Gazer, Software S0168 | MITRE ATT&CK®

Archived: 2026-04-05 16:31:13 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Gazer communicates with its C2 servers over HTTP.[1]

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

Gazer can establish persistence by creating a .lnk file in the Start menu.[1][2]

.004 Boot or Logon Autostart Execution: Winlogon Helper DLL

Gazer can establish persistence by setting the value "Shell" with "explorer.exe, %malware_pathfile%" under the Registry key `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon`.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Gazer can establish persistence by creating a .lnk file in the Start menu or by modifying existing .lnk files to execute the malware through cmd.exe.[1][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Gazer uses custom encryption for C2 that uses 3DES.[1][2]

.002 Encrypted Channel: Asymmetric Cryptography

Gazer uses custom encryption for C2 that uses RSA.[1][2]

Enterprise T1546 .002 Event Triggered Execution: Screensaver

Gazer can establish persistence through the system screensaver by configuring it to execute the malware.[1]

Enterprise T1480 .002 Execution Guardrails: Mutual Exclusion

Gazer creates a mutex using the hard-coded value `{531511FA-190D-5D85-8A4A-279F2F592CC7}` to ensure that only one instance of itself is running.[1]

Enterprise T1564 .004 Hide Artifacts: NTFS File Attributes

Gazer stores configuration items in alternate data streams (ADSs) if the Registry is not accessible.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Gazer has commands to delete files and persistence mechanisms from the victim.[1][2]

.006 Indicator Removal: Timestomp

For early Gazer versions, the compilation timestamp was faked.[1]

Enterprise T1105 Ingress Tool Transfer

Gazer can execute a task to download a file.[1][2]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Gazer logs its actions into files that are encrypted with 3DES. It also uses RSA to encrypt resources.[2]

Enterprise T1055 Process Injection

Gazer injects its communication module into an Internet accessible process through which it performs C2.[1][2]

.003 Thread Execution Hijacking

Gazer performs thread execution hijacking to inject its orchestrator into a running thread from a remote process.[1] [2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Gazer can establish persistence by creating a scheduled task.[1][2]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Gazer versions are signed with various valid certificates; one was likely faked and issued by Comodo for "Solid Loop Ltd," and another was issued for "Ultimate Computer Support Ltd."[1][2]

Enterprise T1033 System Owner/User Discovery

Gazer obtains the current user's security identifier.[2]
