gh0st RAT, Software S0032 | MITRE ATT&CK®

Archived: 2026-04-05 14:30:07 UTC

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

gh0st RAT has added a Registry Run key to establish persistence.[3][5]

Enterprise T1059 Command and Scripting Interpreter

gh0st RAT is able to open a remote shell to execute commands.[1][3]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

gh0st RAT can create a new service to establish persistence.[3][5]

Enterprise T1132 .001 Data Encoding: Standard Encoding

gh0st RAT has used Zlib to compress C2 communications data before encrypting it.[5]

Enterprise T1140 Deobfuscate/Decode Files or Information

gh0st RAT has decrypted and loaded the gh0st RAT DLL into memory, once the initial dropper executable is launched.[5]

Enterprise T1568 .001 Dynamic Resolution: Fast Flux DNS

gh0st RAT operators have used dynamic DNS to mask the true location of their C2 behind rapidly changing IP addresses.[5]

Enterprise T1573 Encrypted Channel

gh0st RAT has encrypted TCP communications to evade detection.[5]

.001 Symmetric Cryptography

gh0st RAT uses RC4 and XOR to encrypt C2 traffic.[3]

Enterprise T1574 .001 Hijack Execution Flow: DLL

A gh0st RAT variant has used DLL side-loading.[2]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

gh0st RAT is able to wipe event logs.[1][5]

.004 Indicator Removal: File Deletion

gh0st RAT has the capability to to delete files.[1][5]

Enterprise T1105 Ingress Tool Transfer

gh0st RAT can download files to the victim’s machine.[3][5]

Enterprise T1056 .001 Input Capture: Keylogging

gh0st RAT has a keylogger.[6][5]

Enterprise T1112 Modify Registry

gh0st RAT has altered the InstallTime subkey.[5]

Enterprise T1106 Native API

gh0st RAT has used the `InterlockedExchange`, `SeShutdownPrivilege`, and `ExitWindowsEx` Windows API functions.[5]

Enterprise T1095 Non-Application Layer Protocol

gh0st RAT has used an encrypted protocol within TCP segments to communicate with the C2.[5]

Enterprise T1057 Process Discovery

gh0st RAT has the capability to list processes.[1]

Enterprise T1055 Process Injection

gh0st RAT can inject malicious code into process created by the "Command_Create&Inject" function.[5]

Enterprise T1012 Query Registry

gh0st RAT has checked for the existence of a Service key to determine if it has already been installed on the system.[5]

Enterprise T1113 Screen Capture

gh0st RAT can capture the victim’s screen remotely.[3]

Enterprise T1129 Shared Modules

gh0st RAT can load DLLs into memory.[5]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

A gh0st RAT variant has used rundll32 for execution.[2]

Enterprise T1082 System Information Discovery

gh0st RAT has gathered system architecture, processor, OS configuration, and installed hardware information.[5]

Enterprise T1569 .002 System Services: Service Execution

gh0st RAT can execute its service if the Service key exists. If the key does not exist, gh0st RAT will create and run the service.[5]
