Andromeda (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:08:49 UTC

There is no description at this point.

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 2023-01-24 · Trellix · Daksh Kapur, John Fokker, Robert Venal, Tomer Shloman
Cyberattacks Targeting Ukraine Increase 20-fold at End of 2022 Fueled by Russia-linked Gamaredon Activity
Andromeda Formbook Houdini Remcos 2023-01-05 · Mandiant · Eduardo Mattos, Gabby Roncone, John Wolfram, Sarah Hawley, Tyler McLellan
Turla: A Galaxy of Opportunity
KopiLuwak Andromeda QUIETCANARY 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 2021-11-18 · Red Canary · The Red Canary Team
Intelligence Insights: November 2021
Andromeda Conti LockBit QakBot Squirrelwaffle 2021-03-31 · Red Canary · Red Canary
2021 Threat Detection Report
Shlayer Andromeda Cobalt Strike Dridex Emotet IcedID MimiKatz QakBot TrickBot 2020-12-16 · CrowdStrike · David Rojas, Mark Robinson
Hiding in Plain Sight: Remediating “Hidden” Malware with Real Time Response
Andromeda 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 2020-03-15 · The Shadowserver Foundation · Shadowserver Foundation
Has The Sun Set On The Necurs Botnet?
Andromeda Cutwail Kelihos Necurs Pushdo 2018-02-08 · Virus Bulletin · Bahare Sabouri, He Xu
A review of the evolution of Andromeda over the years before we say goodbye
Andromeda 2017-12-04 · Microsoft · Microsoft Defender ATP Research Team, Microsoft Digital Crimes Unit
Microsoft teams up with law enforcement and other partners to disrupt Gamarue (Andromeda)
Andromeda 2017-12-04 · Europol · Europol
Andromeda botnet dismantled in international cyber operation
Andromeda 2017-03-13 · Morphisec · Roy Moshailov
Moving Target Defense Blog
Andromeda 2016-04-06 · Avast · Threat Intelligence Team
Andromeda under the microscope

Andromeda 2016-03-01 · Proofpoint · Darien Huss

Operation Transparent Tribe

Andromeda beendoor Bezigate Crimson RAT Luminosity RAT Operation C-Major 2015-09-29 · InfoSec Institute · Ayoub Faouzi

Andromeda Bot Analysis part 1

Andromeda 2015-09-29 · InfoSec Institute · Ayoub Faouzi

Andromeda Bot Analysis part 2

Andromeda 2015-04-17 · Eternal Todo · Jose Miguel Esparza

Andromeda/Gamarue bot loves JSON too (new versions details)

Andromeda 2015-04-15 · ByteAtlas

Knowledge Fragment: Bruteforcing Andromeda Configuration Buffers

Andromeda 2013-09-01 · Eternal Todo · Jose Miguel Esparza

Yet another Andromeda / Gamarue analysis

Andromeda 2013-08-01 · Virus Bulletin · Suweera De Souza

Andromeda 2.7 features

Andromeda 2013-03-30 · 0xEBFE Blog about life · 0xEBFE

Fooled by Andromeda

Andromeda 2012-12-05 · Malware Don't Need Coffee · Kafeine

The path to infection - Eye glance at the first line of "Russian Underground" - focused on Ransomware

RunForestRun Andromeda Citadel Lyposit Matsnu Reveton Sinowal UPAS Urausy

▶ [TLP:WHITE] win_andromeda_auto (20251219 | Detects win.andromeda.)
