GALLIUM, Granite Typhoon, Group G0093

Archived: 2026-04-05 13:21:04 UTC

Enterprise T1583 .004 Acquire Infrastructure: Server

GALLIUM has used Taiwan-based servers that appear to be exclusive to GALLIUM.[2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

GALLIUM used WinRAR to compress and encrypt stolen data prior to exfiltration.[1][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

GALLIUM used PowerShell for execution to assist in lateral movement as well as for dumping credentials stored on compromised machines.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

GALLIUM used the Windows command shell to execute commands.[1]

Enterprise T1136 .002 Create Account: Domain Account

GALLIUM created high-privileged domain user accounts to maintain access to victim networks.[1][2]

Enterprise T1005 Data from Local System

GALLIUM collected data from the victim's local system, including password hashes from the SAM hive in the Registry.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

GALLIUM compressed and staged files in multi-part archives in the Recycle Bin prior to exfiltration.[1]

Enterprise T1041 Exfiltration Over C2 Channel

GALLIUM used Web shells and HTRAN for C2 and to exfiltrate data.[1]

Enterprise T1190 Exploit Public-Facing Application

GALLIUM exploited a publicly-facing servers including Wildfly/JBoss servers to gain access to the network.[1][2]

Enterprise T1133 External Remote Services

GALLIUM has used VPN services, including SoftEther VPN, to access and maintain persistence in victim environments.[1][2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

GALLIUM used DLL side-loading to covertly load PoisonIvy into memory on the victim machine.[1]

Enterprise T1105 Ingress Tool Transfer

GALLIUM dropped additional tools to victims during their operation, including portqry.exe, a renamed cmd.exe file, winrar, and HTRAN.[1][2]

Enterprise T1570 Lateral Tool Transfer

GALLIUM has used PsExec to move laterally between hosts in the target network.[2]

Enterprise T1036 .003 Masquerading: Rename Legitimate Utilities

GALLIUM used a renamed cmd.exe file to evade detection.[1]

Enterprise T1027 Obfuscated Files or Information

GALLIUM used a modified version of HTRAN in which they obfuscated strings such as debug messages in an apparent attempt to evade detection.[1]

.002 Software Packing

GALLIUM packed some payloads using different types of packers, both known and custom.[1]

.005 Indicator Removal from Tools

GALLIUM ensured each payload had a unique hash, including by using different types of packers.[1]

Enterprise T1588 .002 Obtain Capabilities: Tool

GALLIUM has used a variety of widely-available tools, which in some cases they modified to add functionality and/or subvert antimalware solutions.[2]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

GALLIUM used a modified version of Mimikatz along with a PowerShell-based Mimikatz to dump credentials on the victim machines.[1][2]

.002 OS Credential Dumping: Security Account Manager

GALLIUM used `reg` commands to dump specific hives from the Windows Registry, such as the SAM hive, and obtain password hashes.[1]

Enterprise T1090 .002 Proxy: External Proxy

GALLIUM used a modified version of HTRAN to redirect connections between networks.[1]

Enterprise T1018 Remote System Discovery

GALLIUM used a modified version of NBTscan to identify available NetBIOS name servers over the network as well as `ping` to identify remote systems.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

GALLIUM established persistence for PoisonIvy by created a scheduled task.[1]

Enterprise T1505 .003 Server Software Component: Web Shell

GALLIUM used Web shells to persist in victim environments and assist in execution and exfiltration.[1][2]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

GALLIUM has used stolen certificates to sign its tools including those from Whizzimo LLC.[2]

Enterprise T1016 System Network Configuration Discovery

GALLIUM used `ipconfig /all` to obtain information about the victim network configuration. The group also ran a modified version of NBTscan to identify available NetBIOS name servers.[1]

Enterprise T1049 System Network Connections Discovery

GALLIUM used `netstat -oan` to obtain information about the victim network connections.[1]

Enterprise T1033 System Owner/User Discovery

GALLIUM used `whoami` and `query user` to obtain information about the victim user.[1]

Enterprise T1550 .002 Use Alternate Authentication Material: Pass the Hash

GALLIUM used dumped hashes to authenticate to other machines via pass the hash.[1]

Enterprise T1078 Valid Accounts

GALLIUM leveraged valid accounts to maintain access to a victim network.[1]

Enterprise T1047 Windows Management Instrumentation

GALLIUM used WMI for execution to assist in lateral movement as well as for installing tools across multiple assets.[1]

Source: https://attack.mitre.org/groups/G0093/