GoldMax (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:16:44 UTC

GoldMax

aka: SUNSHUTTLE

Actor(s): UNC2452

Gold Max is a Golang written command and control backdoor used by the NOBELIUM threat actor group. It uses several different techniques to obfuscate its actions and evade detection. The malware writes an encrypted configuration file to disk, where the file name and AES-256 cipher keys are unique per implant and based on environmental variables and information about the network where it is running.

References

2023-08-30 · Kaspersky Labs ·
IT threat evolution in Q2 2023
3CX Backdoor Bankshot BLINDINGCAN GoldMax Kazuar QUIETCANARY tomiris GoldenJackal

2023-05-19 · YouTube (NorthSec) · Ivan Kwiatkowski
Go reverse-engineering workshop
GoldMax

2023-04-24 · Kaspersky Labs · Ivan Kwiatkowski, Pierre Delcher
Tomiris called, they want their Turla malware back
KopiLuwak Andromeda Ave Maria GoldMax JLORAT Kazuar Meterpreter QUIETCANARY RATel Roopy Telemiris tomiris Topinambour Storm-0473

2022-04-20 · CISA · Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), CISA, FBI, Government Communications Security Bureau, National Crime Agency (NCA), NCSC UK, NSA
AA22-110A Joint CSA: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader

2022-04-20 · CISA · CISA
Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader Killnet

2022-01-27 · CrowdStrike · CrowdStrike Intelligence Team

Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign

GoldMax

2021-10-27 · Kaspersky · Ivan Kwiatkowski

Extracting type information from Go binaries

GoldMax

2021-10-26 · Kaspersky · Kaspersky Lab ICS CERT

APT attacks on industrial organizations in H1 2021

8.t Dropper AllaKore AsyncRAT GoldMax LimeRAT NjRAT NoxPlayer Raindrop ReverseRAT ShadowPad Zebrocy

2021-06-01 · Cisco · Josh Pyorre

Backdoors, RATs, Loaders evasion techniques

BazarNimrod GoldMax Oblique RAT

2021-04-15 · CISA · US-CERT

Malware Analysis Report (AR21-105A): SUNSHUTTLE

GoldMax

2021-03-08 · x0r19x91.gitlab.io · Suvaditya Sur

Sunshuttle Malware

GoldMax

2021-03-04 · Microsoft · Andrea Lelli, Ramin Nafisi

GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM’s layered persistence

GoldMax

There is no Yara-Signature yet.
