Threat Name: APT_Backdoor_Win_GORAT

Threat Category: Advanced Persistent Threat (APT), Malware Loader

Threat Description: The YARA rule APT_Backdoor_Win_GORAT_1 detects GORAT malware, which consists of multiple loader stages and a network-based Command & Control (C2) mechanism.

Indicators of Compromise (IoCs):

Strings associated with GORAT loader and communication modules:

"Cookie: SID1=%s" ascii wide

"Global\\" ascii wide

"stage0.dll" ascii wide

"runCommand" ascii wide

"getData" ascii wide

"initialize" ascii wide

"Windows NT %d.%d;" ascii wide

"!This program cannot be run in DOS mode." ascii wide

MD5 Hash: 66cdaa156e4d372cfa3dea0137850d20

Detection Mechanism:

Matches hardcoded C2 parameters and unique strings found in stage0 loaders.

Possible Attribution & Use Cases:

Used for covert access and persistence in targeted APT operations.

Recommended Actions:

Block suspicious network traffic to known GORAT C2 domains.

Investigate unauthorized system modifications.

Rule Author: FireEye