Ave Maria (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:56:32 UTC

Information stealer which uses AutoIT for wrapping.

2025-05-15 · Medium b.magnezi ·
Ave Maria Malware Analysis
Ave Maria 2024-04-13 · cyber5w · cyber5w, M4lcode
Analysis of malicious Microsoft office macros
AsyncRAT Ave Maria 2024-04-09 · kienmanowar Blog · m4n0w4r, Tran Trung Kien
[QuickNote] Phishing email distributes WarZone RAT via DBatLoader
Ave Maria DBatLoader 2024-02-12 · Europol · Europol
International cybercrime malware service targeting thousands of unsuspecting consumers dismantled
Ave Maria 2024-02-12 · BleepingComputer · Bill Toulas
FBI seizes Warzone RAT infrastructure, arrests malware vendor
Ave Maria 2024-02-09 · Department of Justice · Office of Public Affairs
International Cybercrime Malware Service Dismantled by Federal Authorities: Key Malware Sales and Support Actors in Malta and Nigeria Charged in Federal Indictments
Ave Maria 2023-11-16 · CISA · CISA
Scattered Spider
Ave Maria BlackCat Raccoon Vidar 2023-11-16 · CISA · CISA
Scattered Spider
BlackCat Ave Maria Raccoon Vidar 2023-10-25 · Cisco Talos · Asheer Malhotra, Vitor Ventura
Kazakhstan-associated YoroTrooper disguises origin of attacks as Azerbaijan
Ave Maria Loda YoroTrooper 2023-10-12 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q3 2023
FluBot AsyncRAT Ave Maria Cobalt Strike DCRat Havoc IcedID ISFB Nanocore RAT NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Stealc Tofsee Vidar 2023-09-08 · Gi7w0rm
Uncovering DDGroup — A long-time threat actor
AsyncRAT Ave Maria BitRAT DBatLoader NetWire RC Quasar RAT XWorm 2023-08-25 · Github (muha2xmad) · Muhammad Hasan Ali
Warzone RAT configuration extractor
Ave Maria 2023-08-25 · Github (muha2xmad) · Muhammad Hasan Ali
Technical analysis of WarZoneRAT malware
Ave Maria 2023-07-11 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q2 2023
Hydra AsyncRAT Aurora Stealer Ave Maria BumbleBee Cobalt Strike DCRat Havoc IcedID ISFB NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee 2023-06-23 · Securonix · Den Iyzvyk, Oleg Kolesnikov, Tim Peck

Detecting New MULTI#STORM Attack Campaign Involving Python-based Loader Masquerading as OneDrive Utilities to Drop Multiple RAT Payloads With Security Analytics

Ave Maria 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 2023-04-12 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q1 2023

FluBot Amadey AsyncRAT Aurora Ave Maria BumbleBee Cobalt Strike DCRat Emotet IcedID ISFB NjRAT QakBot RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee Vidar 2023-03-25 · kienmanowar Blog · m4n0w4r, Tran Trung Kien

[QuickNote] Decrypting the C2 configuration of Warzone RAT

Ave Maria 2023-02-03 · Huntress Labs · Chad Hudson

Ave Maria and the Chambers of Warzone RAT

Ave Maria 2023-01-17 · Qianxin · Red Raindrop Team

Kasablanka Group Probably Conducted Compaigns Targeting Russia

Ave Maria Loda 2022-11-24 · ExploitReversing · Alexandre Borges

Malware Analysis Series (MAS): Article 6

Ave Maria 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 2022-09-19 · Recorded Future · Insikt Group®

Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine

Ave Maria Colibri Loader DCRat 2022-07-21 · ASEC · ASEC Analysis Team

Malware Being Distributed by Disguising Itself as Icon of V3 Lite

Ave Maria 2022-05-31 · Uptycs · Pritam Salunkhe, Shilpesh Trivedi

WarzoneRAT Can Now Evade Detection With Process Hollowing

Ave Maria 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 2022-05-12 · FortiGuard Labs · Xiaopeng Zhang

Phishing Campaign Delivering Three Fileless Malware: AveMariaRAT / BitRAT / PandoraHVNC – Part I

Ave Maria BitRAT Pandora RAT 2022-05-12 · Morphisec · Hido Cohen

New SYK Crypter Distributed Via Discord

AsyncRAT Ave Maria Nanocore RAT NjRAT Quasar RAT RedLine Stealer 2022-05-02 · cocomelonc · cocomelonc

Malware development: persistence - part 3. COM DLL hijack. Simple C++ example

Agent.BTZ Ave Maria Konni Mosquito TurlaRPC 2021-12-16 · Blackberry · The BlackBerry Research & Intelligence Team

Threat Thursday: Warzone RAT Breeds a Litter of ScriptKiddies

Ave Maria 2021-10-21 · Netskope · Gustavo Palazolo

DBatLoader: Abusing Discord to Deliver Warzone RAT

Ave Maria DBatLoader 2021-09-23 · Talos · Asheer Malhotra, Justin Thattil, Vanja Svajcer

Operation “Armor Piercer:” Targeted attacks in the Indian subcontinent using commercial RATs

Ave Maria NetWire RC 2021-09-20 · Trend Micro · Aliakbar Zahravi, William Gamazo Sanchez

Water Basilisk Uses New HCrypt Variant to Flood Victims with RAT Payloads

Ave Maria BitRAT LimeRAT Nanocore RAT NjRAT Quasar RAT 2021-09-13 · Trend Micro · Daniel Lunghi, Jaromír Hořejší

APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs (IOCs)

AsyncRAT Ave Maria BitRAT Imminent Monitor RAT LimeRAT NjRAT Remcos 2021-09-13 · Trend Micro · Daniel Lunghi, Jaromír Hořejší

APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs

AsyncRAT Ave Maria BitRAT Imminent Monitor RAT LimeRAT NjRAT Remcos 2021-07-21 · Youtube (OALabs) · OALabs

Warzone RAT Config Extraction With Python and IDA Pro

Ave Maria 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 2021-07-01 · Quick Heal · Ayush Puri

WARZONE RAT – Beware Of The Trojan Malware Stealing Data Triggering From Various Office Documents

Ave Maria 2021-05-19 · Youtube (OALabs) · Sergei Frankoff

Reverse Engineering Warzone RAT - Part 1

Ave Maria 2021-02-28 · PWC UK · PWC UK

Cyber Threats 2020: A Year in Retrospect

elf.wellmess FlowerPower PowGoop 8.t Dropper Agent.BTZ Agent Tesla Appleseed Ave Maria Bankshot BazarBackdoor BLINDINGCAN Chinoxy Conti Cotx RAT Crimson RAT DUSTMAN Emotet FriedEx FunnyDream Hakbit Mailto Maze METALJACK Nefilim Oblique RAT Pay2Key PlugX QakBot REvil Ryuk StoneDrill StrongPity SUNBURST SUPERNOVA TrickBot TurlaRPC Turla SilentMoon WastedLocker WellMess Winnti ZeroCleare APT10 APT23 APT27 APT31 APT41 BlackTech BRONZE EDGEWOOD Inception Framework MUSTANG PANDA Red Charon Red Nue Sea Turtle Tonto Team 2021-02-06 · · Clairvoyance Security Lab · Advanced threat research team

Mo Luoxiu (Confucius) organizes a new round of secret theft attacks on South Asian military enterprises

Ave Maria 2021-01-27 · Youtube (OALabs) · Sergei Frankoff

IDA Pro Decompiler Basics Microcode and x86 Calling Conventions

Ave Maria 2021-01-21 · · 360 Threat Intelligence Center · Advanced Threat Institute

Disclosure of Manling Flower Organization (APT-C-08) using Warzone RAT attack

Ave Maria 2021-01-12 · Uptycs · Abhijit Mohanta, Ashwin Vamshi

Confucius APT deploys Warzone RAT

Ave Maria Confucius 2020-12-21 · Cisco Talos · JON MUNSHAW

2020: The year in malware

WolfRAT Prometei Poet RAT Agent Tesla Astaroth Ave Maria CRAT Emotet Gozi IndigoDrop JhoneRAT Nanocore RAT NjRAT Oblique RAT SmokeLoader StrongPity WastedLocker Zloader 2020-11-30 · Medium Asuna Amawaka · Asuna Amawaka

Do you want to bake a donut? Come on, let’s go update~ Go away, Maria.

Ave Maria 2020-11-25 · Uptycs · Abhijit Mohanta, Shilpesh Trivedi

Warzone RAT comes with UAC bypass technique

Ave Maria 2020-11-03 · Kaspersky Labs · GReAT

APT trends report Q3 2020

WellMail EVILNUM Janicab Poet RAT AsyncRAT Ave Maria Cobalt Strike Crimson RAT CROSSWALK Dtrack LODEINFO MoriAgent Okrum PlugX POISONPLUG Rover ShadowPad SoreFang Winnti 2020-09-02 · Cisco Talos · Edmund Brumaghin, Holger Unterbrink

Salfram: Robbing the place without removing your name tag

Ave Maria ISFB SmokeLoader Zloader 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 2020-02-03 · Check Point Research · Yaroslav Harakhavik

Warzone: Behind the enemy lines

Ave Maria 2019-07-25 · Team Cymru · Team Cymru

Unmasking AVE_MARIA

Ave Maria 2019-05-08 · Kaspersky Labs · Kaspersky Labs

Fin7 hacking group targets more than 130 companies after leaders’ arrest

Ave Maria ANTHROPOID SPIDER 2019-05-08 · Kaspersky Labs · Félix Aime, Yury Namestnikov

FIN7.5: the infamous cybercrime rig “FIN7” continues its activities

Griffon Ave Maria FIN7 2019-04-11 · Reaqta · Reaqta

Ave_Maria Malware: there's more than meets the eye

Ave Maria 2019-03-01 · Morphisec · Alon Groisman

Threat Alert: AVE Maria infostealer on the rise

Ave Maria 2019-01-11 · Cybaze-Yorio Z-Lab · Antonio Farina, Antonio Pirozzi, Luca Mella

The “AVE_MARIA” Malware

Ave Maria

▶ [TLP:WHITE] win_ave_maria_auto (20251219 | Detects win.ave_maria.)
