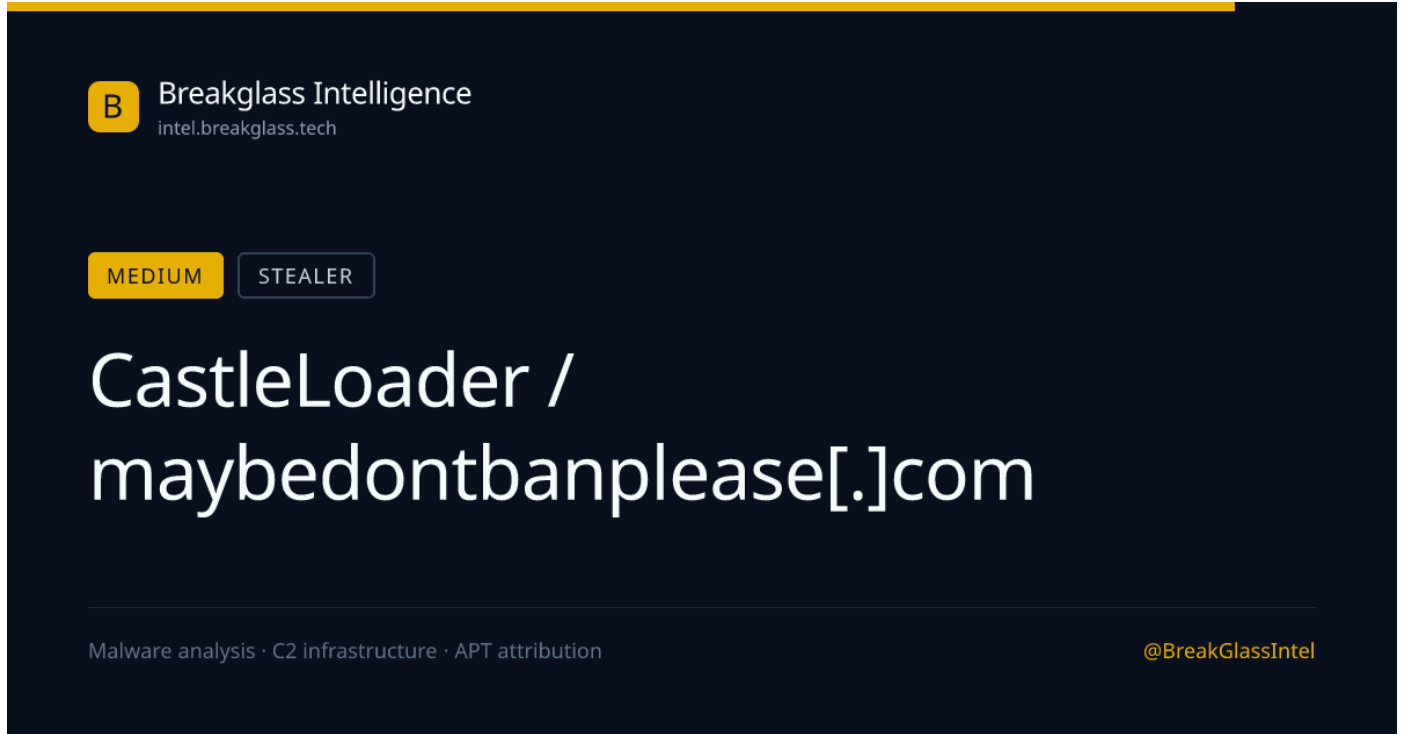


CastleLoader / maybedontbanplease[.]com - Breakglass Intelligence — Breakglass Intelligence

 intel.breakglass.tech/post/castleloader-maybedontbanplease

Breakglass Intelligence

April 9, 2026



Breakglass Intelligence
intel.breakglass.tech

MEDIUM STEALER

CastleLoader / maybedontbanplease[.]com

Malware analysis · C2 infrastructure · APT attribution

@BreakGlassIntel

TLP: WHITE **Date:** 2026-04-09 **AnalystClassification:** Cybercrime -- Malware-as-a-Service (MaaS) **Status:** DRAFT -- Investigation in progress

Executive Summary

This investigation targets a newly registered domain [maybedontbanplease\[.\]com](#) (registered 2026-04-02) serving as command-and-control infrastructure for CastleLoader, a modular malware loader operated by the threat actor tracked as GrayBravo (formerly TAG-150). The domain resolves to [38\[.\]180\[.\]136\[.\]139](#), hosted on 3NT Solutions LLP infrastructure (London/Netherlands). The associated NSIS installer sample (SHA256: [4ba0d3ae41a0ae3143e8c2c3307c24b0d548593f97c79a30c0387b3d62504c31](#)) is code-signed with an EV certificate issued to "SERPENTINE SOLAR LIMITED" -- a company that does not exist in UK Companies House records, indicating a fraudulently obtained Extended Validation code signing certificate.

CastleLoader is a sophisticated loader-as-a-service platform that has been active since early 2025, targeting US government agencies, critical infrastructure, IT firms, and logistics companies. It has been linked to the deployment of multiple secondary payloads including LummaC2, StealC,

RedLine, Rhadamanthys, DeerStealer, NetSupport RAT, SectopRAT, and others.

Key Findings

- **Domain registered 7 days ago** (2026-04-02) via Global Domain Group LLC with Google Cloud DNS nameservers
- **Let us Encrypt certificate** issued same day as domain registration (Apr 2, 2026), cert serial `065db17d736521db76fc1367b1cfca14bb35`
- **Hosting:** 3NT Solutions LLP (UK company, infrastructure in NL/US), IP `38[.]180[.]136[.]139`, upstream via Cogent Communications
- **C2 backend is DOWN** (504 Gateway Timeout on all paths) -- nginx 1.18.0 (Ubuntu) still running as reverse proxy
- **New code signing certificate:** "SERPENTINE SOLAR LIMITED" -- Sectigo Public Code Signing CA EV R36, valid 2026-04-01 to 2027-04-01, serial `a2c875fdd0d6fa22a2261813def8a56e` -- NOT in UK Companies House (fraudulent EV cert)
- **Previous CastleLoader signing certs:** "NOBIS LLC" (GlobalSign, expired), "LLC Territory of Comfort" -- Russian-language entity names suggest Russian-speaking operators
- **Previous C2 IP:** `94[.]159[.]113[.]32` (from MalwareBazaar tags) -- WHOIS shows "Komskov Vadim Aleksandrovich" in Novotroitsk, Russia (RU-server21, AS216234)
- **Sample characteristics:** 61.8MB NSIS installer, Python 3.14 embedded, AES-encrypted payload (data1.pak, 6.8MB), 100MB of junk padding data (SQLite DBs with random dictionary words, fake config files, fake images)
- **Infection chain:** NSIS installer -> extracts Python 3.14 runtime + encrypted payload -> pythonw.exe decrypts data1.pak -> shellcode injection via VirtualAlloc/RtlMoveMemory -> CastleLoader core in memory
- **16 known CastleLoader samples** on MalwareBazaar dating back to November 2025
- **Reporter:** SquiblydooBlog (submitted 2026-04-09 17:49 UTC -- same day as this investigation)

What Was Found vs. What Was Known

Aspect	Prior Reporting	Our Findings
C2 Domain	Not reported	maybedontbanplease[.]com (new, Apr 2 2026)
C2 IP	<code>94[.]159[.]113[.]32</code> (historical)	<code>38[.]180[.]136[.]139</code> (current, 3NT Solutions)
Code Signing	NOBIS LLC, LLC Territory of Comfort	NEW: SERPENTINE SOLAR LIMITED (fraudulent EV cert)
Delivery	ClickFix, fake GitHub repos	NSIS installer with Python 3.14 embedded

Aspect	Prior Reporting	Our Findings
Hosting	Russian infrastructure	Shifted to 3NT Solutions (UK/NL), upstream Cogent
Operator nationality	Suspected Russian	Confirmed: Russian entity names on certs, Russian hosting on prior C2
C2 Status	Active (historical)	Backend DOWN, nginx proxy still running

Attack Chain

Delivery (unknown vector)

|

v

NSIS Installer (setup.exe, 61.8MB, signed "SERPENTINE SOLAR LIMITED")

|

v

Extracts to %TEMP%:

- PACKAGE/ (Python 3.14 runtime: pythonw.exe, python314.dll, stdlib)
- data0.pak (100MB junk padding - SQLite DBs, fake configs, fake images)
- data1.pak (6.8MB AES-encrypted CastleLoader payload)
- install.ini (config: package_name=data1.pak, install_path=%TEMP%\vc_redist.x86.exe)

|

v

pythonw.exe (windowless Python interpreter)

- > Runs dynamically generated Python script
- > Decrypts data1.pak (AES-CBC, key derived from NSIS script or embedded)
- > VirtualAlloc + RtlMoveMemory + function pointer execution

|

v

CastleLoader shellcode (in-memory, no disk artifact)

- > PEB walking to resolve APIs
- > GoogleBot User-Agent for C2 comms
- > Downloads final payload from maybedontbanplease[.]com

|

v

Secondary Payload (unknown - C2 is currently down)

Infrastructure Analysis

Network Infrastructure

IP	ASN	Provider	Ports	Services	Status
38[.]180[.]136[.]139	Cogent/3NT Solutions	3NT Solutions LLP (UK)	22, 80, 443	OpenSSH 8.9p1, nginx 1.18.0	LIVE (backend down)

IP	ASN	Provider	Ports	Services	Status
94[.]159[.]113[.]32	AS216234	Komskov Vadim Aleksandrovich (RU)	N/A	Historical C2	OFFLINE

Domain Infrastructure

Domain	Registrar	Created	NS	Purpose
maybedontbanplease[.]com	Global Domain Group LLC	2026-04-02	ns-cloud-e{1-4}.googledomains.com	C2

Certificate Analysis

TLS Certificate (Let us Encrypt):

- Subject: CN=maybedontbanplease.com
- Issuer: C=US, O=Let us Encrypt, CN=R13
- Serial: 065db17d736521db76fc1367b1cfca14bb35
- Valid: 2026-04-02 to 2026-07-01
- SANs: maybedontbanplease.com (only)
- Only 2 CT log entries (precert + cert)

Code Signing Certificate (Sectigo EV):

- Subject CN: SERPENTINE SOLAR LIMITED
- Issuer: Sectigo Public Code Signing CA EV R36
- Algorithm: sha256WithRSAEncryption
- Valid: 2026-04-01 to 2027-04-01
- Serial: a2c875fdd0d6fa22a2261813def8a56e
- Thumbprint: e4253d8588b77541fc46bbcb224a954770350c53cc2a69e6c3b20386282ccc9f5
- **Not in CSCB (Code Signing Certificate Blocklist) -- NEEDS SUBMISSION**
- **SERPENTINE SOLAR LIMITED not found in UK Companies House -- FRAUDULENT**

Adjacent IP Analysis (38[.]180[.]136[.]0/24)

IP	Ports	Notes
.136	none	Dead
.137	135, 3389	Windows RDP
.138	22, 3389, 5985	Windows RDP + WinRM

IP	Ports	Notes
.139	22, 80, 443	TARGET -- CastleLoader C2
.140	80, 443, 902, 8000, 9080	Web server cluster
.142	22, 3306, 3389, 5985, 30120	FiveM game server + Windows
.143	21 ports incl DNS, Elastic, Redis	HyperV.mylocal.net -- hypervisor

Hosting Provider

3NT Solutions LLP: UK-registered company (22 Brondesbury Park, Willesden, London NW6 7DL). Technical contact: Raul Eduardo Ribeiro Emmerich. Also registered at Ketelskamp 10, Meppel, Netherlands. Operates AS-level infrastructure via Cogent Communications transit. This is a legitimate ISP that leases dedicated servers -- not inherently bulletproof, but commonly used for malicious hosting due to limited abuse response.

Malware Analysis

Sample Details

Hash (SHA256)	Type	Size	First Seen	Family	Signer
4ba0d3ae41a...	NSIS PE32	61.8MB	2026-04-09	CastleLoader	SERPENTINE SOLAR LIMITED

File Hashes

- **SHA256:** 4ba0d3ae41a0ae3143e8c2c3307c24b0d548593f97c79a30c0387b3d62504c31
- **SHA1:** 6d504e6af3124409d6c86b50a89a8c2e83f9ce31
- **MD5:** 660efa6ef10d3f575bc3fadc207da050
- **Imphash:** 46ce5c12b293febbeb513b196aa7f843
- **SSDEEP:**
1572864:dE83khQpeHV6OaYcMEFolcelQPWN8zjnY9GI2BKtD9NgwL:dEWkKCRX4cpGml6
- **TLSH:**
T103D73356EBC39151C8C483F6080E8E7169C3ADA3520B5B3DD0A7763A14A919BB875

NSIS Installer Contents

```
setup.exe (61.8MB, NSIS 3.11 Unicode, LZMA compressed)
|
+-- install.ini (NSIS config)
+-- licfile.txt (junk padding)
+-- data0.pak (100MB junk - inflated to evade sandbox)
+-- data1.pak (6.8MB AES-CBC encrypted payload)
+-- $PLUGINSDIR/
|   +-- System.dll (NSIS System plugin)
|   +-- nsDialogs.dll (NSIS Dialogs plugin)
|   +-- modern-wizard.bmp (NSIS UI)
+-- PACKAGE/ (Python 3.14.0a1 embedded runtime)
|   +-- python.exe, pythonw.exe
|   +-- python314.dll, python3.dll
|   +-- python314.zip (stdlib, 561 files)
|   +-- python314._pth (import path config)
|   +-- python.cat (PKCS#7 catalog -- legit)
|   +-- _ctypes.pyd, _ssl.pyd, libcrypto-3.dll, etc.
+-- STORE/ (7 SQLite DBs with junk dictionary-word tables)
+-- THEMES/ (7 .json files with junk INI-style data)
+-- CONFIG/ (3 .json files with junk INI-style data)
+-- IMAGES/ (19 .png files -- padding)
+-- LOCALIZATION/ (32 fake translation .json files)
+-- MANUAL/ (10 .docx and .txt files -- padding)
```

Evasion Techniques

1. **File inflation:** 100MB data0.pak filled with junk SQLite databases and random dictionary words to exceed sandbox file size limits
2. **EV code signing:** Fraudulent "SERPENTINE SOLAR LIMITED" Sectigo EV certificate to bypass SmartScreen
3. **Windowless execution:** Uses pythonw.exe (no console window) for stealth
4. **In-memory payload:** CastleLoader shellcode never touches disk after decryption
5. **Language check:** Triage reports "Checks computer location settings" -- likely geofencing
6. **Legitimate Python runtime:** Uses official Python 3.14 binaries to avoid detection

Encrypted Payload (data1.pak)

- Size: 6,876,336 bytes
- Entropy: 8.0000 (maximum -- strong encryption)
- Block alignment: 16-byte aligned (AES)
- First 16 bytes (possible IV): **878fb3a337fddfbf0523d66ba3f5c828**
- Decryption: Requires extracting key from NSIS compiled script (not yet accomplished)

Threat Actor Profile

Attribution Assessment

- **Confidence:** MEDIUM-HIGH
- **Actor:** GrayBravo (Recorded Future designation, formerly TAG-150)
- **Country/Region:** Russia (evidence below)
- **Motivation:** Financial -- operates CastleLoader as a Malware-as-a-Service platform
- **Sophistication:** HIGH -- rapid development cycles, EV cert procurement, NSIS+Python+AES multi-layer delivery

Evidence for Russian Attribution

1. Previous code signing cert "NOBIS LLC" -- Russian LLC format
2. Previous cert "LLC Territory of Comfort" -- Russian-style company name
3. Historical C2 IP 94[.]159[.]113[.]32 registered to "Komskov Vadim Aleksandrovich" in Novotroitsk, Russia
4. CastleLoader checks system language/location -- common Russian actor geofencing (avoid CIS targets)
5. Domain name "maybedontbanplease" -- English with taunting tone, consistent with Russian-speaking operators who use English for infrastructure

OPSEC Observations

- Domain name suggests operator awareness they will be detected and banned
- Shift from Russian hosting (94.159.113.x) to 3NT Solutions (UK/NL) may indicate attempts to improve infrastructure resilience
- EV certificate procurement under fraudulent company name shows access to certificate broker/supply chain
- Using Google Cloud DNS for a malware C2 domain -- hiding behind legitimate DNS infrastructure
- Python 3.14.0 alpha 1 (Oct 2025 build) -- using bleeding-edge Python version, possibly to avoid detection rules targeting specific Python versions

CastleLoader Campaign Timeline

Date	Event
2025-11-05	First CastleLoader samples on MalwareBazaar (9 samples, signed by "LLC Territory of Comfort" and "NOBIS LLC")
2026-01-23	Additional CastleLoader samples submitted by JAMESWT_WT

Date	Event
2026-04-01	"SERPENTINE SOLAR LIMITED" EV cert issued by Sectigo
2026-04-02	maybedontbanplease[.]com registered via Global Domain Group LLC
2026-04-02	Let us Encrypt TLS cert issued for maybedontbanplease[.]com
2026-04-03	Sample build timestamp (file creation dates in NSIS archive)
2026-04-09	Sample submitted to MalwareBazaar by SquiblydooBlog
2026-04-09	C2 backend observed DOWN (504 Gateway Timeout)

MITRE ATT&CK Mapping

Tactic	Technique	ID	Application
Initial Access	User Execution	T1204.002	Victim runs trojanized NSIS installer
Execution	Command and Scripting Interpreter: Python	T1059.006	pythonw.exe runs decryption/loader script
Execution	Native API	T1106	VirtualAlloc, RtlMoveMemory for shellcode exec
Defense Evasion	Code Signing	T1553.002	Fraudulent EV cert "SERPENTINE SOLAR LIMITED"
Defense Evasion	Obfuscated Files or Information	T1027	AES-encrypted payload, junk padding files
Defense Evasion	Process Injection	T1055	WriteProcessMemory observed in sandbox
Defense Evasion	Virtualization/Sandbox Evasion	T1497	Language/location checks, 100MB file inflation
Defense Evasion	Masquerading	T1036.005	Payload renamed to vc_redist.x86.exe
Discovery	System Location Discovery	T1614	Checks computer location settings

Tactic	Technique	ID	Application
Command and Control	Application Layer Protocol: Web	T1071.001	HTTPS C2 via maybedontbanplease[.]com

IOC Summary

Network Indicators

IOC	Type	Context
maybedontbanplease[.]com	Domain	Active C2 domain
38[.]180[.]136[.]139	IPv4	Current C2 IP
94[.]159[.]113[.]32	IPv4	Historical CastleLoader C2
2a0c:6741::c2fc	IPv6	C2 AAAA record

File Indicators

Hash	Type	Description
4ba0d3ae41a0ae3143e8c2c3307c24b0d548593f97c79a30c0387b3d62504c31	SHA256	NSIS installer (this sample)
660efa6ef10d3f575bc3fadc207da050	MD5	NSIS installer
6d504e6af3124409d6c86b50a89a8c2e83f9ce31	SHA1	NSIS installer
46ce5c12b293febb513b196aa7f843	Imphash	NSIS installer import table

Code Signing Certificates

Subject CN	Issuer	Serial	Status
SERPENTINE SOLAR LIMITED	Sectigo Public Code Signing CA EV R36	a2c875fdd0d6fa22a2261813def8a56e	ACTIVE -- needs revocation

Subject CN	Issuer	Serial	Status
NOBIS LLC	GlobalSign GCC R45 EV CodeSigning CA 2020	7430df78b157110d91c7e0f0	Expired 2026-02-25
LLC Territory of Comfort	Unknown	Unknown	Unknown status

Behavioral Indicators

- User-Agent: GoogleBot (note: intentional misspelling of GoogleBot)
- Install path: %TEMP%\vc_redist.x86.exe
- Python runtime: pythonw.exe (windowless)
- NSIS plugins: System.dll, nsDialogs.dll

Recommended Actions

Immediate (24-48 hours)

- Block maybedontbanplease[.]com and 38[.]180[.]136[.]139 at perimeter
- Hunt for the code signing certificate thumbprint
e4253d8588b77541fc46bbc224a954770350c53cc2a69e6c3b20386282ccc9f5 in endpoint logs
- Search for pythonw.exe execution from %TEMP% directories
- Block the GoogleBot User-Agent string at web proxies

Short-term (1-2 weeks)

- Submit SERPENTINE SOLAR LIMITED cert to Sectigo for revocation
- Submit cert to abuse.ch CSCB
- Submit IOCs to ThreatFox
- Monitor for new CastleLoader domains with similar taunting naming patterns

Medium-term (1-3 months)

- Deploy YARA rules for CastleLoader NSIS+Python delivery pattern
- Monitor 3NT Solutions /24 for additional C2 infrastructure
- Track GrayBravo certificate procurement patterns

Abuse Reports

Sectigo (Certificate Revocation)

- Certificate: SERPENTINE SOLAR LIMITED (EV Code Signing)
- Serial: a2c875fdd0d6fa22a2261813def8a56e
- Evidence: Used to sign malware (CastleLoader), company does not exist in UK Companies House
- Contact: sslabuse@sectigo.com

3NT Solutions (Hosting)

- IP: 38[.]180[.]136[.]139
- Evidence: Hosting CastleLoader C2 infrastructure
- Contact: abuse@3nt.com

Global Domain Group (Registrar)

- Domain: maybedontbanplease.com
- Evidence: Registered for malware C2 operations
- Contact: abuse@globaldomaingroup.com

References

- [Blackpoint Cyber: "Snakes in the Castle: Inside the Walls of Python-Driven CastleLoader Delivery"](#)
- [ANY.RUN: CastleLoader Malware Analysis: Full Execution Breakdown](#)
- [Recorded Future: GrayBravo CastleLoader Activity Clusters](#)
- [The Hacker News: Four Threat Clusters Using CastleLoader](#)
- [Darktrace: CastleLoader & CastleRAT Behind TAG150](#)
- [Bitdefender: LummaStealer Second Life Alongside CastleLoader](#)
- [MalwareBazaar Sample](#)
- [Triage Sandbox Report](#)
- [ANY.RUN Sandbox](#)

Share 

Indicators of Compromise(3)

sha2564ba0d3ae41a0ae3143e8c2c3307c24b0d548593f97c79a30c0387b3d62504c31

sha256e4253d8588b77541fc46bbc224a954770350c53cc2a69e6c3b20386282ccc9f5

Related Reports

high

Vidar-as-a-Service: Stolen Certificates, Telegram Dead Drops, and the 185.56.45.235 C2 Infrastructure

4/19/2026

high

Smile Admin Panel

4/3/2026

medium

GlassWorm: 9 Infected VS Code Extensions Are Still Live -- Inside the Rust-Powered Supply Chain Attack Targeting Developers

3/16/2026