Loki Password Stealer (PWS) (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:18:42 UTC

Loki Password Stealer (PWS)

aka: Burkina, Loki, LokiBot, LokiPWS

Actor(s): SWEED, The Gorgon Group, Cobalt

VTCollection URLhaus

"Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets." - PhishMe

Loki-Bot employs function hashing to obfuscate the libraries utilized. While not all functions are hashed, a vast majority of them are.

Loki-Bot accepts a single argument/switch of '-u' that simply delays execution (sleeps) for 10 seconds. This is used when Loki-Bot is upgrading itself.

The Mutex generated is the result of MD5 hashing the Machine GUID and trimming to 24-characters. For example: "B7E1C2CC98066B250DDB2123".

Loki-Bot creates a hidden folder within the %APPDATA% directory whose name is supplied by the 8th thru 13th characters of the Mutex. For example: "%APPDATA%\ C98066\".

There can be four files within the hidden %APPDATA% directory at any given time: ".exe," ".lck," ".hdb" and ".kdb." They will be named after characters 13 thru 18 of the Mutex. For example: "6B250D." Below is the explanation of their purpose:

FILE EXTENSION FILE DESCRIPTION
.exe A copy of the malware that will execute every time the user account is logged into
.lck A lock file created when either decrypting Windows Credentials or Keylogging to prevent resource conflicts
.hdb A database of hashes for data that has already been exfiltrated to the C2 server
.kdb A database of keylogger data that has yet to be sent to the C2 server

If the user is privileged, Loki-Bot sets up persistence within the registry under HKEY_LOCAL_MACHINE. If not, it sets up persistence under HKEY_CURRENT_USER.

The first packet transmitted by Loki-Bot contains application data.

The second packet transmitted by Loki-Bot contains decrypted Windows credentials.

The third packet transmitted by Loki-Bot is the malware requesting C2 commands from the C2 server. By default, Loki-Bot will send this request out every 10 minutes after the initial packet it sent.

Communications to the C2 server from the compromised host contain information about the user and system including the username, hostname, domain, screen resolution, privilege level, system architecture, and Operating System.

The first WORD of the HTTP Payload represents the Loki-Bot version.

The second WORD of the HTTP Payload is the Payload Type. Below is the table of identified payload types:

BYTE PAYLOAD TYPE
0x26 Stolen Cryptocurrency Wallet
0x27 Stolen Application Data
0x28 Get C2 Commands from C2 Server
0x29 Stolen File
0x2A POS (Point of Sale?)
0x2B Keylogger Data
0x2C Screenshot

The 11th byte of the HTTP Payload begins the Binary ID. This might be useful in tracking campaigns or specific threat actors. This value value is typically “ckav.ru”. If you come across a Binary ID that is different from this, take note!

Loki-Bot encrypts both the URL and the registry key used for persistence using Triple DES encryption.

The Content-Key HTTP Header value is the result of hashing the HTTP Header values that precede it. This is likely used as a protection against researchers who wish to poke and prod at Loki-Bot’s C2 infrastructure.

Loki-Bot can accept the following instructions from the C2 Server:

BYTE INSTRUCTION DESCRIPTION
0x00 Download EXE & Execute
0x01 Download DLL & Load #1
0x02 Download DLL & Load #2
0x08 Delete HDB File
0x09 Start Keylogger
0x0A Mine & Steal Data
0x0E Exit Loki-Bot
0x0F Upgrade Loki-Bot
0x10 Change C2 Polling Frequency
0x11 Delete Executables & Exit

Suricata Signatures

RULE SID RULE NAME

2024311 ET TROJAN Loki Bot Cryptocurrency Wallet Exfiltration Detected

2024312 ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M1

2024313 ET TROJAN Loki Bot Request for C2 Commands Detected M1

2024314 ET TROJAN Loki Bot File Exfiltration Detected

2024315 ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M1

2024316 ET TROJAN Loki Bot Screenshot Exfiltration Detected

2024317 ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M2

2024318 ET TROJAN Loki Bot Request for C2 Commands Detected M2

2024319 ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M2

References

2024-12-02 · Medium b.magnezi · 0xMrMagnezi

LokiBot Malware Analysis

Loki Password Stealer (PWS)

2024-11-07 · Logpoint · Anish Bogati

Hiding in Plain Sight: The Subtle Art of Loki Malware’s Obfuscation

Loki Password Stealer (PWS)

2024-02-28 · Security Intelligence · Golo Mühr, Ole Villadsen

X-Force data reveals top spam trends, campaigns and senior superlatives in 2023

404 Keylogger Agent Tesla Black Basta DarkGate Formbook IcedID Loki Password Stealer (PWS) Pikabot QakBot Remcos

2023-07-12 · Fortinet · Cara Lin

LokiBot Campaign Targets Microsoft Office Document Using Vulnerabilities and Macros

Loki Password Stealer (PWS)

2023-01-30 · Checkpoint · Arie Olshtein

Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wanted Malware

Agent Tesla Azorult Buer Cerber Cobalt Strike Emotet Formbook HawkEye Keylogger Loki Password Stealer (PWS) Maze NetWire RC Remcos REvil TrickBot

2022-10-13 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q3 2022

FluBot Arkei Stealer AsyncRAT Ave Maria BumbleBee Cobalt Strike DCRat Dridex Emotet Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT QakBot RecordBreaker RedLine Stealer Remcos Socelars Tofsee Vjw0rm

2022-08-08 · Medium CSIS Techblog · Benoît Ancel

An inside view of domain anonymization as-a-service — the BraZZZerSFF infrastructure

Riltok magecart Anubis Azorult BetaBot Buer CoalaBot CryptBot DiamondFox DreamBot GCleaner ISFB

Loki Password Stealer (PWS) MedusaLocker MeguminTrojan Nemty PsiX RedLine Stealer SmokeLoader STOP TinyNuke Vidar Zloader

2022-08-05 · 0xIvan · Twitter (@viljoenivan)
LokiBot Analysis
Loki Password Stealer (PWS)

2022-06-30 · CYBER GEEKS All Things Infosec · CyberMasterV
How to Expose a Potential Cybercriminal due to Misconfigurations
Loki Password Stealer (PWS)

2022-06-30 · Cyber Geeks (CyberMasterV) · Vlad Pasca
How to Expose a Potential Cybercriminal due to Misconfigurations
Loki Password Stealer (PWS)

2022-05-19 · Blackberry · The BlackBerry Research & Intelligence Team
.NET Stubs: Sowing the Seeds of Discord (PureCrypter)
Aberebot AbstractEmu AdoBot 404 Keylogger Agent Tesla Amadey AsyncRAT Ave Maria BitRAT BluStealer Formbook LimeRAT Loki Password Stealer (PWS) Nanocore RAT Orcus RAT Quasar RAT Raccoon RedLine Stealer WhisperGate

2022-04-17 · Malcat · malcat team
Reversing a NSIS dropper using quick and dirty shellcode emulation
Loki Password Stealer (PWS)

2022-03-07 · · LAC WATCH · Cyber Emergency Center
I CAN'T HEAR YOU NOW! INTERNAL BEHAVIOR OF INFORMATION-STEALING MALWARE AND JSOC DETECTION TRENDS
Xloader Agent Tesla Formbook Loki Password Stealer (PWS)

2022-02-11 · Cisco Talos · Talos
Threat Roundup for February 4 to February 11
DarkComet Ghost RAT Loki Password Stealer (PWS) Tinba Tofsee Zeus

2022-01-28 · Atomic Matryoshka · z3r0day_504
Malware Headliners: LokiBot
Loki Password Stealer (PWS)

2021-11-17 · Infoblox · Gaetano Pellegrino
Deep Analysis of a Recent Lokibot Attack
Loki Password Stealer (PWS)

2021-08-25 · Trend Micro · Bin Lin, William Gamazo Sanchez
New Campaign Sees LokiBot Delivered Via Multiple Methods
Loki Password Stealer (PWS)

2021-08-23 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal
[2] Lokibot analyzing - spoofing GULoader and LokiBot C2 [part2] - INetSim + BurpSuite
CloudEyE Loki Password Stealer (PWS)

2021-08-16 · Malcat · malcat team
Statically unpacking a simple .NET dropper
Loki Password Stealer (PWS)

2021-07-12 · Cipher Tech Solutions · Claire Zaboeva, Dan Dash, Melissa Frydrych
RoboSki and Global Recovery: Automation to Combat Evolving Obfuscation
404 Keylogger Agent Tesla AsyncRAT Ave Maria Azorult BitRAT Formbook HawkEye Keylogger Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Quasar RAT RedLine Stealer Remcos

2021-07-12 · IBM · Claire Zaboeva, Dan Dash, Melissa Frydrych
RoboSki and Global Recovery: Automation to Combat Evolving Obfuscation
404 Keylogger Agent Tesla AsyncRAT Ave Maria Azorult BitRAT Formbook HawkEye Keylogger Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Quasar RAT RedLine Stealer Remcos

2021-07-07 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal
[2] Lokibot analyzing - spoofing GULoader and LokiBot C2 [part1] - Own implementation in Python
CloudEyE Loki Password Stealer (PWS)

2021-07-06 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal
[1] Lokibot analyzing - defeating GuLoader with Windbg (Kernel debugging) and Live C2
CloudEyE Loki Password Stealer (PWS)

2021-06-08 · ilbaroni
LOKIBOT - A commodity malware
Loki Password Stealer (PWS)

2021-04-06 · InfoSec Handlers Diary Blog · Jan Kopriva
Malspam with Lokibot vs. Outlook and RFCs
Loki Password Stealer (PWS)

2021-01-06 · Talos · Holger Unterbrink, Irshad Muhammad
A Deep Dive into Lokibot Infection Chain
Loki Password Stealer (PWS)

2020-12-07 · Proofpoint · Proofpoint Threat Research Team
Commodity .NET Packers use Embedded Images to Hide Payloads
Agent Tesla Loki Password Stealer (PWS) Remcos

2020-10-01 · SpiderLabs Blog · Diana Lopera
Evasive URLs in Spam: Part 2
Loki Password Stealer (PWS)

2020-08-26 · Lab52 · Jagaimo Kawaii
A twisted malware infection chain
Agent Tesla Loki Password Stealer (PWS)

2020-07-30 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q2 2020
AdWind Agent Tesla Arkei Stealer AsyncRAT Ave Maria Azorult DanaBot Emotet IcedID ISFB KPOT Stealer Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Pony Raccoon RedLine Stealer Remcos Zloader

2020-05-21 · Malwarebytes · Malwarebytes Labs
Cybercrime tactics and techniques
Ave Maria Azorult DanaBot Loki Password Stealer (PWS) NetWire RC

2020-05-14 · SophosLabs · Markel Picado
RATicate: an attacker’s waves of information-stealing malware
Agent Tesla BetaBot BlackRemote Formbook Loki Password Stealer (PWS) NetWire RC NjRAT Remcos

2020-04-28 · Trend Micro · Miguel Ang
Loki Info Stealer Propagates through LZH Files
Loki Password Stealer (PWS)

2020-03-31 · Click All the Things! Blog · Jamie
LokiBot: Getting Equation Editor Shellcode
Loki Password Stealer (PWS)

2020-03-20 · Bitdefender · Liviu Arsene
5 Times More Coronavirus-themed Malware Reports during March
ostap HawkEye Keylogger Koadic Loki Password Stealer (PWS) Nanocore RAT Remcos

2020-02-14 · Virus Bulletin · Aditya K. Sood
LokiBot: dissecting the C&C panel deployments
Loki Password Stealer (PWS)

2020-02-06 · Prevailion · Danny Adamitis
The Triune Threat: MasterMana Returns
Azorult Loki Password Stealer (PWS)

2019-12-28 · Paul Burbage
The Tale of the Pija-Droid Firefinch
Loki Password Stealer (PWS)

2019-12-12 · FireEye · Chi-en Shen, Oleg Bondarenko
Cyber Threat Landscape in Japan – Revealing Threat in the Shadow
Cerberus TSCookie Cobalt Strike Dtrack Emotet Formbook IcedID Icefog IRONHALO Loki Password Stealer (PWS) PandaBanker PLEAD POISONPLUG TrickBot BlackTech

2019-10-28 · Marco Ramilli's Blog · Marco Ramilli
SWEED Targeting Precision Engineering Companies in Italy
Loki Password Stealer (PWS)

2019-08-10 · Check Point · Omer Gull
SELECT code_execution FROM * USING SQLite;
Azorult Loki Password Stealer (PWS) Pony

2019-07-15 · Cisco Talos · Edmund Brumaghin
SWEED: Exposing years of Agent Tesla campaigns
Agent Tesla Formbook Loki Password Stealer (PWS) SWEED

2019-04-05 · Trustwave · Phil Hay, Rodel Mendrez
Spammed PNG file hides LokiBot
Loki Password Stealer (PWS)

2018-12-04 · Brad Duncan
Malspam pushing Lokibot malware
Loki Password Stealer (PWS)

2018-08-29 · Kaspersky Labs · Tatyana Shcherbakova
Loki Bot: On a hunt for corporate passwords
Loki Password Stealer (PWS)

2018-08-02 · Palo Alto Networks Unit 42 · David Fuertes, Josh Grunzweig, Kyle Wilhoit, Robert Falcone
The Gorgon Group: Slithering Between Nation State and Cybercrime
Loki Password Stealer (PWS) Nanocore RAT NjRAT Quasar RAT Remcos Revenge RAT

2018-07-06 · Github (d00rt) · d00rt
LokiBot Infostealer Jihacked Version
Loki Password Stealer (PWS)

2017-12-19 · Lastline · Andy Norton
Novel Excel Spreadsheet Attack Launches Password Stealing Malware Loki Bot
Loki Password Stealer (PWS)

2017-06-22 · SANS Institute Information Security Reading Room · Rob Pantazopoulos
Loki-Bot: InformationStealer, Keylogger, &More!
Loki Password Stealer (PWS)

2017-05-17 · Fortinet · Hua Liu, Xiaopeng Zhang
New Loki Variant Being Spread via PDF File
Loki Password Stealer (PWS)

2017-05-07 · R3MRUM · R3MRUM
Loki-Bot: Come out, come out, wherever you are!
Loki Password Stealer (PWS)

2017-05-05 · Github (R3MRUM) · R3MRUM
loki-parse
Loki Password Stealer (PWS)

2017-03-23 · Cofense · Cofense
Tales from the Trenches: Loki Bot Malware
Loki Password Stealer (PWS)

2017-02-16 · Cysinfo · Winston M
Nefarious Macro Malware drops “Loki Bot” to steal sensitive information across GCC countries!
Loki Password Stealer (PWS)

Yara Rules

▶ [TLP:WHITE] win_lokipws_auto (20251219 | Detects win.lokipws.)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.lokipws