GoldMax, Software S0588 | MITRE ATT&CK®

Archived: 2026-04-05 16:49:16 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

GoldMax has used HTTPS and HTTP GET requests with custom HTTP cookies for C2.[1][2]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

GoldMax can spawn a command shell, and execute native commands.[1][2]

Enterprise T1001 .001 Data Obfuscation: Junk Data

GoldMax has used decoy traffic to surround its malicious network traffic to avoid detection.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

GoldMax has decoded and decrypted the configuration file when executed.[1][2]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

GoldMax has RSA-encrypted its communication with the C2 server.[1]

Enterprise T1041 Exfiltration Over C2 Channel

GoldMax can exfiltrate files over the existing C2 channel.[1][2]

Enterprise T1564 .011 Hide Artifacts: Ignore Process Interrupts

The GoldMax Linux variant has been executed with the `nohup` command to ignore hangup signals and continue to run if the terminal session was terminated.[3]

Enterprise T1105 Ingress Tool Transfer

GoldMax can download and execute additional files.[1][2]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

GoldMax has impersonated systems management software to avoid detection.[1]

.005 Masquerading: Match Legitimate Resource Name or Location

GoldMax has used filenames that matched the system name, and appeared as a scheduled task impersonating systems management software within the corresponding ProgramData subfolder.[1][3]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

GoldMax has been packed for obfuscation.[2]

.013 Obfuscated Files or Information: Encrypted/Encoded File

GoldMax has written AES-encrypted and Base64-encoded configuration files to disk.[1][2]

Enterprise T1053 .003 Scheduled Task/Job: Cron

The GoldMax Linux variant has used a crontab entry with a `@reboot` line to gain persistence.[3]

.005 Scheduled Task/Job: Scheduled Task

GoldMax has used scheduled tasks to maintain persistence.[1]

Enterprise T1016 System Network Configuration Discovery

GoldMax retrieved a list of the system's network interface after execution.[1]

Enterprise T1124 System Time Discovery

GoldMax can check the current date-time value of the compromised system, comparing it to the hardcoded execution trigger and can send the current timestamp to the C2 server.[1][2]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

GoldMax will check if it is being run in a virtualized environment by comparing the collected MAC address to `c8:27:cc:c2:37:5a`.[1][2]

.003 Virtualization/Sandbox Evasion: Time Based Checks

GoldMax has set an execution trigger date and time, stored as an ASCII Unix/Epoch time value.[1]
