GootKit (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:27:47 UTC

Gootkit is a banking trojan consisting of an x86 loader and a payload embedding nodejs as well as a set of js scripts. The loader downloads the payload, stores it in registry and injects it in a copy of the loader process. The loader also contains two encrypted DLLs intended to be injected into each browser process launched in order to place the payload in man in the browser and allow it to apply the webinjects received from the command and control server on HTTPx exchanges. This allows Gootkit to intercept HTTPx requests and responses, steal their content or modify it according to the webinjects.

2023-01-09 · Trendmicro · Fe Cureg, Hitomi Kimura, Ryan Maglaque, Trent Bessell
Gootkit Loader Actively Targets Australian Healthcare Industry
GootLoader GootKit 2022-09-22 · deepwatch ·
Is Gootloader Working with a Foreign Intelligence Service?
GootKit 2022-07-27 · Trend Micro · Buddy Tancio, Jed Valderama
Gootkit Loader’s Updated Tactics and Fileless Delivery of Cobalt Strike
Cobalt Strike GootKit Kronos REvil SunCrypt 2022-05-09 · The DFIR Report · The DFIR Report
SEO Poisoning – A Gootloader Story
GootLoader LaZagne Cobalt Strike GootKit 2022-03-22 · Red Canary · Red Canary
2022 Threat Detection Report
FAKEUPDATES Silver Sparrow BazarBackdoor Cobalt Strike GootKit Yellow Cockatoo RAT 2021-11-26 · Twitter (@jhencinski) · Jon Hencinski
Twitter Thread on weelky MDR recap from expel.io
GootKit Squirrelwaffle 2021-11-10 · Blackberry · Codi Starks, Ryan Chapman
REvil Under the Microscope
GootKit REvil 2021-09-03 · Trend Micro · Mohamad Mokbel
The State of SSL/TLS Certificate Usage in Malware C&C Communications
AdWind ostap AsyncRAT BazarBackdoor BitRAT Buer Chthonic CloudEyE Cobalt Strike DCRat Dridex FindPOS GootKit Gozi IcedID ISFB Nanocore RAT Orcus RAT PandaBanker Qadars QakBot Quasar RAT Rockloader ServHelper Shifu SManager TorrentLocker TrickBot Vawtrak Zeus Zloader 2021-06-07 · Kaspersky · Anton Kuzmenko
Gootkit: the cautious Trojan
GootKit 2021-03-02 · Github (microsoft) · Microsoft
Microsoft-365-Defender-Hunting-Queries for hunting Gootkit malware delivery and C2
GootKit 2021-03-02 · Twitter (@MsftSecIntel) · Microsoft Security Intelligence
Tweet on Gootkit malware campaign
GootKit 2021-03-01 · Sophos Labs · Andrew Brandt, Gabor Szappanos
“Gootloader” expands its payload delivery options
GootKit 2021-02-02 · · CRONUP · Germán Fernández

De ataque con Malware a incidente de Ransomware

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DanaBot Dharma Dridex Egregor Emotet Empire Downloader FriedEx GootKit IcedID MegaCortex Nemty Phorpiex PwndLocker PyXie QakBot RansomEXX REvil Ryuk SDBbot SmokeLoader TrickBot Zloader 2021-01-19 · Palo Alto Networks Unit 42 · Brad Duncan

Wireshark Tutorial: Examining Emotet Infection Traffic

Emotet GootKit IcedID QakBot TrickBot 2020-12-11 · Trend Micro · Marc Lanzendorfer

Investigating the Gootkit Loader

GootKit 2020-11-30 · Malwarebytes · hasherezade, Jérôme Segura

German users targeted with Gootkit banker or REvil ransomware

GootKit REvil 2020-04-13 · Blackberry · Masaki Kasuya, Tatsuya Hasegawa

Threat Spotlight: Gootkit Banking Trojan

Azorult GootKit 2019-10-02 · Dissecting Malware · Marius Genheimer

Nicht so goot - Breaking down Gootkit and Jasper (+ FTCODE)

FTCODE JasperLoader GootKit 2019-08-29 · SentinelOne · Daniel Bunce

Gootkit Banking Trojan | Part 2: Persistence & Other Capabilities

GootKit 2019-08-15 · SentinelOne · Daniel Bunce

Gootkit Banking Trojan | Deep Dive into Anti-Analysis Features

GootKit 2019-08-15 · Sentinel LABS · Daniel Bunce

Gootkit Banking Trojan | Deep Dive into Anti-Analysis Features

GootKit 2019-03-23 · Open Malware · Danny Quist

Reverse Engineering Gootkit with Ghidra Part I

GootKit 2019-02-14 · Certego · Matteo Lodi

Malware Tales: Gootkit

GootKit 2018-11-01 · · CERT La Poste · Christophe Rieunier, Thomas Dubier

Analyse du malware bancaire Gootkit et de ses mécanismes de protection

GootKit 2018-05-20 · Youtube (OALabs) · Sergei Frankoff

Unpacking Gootkit Part 2 - Debugging Anti-Analysis Tricks With IDA Pro and x64dbg

GootKit 2018-03-04 · Youtube (OALabs) · Sergei Frankoff

Unpacking Gootkit Malware With IDA Pro and X64dbg - Subscriber Request

Cold$eal GootKit 2018-02-13 · Juniper · Paul Kimayong

New Gootkit Banking Trojan variant pushes the limits on evasive behavior

GootKit 2017-03-01 · SecurityIntelligence · Gadi Ostrovsky, Limor Kessem

GootKit Developers Dress It Up With Web Traffic Proxy

GootKit 2016-12-01 · US-CERT · US-CERT

Alert (TA16-336A): Avalanche (crimeware-as-a-service infrastructure)

GootKit 2016-10-27 · Kaspersky Labs · Alexey Shulmin, Sergey Yunakovsky

Inside the Gootkit C&C server

GootKit 2016-07-08 · SecurityIntelligence · Limor Kessem

GootKit: Bobbing and Weaving to Avoid Prying Eyes

GootKit 2015-04-13 · CERT Societe Generale · CERT Societe Generale

Analyzing Gootkit's persistence mechanism (new ASEP inside!)

GootKit 2015-03-30 · Trend Micro · Cedric Pernet, Dark Luo

Fake Judicial Spam Leads to Backdoor with Fake Certificate Authority

GootKit 2014-04-09 · Dr.Web · Dr.Web

BackDoor.Gootkit.112—a new multi-purpose backdoor

GootKit 2012-08-01 · Kaspersky · Marta Janus

“RunForestRun”, “gootkit” and random domain name generation

RunForestRun GootKit

▶ [TLP:WHITE] win_gootkit_auto (20251219 | Detects win.gootkit.)
