AdWind (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:38:48 UTC

AdWind

aka: AlienSpy, JSocket, Frutas, UNRECOM, JBifrost, Sockrat

URLhaus

Part of Malware-as-service platform
Used as a generic name for Java-based RAT
Functionality
- collect general system and user information
- terminate process
-log keystroke
-take screenshot and access webcam
- steal cache password from local or web forms
- download and execute Malware
- modify registry
- download components
- Denial of Service attacks
- Acquire VPN certificates

Initial infection vector
1. Email to JAR files attached
2. Malspam URL to downlaod the malware

Persistence
- Runkey - HKCU\Software\Microsoft\Windows\current version\run

Hiding
Uses attrib.exe

Notes on Adwind
The malware is not known to be proxy aware

References

2021-11-23 · HP ·
RATDispenser: Stealthy JavaScript Loader Dispensing RATs into the Wild

AdWind Ratty STRRAT CloudEyE Formbook Houdini Panda Stealer Remcos

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

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

2020-06-28 · Security-in-Bits · Security-in-Bits

Interesting tactic by Ratty & Adwind for distribution of JAR appended to signed MSI

AdWind Ratty

2020-04-29 · Zscaler · Sudeep Singh

Compromised Wordpress sites used to distribute Adwind RAT

AdWind

2019-05-20 · Check Point · Ben Herzog

Malware Against the C Monoculture

AdWind jRAT GhostMiner Zebrocy

2018-09-24 · Cisco Talos · Paul Rascagnères, Robert Perica, Tomislav Pericin, Vitor Ventura

Adwind Dodges AV via DDE

AdWind

2018-08-20 · Marco Ramilli's Blog · Marco Ramilli

Interesting hidden threat since years ?

AdWind

2018-03-12 · Github (herrcore) · Sergei Frankoff

Python decryptor for newer AdWind config file

AdWind

2018-02-16 · Fortinet · Xiaopeng Zhang

New jRAT/Adwind Variant Being Spread With Package Delivery Scam

AdWind

2017-10-03 · Seqrite · Pavankumar Chaudhari

Evolution of jRAT JAVA Malware

AdWind

2017-07-11 · Trend Micro · Marshall Chen, Rubio Wu Spam Campaign Delivers Cross-platform Remote Access Trojan Adwind AdWind
2017-07-04 · Malware Traffic Analysis · Brad Duncan MALSPAM WITH JAVA-BASED RAT AdWind
2015-12-08 · The Citizenlab · Claudio Guarnieri, John Scott-Railton, Marion Marschalek, Morgan Marquis-Boire Packrat: Seven Years of a South American Threat Actor AdWind Adzok CyberGate Xtreme RAT Packrat

Yara Rules

▶ [TLP:WHITE] jar_adwind_w0 (20170803 | Adwind RAT)	
▶ [TLP:WHITE] jar_adwind_w1 (20170803 | Alien Spy Remote Access Trojan)	

Download all Yara Rules
