ZXShell (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:43:23 UTC

ZXShell

aka: Sensocode

Actor(s): APT41, EMISSARY PANDA, Leviathan

According to FireEye, ZXSHELL is a backdoor that can be downloaded from the internet, particularly Chinese hacker websites. The backdoor can launch port scans, run a keylogger, capture screenshots, set up an HTTP or SOCKS proxy, launch a reverse command shell, cause SYN floods, and transfer/delete/run files. The publicly available version of the tool provides a graphical user interface that malicious actors can use to interact with victim backdoors. Simplified Chinese is the language used for the bundled ZXSHELL documentation.

References

2023-05-15 · Symantec · Threat Hunter Team
Lancefly: Group Uses Custom Backdoor to Target Orgs in Government, Aviation, Other Sectors
Merdoor PlugX ShadowPad ZXShell Lancefly

2022-07-18 · Palo Alto Networks Unit 42 · Unit 42
Iron Taurus
CHINACHOPPER Ghost RAT Wonknu ZXShell APT27

2022-05-09 · · Qianxin Threat Intelligence Center · Red Raindrops Team
Operation EviLoong: An electronic party of "borderless" hackers
ZXShell

2020-07-20 · Risky.biz · Daniel Gordon
What even is Winnti?
CCleaner Backdoor Ghost RAT PlugX ZXShell

2020-04-07 · Blackberry · Blackberry Research
Decade of the RATS: Cross-Platform APT Espionage Attacks Targeting Linux, Windows and Android
Penquin Turla XOR DDoS ZXShell

2020-01-13 · Lab52 · Jagaimo Kawaii
APT27 ZxShell RootKit module updates
ZXShell

2020-01-01 · Secureworks · SecureWorks
BRONZE KEYSTONE
9002 RAT BLACKCOFFEE DeputyDog Derusbi HiKit PlugX Poison Ivy ZXShell APT17

2020-01-01 · Secureworks · SecureWorks
BRONZE UNION
9002 RAT CHINACHOPPER Enfal Ghost RAT HttpBrowser HyperBro owaauth PlugX Poison Ivy ZXShell APT27

2019-11-19 · FireEye · Kelli Vanderlee, Nalani Fraser
Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions
MESSAGETAP TSCookie ACEHASH CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT HIGHNOON HTran MimiKatz NetWire RC POISONPLUG Poison Ivy pupy Quasar RAT ZXShell

2019-11-06 · VirusBulletin · Bowen Pan, Lion Gu
A vine climbing over the Great Firewall: a long-term attack against China
Poison Ivy ZXShell GreenSpot

2019-09-23 · MITRE · MITRE ATT&CK
APT41
Derusbi MESSAGETAP Winnti ASPXSpy BLACKCOFFEE CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT MimiKatz NjRAT PlugX ShadowPad Winnti ZXShell APT41

2019-09-19 · MeltX0R
Emissary Panda APT: Recent infrastructure and RAT analysis
ZXShell

2019-02-27 · Secureworks · CTU Research Team
A Peek into BRONZE UNION's Toolbox
Ghost RAT HyperBro ZXShell

2019-01-01 · Virus Bulletin · Bowen Pan, Lion Gu
A vine climbing over the Great Firewall: A long-term attack against China
Poison Ivy ZXShell

2017-05-31 · MITRE · MITRE ATT&CK
Axiom
Derusbi 9002 RAT BLACKCOFFEE Derusbi Ghost RAT HiKit PlugX ZXShell APT17

2016-10-28 · Github (smb01) · smb01
zxshell repository
ZXShell

2014-10-28 · Cisco · Alain Zidouemba, Andrea Allievi, Douglas Goddard, Shaun Hurley
Threat Spotlight: Group 72, Opening the ZxShell
ZXShell

Yara Rules

▶ [TLP:WHITE] win_zxshell_w0 (20180301 | No description)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.zxshell