PingPull, Software S1031 | MITRE ATT&CK®

Archived: 2026-04-05 14:12:44 UTC

PingPull is a remote access Trojan (RAT) written in Visual C++ that has been used by GALLIUM since at least June 2022. PingPull has been used to target telecommunications companies, financial institutions, and government entities in Afghanistan, Australia, Belgium, Cambodia, Malaysia, Mozambique, the Philippines, Russia, and Vietnam.[1]

ID: S1031

ⓘ

Type: MALWARE

ⓘ

Platforms: Windows

Contributors: Yoshihiro Kori, NEC Corporation; Pooja Natarajan, NEC Corporation India; Manikantan Srinivasan, NEC Corporation India

Version: 1.0

Created: 09 August 2022

Last Modified: 16 April 2025

Version Permalink

Live Version

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	A PingPull variant can communicate with its C2 servers by using HTTPS.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	PingPull can use `cmd.exe` to run various commands as a reverse shell.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	PingPull has the ability to install itself as a service.[1]

Domain	ID		Name	Use
Enterprise	T1132	.001	Data Encoding: Standard Encoding	PingPull can encode C2 traffic with Base64. [1]
Enterprise	T1005		Data from Local System	PingPull can collect data from a compromised host.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	PingPull can decrypt received data from its C2 server by using AES.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	PingPull can use AES, in cipher block chaining (CBC) mode padded with PKCS5, to encrypt C2 server communications.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	PingPull has the ability to exfiltrate stolen victim data through its C2 channel.[1]
Enterprise	T1083		File and Directory Discovery	PingPull can enumerate storage volumes and folder contents of a compromised host. [1]
Enterprise	T1070	.006	Indicator Removal: Timestomp	PingPull has the ability to timestomp a file. [1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	PingPull can mimic the names and descriptions of legitimate services such as `iphlpsvc`, `IP Helper`, and `Onedrive` to evade detection.[1]
Enterprise	T1095		Non-Application Layer Protocol	PingPull variants have the ability to communicate with C2 servers using ICMP or TCP.[1]

Domain	ID	Name	Use
Enterprise	T1571	Non-Standard Port	PingPull can use HTTPS over port 8080 for C2.[1]
Enterprise	T1082	System Information Discovery	PingPull can retrieve the hostname of a compromised host.[1]
Enterprise	T1016	System Network Configuration Discovery	PingPull can retrieve the IP address of a compromised host.[1]
