DanaBot (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:12:48 UTC

Proofpoints describes DanaBot as the latest example of malware focused on persistence and stealing useful information that can later be monetized rather than demanding an immediate ransom from victims. The social engineering in the low-volume DanaBot campaigns we have observed so far has been well-crafted, again pointing to a renewed focus on “quality over quantity” in email-based threats. DanaBot’s modular nature enables it to download additional components, increasing the flexibility and robust stealing and remote monitoring capabilities of this banker.

2025-07-14 · Spamhaus ·
Spamhaus Botnet Threat Update January to June 2025
Coper FluBot Hook Joker Mirai AsyncRAT BianLian BumbleBee Chaos Cobalt Strike DanaBot DCRat Havoc Latrodectus NjRAT Quasar RAT RedLine Stealer Remcos Rhadamanthys Sliver ValleyRAT WarmCookie XWorm
2025-06-09 · Zscaler · ThreatLabZ research team, Zscaler
DanaBleed: DanaBot C2 Server Memory Leak Bug
DanaBot 2025-05-22 · ESET Research · Tomáš Procházka
Danabot: Analyzing a fallen empire
DanaBot 2025-05-22 · Flashpoint · Flashpoint
Operation Endgame: Global Law Enforcement Takes Down DanaBot Malware Scheme
DanaBot 2025-05-22 · KrebsOnSecurity · Brian Krebs
Oops: DanaBot Malware Devs Infected Their Own PCs
DanaBot 2025-04-08 · Team Cymru · S2 Research Team
Inside DanaBot’s Infrastructure: In Support of Operation Endgame II
DanaBot 2025-01-10 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update July to December 2024
Coper FluBot Hook Mirai FAKEUPDATES AsyncRAT BianLian Brute Ratel C4 Cobalt Strike DanaBot DCRat Havoc Latrodectus NjRAT Quasar RAT RedLine Stealer Remcos Rhadamanthys Sliver Stealc 2024-11-18 · Proofpoint · Proofpoint Threat Research Team, Selena Larson, Tommy Madjar
Security Brief: ClickFix Social Engineering Technique Floods Threat Landscape
AsyncRAT Brute Ratel C4 DanaBot DarkGate Latrodectus Lumma Stealer NetSupportManager RAT XWorm
2024-08-15 · Kaspersky · AbdulRhman Alfaifi, Elsayed Elrefaei
Tusk campaign uses infostealers and clippers for financial gain
DanaBot HijackLoader Stealc 2023-12-14 · Mandiant · Adrian McCabe, Geoff Ackerman, Rufus Brown, Ryan Tomcik
Opening a Can of Whoop Ads: Detecting and Disrupting a Malvertising Campaign Distributing Backdoors
DanaBot DarkGate 2023-12-14 · Mandiant · Adrian McCabe, Geoff Ackerman, Rufus Brown, Ryan Tomcik
Opening a Can of Whoop Ads: Detecting and Disrupting a Malvertising Campaign Distributing Backdoors
DanaBot DarkGate UNC4393 2023-12-12 · Youtube (OALabs) · Sergei Frankoff
Tips For Analyzing Delphi Binaries in IDA (Danabot)

DanaBot 2023-12-07 · eSentire · eSentire

DanaBot's Latest Move: Deploying Latrodectus

DanaBot HijackLoader Latrodectus 2023-12-01 · Twitter (@MsftSecIntel) · Microsoft Threat Intelligence

Tweet about Storm-1044 and Storm-0216, Danabot leading to Cactus ransomware

Cactus DanaBot TA2101 2023-12-01 · Twitter (@MsftSecIntel) · Microsoft Threat Intelligence

Tweet on Danabot leading to cactus ransomware

Cactus DanaBot Storm-1044 2023-11-02 · eSentire · eSentire Threat Response Unit (TRU)

From DarkGate to DanaBot

DanaBot DarkGate 2023-07-17 · Flashpoint · Flashpoint

The New Release of Danabot Version 3: What You Need to Know

DanaBot 2022-12-06 · Zscaler · Dennis Schwarz

Technical Analysis of DanaBot Obfuscation Techniques

DanaBot 2022-09-26 · Kaspersky · Artem Ushkov, Haim Zigel, Oleg Kupreev

NullMixer: oodles of Trojans in a single dropper

ColdStealer DanaBot GCleaner Nullmixer PrivateLoader PseudoManuscrypt RedLine Stealer SmokeLoader Vidar 2022-09-15 · Sekoia · Threat & Detection Research Team

PrivateLoader: the loader of the prevalent ruzki PPI service

Agent Tesla Coinminer DanaBot DCRat Eternity Stealer Glupteba Mars Stealer NetSupportManager RAT Nymaim Nymaim2 Phoenix Keylogger PrivateLoader Raccoon RedLine Stealer SmokeLoader Socelars STOP Vidar YTStealer 2022-08-07 · Malverse · greenplan

Config Extractor per DanaBot (PARTE 1)

DanaBot 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 2022-04-20 · 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 2022-03-15 · Security Soup Blog · Ryan Campbell

Decoding a DanaBot Downloader

DanaBot 2022-03-02 · Zscaler · Brett Stone-Gross, Dennis Schwarz

DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense

DanaBot 2022-03-01 · VirusTotal · VirusTotal

VirusTotal's 2021 Malware Trends Report

Anubis AsyncRAT BlackMatter Cobalt Strike DanaBot Dridex Khonsari MimiKatz Mirai Nanocore RAT Orcus RAT 2022-01-03 · AhnLab · ASEC Analysis Team

Distribution of Redline Stealer Disguised as Software Crack

DanaBot RedLine Stealer Vidar 2021-12-15 · Mandiant · Alessandro Parilli, James Maclachlan

No Unaccompanied Miners: Supply Chain Compromises Through Node.js Packages (UNC3379)

DanaBot 2021-11-18 · Blackberry · The BlackBerry Research & Intelligence Team

Threat Thursday: DanaBot’s Evolution from Bank Fraud to DDos Attacks

DanaBot 2021-11-14 · Twitter (@f0wlsec) · Marius Genheimer

A static config extractor for the main component of DanaBot

DanaBot 2021-11-08 · Bitdefender · Silviu Stahie

Popular NPM Repositories Compromised in Man-in-the-Middle Attack

DanaBot 2021-11-05 · Zscaler · Dennis Schwarz

Spike in DanaBot Malware Activity

DanaBot 2021-10-24 · Sophos · Sean Gallagher

Node poisoning: hijacked package delivers coin miner and credential-stealing backdoor

DanaBot Monero Miner 2021-09-20 · Lexfo · Lexfo

DanaBot Communications Update

DanaBot 2021-03-31 · Kaspersky · Kaspersky

Financial Cyberthreats in 2020

BetaBot DanaBot Emotet Gozi Ramnit RTM SpyEye TrickBot Zeus 2021-02-23 · CrowdStrike · CrowdStrike

2021 Global Threat Report

RansomEXX Amadey Anchor Avaddon BazarBackdoor Clop Cobalt Strike Conti Cutwail DanaBot DarkSide DoppelPaymer Dridex Egregor Emotet Hakbit IcedID JSOutProx KerrDown LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker NedDnLoader Nemty Pay2Key PlugX Pushdo PwndLocker PyXie QakBot Quasar RAT RagnarLocker Ragnarok RansomEXX REvil Ryuk Sekhmet ShadowPad SmokeLoader Snake SUNBURST SunCrypt TEARDROP TrickBot WastedLocker Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER 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 2021-01-26 · Proofpoint · Axel F., Brandon Murphy, Dennis Schwarz

New Year, New Version of DanaBot

DanaBot 2021-01-09 · Marco Ramilli's Blog · Marco Ramilli

Command and Control Traffic Patterns

ostap LaZagne Agent Tesla Azorult Buer Cobalt Strike DanaBot DarkComet Dridex Emotet Formbook IcedID ISFB NetWire RC PlugX Quasar RAT SmokeLoader TrickBot 2020-08-09 · F5 Labs · Debbie Walkowski, Remi Cohen

Banking Trojans: A Reference Guide to the Malware Family Tree

BackSwap Carberp Citadel DanaBot Dridex Dyre Emotet Gozi Kronos PandaBanker Ramnit Shylock SpyEye Tinba TrickBot Vawtrak Zeus 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 2020-07-29 · ESET Research · welivesecurity

THREAT REPORT Q2 2020

DEFENSOR ID HiddenAd Bundlore Pirrit Agent.BTZ Cerber ClipBanker CROSSWALK Cryptowall CTB Locker DanaBot Dharma Formbook Gandcrab Grandoreiro Houdini ISFB LockBit Locky Mailto Maze Microcin Nemty NjRAT Phobos PlugX Pony REvil Socelars STOP Tinba TrickBot WannaCryptor 2020-07-12 · Malware and Stuff · Andreas Klopsch

Deobfuscating DanaBot's API Hashing

DanaBot 2020-06-02 · Lastline Labs · James Haughom, Stefano Ortolani

Evolution of Excel 4.0 Macro Weaponization

Agent Tesla DanaBot ISFB TrickBot Zloader 2020-05-21 · Malwarebytes · Malwarebytes Labs

Cybercrime tactics and techniques

Ave Maria Azorult DanaBot Loki Password Stealer (PWS) NetWire RC 2020-03-04 · CrowdStrike · CrowdStrike

2020 CrowdStrike Global Threat Report

MESSAGETAP More_eggs 8.t Dropper Anchor BabyShark BadNews Clop Cobalt Strike CobInt Cobra Carbon System Cutwail DanaBot Dharma DoppelDridex DoppelPaymer Dridex Emotet FlawedAmmyy FriedEx Gandcrab Get2 IcedID ISFB KerrDown LightNeuron LockerGoga Maze MECHANICAL Necurs Nokki Outlook Backdoor Phobos Predator The Thief QakBot REvil RobinHood Ryuk SDBbot Skipper SmokeLoader TerraRecon TerraStealer TerraTV TinyLoader TrickBot Vidar Winnti ANTHROPOID SPIDER APT23 APT31 APT39 APT40 BlackTech BuhTrap Charming Kitten CLOCKWORK SPIDER DOPPEL SPIDER FIN7 Gamaredon Group GOBLIN PANDA MONTY SPIDER MUSTANG PANDA NARWHAL SPIDER NOCTURNAL SPIDER PINCHY SPIDER SALTY SPIDER SCULLY SPIDER SMOKY SPIDER Thrip VENOM SPIDER VICEROY TIGER 2019-06-20 · Check Point · Aliaksandr Chailytko, Yaroslav Harakhavik

DanaBot Demands a Ransom Payment

DanaBot 2019-05-09 · G Data · G-Data

Strange Bits: HTML Smuggling and GitHub Hosted Malware

DanaBot 2019-05-08 · Verizon Communications Inc. · Verizon Communications Inc.

2019 Data Breach Investigations Report

BlackEnergy Cobalt Strike DanaBot Gandcrab GreyEnergy Mirai Olympic Destroyer SamSam 2019-03-13 · Proofpoint · Dennis Schwarz, Proofpoint Threat Insight Team

DanaBot control panel revealed

DanaBot 2019-03-01 · Fortinet · FortiGuard SE Team

Breakdown of a Targeted DanaBot Attack

DanaBot 2019-02-07 · ESET Research · ESET Research

DanaBot updated with new C&C communication

DanaBot 2018-12-20 · Yoroi · Antonio Pirozzi, Davide Testa, Luca Mella, Luigi Martire

Dissecting the Danabot Payload Targeting Italy

DanaBot 2018-12-06 · ESET Research · ESET Research

DanaBot evolves beyond banking Trojan with new spam-sending capability

DanaBot 2018-10-02 · Proofpoint · Proofpoint Staff

DanaBot Gains Popularity and Targets US Organizations in Large Campaigns

DanaBot 2018-09-21 · ESET Research · ESET Research

DanaBot shifts its targeting to Europe, adds new features

DanaBot 2018-07-16 · SpiderLabs Blog · Fahim Abbasi

DanaBot Riding Fake MYOB Invoice Emails

DanaBot 2018-05-31 · Proofpoint · Proofpoint Staff

DanaBot - A new banking Trojan surfaces Down Under

DanaBot

▶ [TLP:WHITE] win_danabot_auto (20251219 | Detects win.danabot.)
