

What Is gh0st RAT? How It Works, Spreads, and Steals Data

 cyberint.com/blog/dark-web/what-is-ghost-rat-how-it-works-spreads-and-steals-data

Adi Bleih

August 9, 2026

Dark Web

Introduction to gh0st RAT

Ghost RAT ([Remote Access Trojan](#)) is a type of sophisticated malicious software that operates covertly, enabling unauthorized remote access and control of a victim's computer system. Often deployed with malicious intent by cybercriminals, Ghost RATs are designed to evade detection and provide the attacker with a range of powerful capabilities, such as data theft, system manipulation, and surveillance. By exploiting vulnerabilities in security defenses, Ghost RAT [malware](#) can compromise the integrity and confidentiality of sensitive information, posing significant threats to both individuals and organizations alike. Understanding the inner workings of Ghost RAT malware is essential for safeguarding against its detrimental effects and fortifying cybersecurity measures in an ever-evolving digital landscape.

Delivery Methods of gh0st RAT

Lacking an out-of-the-box distribution method, recently observed [Redline incidents](#) appear to begin with the delivery of malicious document attachments sent via an indiscriminate unsolicited email (malspam) campaign, Twitter, and Instagram Direct Messaging. Mostly targeting service or content providers individuals such as 3D artists and streamers, financial advisers, and more based mostly in North America and Europe.

In addition, The malware is spread through YouTube videos that lure victims into downloading a fake bot to automatically buy Binance NFT Mystery Boxes.

Another delivery method is via Discord communities which leads to the download of malicious file that loads Redline into memory.

Gh0st RAT consists of two primary components: the client and the server.

Client (Controller Application): Often referred to as the "client," this is a Windows-based application used to manage and control Gh0st servers deployed on compromised remote systems. Its two key functions are:

1. Overseeing the operation of Gh0st server instances.

2. Creating custom server installation packages for deployment.
3. Server (Windows DLL – User-Level Binary): The server component is implemented as a Windows DLL named SVCHOST.DLL, which is installed as a Windows service on the infected machine. Once active, it connects to the Gh0st client and waits for further commands. This DLL is deployed and installed via a dropper application named SERVER.EXE, which automates its setup as a persistent service.
4. Dropper (INSTALL.EXE): This stand-alone Windows application is responsible for installing SVCHOST.DLL. It includes all the necessary logic to prepare a host for infection, install the Gh0st RAT server component, and launch it as a Windows service.
5. Kernel-Level Component (RESSDT.SYS): RESSDT.SYS is the only kernel-mode binary in the Gh0st toolset. It is a minimal device driver whose sole function is to reset the System Service Dispatch Table (SSDT). It executes at system startup to remove any SSDT hooks, thereby helping evade detection or interference.
6. Installer (Dropper Program): Commonly referred to simply as the “dropper,” this program bundles both the user-level and kernel-level binaries. It performs all the necessary actions to install the Gh0st server on a target machine and initiate the malicious service.

Impact of gh0st RAT

It collects various information from browsers, such as saved credentials, autocomplete data, and credit card information, as well as A system information of the target machine, that includes username, geo-location, hardware configuration, and installed software.

Recent versions of RedLine has the ability to steal cryptocurrency, FTP and IM clients information.

About Check Point Exposure Management

Check Point Exposure Management is an intelligence-led, validation-driven, remediation-first unified platform that helps security teams move quickly and safely from exposure visibility to exposure reduction. Delivered through a single UI, it brings together threat intelligence, exposure prioritization, Agentic Exposure Validation, and safe remediation so teams can understand risk, prove exploitability, and act from one place.

Schedule Your Demo Now

gh0st RAT TTPS

Tactic Name	Technique
Defense Evasion	T1218 – System Binary Proxy Execution
Command and Control	T1071.001 – Web Protocols
Lateral Movement	T1080 – Taint Shared Content
Defense Evasion	T1222 – File and Directory Permissions Modification
Reconnaissance	T1590 – Gather Victim Network Information
Initial Access	T1199 – Trusted Relationship
Initial Access	T1189 – Drive-by Compromise
Initial Access	T1195 – Supply Chain Compromise
Initial Access	T1456 – Drive-By Compromise
Reconnaissance	T1592 – Gather Victim Host Information
Initial Access	T1190 – Exploit Public-Facing Application
Lateral Movement	T0859 – Valid Accounts
Persistence	T0859 – Valid Accounts
Initial Access	T0817 – Drive-by Compromise
Initial Access	T0862 – Supply Chain Compromise
Reconnaissance	T1591 – Gather Victim Org Information
Initial Access	T1566 – Phishing
Initial Access	T0819 – Exploit Public-Facing Application
Initial Access	T1474 – Supply Chain Compromise
Defense Evasion	T1078 – Valid Accounts
Initial Access	T1078 – Valid Accounts

Tactic Name	Technique
Privilege Escalation	T1078 – Valid Accounts
Persistence	T1078 – Valid Accounts
Command and Control	T1043 – Commonly Used Port
Command and Control	T1573 – Encrypted Channel
Command and Control	T1132.001 – Standard Encoding
Credential Access	T1056.001 – Keylogging
Collection	T1056.001 – Keylogging
Command and Control	T1568.001 – Fast Flux DNS
Collection	T1113 – Screen Capture
Defense Evasion	T1070.004 – File Deletion
Discovery	T1082 – System Information Discovery
Defense Evasion	T1070.001 – Clear Windows Event Logs
Privilege Escalation	T1547.001 – Registry Run Keys / Startup Folder
Persistence	T1547.001 – Registry Run Keys / Startup Folder
Privilege Escalation	T1543.003 – Windows Service
Persistence	T1543.003 – Windows Service
Discovery	T1057 – Process Discovery
Execution	T1106 – Native API
Command and Control	T1095 – Non-Application Layer Protocol
Command and Control	T1573.001 – Symmetric Cryptography
Defense Evasion	T1140 – Deobfuscate/Decode Files or Information
Discovery	T1012 – Query Registry

Tactic Name	Technique
Execution	T1059 – Command and Scripting Interpreter
Defense Evasion	T1574.002 – DLL Side-Loading
Privilege Escalation	T1574.002 – DLL Side-Loading
Persistence	T1574.002 – DLL Side-Loading
Execution	T1569.002 – Service Execution
Defense Evasion	T1218.011 – Rundll32
Defense Evasion	T1055 – Process Injection
Privilege Escalation	T1055 – Process Injection
Command and Control	T1105 – Ingress Tool Transfer
Defense Evasion	T1112 – Modify Registry
Execution	T1129 – Shared Modules

gh0st RAT IOCs (Sample of 50)

Type	Date Added	Value
SHA-256	2026-08-05	8bf367564afbbc28d3101d21124b5bfc3ec006fb32d4a2ba3fb9ccf1414fad8b
SHA-256	2026-07-30	69e8a73e215114989a0d9c5c9c666587057e2bcf1c29b1fb7d45e1cb38a715de
SHA-256	2026-07-20	96c0911c225219cfd380076f5196d7ee87c617cddb968d3d465122473e20d6fb
SHA-256	2026-07-20	af9a6dacb2a9618866cf398d615b2fe1c1c98ec7254d38a01c7c2d6869821bbe

Type	Date Added	Value
SHA-256	2026-07-20	3fc95667b98c637ba785b67dff1bd15ff7a21f082d25894c3a78ec1b6206fcd7
SHA-256	2026-07-18	6aa982f7c6167752e8f58083dc5f1c11ff0aa63b3c3d2e192009cce2cef84ee0
SHA-256	2026-07-17	e4283d10ea2d8bfe524e2da68870d67653ce895ff4fcafedf68edc47576a5e3c
SHA-256	2026-07-17	8a72afcb3bdd892ae106b2e6c7bd3df4e4be98f151342509603e31d7efd555f3
SHA-256	2026-07-16	0e8553970999b60c3a0a2637e0c282ca52b33d3e3ae88c99b6fa426bddc0075d
SHA-256	2026-07-14	93b19bc56952ae1e82f1f41db49f455316736e2b8d161e64b115a150d8dcf204
SHA-256	2026-07-14	8635730e272497621742ceaf5f6c7a54238c431f1b1e3db8488a17976c9fc576
SHA-256	2026-07-14	4f4d405d32d76a170ca2899c70b48ef6ffaaef792e024b6f8aab98d4ae55eae4
SHA-256	2026-07-13	df603ed55cbf6f9d74068b956ab966a7b785eb102e1045f343d96255eb2cdc24
SHA-256	2026-07-13	4d9a77f6f96f6089a0690281a6b15e1285559c498741d6c1eabba534f3b98ca6
SHA-256	2026-07-08	69e2433df06b829e98e5a6c8f552b9371795fb65df62fa4cfb7362970d1ce744
SHA-256	2026-07-07	7152f5f392339e30c5436450f02d25e5a68ae18ab10729d9e7fbed15d9d10fa9
SHA-256	2026-07-06	35e0b22139fb27d2c9721aedef5770d893423bf029e1f56be92485ff8fce210f3

Type	Date Added	Value
SHA-256	2026-07-06	82611e60a2c5de23a1b976bb3b9a32c4427cb60a002e4c27cadfa84031d87999
SHA-256	2026-07-06	7b2599ed54b72daec0acfd32744c7a9a77b19e6cf4e1651837175e4606dbc958
IPv4 Addresses	2026-07-06	38.246.250.201
IPv4 Addresses	2026-07-06	45.207.220.12
Domain	2026-06-09	bj2.xyz
Domain	2026-07-06	gd.bj2.xyz
SHA-256	2026-07-05	7b63ddaf3b217f9e7b08575ee6f80fff1d2d9e12522d862ccc192ef3d08a0dd3
SHA-256	2026-07-05	7aa50ba59b38494cc524dbd31519bd3a218133aed64d9037eef02d697b8e99d0
SHA-256	2026-06-29	7367ea4cb0851baf6e17d42347060d4c60fd40d18d3faa7af146992cdead2999
SHA-256	2026-06-28	fcd0a4054eba07a6e2c6697c7e6f116afe494e43cce7ceb99cea6d1ba6faf0b4
SHA-256	2026-06-27	7317d297686d154b4d78217e100df5f57949f05efe095f1a017b5988cddef98b
SHA-256	2026-06-26	12d72753c1e65457eccc9957b4501e26397e28379eafc363440f6b81060d5f4

Type	Date Added	Value
SHA-256	2026-06-26	f755d085c61879c1805115cdb6f344e9c8ff3b5f7b0e261cd59694c1d82dda18
SHA-256	2026-06-24	a54318d38eb5b85ffa139155072f9581b55eab73b03aed1cfba6431dda1fc7c6
IPv4 Addresses	2026-01-24	202.61.160.201
SHA-256	2026-06-22	8eae6ca0380279f0c047e6b5d49808db591f9e14d106226017eaae62b79c1a10
SHA-256	2026-06-21	b6a854625fc19895e2520b9e055b9afd74d15e30879d48b6d35e419215a18ba6
SHA-256	2026-06-19	b28c2832db2275496441568ca94960333d143b363e911d087f41e484f04fb515
SHA-256	2026-06-17	0fb2a4a9e5a714b605354bc6e59a6b1f23b94e3743dbc1fb9f86799450d27fbe
SHA-256	2026-06-11	258e579ba8eba614c77a415a4d68ef9a0b17917e4a9df8acafba9d935e49a434
SHA-256	2026-06-11	446aad1d86aaf82a32f7e63bd0dd34cb2ac85ca2a412b9bea2122fb5506ddac1
SHA-256	2026-06-10	baa25e933aa75148368de25aedfe804f10cba3d6825860dd2b34a34d6e2ceff0
SHA-256	2026-06-09	d9d07a5ef476e789d4c7abadfa120bdfe55e11b529ead26492da3925d6399614
SHA-256	2026-06-05	b29f131d9bcc54b1bed5287c18ed3b8b0ac78933dca14c14a0eded4eb91df2db
SHA-256	2026-06-01	17fc02be307af162f241917f3a0f23c89fc83d3334000b4e5fb88c6cdad3e956

Type	Date Added	Value
SHA-256	2026-05-29	fdaabbf7b7585cc473502c21a1471f95de45d5492216e8e6c035e1856d6af9b1
SHA-256	2026-05-28	27d4b34d2ea281766a07da52b6700b196bcba749aaf73c96b0320512479e55b8
SHA-256	2026-05-25	a055948debb0fadb80965850a2e2d701ada83744c472e4df28ef7323088e5ea8
SHA-256	2026-05-25	fa9996838c5459b9124f9f06f75bec832cfc0368782b33466563fd50774b5ae2
SHA-256	2026-05-24	003618d0fbf5845524c8f1487e1ca6665d2374631b65b0f8057169c462ef21a3
SHA-256	2026-05-21	ca70bc178c645aa50bb22b4845b552fedeea69d4023922cfbc57d79ce27b31d4
SHA-256	2026-05-18	c98ac997e2f9def83ee2dc5c7e84e004423aa35f74c96058141e41cffa9db1cd
SHA-256	2026-05-06	95f3db5aa7d2d2251c22708368ab6bd55457c7cc51fae2a817bf88dc0e1648b6