

CTI Report: ShadowByt3\$ Ransomware Group

barricadecyber.com/cti-report-shadowbyt3-ransomware-group

Eric J. Taylor

Published: 2026-04-15

Classification: TLP: CLEAR

Prepared by: Barricade Cyber Solutions

Source: Primary source analysis — leaked source code, Telegram channel export, DLS screenshots, PwnForums posts, Rootsploit forum activity, VirusTotal submissions, blockchain explorer data

They Want to Be the Next LockBit. They Are Not.

ShadowByt3\$ is a ransomware group that wants you to believe they are a sophisticated criminal enterprise. Their leak site lists Starbucks and the University of Georgia as victims. Their documentation compares their ransomware to BlackCat and LockBit. They applied to join the Qilin RaaS program as pentesters.

The reality is different. Their ransomware encrypts its own ransom note. Their BTC wallet shows small transactions but no significant ransom payments. Their Windows build was broken for weeks. They leaked their own source code on AnonFiles. And the AI-generated documentation they ship with their ransomware still contains the ChatGPT prompt artifact “Would you like me to show you how to add a Recursive Depth limit...”

But dismissing them would be a mistake.

Their Linux payload achieves a 4 out of 72 detection rate on VirusTotal. The encryption scheme is cryptographically sound — AES-256-GCM with per-file RSA-2048 key wrapping. The polymorphic builder generates a unique binary hash for every build. And their affiliate portal is live, accepting new operators.

ShadowByt3\$ emerged in late October 2025 and has been actively recruiting affiliates across multiple dark web forums and Telegram channels since then. Despite aggressive self-promotion, the group demonstrates consistently amateur tradecraft.

Profile:

- **Also known as:** ShadowByt3S, Shadow\$\$21 (Rootsploit forum), Byt3\$ tech 2.0 (Telegram)
- **Status:** Active as of April 2026
- **Operating model:** Ransomware-as-a-Service with affiliate enrollment
- **First documented:** Mjolnir Security intelligence report
- **Operating since:** Approximately October 27, 2025 (per PwnForums introduction)
- **Platforms:** Linux (primary, functional), Windows (secondary, unstable)
- **Communication:** ProtonMail, Telegram, Tox messenger
- **Revenue:** Minimal — BTC wallet shows small transactions received and moved out (current balance \$0.00), ETH wallet has no activity
- **Claimed victims:** Starbucks, University of Georgia, IMBA Argentina just to name a few



What they claim vs. what the evidence shows:

- They claim to rival LockBit and BlackCat — their documentation is AI-generated and includes unedited ChatGPT response artifacts
- They claim multiple high-profile victims — none have been verified, and most download links on the leak site are non-functional
- They claim a “better builder” prompted them to leak version 1.0 — the leaked code reveals a basic Go file encryptor with no anti-debugging, no privilege escalation, no lateral movement, and no backup destruction
- They applied to join the Qilin RaaS as a pentester in January 2026 on the Rootsploit forum under the alias “Shadow\$\$21” — they were not accepted



The Problem: A Live RaaS With a Functional Encryptor

Despite the amateur presentation, the underlying ransomware is technically functional. Barricade obtained and analyzed the complete source code from the group's own public leak. The analysis reveals two distinct variants — one for Windows and one for Linux — with different encryption schemes, different contact information, and different capabilities.

Two Variants, Two Encryption Schemes

The leaked archive contains two independent ransomware projects, not a single cross-platform build:

Linux Variant (Primary — Functional):

- Written in Go, compiled as a statically linked ELF binary
- Encryption: AES-256-GCM (file data) with RSA-2048-OAEP (key wrapping)
- Per-file unique AES session key — no universal decryption key exists in the binary
- Builder generates unique RSA-2048 keypair per build (polymorphic — every build has a different SHA-256 hash)
- Excludes system-critical directories: /bin, /boot, /dev, /etc, /lib, /proc, /run, /sys
- Excludes system files: vmlinuz, initrd.img, grub.cfg, fstab, passwd, shadow, sudoers
- Build flags: -trimpath -ldflags="-s -w" (strips debug symbols and developer paths)
- Cross-compiled from Windows: GOOS=linux GOARCH=amd64 CGO_ENABLED=0
- VirusTotal: 0/65 detection rate on clean build

Windows Variant (Secondary — Unstable):

- Written in Go, compiled as a Windows PE executable
- Encryption: ECIES (Elliptic Curve) + ChaCha20 (stream cipher) — completely different scheme from Linux
- Uses github.com/ecies/go for key exchange, golang.org/x/crypto/chacha20 for file encryption
- Enumerates all drive letters A-Z for encryption targets
- Downloads custom wallpaper from postimg.cc and sets it via PowerShell SystemParametersInfo API

- Runs without console window (-H=windowsgui linker flag)
- Known broken: Telegram messages from April 13, 2026 state “Linux works just fine but windows needs to be fixed”
- VirusTotal: 4/72 detection rate



Ransom Note Differences

The source code reveals hardcoded ransom notes with different contact information between variants — a significant OPSEC inconsistency:

Windows ransom note references:

- Telegram: <https://t.me/ShadowS22>
- Email: ShadowByt3S@proton[.]me (listed as “alternative”)
- Chat ID: 2242026124
- Affiliate ID: ecd8fa130c93246ab34e424272e3924eaab1

Linux ransom note references:

- Email: ShadowByt3S@proton[.]me (listed as primary)
- No Telegram link
- Chat ID: 224261212 (different from Windows)
- Affiliate ID: ecd8fa130c93246ab34e424272e3924eaab1 (same)

Both notes reference the clearnet leak site [shadowsblog.cloud-ip\[.\]cc](https://shadowsblog.cloud-ip[.]cc) and threaten data publication on the (now banned) Telegram channel @ShadowByt3S.



Builder Architecture

The Builder component is the most operationally significant piece. It functions as a factory:

1. Generates a unique RSA-2048 keypair (Linux) or ECIES keypair (Windows)
2. Base64-encodes the public key and ransom note
3. Injects them into the configuration source file
4. Cross-compiles for the target platform
5. Outputs two binaries: encryptor and decryptor

Because the keys change every build, each payload has a unique SHA-256 hash. This is the group's primary — and only effective — evasion technique.

What the Ransomware Does NOT Do

Notably absent from the source code:

- No shadow copy deletion (vssadmin, wbadmin)
- No backup destruction
- No process/service termination
- No anti-debugging or anti-VM checks
- No privilege escalation
- No lateral movement or network propagation
- No C2 communication — fully autonomous
- No anti-forensic log clearing
- No persistence mechanisms

This is a file encryptor and nothing more. It has no pre-encryption preparation, no post-encryption cleanup, and no way to spread beyond the machine it is executed on.

The Forum Trail

ShadowByt3\$ has left a visible trail across multiple forums:



PwnForums (March–April 2026):

- Introduced themselves as operating since October 2025
- Posted their leak site URLs and contact information
- Requested moderator/admin access — denied
- Account created March 2026, 4 posts, 1 reputation

Rootsploit Forum (January 2026):

- Used the alias “Shadow\$\$21”
- Posted in the Qilin RaaS recruitment thread
- Requested to join as a pentester: “I am the person who created the group the main person and I am willing to work as a pentester for you guys to get are status up”
- No evidence of acceptance

Telegram:

- Original channel @ShadowByt3S — banned
- Recreated as @techfood247 (“Byt3\$ tech 2.0”) on April 12, 2026
- Support channel: @shadows_supp
- 63 subscribers as of mid-April 2026
- Messages reveal ongoing development issues and build distribution via Mega.nz



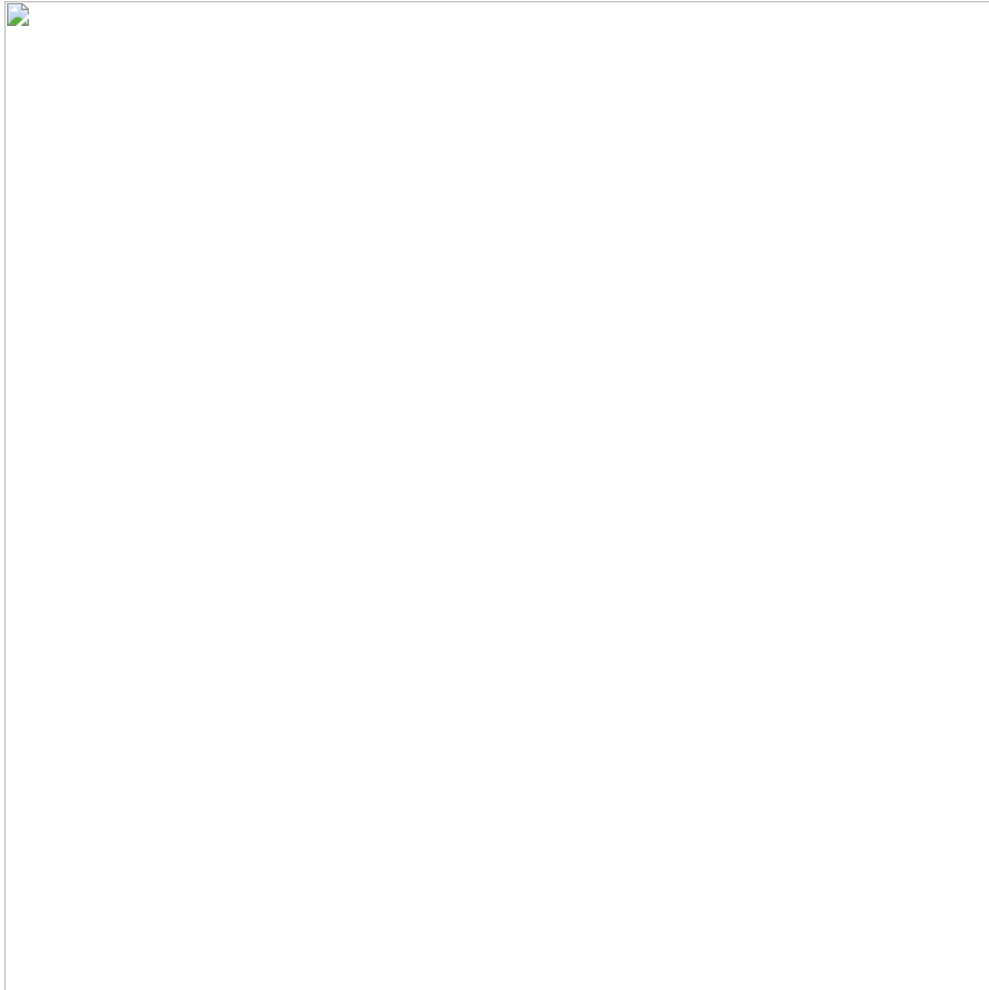
The Money Trail

ShadowByt3\$ operates three cryptocurrency wallets. All have been verified on blockchain explorers:

Bitcoin: bc1qh4ynm9fj69apv2t0kv7xu6jmtqptna4q8v5rgl

- Current balance: \$0.00

- Activity: Multiple transactions visible — small amounts received and subsequently moved out. Current balance is zero because funds were transferred, not because the wallet was unused. Transaction amounts appear consistent with small payments or test transactions rather than significant ransom payments.



Ethereum: 0xD9E1D84369bf37Cdf06290846C95800e68A4Ff61

– Balance: \$0.00

– Activity: Zero transactions



Monero: 47NHwQtgTEo8ioJeWUM1rjjVwMHrFfMfyKmP16ab3pszUVpfVJMX3q8Ce2XAq7PLXX5uRBzGPCkBu7SQrx64NVdUUVRaA9a
– Balance: Unverifiable (Monero is privacy-focused)



The Plan: Detection and Defense

Block These IOCs Now

Tor Hidden Services:

- mfbbt65kir2drc7tuoukwibikgvxquauscnzgbeltkmidjtgqlzm2qad[.]onion/leaks.php (primary DLS)
- sdwbytb664krp2wz2qs3lxxah2rhneuotot5hy7g4jpn2pindigcad[.]onion (alternate DLS)
- mfbbt65kir2drc7tuoukwibikgvxquauscnzgbeltkmidjtgqlzm2qad[.]onion/leaks.php (affiliate portal)

Cleartext:

- shadowsblog.cloud-ip[.]cc (leak site / recruitment — referenced in ransom notes)
- posting[.]cc/XBCvNbMS (wallpaper image downloaded by Windows variant)

Email:

- ShadowByt3S@proton[.]me

File Indicators:

- Extension: .SHADOWBYT3S appended to encrypted files
- Ransom note filename: README2DECRYPT (dropped in traversed directories)
- Linux binary name pattern: shadowbyt3S-built.elf
- Windows binary name pattern: \$HADOWBYT3S-Built.exe
- Decryptor name pattern: decryption-built.elf / Decryptor-Built.exe

Detection Engineering

File system indicators:

- Monitor for mass file rename operations appending .SHADOWBYT3S extension
- Alert on README2DECRYPT file creation across multiple directories
- Watch for ELF binary execution from non-standard paths with root privileges

Windows-specific:

- Alert on PowerShell downloading images from postimg.cc
- Detect SystemParametersInfo calls to change wallpaper from non-standard processes
- Monitor for processes enumerating all drive letters A-Z sequentially

Linux-specific:

- Alert on processes performing recursive file operations starting from / with high I/O
- Monitor for Go-compiled ELF binaries (static linking, stripped symbols) executing as root
- Detect mass AES-256-GCM encryption patterns (high entropy file writes at scale)

Network indicators:

- Block connections to shadowsblog.cloud-ip.cc
- Monitor for Mega.nz uploads (used for build distribution per Telegram messages)
- Alert on Tox messenger protocol traffic

Build YARA Rules

The following strings are present in unstripped builds and can be used for YARA detection:

- “SHADOWBYT3S” (encrypted extension string)
- “README2DECRYPT” (ransom note filename)
- “.SHADOWBYT3S” (configuration constant)
- “shadowbyt3s/Encryptor” (Go package path — present in non-trimpath builds)
- “configuration.GetPublicKey” (Go function — present in non-stripped builds)
- “configuration.GetProcessInfo” (Go function — ransom note retrieval)

—

What Happens If You Ignore This

- ShadowByt3\$ is actively recruiting affiliates and distributing builds via Telegram and Mega.nz — the operator count will grow
- The 0/65 VirusTotal detection rate means the Linux payload will bypass signature-based defenses
- The polymorphic builder ensures every deployment is a unique hash — retroactive IOC blocking will not protect you
- While the current operation is amateur, the underlying cryptography is sound — files encrypted by ShadowByt3\$ cannot be decrypted without the matching private key
- Groups that start small can mature rapidly when they acquire experienced affiliates — ShadowByt3\$ is actively seeking them

—

The Outcome: What Success Looks Like

Organizations that act on this intelligence will:

- **Block the infrastructure** before ShadowByt3\$ builds hit their environment
- **Detect the behavioral patterns** (mass file encryption, wallpaper change, extension rename) that remain constant regardless of the polymorphic binary hash
- **Recognize the ransom note** and affiliate ID format to attribute incidents correctly
- **Track the evolution** of this group as they fix their Windows build, develop new capabilities, and potentially attract experienced affiliates from other RaaS operations

—

MITRE ATT&CK Mapping



TACTIC	ID	TECHNIQUE	EVIDENCE
Execution	T1059.001	PowerShell	Windows variant uses PowerShell to download wallpaper from postimg.cc and set it via SystemParametersInfo API
Execution	T1059.004	Unix Shell	Linux ELF payload requires chmod +x and bash/terminal execution, root recommended
Defense Evasion	T1027	Obfuscated Files or Information	Ransom note and RSA keys Base64-encoded in configuration; symbols stripped with -s -w flags; paths stripped with -trimpath
Defense Evasion	T1140	Deobfuscate/Decode Files	Base64-encoded ransom note and public key decoded at runtime via base64.StdEncoding.DecodeString()
Defense Evasion	T1480	Execution Guardrails	Linux variant excludes /proc, /sys, /dev, /boot, /etc, /bin, /lib to avoid bricking the OS
Resource Development	T1583.001	Acquire Infrastructure: Domains	Two .onion domains for DLS, clearnet domain shadowsblog.cloud-ip.cc, postimg.cc for wallpaper hosting
Resource Development	T1588.001	Obtain Capabilities: Malware	Attempted to join Qilin RaaS as pentester (Rootsploit, January 2026); Windows variant forked from Prince ransomware per README
Exfiltration	T1567.002	Exfiltration to Cloud Storage	Builds distributed via Mega.nz per Telegram messages; ransom note threatens data leak
Impact	T1486	Data Encrypted for Impact	Core function — AES-256-GCM + RSA-2048 (Linux) or ECIES + ChaCha20 (Windows), .SHADOWBYT3S extension
Impact	T1491.001	Internal Defacement	Windows variant downloads custom wallpaper from postimg.cc and sets it as desktop background via PowerShell

IOC Summary

TYPE	VALUE	CONTEXT
SHA-256	edcc20a3162905a4ae84b3dc2f3c175797927031513328c16ac8583277c61835e	shadow_e — Linux E payload (4
SHA-256	ccae7ab0a069b628aed34ed696704f5b4d1df6843c5e58b5dec821084c275d68	y1kz3.exe Windows f payload (4
SHA-256	3a253393fab8606296654cff93e033b9912324c21e802d175b0329fa865827bc	shadowby built.elf — build from source (0/
Onion Domain	mfbbt65kir2drc7tuoukwibikgvxquauscnzgbeltkmidjtqqlzm2qad.onion	Primary D/ affiliate en portal
Onion Domain	sdwbytbqeb664krp2wz2qs3lxxah2rhneuotot5hy7g4jpn2pindigcad.onion	Alternate f site
Domain	shadowsblog.cloud-ip.cc	Cleartext k (from rans and READ
Email	ShadowByt3S@proton.me	Primary cc in both rar notes
BTC Wallet	bc1qh4ynm9fj69apv2t0kv7xu6jmtqptna4q8v5rgl	Current ba \$0.00 — s transaction received a moved out
ETH Wallet	0xD9E1D84369bf37Cdf06290846C95800e68A4Ff61	Zero activi
XMR Wallet	47NHwQtgTEo8ioJeWUM1rjJVwMHRfFmfyKmP16ab3pszuVpFVJMX3q8Ce2XAq7PLXX5uRBzGPCKBu7SQrx64NVdUUVRaA9a	Monero dc address
Tox ID	A96D94423D3E30DDA8CC70664D5630C43F235B3BE773E6CE01FDDAF089634A5B86321A69743F	Operator 1 messenger account
Telegram	https://t.me/shadows_sup	Support ch
Telegram	https://t.me/techfood247	Current ch (replacem banned @Shadow
Telegram	https://t.me/Shadows22	Contact in Windows r note
Telegram	https://t.me/ShadowByt3S	Original ch (banned)
URL	https://posting.cc/XBCvNbMS	Wallpaper download Windows \
Affiliate ID	ecd8fa130c93246ab34e424272e3924eaab1	Hardcode Windows ; Linux rans notes
File Extension	.SHADOWBYT3S	Appended encrypted
Ransom Note	README2DECRYPT	Dropped in traversed directories

FEATURE	LINUX VARIANT	WINDOWS VARIANT
Language	Go (statically linked ELF)	Go (Windows PE, -H=windowsgui)
File Encryption	AES-256-GCM	ChaCha20 (unauthenticated)
Key Wrapping	RSA-2048-OAEP	ECIES (Elliptic Curve)
Key Generation	crypto/rsa (standard library)	github.com/ecies/go (third-party)
Target Scope	/ with directory exclusions	All drive letters A-Z
System Exclusions	/proc, /sys, /dev, /boot, /etc, /bin, /lib, /run	Windows, System32, ProgramData, Program Files
Wallpaper Change	No	Yes — downloads from postimg.cc via PowerShell
Console Window	Terminal output with ASCII banner	Hidden (-H=windowsgui)
Build Status	Functional	Broken (acknowledged April 13, 2026)
VT Detection	0/65 (clean build)	4/72
Contact Method	Email (ShadowByt3S@proton.me)	Telegram (t.me/Shadows22) + email as backup
Chat ID	224261212	2242026124