Agent Tesla (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:54:37 UTC

A .NET based information stealer readily available to actors due to leaked builders. The malware is able to log keystrokes, can access the host's clipboard and crawls the disk for credentials or other valuable information. It has the capability to send information back to its C&C via HTTP(S), SMTP, FTP, or towards a Telegram channel.

2026-02-25 · FortiGuard Labs · Ariel Davidpur
Unmasking Agent Tesla: A Deep Dive into a Multi-Stage Campaign
Agent Tesla 2025-11-02 · Symantec · Broadcom, Symantec
Multi-Stage In-Memory Agent Tesla Campaign Targets LATAM
Agent Tesla 2024-10-16 · BitSight · André Tavares
Exfiltration over Telegram Bots: Skidding Infostealer Logs
404 Keylogger Agent Tesla 2024-08-01 · Idan Malihi
Dissecting Agent Tesla: Unveiling Threat Vectors and Defense Mechanisms
Agent Tesla 2024-06-06 · Medium b.magnezi · 0xMrMagnezi
Agent Tesla Analysis
Agent Tesla 2024-05-14 · Check Point Research · Antonis Terefos, Tera0017
Foxit PDF “Flawed Design” Exploitation
Rafel RAT Agent Tesla AsyncRAT DCRat DONOT Nanocore RAT NjRAT Pony Remcos Venom RAT XWorm
2024-05-06 · Cyber-Forensics · Cyber-Forensics
Agent Tesla Malware Analysis
Agent Tesla 2024-04-15 · Positive Technologies · Aleksandr Badaev, Kseniya Naumova
SteganoAmor campaign: TA558 mass-attacking companies and public institutions all around the world
LokiBot 404 Keylogger Agent Tesla CloudEyE Formbook Remcos XWorm 2024-04-02 · Check Point Research · Antonis Terefos, Raman Ladutska
Agent Tesla Targeting United States & Australia: Revealing the Attackers' Identities
Agent Tesla Bignosa 2024-03-26 · EchoCTI · Bilal BAKARTEPE, bixploit
Agent Tesla Technical Analysis Report
Agent Tesla 2024-03-01 · Ryan Weil · Ryan Weil
Agent Tesla Analysis [Part 2: Deobfuscation]
Agent Tesla 2024-03-01 · Logpoint · Nischal khadgi
A Comprehensive Overview on Stealer Malware Families
Agent Tesla Formbook RedLine Stealer Remcos Vidar 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 2024-02-16 · Medium b.magnezi · 0xMrMagnezi
Malware Analysis — AgentTesla
Agent Tesla 2024-02-06 · Medium osamaellahi · Osama Ellahi

Unfolding Agent Tesla: The Art of Credentials Harvesting.

Agent Tesla 2024-02-02 · Stairwell · Threat Research at Stairwell

Proactive response: AnyDesk, any breach

Agent Tesla 2024-01-09 · BitSight · André Tavares

Data Insights on AgentTesla and OriginLogger Victims

Agent Tesla OriginLogger 2024-01-08 · YouTube (Embee Research) · Embee_research

Javascript Malware Analysis - Decoding an AgentTesla Loader

Agent Tesla 2023-12-20 · ropgadget.com · Jeff White

The Origin of OriginLogger & Agent Tesla

Agent Tesla OriginLogger 2023-10-12 · Cluster25 · Cluster25 Threat Intel Team

CVE-2023-38831 Exploited by Pro-Russia Hacking Groups in RU-UA Conflict Zone for Credential Harvesting Operations

Agent Tesla Crimson RAT Nanocore RAT SmokeLoader 2023-10-01 · Infinitum IT · Kerime Gencay

Agent Tesla Technical Analysis Report (Paywall)

Agent Tesla 2023-09-29 · Intrinsec · CTI Intrinsec, Intrinsec

Ongoing threats targeting the energy industry

Agent Tesla CloudEyE 2023-08-29 · Viuleeenz · Alessandro Strino

Agent Tesla - Building an effective decryptor

Agent Tesla 2023-05-07 · Twitter (@embee_research) · Matthew

AgentTesla - Full Loader Analysis - Resolving API Hashes Using Conditional Breakpoints

Agent Tesla 2023-04-16 · OALabs · Sergei Frankoff

XORStringsNet

Agent Tesla RedLine Stealer 2023-04-10 · Check Point · Check Point

March 2023’s Most Wanted Malware: New Emotet Campaign Bypasses Microsoft Blocks to Distribute Malicious OneNote Files

Agent Tesla CloudEyE Emotet Formbook Nanocore RAT NjRAT QakBot Remcos Tofsee 2023-04-07 · Elastic · Salim Bitam

Attack chain leads to XWORM and AGENTTESLA

Agent Tesla XWorm 2023-03-30 · loginsoft · Saharsh Agrawal

From Innocence to Malice: The OneNote Malware Campaign Uncovered

Agent Tesla AsyncRAT DOUBLEBACK Emotet Formbook IcedID NetWire RC QakBot Quasar RAT RedLine Stealer XWorm 2023-03-23 · Logpoint · Anish Bogati

Emerging Threats: AgentTesla – A Review and Detection Strategies

Agent Tesla 2023-03-16 · Trend Micro · Cedric Pernet, Jaromír Hořejší, Loseway Lu

IPFS: A New Data Frontier or a New Cybercriminal Hideout?

Agent Tesla Formbook RedLine Stealer Remcos 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 2023-01-16 · Difesa & Sicurezza · Francesco Bussoletti

Cybercrime, RFQ from Turkey carries AgentTesla and zgRAT

Agent Tesla zgRAT 2022-12-18 · SANS ISC · Guy Bruneau

Infostealer Malware with Double Extension

Agent Tesla 2022-11-21 · Malwarebytes · Malwarebytes

2022-11-21 Threat Intel Report

404 Keylogger Agent Tesla Formbook Hive Remcos 2022-11-16 · splunk · Splunk Threat Research Team

Inside the Mind of a ‘Rat’ - Agent Tesla Detection and Analysis

Agent Tesla 2022-11-09 · Cisco Talos · Edmund Brumaghin

Threat Spotlight: Cyber Criminal Adoption of IPFS for Phishing, Malware Campaigns

Agent Tesla 2022-09-23 · Kaspersky · Artem Ushkov, Roman Dedenok

Mass email campaign with a pinch of targeted spam

Agent Tesla 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 2022-09-13 · Palo Alto Networks Unit 42 · Jeff White

OriginLogger: A Look at Agent Tesla’s Successor

Agent Tesla OriginLogger 2022-08-29 · · 360 netlab · wanghao

PureCrypter Loader continues to be active and has spread to more than 10 other families

404 Keylogger Agent Tesla AsyncRAT Formbook RedLine Stealer 2022-08-29 · 360 netlab · wanghao

PureCrypter is busy pumping out various malicious malware families

Agent Tesla PureCrypter RedLine Stealer 2022-08-17 · Secureworks · Counter Threat Unit ResearchTeam

DarkTortilla Malware Analysis

Agent Tesla AsyncRAT Cobalt Strike DarkTortilla Nanocore RAT RedLine Stealer 2022-07-30 · cocomelonc

Malware AV evasion - part 8. Encode payload via Z85

Agent Tesla Carbanak Carberp Cardinal RAT Cobalt Strike donut_injector 2022-07-20 · · Cert-UA · Cert-UA

Cyberattack on State Organizations of Ukraine using the topic OK "South" and the malicious program AgentTesla (CERT-UA#4987)

Agent Tesla 2022-07-12 · Team Cymru · Kyle Krejci

An Analysis of Infrastructure linked to the Hagga Threat Actor

Agent Tesla 2022-05-19 · Blackberry · The BlackBerry Research & Intelligence Team

.NET Stubs: Sowing the Seeds of Discord

Agent Tesla Quasar RAT WhisperGate 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 · Palo Alto Networks Unit 42 · Tyler Halfpop

Harmful Help: Analyzing a Malicious Compiled HTML Help File Delivering Agent Tesla

Agent Tesla 2022-05-05 · Malwarebytes Labs · Threat Intelligence Team

Nigerian Tesla: 419 scammer gone malware distributor unmasked

Agent Tesla 2022-04-20 · cocomelonc · cocomelonc

Malware development: persistence - part 1. Registry run keys. C++ example.

Agent Tesla Amadey BlackEnergy Cobian RAT COZYDUKE Emotet Empire Downloader Kimsuky 2022-04-15 · Center for Internet Security · CIS

Top 10 Malware March 2022

Mirai Shlayer Agent Tesla Ghost RAT Nanocore RAT SectopRAT solarmarker Zeus 2022-04-12 · Check Point · Check Point Research

March 2022’s Most Wanted Malware: Easter Phishing Scams Help Emotet Assert its Dominance

Alien FluBot Agent Tesla Emotet 2022-03-31 · APNIC · Debashis Pal

How to: Detect and prevent common data exfiltration attacks

Agent Tesla DNSMessenger PingBack Rising Sun 2022-03-26 · forensicitguy · Tony Lambert

An AgentTesla Sample Using VBA Macros and Certutil

Agent Tesla 2022-03-25 · GOV.UA · State Service of Special Communication and Information Protection of Ukraine (CIP)

Who is behind the Cyberattacks on Ukraine's Critical Information Infrastructure: Statistics for March 15-22

Xloader Agent Tesla CaddyWiper Cobalt Strike DoubleZero GraphSteel GrimPlant HeaderTip HermeticWiper IsaacWiper MicroBackdoor Pandora RAT 2022-03-07 · Fortinet · Fred Gutierrez, James Slaughter, Val Saengphaibul

Fake Purchase Order Used to Deliver Agent Tesla

Agent Tesla 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) 2022-03-04 · Bleeping Computer · Bill Toulas

Russia-Ukraine war exploited as lure for malware distribution

Agent Tesla Remcos 2022-03-04 · Bitdefender · Alina Bizga

Bitdefender Labs Sees Increased Malicious and Scam Activity Exploiting the War in Ukraine

Agent Tesla Remcos 2022-02-23 · · Weixin · 360 Threat Intelligence Center

APT-C-58 (Gorgon Group) attack warning

Agent Tesla 2022-02-06 · forensicitguy · Tony Lambert

AgentTesla From RTF Exploitation to .NET Tradecraft

Agent Tesla 2022-02-02 · Qualys · Ghanshyam More

Catching the RAT called Agent Tesla

Agent Tesla 2022-01-25 · Palo Alto Networks Unit 42 · Yaron Samuel

Weaponization of Excel Add-Ins Part 1: Malicious XLL Files and Agent Tesla Case Studies

Agent Tesla 2022-01-24 · Proofpoint · Proofpoint

DTPacker – a .NET Packer with a Curious Password

Agent Tesla TA2536 2022-01-24 · Netskope · Ghanashyam Satpathy, Gustavo Palazolo

Infected PowerPoint Files Using Cloud Services to Deliver Multiple Malware

Agent Tesla 2022-01-21 · MalGamy · Gameel Ali

Deep Analysis Agent Tesla Malware

Agent Tesla 2022-01-12 · Guillaume Orlando

2021 Gorgon Group APT Operation

Agent Tesla 2022-01-12 · MalGamy

Deep analysis agent tesla malware

Agent Tesla 2022-01-12 · Guillaume Orlando

Malware Analysis - AgentTesla v3

Agent Tesla 2022-01-03 · forensicitguy · Tony Lambert

A Tale of Two Dropper Scripts for Agent Tesla

Agent Tesla 2021-12-31 · InfoSec Handlers Diary Blog · Jan Kopriva

Do you want your Agent Tesla in the 300 MB or 8 kB package?

Agent Tesla 2021-12-30 · InfoSec Handlers Diary Blog · Brad Duncan

Agent Tesla Updates SMTP Data Exfiltration Technique

Agent Tesla 2021-12-20 · InfoSec Handlers Diary Blog · Alef Nula, Jan Kopriva

PowerPoint attachments, Agent Tesla and code reuse in malware

Agent Tesla 2021-12-17 · Yoroi · Carmelo Ragusa, Luca Mella, Luigi Martire

Serverless InfoStealer delivered in Est European Countries

Agent Tesla 2021-12-08 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal

Full malware analysis Work-Flow of AgentTesla Malware

Agent Tesla 2021-12-06 · MalwareBookReports · muzi

AGENT TESLAGGAH

Agent Tesla 2021-12-02 · · AhnLab · ASEC Analysis Team

Spreading AgentTesla through more sophisticated malicious PPT

Agent Tesla 2021-11-22 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal

Powershell and DnSpy tricks in .NET reversing – AgentTesla [Part1]

Agent Tesla 2021-11-22 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal

Powershell and DnSpy tricks in .NET reversing – AgentTesla [Part2]

Agent Tesla 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 · Living Code · Dominik Degroot

AgentTesla dropped via NSIS installer

Agent Tesla 2021-11-02 · InQuest · Dmitry Melikov

Adults Only Malware Lures

Agent Tesla 2021-10-06 · zimperium · Jordan Herman

Malware Distribution with Mana Tools

Agent Tesla Azorult 2021-09-15 · Telsy · Telsy

REMCOS and Agent Tesla loaded into memory with Rezer0 loader

Agent Tesla Remcos 2021-09-08 · Juniper · Paul Kimayong

Aggah Malware Campaign Expands to Zendesk and GitHub to Host Its Malware

Agent Tesla 2021-07-28 · RiskIQ · Jennifer Grob, Jordan Herman

Use of XAMPP Web Component to Identify Agent Tesla Infrastructure

Agent Tesla 2021-07-24 · InfoSec Handlers Diary Blog · Xavier Mertens

Agent.Tesla Dropped via a .daa Image and Talking to Telegram

Agent Tesla 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 2021-07-12 · 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 2021-06-29 · Yoroi · Luca Mella, Luigi Martire

The "WayBack” Campaign: a Large Scale Operation Hiding in Plain Sight

Agent Tesla Cobian RAT Oski Stealer 2021-06-24 · Trustwave · Diana Lopera

Yet Another Archive Format Smuggling Malware

Agent Tesla 2021-06-24 · Blackberry · The BlackBerry Research and Intelligence Team

Threat Thursday: Agent Tesla Infostealer

Agent Tesla 2021-06-11 · · NSFOCUS · Fuying Laboratory

Nigerian Hacker Organization SWEED is Distributing Phishing Documents Targeting the Logistics Industry

Agent Tesla 2021-06-04 · Fortinet · Xiaopeng Zhang

Phishing Malware Hijacks Bitcoin Addresses and Delivers New Agent Tesla Variant

Agent Tesla 2021-06-02 · Sophos · Sean Gallagher

AMSI bypasses remain tricks of the malware trade

Agent Tesla Cobalt Strike Meterpreter 2021-05-18 · Youtube (AhmedS Kasmani) · AhmedS Kasmani

Malware Analysis: Agent Tesla Part 1/2 Extraction of final payload from dropper.

Agent Tesla 2021-05-11 · Twitter (@MsftSecIntel) · Microsoft Security Intelligence

Tweet on Snip3 crypter delivering AsyncRAT or AgentTesla

Agent Tesla AsyncRAT 2021-05-11 · VMRay · Mateusz Lukaszewski, VMRay Labs Team

Threat Bulletin: Exploring the Differences and Similarities of Agent Tesla v2 & v3

Agent Tesla 2021-05-07 · Morphisec · Nadav Lorber

Revealing the ‘Snip3’ Crypter, a Highly Evasive RAT Loader

Agent Tesla AsyncRAT NetWire RC Revenge RAT 2021-05-05 · Zscaler · Aniruddha Dolas, Manohar Ghule, Mohd Sadique

Catching RATs Over Custom Protocols Analysis of top non-HTTP/S threats

Agent Tesla AsyncRAT Crimson RAT CyberGate Ghost RAT Nanocore RAT NetWire RC NjRAT Quasar RAT Remcos 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 2021-04-04 · menshaway blogspot · Mahmoud Morsy

Technical report of AgentTesla

Agent Tesla 2021-03-17 · HP · HP Bromium

Threat Insights Report Q4-2020

Agent Tesla BitRAT ComodoSec Dridex Emotet Ficker Stealer Formbook Zloader 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 2021-02-25 · Minerva · Minerva Labs

Preventing AgentTelsa Infiltration

Agent Tesla 2021-02-12 · Trustwave · Diana Lopera, Rodel Mendrez

The Many Roads Leading To Agent Tesla

Agent Tesla 2021-02-12 · InfoSec Handlers Diary Blog · Xavier Mertens

AgentTesla Dropped Through Automatic Click in Microsoft Help File

Agent Tesla 2021-02-11 · InfoSec Handlers Diary Blog · Jan Kopriva

Agent Tesla hidden in a historical anti-malware tool

Agent Tesla 2021-01-21 · DENEXUS · Markel Picado

Spear Phishing Targeting ICS Supply Chain - Analysis

Agent Tesla 2021-01-11 · ESET Research · Matías Porolli

Operation Spalax: Targeted malware attacks in Colombia

Agent Tesla AsyncRAT NjRAT Remcos 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 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD GALLEON

Agent Tesla HawkEye Keylogger Pony GOLD GALLEON 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 2020-12-18 · Trend Micro · Junestherry Salvador, Matthew Camacho, Raphael Centeno

Negasteal Uses Hastebin for Fileless Delivery of Crysis Ransomware

Agent Tesla Dharma 2020-12-15 · Cofense · Aaron Riley

Strategic Analysis: Agent Tesla Expands Targeting and Networking Capabilities

Agent Tesla 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 2020-12-07 · Proofpoint · Proofpoint Threat Research Team

Commodity .NET Packers use Embedded Images to Hide Payloads

Agent Tesla Loki Password Stealer (PWS) Remcos 2020-12-04 · Inde · Chris Campbell

Inside a .NET Stealer: AgentTesla

Agent Tesla 2020-12-03 · Telsy · Telsy Research Team

When a false flagdoesn’t work: Exploring the digital-crimeunderground at campaign preparation stage

Agent Tesla 2020-11-27 · HP · Alex Holland

Aggah Campaign’s Latest Tactics: Victimology, PowerPoint Dropper and Cryptocurrency Stealer

Agent Tesla 2020-11-18 · Sophos · Sophos

SOPHOS 2021 THREAT REPORT Navigating cybersecurity in an uncertain world

Agent Tesla Dridex TrickBot Zloader 2020-11-18 · G Data · G-Data

Business as usual: Criminal Activities in Times of a Global Pandemic

Agent Tesla Nanocore RAT NetWire RC Remcos 2020-11-05 · Morphisec · Michael Gorelik

Agent Tesla: A Day in a Life of IR

Agent Tesla 2020-10-16 · Hornetsecurity · Hornetsecurity Security Lab

VBA Purging Malspam Campaigns

Agent Tesla Formbook 2020-10-05 · Juniper · Paul Kimayong

New pastebin-like service used in multiple malware campaigns

Agent Tesla LimeRAT RedLine Stealer 2020-09-03 · Medium mariohenkel · Mario Henkel

Decrypting AgentTesla strings and config

Agent Tesla 2020-08-27 · MalWatch · MalWatch

Win.Trojan.AgentTesla - Malware analysis & threat intelligence report

Agent Tesla 2020-08-26 · Lab52 · Jagaimo Kawaii

A twisted malware infection chain

Agent Tesla Loki Password Stealer (PWS) 2020-08-10 · SentinelOne · Jim Walter

Agent Tesla | Old RAT Uses New Tricks to Stay on Top

Agent Tesla 2020-08-10 · Seqrite · Pavankumar Chaudhari

Gorgon APT targeting MSME sector in India

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

Evolution of Excel 4.0 Macro Weaponization

Agent Tesla DanaBot ISFB TrickBot Zloader 2020-05-23 · InfoSec Handlers Diary Blog · Xavier Mertens

AgentTesla Delivered via a Malicious PowerPoint Add-In

Agent Tesla 2020-05-22 · Yoroi · Antonio Pirozzi, Giacomo d'Onofrio, Luca Mella, Luigi Martire

Cyber-Criminal espionage Operation insists on Italian Manufacturing

Agent Tesla 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 2020-04-16 · Malwarebytes · Hossein Jazi

New AgentTesla variant steals WiFi credentials

Agent Tesla 2020-04-15 · Suraj Malhotra

How Analysing an AgentTesla Could Lead To Attackers Inbox - Part II

Agent Tesla 2020-04-14 · Palo Alto Networks Unit 42 · Adrian McCabe, Juan Cortes, Vicky Ray

Malicious Attackers Target Government and Medical Organizations With COVID-19 Themed Phishing Campaigns

Agent Tesla EDA2 2020-04-13 · Suraj Malhotra

How Analysing an AgentTesla Could Lead To Attackers Inbox - Part I

Agent Tesla 2020-04-05 · MalwrAnalysis · Anurag

Trojan Agent Tesla – Malware Analysis

Agent Tesla 2020-03-24 · RiskIQ · Wes Smiley

Exploring Agent Tesla Infrastructure

Agent Tesla 2020-03-18 · Proofpoint · Axel F, Sam Scholten

Coronavirus Threat Landscape Update

Agent Tesla Get2 ISFB Remcos 2020-02-26 · MalwareLab.pl · Maciej Kotowicz

(Ab)using bash-fu to analyze recent Aggah sample

Agent Tesla 2020-02-02 · Sophos Labs · Markel Picado, Sean Gallagher

Agent Tesla amps up information stealing attacks

Agent Tesla 2020-01-01 · Secureworks · SecureWorks

GOLD GALLEON

Agent Tesla HawkEye Keylogger Pony Predator The Thief 2019-09-26 · Proofpoint · Bryan Campbell, Jeremy Hedges, Proofpoint Threat Insight Team

New WhiteShadow downloader uses Microsoft SQL to retrieve malware

WhiteShadow Agent Tesla Azorult Crimson RAT Formbook Nanocore RAT NetWire RC NjRAT Remcos 2019-07-15 · Cisco Talos · Edmund Brumaghin

SWEED: Exposing years of Agent Tesla campaigns

Agent Tesla Formbook Loki Password Stealer (PWS) SWEED 2019-07-01 · Talos Intelligence · Holger Unterbrink

RATs and stealers rush through “Heaven’s Gate” with new loader

Agent Tesla HawkEye Keylogger Remcos 2018-04-18 · Secureworks · Counter Threat Unit ResearchTeam

GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry

Agent Tesla HawkEye Keylogger Pony GOLD GALLEON 2018-04-05 · Fortinet · Xiaopeng Zhang

Analysis of New Agent Tesla Spyware Variant

Agent Tesla 2018-01-12 · Stormshield · Rémi Jullian

Analyzing an Agent Tesla campaign: from a word document to the attacker credentials

Agent Tesla 2017-09-25 · Palo Alto Networks Unit 42 · Jeff White

Analyzing the Various Layers of AgentTesla’s Packing

Agent Tesla 2017-06-28 · Fortinet · Xiaopeng Zhang

In-Depth Analysis of A New Variant of .NET Malware AgentTesla

Agent Tesla 2016-08-01 · Zscaler · Deepen Desai

Agent Tesla Keylogger delivered using cybersquatting

Agent Tesla

- ▶ [TLP:WHITE] win_agent_tesla_w0 (20190731 | No description)
- ▶ [TLP:WHITE] win_agent_tesla_w1 (20200506 | Detect Agent Tesla based on common .NET code sequences)
