscape.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Gallium APT – Pulls out a new RAT

Indicators of Compromise: IP Addresses	
5.8.71[.]97	92.38.149[.]241
5.181.25[.]55	92.223.93[.]222
81.28.13[.]48	92.223.93[.]148
92.38.135[.]62	92.223.30[.]232
92.38.149[.]88	89.43.107[.]191
92.223.59[.]84	89.43.107[.]190
5.188.33[.]237	79.133.124[.]88
103.85.24[.]81	47.254.192[.]79
45.128.221[.]169	43.254.218[.]114
2.58.242[.]232	212.115.54[.]241
2.58.242[.]229	43.254.218[.]104
2.58.242[.]236	103.192.226[.]43
101.36.102[.]93	45.133.238[.]234
92.223.90[.]174	45.128.221[.]169
92.223.30[.]52	185.239.227[.]34
103.169.91[.]94	167.88.182[.]107
45.121.50[.]230	152.32.255[.]145
103.169.91[.]93	45.134.169[.]147
103.85.24[.]121	45.128.221[.]229
89.43.107[.]190	45.128.221[.]186
89.43.107[.]191	45.128.221[.]172
43.254.218[.]43	152.32.221[.]242
43.254.218[.]98	146.185.218[.]65
43.254.218[.]57	47.254.250[.]117
137.220.55[.]38	45.128.221[.]182
45.136.187[.]41	194.29.100[.]173
37.61.229[.]106	185.239.227[.]12
196.46.190[.]27	176.113.71[.]168
176.113.68[.]12	118.193.56[.]131
165.154.70[.]62	47.254.250[.]117
103.61.139[.]74	103.123.134[.]240
45.154.14[.]191	103.123.134[.]165
92.38.171[.]127	103.123.134[.]161
92.223.90[.]174	103.123.134[.]145

KPMG

KPMG Cyber Threat Intelligence Platform

Gallium APT – Pulls out a new RAT

Indicators of Compromise: IP Addresses	
146.185.218[.]176	188.241.250[.]152
185.239.226[.]203	185.101.139[.]176
107.150.110[.]233	107.150.127[.]140
103.170.132[.]199	107.150.112[.]211
193.187.117[.]144	103.137.185[.]249
188.241.250[.]153	

Indicators of Compromise: Domains	
micfkbeljacob[.]com	helpinfo.publicvm[.]com
df.micfkbeljacob[.]com	jack.micfkbeljacob[.]com
df.micfkbeljacob[.]com	

Indicators of Compromise: Hashes
9ad380e7b6d9c83b88ed1b307107912e
Dca83f08d448911a14c22ebcacc5ad57
1a96767957e193c45b1bf642f3293350
E12c09cf7ec74e8dfa412f9fdc8e1ee3
D58c5fe6a5b5b3d494bae50d1df310f5
7e01d776a0eb044a11bf91f3a68ce6f5
B4dd22013aefae6f721f0b67be61dc91
83f860e22cadb5c3f247ad6dc834059a
241b74dee500d61bb10ccfca598979499e40fdff
6d4cc7f30e0a67432244d1a3bb7c058be7c1795f
177f953496b10a4256431166c6247cc5a135e343
97713366202b6914e6defc4dfcbdff430785f407
98aa72ecd43556837f94208431cb710d7eb803e7
5c37b9701a1944b5df6437f7a76097ee1392b1a7
A121f00aba46b8c8db956756723f357e9eacb6cc
91270525521b7fe0d986db19747f47d34b6318ad
F86ebeb6b3c7f12ae98fe278df707d9ebdc17b19be0c773309f9af599243d0a3
B4aabfb8f0327370ce80970c357b84782eaf0aabfc70f5e7340746f25252d541
1ce1eb64679689860a1eacb76def7c3e193504be53ebb0588cddcbde9d2b9fe6
8b664300fff1238d6c741ac17294d714098c5653c3ef992907fc498655ff7c20