FlawedAmmyy (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:00:06 UTC

FlawedAmmyy is a well-known Remote Access Tool (RAT) attributed to criminal gang TA505 and used to get the control of target machines. The name reminds the strong link with the leaked source code of Ammyy Admin from which it took the main structure.

2021-06-16 · · Національної поліції України ·
Cyberpolice exposes hacker group in spreading encryption virus and causing half a billion dollars in damage to foreign companies
Clop Cobalt Strike FlawedAmmyy 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 2020-05-21 · 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 2020-05-20 · PTSecurity · PT ESC Threat Intelligence
Operation TA505: how we analyzed new tools from the creators of the Dridex trojan, Locky ransomware, and Neutrino botnet
FlawedAmmyy 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 2020-02-28 · Financial Security Institute · Financial Security Institute
Profiling of TA505 Threat Group That Continues to Attack the Financial Sector
Amadey Clop FlawedAmmyy Rapid Ransom SDBbot TinyMet 2020-02-13 · Qianxin · Qi Anxin Threat Intelligence Center

APT Report 2019

Chrysaor Exodus Dacls VPNFilter DNSRat Griffon KopiLuwak More_eggs SQLRat AppleJeus BONDUPDATER Agent.BTZ Anchor AndroMut AppleJeus BOOSTWRITE Brambul Carbanak Cobalt Strike Dacls DistTrack DNSpionage Dtrack ELECTRICFISH FlawedAmmyy FlawedGrace Get2 Grateful POS HOPLIGHT Imminent Monitor RAT jason Joanap KerrDown KEYMARBLE Lambert LightNeuron LoJax MiniDuke PolyglotDuke PowerRatankba Rising Sun SDBbot ServHelper Snatch Stuxnet TinyMet tRat TrickBot Volgmer X-Agent Zebrocy 2020-01-01 · Secureworks · SecureWorks

GOLD TAHOE

Clop FlawedAmmyy FlawedGrace Get2 SDBbot ServHelper TA505 2019-08-29 · ThreatRecon · ThreatRecon Team

SectorJ04 Group’s Increased Activity in 2019

FlawedAmmyy ServHelper TA505 2019-08-27 · Trend Micro · Hara Hiroaki, Jaromír Hořejší, Loseway Lu

TA505 At It Again: Variety is the Spice of ServHelper and FlawedAmmyy

FlawedAmmyy ServHelper 2019-07-02 · Proofpoint · Dennis Schwarz, Matthew Mesa, Proofpoint Threat Insight Team

TA505 begins summer campaigns with a new pet malware downloader, AndroMut, in the UAE, South Korea, Singapore, and the United States

AndroMut FlawedAmmyy 2019-05-31 · Youtube (0verfl0w_) · 0verfl0w_

Defeating Commercial and Custom Packers like a Pro - VMProtect, ASPack, PECompact, and more

FlawedAmmyy Ramnit 2019-05-28 · MITRE · MITRE

FlawedAmmyy

FlawedAmmyy 2019-04-22 · SANS · Mike Downey

Unpacking & Decrypting FlawedAmmyy

FlawedAmmyy 2018-10-01 · · Macnica Networks · Macnica Networks

Trends in cyber espionage (targeted attacks) targeting Japan | First half of 2018

Anel Cobalt Strike Datper FlawedAmmyy Quasar RAT RedLeaves taidoor Winnti xxmm 2018-07-19 · Proofpoint · Proofpoint Staff

TA505 Abusing SettingContent-ms within PDF files to Distribute FlawedAmmyy RAT

FlawedAmmyy 2018-06-28 · Secrary Blog · Lasha Khasaia

A Brief Overview of the AMMYY RAT Downloader

FlawedAmmyy 2018-03-07 · Proofpoint · Proofpoint Staff

Leaked Ammyy Admin Source Code Turned into Malware

FlawedAmmyy QuantLoader 2016-10-11 · Symantec · Symantec Security Response

Odinaff: New Trojan used in high level financial attacks

Batel FlawedAmmyy Odinaff RMS FIN7

▶ [TLP:WHITE] win_flawedammyy_auto (20251219 | Detects win.flawedammyy.)
