Dridex (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:42:30 UTC

OxCERT blog describes Dridex as "an evasive, information-stealing malware variant; its goal is to acquire as many credentials as possible and return them via an encrypted tunnel to a Command-and-Control (C&C) server. These C&C servers are numerous and scattered all over the Internet, if the malware cannot reach one server it will try another. For this reason, network-based measures such as blocking the C&C IPs is effective only in the short-term."
According to MalwareBytes, "Dridex uses an older tactic of infection by attaching a Word document that utilizes macros to install malware. However, once new versions of Microsoft Office came out and users generally updated, such a threat subsided because it was no longer simple to infect a user with this method."
IBM X-Force discovered "a new version of the Dridex banking Trojan that takes advantage of a code injection technique called AtomBombing to infect systems. AtomBombing is a technique for injecting malicious code into the 'atom tables' that almost all versions of Windows uses to store certain application data. It is a variation of typical code injection attacks that take advantage of input validation errors to insert and to execute malicious code in a legitimate process or application. Dridex v4 is the first malware that uses the AtomBombing process to try and infect systems."

2024-02-12 · Estrellas's Blog ·
Unveiling custom packers: A comprehensive guide
Dridex Simda 2023-02-27 · PRODAFT Threat Intelligence · PRODAFT
RIG Exploit Kit: In-Depth Analysis
Dridex IcedID ISFB PureCrypter Raccoon RecordBreaker RedLine Stealer Royal Ransom Silence SmokeLoader Zloader 2022-10-31 · paloalto Netoworks: Unit42 · Or Chechik
Banking Trojan Techniques: How Financially Motivated Malware Became Infrastructure
Dridex Kronos TrickBot Zeus 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 2022-09-01 · IBM · Emmy Ebanks, Kevin Henson
Raspberry Robin and Dridex: Two Birds of a Feather
Dridex Raspberry Robin 2022-08-24 · Github (rad9800) · Rad Kawar
Malware Madness: EXCEPTION edition
Dridex 2022-07-09 · Artik Blue · Artik Blue
Malware analysis with IDA/Radare2 - Basic Unpacking (Dridex first stage)
Dridex 2022-06-13 · Jorge Testa · Jorge Testa
Killing The Bear - Evil Corp
FAKEUPDATES Babuk Blister DoppelPaymer Dridex Entropy FriedEx Hades Macaw Phoenix Locker WastedLoader WastedLocker 2022-06-02 · Mandiant · Mandiant Intelligence

To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions

FAKEUPDATES Blister Cobalt Strike DoppelPaymer Dridex FriedEx Hades LockBit Macaw MimiKatz Phoenix Locker WastedLocker 2022-05-24 · Deep instinct · Bar Block

Blame the Messenger: 4 Types of Dropper Malware in Microsoft Office & How to Detect Them

Dridex Emotet 2022-05-19 · Palo Alto Networks Unit 42 · Saqib Khanzada

Weaponization of Excel Add-Ins Part 2: Dridex Infection Chain Case Studies

Dridex 2022-05-10 · RiskIQ · RiskIQ

RiskIQ: Identifying Dridex C2 via SSL Certificate Patterns

Dridex 2022-04-27 · · ANSSI · ANSSI

LE GROUPE CYBERCRIMINEL FIN7

Bateleur BELLHOP Griffon SQLRat POWERSOURCE Andromeda BABYMETAL BlackCat BlackMatter BOOSTWRITE Carbanak Cobalt Strike DNSMessenger Dridex DRIFTPIN Gameover P2P MimiKatz Murofet Qadars Ranbyus SocksBot 2022-03-13 · Malcat · malcat team

Cutting corners against a Dridex downloader

Dridex 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 2022-02-23 · Sentinel LABS · Antonio Pirozzi, Antonis Terefos, Idan Weizman

Sanctions Be Damned | From Dridex to Macaw, The Evolution of Evil Corp

Dridex WastedLocker 2022-02-23 · SophosLabs Uncut · Andrew Brandt

Dridex bots deliver Entropy ransomware in recent attacks

Cobalt Strike Dridex Entropy 2022-02-08 · Intel 471 · Intel 471

PrivateLoader: The first step in many malware schemes

Dridex Kronos LockBit Nanocore RAT NjRAT PrivateLoader Quasar RAT RedLine Stealer Remcos SmokeLoader STOP Tofsee TrickBot Vidar 2022-02-01 · Sentinel LABS · Antonio Pirozzi, Antonis Terefos, Idan Weizman

Sanctions be Damned | From Dridex To Macaw, The Evolution of Evil Corp

Dridex FriedEx Hades Phoenix Locker WastedLocker 2022-01-18 · Recorded Future · Insikt Group®

2021 Adversary Infrastructure Report

BazarBackdoor Cobalt Strike Dridex IcedID QakBot TrickBot 2022-01-14 · RiskIQ · Jordan Herman

RiskIQ: Unique SSL Certificates and JARM Hash Connected to Emotet and Dridex C2 Servers

Dridex Emotet 2022-01-11 · muha2xmad · Muhammad Hasan Ali

Unpacking Dridex malware

Dridex 2022-01-09 · Atomic Matryoshka · z3r0day_504

Malware Headliners: Dridex

Dridex 2021-12-23 · Symantec · Siddhesh Chandrayan

Log4j Vulnerabilities: Attack Insights

Tsunami Conti Dridex Khonsari Orcus RAT TellYouThePass 2021-12-20 · InQuest · Nick Chalard

(Don't) Bring Dridex Home for the Holidays

DoppelDridex Dridex 2021-11-21 · Cyber-Anubis · Nidal Fikri

Dridex Trojan | Defeating Anti-Analysis | Strings Decryption | C&C Extraction

DoppelDridex Dridex 2021-11-16 · Yoroi · Carmelo Ragusa, Luca Mella, Luigi Martire

Office Documents: May the XLL technique change the threat Landscape in 2022?

Agent Tesla Dridex Formbook 2021-11-12 · Recorded Future · Insikt Group®

The Business of Fraud: Botnet Malware Dissemination

Mozi Dridex IcedID QakBot TrickBot 2021-09-15 · Palo Alto Networks Unit 42 · Anna Chung, Swetha Balla

Phishing Eager Travelers

Dridex 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 2021-08-19 · Blackberry · BlackBerry Research & Intelligence Team

BlackBerry Prevents: Threat Actor Group TA575 and Dridex Malware

Cobalt Strike Dridex TA575 2021-07-30 · HP · Patrick Schläpfer

Detecting TA551 domains

Valak Dridex IcedID ISFB QakBot 2021-07-02 · MalwareBookReports · muzi

Skip the Middleman: Dridex Document to Cobalt Strike

Cobalt Strike Dridex 2021-06-22 · Twitter (@Cryptolaemus1) · Cryptolaemus, dao ming si, Kirk Sayre

Tweet on TA575, a Dridex affiliate delivering cobaltstrike (packed withe Cryptone) directly via the macro docs

Cobalt Strike Dridex 2021-06-08 · Intel 471 · Intel 471

The blurry boundaries between nation-state actors and the cybercrime underground

Dridex Gameover P2P 2021-06-03 · YouTube (FIRST) · Felipe Domingues, Gustavo Palazolo

Breaking Dridex Malware

Dridex 2021-05-26 · DeepInstinct · Ron Ben Yizhak

A Deep Dive into Packing Software CryptOne

Cobalt Strike Dridex Emotet Gozi ISFB Mailto QakBot SmokeLoader WastedLocker Zloader 2021-04-21 · SophosLabs Uncut · Anand Aijan, Andrew Brandt, Markel Picado, Michael Wood, Sean Gallagher, Sivagnanam Gn, Suriya Natarajan

Nearly half of malware now use TLS to conceal communications

Agent Tesla Cobalt Strike Dridex SystemBC 2021-04-15 · Twitter (@felixw3000) · Felix

Tweet on Dridex's evasion technique

Dridex 2021-04-15 · Proofpoint · Selena Larson

Threat Actors Pair Tax-Themed Lures With COVID-19, Healthcare Themes

Dridex TrickBot 2021-04-12 · PTSecurity · PTSecurity

PaaS, or how hackers evade antivirus software

Amadey Bunitu Cerber Dridex ISFB KPOT Stealer Mailto Nemty Phobos Pony Predator The Thief QakBot Raccoon RTM SmokeLoader Zloader 2021-04-06 · Lexfo · Lexfo

Dridex Loader Analysis

Dridex 2021-03-31 · Red Canary · Red Canary

2021 Threat Detection Report

Shlayer Andromeda Cobalt Strike Dridex Emotet IcedID MimiKatz QakBot TrickBot 2021-03-29 · VMWare Carbon Black · Giovanni Vigna, Jason Zhang, Oleg Boyarchuk

Dridex Reloaded: Analysis of a New Dridex Campaign

Dridex 2021-03-18 · PRODAFT Threat Intelligence · PRODAFT

SilverFish GroupThreat Actor Report

Cobalt Strike Dridex Koadic 2021-03-17 · HP · HP Bromium

Threat Insights Report Q4-2020

Agent Tesla BitRAT ComodoSec Dridex Emotet Ficker Stealer Formbook Zloader 2021-03-11 · IBM · Dave McMillen, Limor Kessem

Dridex Campaign Propelled by Cutwail Botnet and Poisonous PowerShell Scripts

Cutwail Dridex 2021-03-01 · Group-IB · Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

Ransomware Uncovered 2020/2021

RansomEXX BazarBackdoor Buer Clop Conti DoppelPaymer Dridex Egregor IcedID Maze PwndLocker QakBot RansomEXX REvil Ryuk SDBbot TrickBot Zloader 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 2021-02-15 · Medium s2wlab · Sojun Ryu

Operation SyncTrek

AbaddonPOS Azorult Clop DoppelDridex DoppelPaymer Dridex PwndLocker 2021-02-07 · Technical Blog of Ali Aqeel · Ali Aqeel

Dridex Malware Analysis

Dridex 2021-02-02 · Twitter (@TheDFIRReport) · The DFIR Report

Tweet on recent dridex post infection activity

Cobalt Strike Dridex 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 2021-02-01 · Microsoft · Microsoft 365 Defender Threat Intelligence Team

What tracking an attacker email infrastructure tells us about persistent cybercriminal operations

Dridex Emotet Makop Ransomware SmokeLoader TrickBot 2021-01-19 · HP · Patrick Schläpfer

Dridex Malicious Document Analysis: Automating the Extraction of Payload URLs

Dridex 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 2021-01-04 · Check Point · Check Point Research

DRIDEX Stopping Serial Killer: Catching the Next Strike

Dridex 2021-01-01 · SecureWorks

Threat Profile: GOLD DRAKE

Cobalt Strike Dridex FriedEx Koadic MimiKatz WastedLocker Evil Corp 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD HERON

DoppelPaymer Dridex Empire Downloader DOPPEL SPIDER 2020-12-10 · US-CERT · FBI, MS-ISAC, US-CERT

Alert (AA20-345A): Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data

PerlBot Shlayer Agent Tesla Cerber Dridex Ghost RAT Kovter Maze MedusaLocker Nanocore RAT Nefilim REvil Ryuk Zeus 2020-11-20 · ZDNet · Catalin Cimpanu

The malware that usually installs ransomware and you need to remove right away

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DoppelPaymer Dridex Egregor Emotet FriedEx MegaCortex Phorpiex PwndLocker QakBot Ryuk SDBbot TrickBot Zloader 2020-11-18 · Sophos · Sophos

SOPHOS 2021 THREAT REPORT Navigating cybersecurity in an uncertain world

Agent Tesla Dridex TrickBot Zloader 2020-10-29 · CERT-FR · CERT-FR

LE MALWARE-AS-A-SERVICE EMOTET

Dridex Emotet ISFB QakBot 2020-10-15 · Department of Justice · Department of Justice

Officials Announce International Operation Targeting Transnational Criminal Organization QQAAZZ that Provided Money Laundering Services to High-Level Cybercriminals

Dridex ISFB TrickBot 2020-10-03 · Wikipedia · Wikpedia

Wikipedia Page: Maksim Yakubets

Dridex Feodo Evil Corp 2020-09-29 · PWC UK · Andy Auld

What's behind the increase in ransomware attacks this year?

DarkSide Avaddon Clop Conti DoppelPaymer Dridex Emotet FriedEx Mailto PwndLocker QakBot REvil Ryuk SMAUG SunCrypt TrickBot WastedLocker 2020-09-18 · AppGate · Felipe Duarte, Gustavo Palazolo

Reverse Engineering Dridex and Automating IOC Extraction

Dridex 2020-09-10 · SANS ISC InfoSec Forums · Brad Duncan

Recent Dridex activity

Dridex 2020-09-07 · Github (pan-unit42) · Brad Duncan

Collection of recent Dridex IOCs

Cutwail Dridex 2020-08-21 · Palo Alto Networks Unit 42 · Brad Duncan

Wireshark Tutorial: Decrypting HTTPS Traffic

Dridex 2020-08-20 · CERT-FR · CERT-FR

Development of the Activity of the TA505 Cybercriminal Group

AndroMut Bart Clop Dridex FlawedAmmyy FlawedGrace Get2 Locky Marap QuantLoader SDBbot ServHelper tRat 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 2020-08-03 · The DFIR Report

Dridex – From Word to Domain Dominance

Dridex 2020-07-17 · CERT-FR · CERT-FR

The Malware Dridex: Origins and Uses

Andromeda CryptoLocker Cutwail DoppelPaymer Dridex Emotet FriedEx Gameover P2P Gandcrab ISFB Murofet Necurs Predator The Thief Zeus 2020-06-24 · Morphisec · Arnold Osipov

Obfuscated VBScript Drops Zloader, Ursnif, Qakbot, Dridex

Dridex ISFB QakBot Zloader 2020-06-22 · · CERT-FR · CERT-FR

Évolution De Lactivité du Groupe Cybercriminel TA505

Amadey AndroMut Bart Clop Dridex FlawedGrace Gandcrab Get2 GlobeImposter Jaff Locky Marap Philadephia Ransom QuantLoader Scarab Ransomware SDBbot ServHelper Silence tRat TrickBot 2020-06-19 · Reaqta · Reaqta

Dridex: the secret in a PostMessage()

Dridex 2020-06-05 · Votiro · Votiro's Research Team

Anatomy of a Well-Crafted UPS, FedEx, and DHL Phishing Email During COVID-19

Dridex 2020-05-31 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

WastedLoader or DridexLoader?

Dridex WastedLocker 2020-05-27 · GAIS-CERT · GAIS-CERT

Dridex Banking Trojan Technical Analysis Report

Dridex 2020-05-25 · · CERT-FR · CERT-FR

Le Code Malveillant Dridex: Origines et Usages

Dridex 2020-05-25 · · CERT-FR · CERT-FR

INDICATEURS DE COMPROMISSION DU CERT-FR - Objet: Le code malveillant Dridex

Dridex 2020-05-21 · Intel 471 · Intel 471

A brief history of TA505

AndroMut Bart Dridex FlawedAmmyy FlawedGrace Gandcrab Get2 GlobeImposter Jaff Kegotip Locky Necurs Philadephia Ransom Pony QuantLoader Rockloader SDBbot ServHelper Shifu Snatch TrickBot 2020-03-30 · Intezer · Michael Kajiloti

Fantastic payloads and where we find them

Dridex Emotet ISFB TrickBot 2020-03-05 · Microsoft · Microsoft Threat Protection Intelligence Team

Human-operated ransomware attacks: A preventable disaster

Dharma DoppelPaymer Dridex EternalPetya Gandcrab Hermes LockerGoga MegaCortex MimiKatz REvil RobinHood Ryuk SamSam TrickBot WannaCryptor PARINACOTA 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 2020-03-03 · PWC UK · PWC UK

Cyber Threats 2019:A Year in Retrospect

KevDroid MESSAGETAP magecart AndroMut Cobalt Strike CobInt Crimson RAT DNSpionage Dridex Dtrack Emotet FlawedAmmyy FlawedGrace FriedEx Gandcrab Get2 GlobeImposter Grateful POS ISFB Kazuar LockerGoga Nokki QakBot Ramnit REvil Rifdoor RokRAT Ryuk shadowhammer ShadowPad Shifu Skipper StoneDrill Stuxnet TrickBot Winnti ZeroCleare APT41 MUSTANG PANDA Sea Turtle 2020-02-18 · Sophos Labs · Luca Nagy

Nearly a quarter of malware now communicates using TLS

Dridex IcedID TrickBot 2020-01-31 · Virus Bulletin · Michal Poslušný, Peter Kálnai

Rich Headers: leveraging this mysterious artifact of the PE format

Dridex Exaramel Industroyer Neutrino RCS Sathurbot 2020-01-01 · Secureworks · SecureWorks

GOLD DRAKE

Dridex Empire Downloader FriedEx Koadic MimiKatz 2020-01-01 · Secureworks · SecureWorks

GOLD HERON

DoppelPaymer Dridex Empire Downloader 2019-12-19 · KrebsOnSecurity · Brian Krebs

Inside ‘Evil Corp,’ a $100M Cybercrime Menace

Dridex Gameover P2P Zeus Evil Corp 2019-12-05 · U.S. Department of the Treasury · U.S. Department of the Treasury

Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware

Dridex 2019-09-09 · McAfee · Chintan Shah, Marc Rivero López, Thomas Roccia

Evolution of Malware Sandbox Evasion Tactics – A Retrospective Study

Cutwail Dridex Dyre Kovter Locky Phorpiex Simda 2019-08-13 · Adalogics · David Korczynski

The state of advanced code injections

Dridex Emotet Tinba 2019-07-12 · CrowdStrike · Bex Hartley, Brett Stone-Gross, Sergei Frankoff

BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0

DoppelDridex DoppelPaymer Dridex FriedEx 2019-05-14 · GovCERT.ch · GovCERT.ch

The Rise of Dridex and the Role of ESPs

Dridex 2018-12-18 · Trend Micro · Trendmicro

URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader

Dridex Emotet FriedEx ISFB 2018-01-26 · ESET Research · Michal Poslušný

FriedEx: BitPaymer ransomware the work of Dridex authors

Dridex FriedEx 2018-01-12 · Proofpoint · Proofpoint Staff

Holiday lull? Not so much

Dridex Emotet GlobeImposter ISFB Necurs PandaBanker UrlZone NARWHAL SPIDER 2017-08-01 · Panda Security · Panda Security

Malware Report: Dridex Version 4

Dridex 2017-07-25 · Github (viql) · Johannes Bader

Dridex Loot

Dridex 2017-07-18 · Elastic · Ashkan Hosseini

Ten process injection techniques: A technical survey of common and trending process injection techniques

Cryakl CyberGate Dridex FinFisher RAT Locky 2017-05-25 · Kaspersky Labs · Nikita Slepogin

Dridex: A History of Evolution

Dridex Feodo 2017-05-15 · Secureworks · Counter Threat Unit ResearchTeam

Evolution of the GOLD EVERGREEN Threat Group

CryptoLocker Dridex Dyre Gameover P2P Murofet TrickBot Zeus GOLD EVERGREEN 2017-02-28 · Security Intelligence · Magal Baz, Or Safran

Dridex’s Cold War: Enter AtomBombing

Dridex 2017-01-26 · Flashpoint · Flashpoint

Dridex Banking Trojan Returns, Leverages New UAC Bypass Method

Dridex 2016-02-16 · Symantec · Dick O'Brien

Dridex: Tidal waves of spam pushing dangerous financial Trojan

Dridex 2015-11-10 · CERT.PL · CERT.PL

Talking to Dridex (part 0) – inside the dropper

Dridex 2015-10-26 · Blueliv · Blueliv

Chasing cybercrime: network insights of Dyre and Dridex Trojan bankers

Dridex Dyre 2015-10-15 · BitSight · AnubisLabs

Dridex: Chasing a botnet from the inside

Dridex 2015-10-13 · Secureworks · Brett Stone-Gross

Dridex (Bugat v5) Botnet Takeover Operation

Dridex Evil Corp

▶ [TLP:WHITE] win_dridex_auto (20251219 | Detects win.dridex.)
