Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

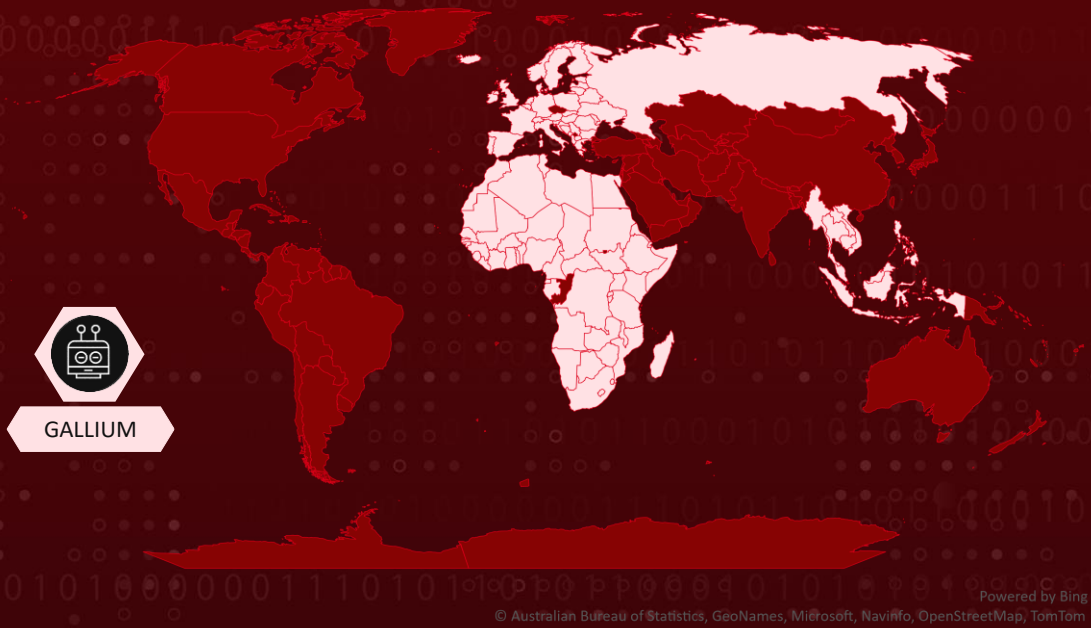
GALLIUM targets Telecommunications sector using new PingPull tool

Date of Publication	Admiralty code	TA Number
June 16, 2022	A1	TA2022125

Summary

A new, difficult-to-detect remote access trojan known as PingPull has been discovered and is used by GALLIUM (also known as Softcell), an APT group. They have expanded by targeting telecommunications, finance and government sectors with the new PingPull tool.

Actor Map



Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**TA0011** Command and Control	**TA0002** Execution	**TA0009** Collection
T1095 Non-Application Layer Protocol	**T1553** Subvert Trust Controls	**T1059** Command and Scripting Interpreter	**T1140** Deobfuscate/Decode Files or Information
T1102 Web Service	**T1560** Archive Collected Data		

Technical Details

#1

GALLIUM, a Chinese state-sponsored group has established themselves by targeting telecommunications companies operating in Southeast Asia, Europe or Africa. Over the past year, they have expanded their targeting from telecommunications to the financial institutions and government entities as well.

#2

PingPull malware is developed in C++ and enables the threat actor to execute commands and gain access to reversed shells on compromised hosts. PingPull has three variants that are functionally equivalent but communicate with their command-and-control(C2) server over different protocols such as HTTP(S), ICMP, and raw TCP.

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONS	TARGET INDUSTRIES
GALLIUM (Soft Cell, Phantom Panda)	China	Information theft and espionage	SouthEast Asia, Europe, Africa, Afghanistan, Australia, Belgium, Cambodia, Malaysia, Mozambique, Philippines, Russia, Vietnam	Telecommunications, Finance, Government sectors

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	de14f22c88e552b61c62ab28d27a617fb8c0737350ca7c631de5680850282761 b4aabfb8f0327370ce80970c357b84782eaf0aabfc70f5e7340746f25252d541 fc2147ddd8613f08dd833b6966891de9e5309587a61e4b35408d56f43e72697e c55ab8fdd060fb532c599ee6647d1d7b52a013e4d8d3223b361db86c1f43e845 f86ebeb6b3c7f12ae98fe278df707d9ebdc17b19be0c773309f9af599243d0a3 8b664300fff1238d6c741ac17294d714098c5653c3ef992907fc498655ff7c20 1ce1eb64679689860a1eacb76def7c3e193504be53ebb0588cddcbde9d2b9fe6
Domain	micfkbeljacob[.]com df.micfkbeljacob[.]com jack.micfkbeljacob[.]com hinitial[.]com t1.hinitial[.]com v2.hinitial[.]com v3.hinitial[.]com v4.hinitial[.]com v5.hinitial[.]com goodjob36.publicvm[.]com goodluck23.jp[.]us helpinfo.publicvm[.]com Mailedc.publicvm[.]com
C2	df.micfkbeljacob[.]com t1.hinitial[.]com 5.181.25[.]55 92.38.135[.]62 5.8.71[.]97
IPV4	202.87.223[.]27 212.115.54[.]54 37.61.229[.]104 45.116.13[.]153 45.128.221[.]61 45.128.221[.]66 45.136.187[.]98

TYPE	VALUE
IPV4	92.38.135[.].62 5.181.25[.]55 5.8.71[.]97 101.36.102[.]34 101.36.102[.]93 101.36.114[.]167 101.36.123[.]191 103.116.47[.]65 103.179.188[.]93 103.22.183[.]131 103.22.183[.]138 103.22.183[.]141 103.22.183[.]146 103.51.145[.]143 103.61.139[.]71 103.61.139[.]72 103.61.139[.]75 103.61.139[.]78 103.61.139[.]79 103.78.242[.]62 118.193.56[.]130 118.193.62[.]232 123.58.196[.]208 123.58.198[.]205 123.58.203[.]19 128.14.232[.]56 152.32.165[.]70 152.32.203[.]199 152.32.221[.]222 152.32.245[.]157 154.222.238[.]50 154.222.238[.]51 165.154.52[.]41 165.154.70[.]51 167.88.182[.]166 176.113.71[.]62 2.58.242[.]230 2.58.242[.]231 2.58.242[.]235

References

https://unit42.paloaltonetworks.com/pingpull-gallium/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

June 16, 2022 • 7:00 AM

More at www.hivepro.com