Ghost RAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:45:22 UTC

According to Security Ninja, Gh0st RAT (Remote Access Terminal) is a trojan “Remote Access Tool” used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth.

Below is a list of Gh0st RAT capabilities.
Take full control of the remote screen on the infected bot.
Provide real time as well as offline keystroke logging.
Provide live feed of webcam, microphone of infected host.
Download remote binaries on the infected remote host.
Take control of remote shutdown and reboot of host.
Disable infected computer remote pointer and keyboard input.
Enter into shell of remote infected host with full control.
Provide a list of all the active processes.
Clear all existing SSDT of all existing hooks.

2025-08-05 · Defentive · Defentive Threat Research
Lost in Translation: Threat Actors Use SEO Poisoning and Fake DeepL Sites to Distribute Gh0st RAT
Ghost RAT 2025-06-24 · Bridewell · Bridewell
2025 Cyber Threat Intelligence Report
AsyncRAT Brute Ratel C4 Cobalt Strike Fog Ghost RAT Lumma Stealer Meduza Stealer Quasar RAT RedLine Stealer Sliver 2025-04-30 · · AhnLab · ASEC
(Larva-25003) Web server target IIS malware dissemination case
Ghost RAT 2024-07-10 · Akamai · Allen West, Kyle Lefton, Sam Tinklenberg
CVE-2024-4577 Exploits in the Wild One Day After Disclosure
Tsunami Ghost RAT xmrig 2024-05-23 · Palo Alto Networks Unit 42 · Daniel Frank, Lior Rochberger
Operation Diplomatic Specter: An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set to Target Governmental Entities in the Middle East, Africa and Asia
Agent Racoon CHINACHOPPER Ghost RAT JuicyPotato MimiKatz Ntospy PlugX SweetSpecter TunnelSpecter
CL-STA-0043 2023-05-03 · Sophos · Andrew Brandt, Gabor Szappanos, Xinran Wu
A doubled “Dragon Breath” adds new air to DLL sideloading attacks
Ghost RAT DragonBreath 2023-04-24 · Cofense · Austin Jones
Open-Source Gh0st RAT Still Haunting Inboxes 15 Years After Release
Ghost RAT 2023-04-13 · Intel 471 · Jorge Rodriguez, Souhail Hammou
From GhostNet to PseudoManuscrypt - The evolution of Gh0st RAT
BBSRAT Gh0stTimes Ghost RAT PseudoManuscrypt 2022-09-15 · Symantec · Threat Hunter Team
Webworm: Espionage Attackers Testing and Using Older Modified RATs
9002 RAT Ghost RAT Trochilus RAT 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42

Iron Taurus

CHINACHOPPER Ghost RAT Wonknu ZXShell APT27 2022-05-23 · Trend Micro · Daniel Lunghi, Jaromír Hořejší

Operation Earth Berberoka

reptile oRAT Ghost RAT PlugX pupy Earth Berberoka 2022-04-27 · Trend Micro · Daniel Lunghi, Jaromír Hořejší

New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware

HelloBot AsyncRAT Ghost RAT HelloBot PlugX Quasar RAT Earth Berberoka 2022-04-27 · Trendmicro · Daniel Lunghi, Jaromír Hořejší

Operation Gambling Puppet

reptile oRAT AsyncRAT Cobalt Strike DCRat Ghost RAT PlugX Quasar RAT Trochilus RAT Earth Berberoka 2022-04-15 · Center for Internet Security · CIS

Top 10 Malware March 2022

Mirai Shlayer Agent Tesla Ghost RAT Nanocore RAT SectopRAT solarmarker Zeus 2022-04-01 · The Hacker News · Ravie Lakshmanan

Chinese Hackers Target VMware Horizon Servers with Log4Shell to Deploy Rootkit

Fire Chili Ghost RAT 2022-03-30 · Fortinet · Eliran Voronovitch, Rotem Sde-Or

New Milestones for Deep Panda: Log4Shell and Digitally Signed Fire Chili Rootkits

Fire Chili Ghost RAT 2022-03-16 · AhnLab · ASEC Analysis Team

Gh0stCringe RAT Being Distributed to Vulnerable Database Servers

Ghost RAT Kingminer 2022-02-11 · Cisco Talos · Talos

Threat Roundup for February 4 to February 11

DarkComet Ghost RAT Loki Password Stealer (PWS) Tinba Tofsee Zeus 2021-12-14 · Trend Micro · Nick Dai, Ted Lee, Vickie Su

Collecting In the Dark: Tropic Trooper Targets Transportation and Government

ChiserClient Ghost RAT Lilith Quasar RAT xPack APT23 2021-10-05 · Blackberry · The BlackBerry Research & Intelligence Team

Drawing a Dragon: Connecting the Dots to Find APT41

Cobalt Strike Ghost RAT 2021-10-04 · JPCERT/CC · Shusei Tomonaga

Malware Gh0stTimes Used by BlackTech

Gh0stTimes Ghost 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 2021-04-28 · Trend Micro · Jaromír Hořejší, Joseph C Chen

Water Pamola Attacked Online Shops Via Malicious Orders

Ghost RAT 2021-04-02 · Dr.Web · Dr.Web

Study of targeted attacks on Russian research institutes

Cotx RAT Ghost RAT TA428 2021-02-22 · tccontre Blog · tcontre

Gh0stRat Anti-Debugging: Nested SEH (try - catch) to Decrypt and Load its Payload

Ghost RAT 2021-02-01 · ESET Research · Ignacio Sanmillan, Matthieu Faou

Operation NightScout: Supply-chain attack targets online gaming in Asia

Ghost RAT NoxPlayer Poison Ivy Red Dev 17 2021-01-15 · Swisscom · Markus Neis

Cracking a Soft Cell is Harder Than You Think

Ghost RAT MimiKatz PlugX Poison Ivy Trochilus RAT 2020-12-18 · Seqrite · Pavankumar Chaudhari

RAT used by Chinese cyberspies infiltrating Indian businesses

Ghost RAT 2020-12-10 · Intel 471 · Intel 471

No pandas, just people: The current state of China’s cybercrime underground

Anubis SpyNote AsyncRAT Cobalt Strike Ghost RAT NjRAT 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 2020-10-27 · Dr.Web · Dr.Web

Study of the ShadowPad APT backdoor and its relation to PlugX

Ghost RAT PlugX ShadowPad 2020-07-28 · · NTT · NTT Security

CraftyPanda 標的型攻撃解析レポート

Ghost RAT PlugX 2020-07-20 · Risky.biz · Daniel Gordon

What even is Winnti?

CCleaner Backdoor Ghost RAT PlugX ZXShell 2020-06-14 · BushidoToken · BushidoToken

Deep-dive: The DarkHotel APT

Asruex Ghost RAT Ramsay Retro Unidentified 076 (Higaisa LNK to Shellcode) 2020-06-05 · Prevailion · Danny Adamitis

The Gh0st Remains the Same

Ghost RAT 2020-06-04 · PTSecurity · PT ESC Threat Intelligence

COVID-19 and New Year greetings: an investigation into the tools and methods used by the Higaisa group

Ghost RAT SongXY 2020-05-20 · Medium Asuna Amawaka · Asuna Amawaka

What happened between the BigBadWolf and the Tiger?

Ghost RAT 2020-05-14 · Avast Decoded · Luigino Camastra

APT Group Planted Backdoors Targeting High Profile Networks in Central Asia

BYEBY Ghost RAT Microcin MimiKatz Vicious Panda 2020-03-05 · SophosLabs · Sergei Shevchenko

Cloud Snooper Attack Bypasses AWS Security Measures

Cloud Snooper Ghost RAT 2020-01-01 · Secureworks · SecureWorks

BRONZE EDISON

Ghost RAT sykipot APT4 SAMURAI PANDA 2020-01-01 · Secureworks · SecureWorks

BRONZE FLEETWOOD

Binanen Ghost RAT OrcaRAT APT5 2020-01-01 · Secureworks · SecureWorks

BRONZE GLOBE

EtumBot Ghost RAT APT12 2020-01-01 · Secureworks · SecureWorks

BRONZE UNION

9002 RAT CHINACHOPPER Enfal Ghost RAT HttpBrowser HyperBro owaauth PlugX Poison Ivy ZXShell APT27 2019-12-12 · Microsoft · Microsoft Threat Intelligence Center

GALLIUM: Targeting global telecom

CHINACHOPPER Ghost RAT HTran MimiKatz Poison Ivy GALLIUM 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 2019-11-04 · · Tencent · Tencent Security Mikan TIC

APT attack group "Higaisa" attack activity disclosed

Ghost RAT Higaisa 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 2019-09-17 · Talos · Christopher Evans, David Liebenberg

Cryptocurrency miners aren't dead yet: Documenting the voracious but simple "Panda"

Ghost RAT 2019-04-25 · · DATANET · Kim Seon-ae

Chinese-based hackers attack domestic energy institutions

CALMTHORN Ghost RAT 2019-02-27 · Secureworks · CTU Research Team

A Peek into BRONZE UNION's Toolbox

Ghost RAT HyperBro ZXShell 2019-01-07 · Intezer · Ignacio Sanmillan

ChinaZ Revelations: Revealing ChinaZ Relationships with other Chinese Threat Actor Groups

Ghost RAT 2018-09-19 · Möbius Strip Reverse Engineering · Rolf Rolles

Hex-Rays Microcode API vs. Obfuscating Compiler

Ghost RAT 2018-04-20 · NCC Group · Nikolaos Pantazopoulos

Decoding network data from a Gh0st RAT variant

Ghost RAT APT27 2018-04-17 · NCC Group · Nikolaos Pantazopoulos

Decoding network data from a Gh0st RAT variant

Ghost RAT APT27 2018-02-01 · Bitdefender · Bitdefender Team

Operation PZCHAO Inside a highly specialized espionage infrastructure

Ghost RAT APT27 2018-01-04 · Malware Traffic Analysis · Brad Duncan

MALSPAM PUSHING PCRAT/GH0ST

Ghost RAT 2017-12-19 · Proofpoint · Darien Huss

North Korea Bitten by Bitcoin Bug: Financially motivated campaigns reveal new dimension of the Lazarus Group

Ghost RAT 2017-12-19 · Proofpoint · Darien Huss

North Korea Bitten by Bitcoin Bug

QUICKCAFE PowerSpritz Ghost RAT PowerRatankba 2017-05-31 · MITRE · MITRE ATT&CK

PittyTiger

Enfal Ghost RAT MimiKatz Poison Ivy APT24 2017-05-31 · MITRE · MITRE ATT&CK

Axiom

Derusbi 9002 RAT BLACKCOFFEE Derusbi Ghost RAT HiKit PlugX ZXShell APT17 2017-05-31 · MITRE · MITRE

APT18

Ghost RAT HttpBrowser APT18 2017-02-25 · Financial Security Institute · Kyoung-Ju Kwak (郭炅周)

Silent RIFLE: Response Against Advanced Threat

Ghost RAT 2016-04-22 · Cylance · Isaac Palmer

The Ghost Dragon

Ghost RAT 2012-01-01 · Norman ASA · Snorre Fagerland

The many faces of Gh0st Rat

Ghost RAT 2011-06-29 · Symantec · John McDonald

Inside a Back Door Attack

Ghost RAT Dust Storm 2009-03-28 · Infinitum Labs · Information Warfare Monitor

Tracking GhostNet: Investigating a Cyber Espionage Network

Ghost RAT GhostNet

▶ [TLP:WHITE] win_ghost_rat_auto (20251219 | Detects win.ghost_rat.)
