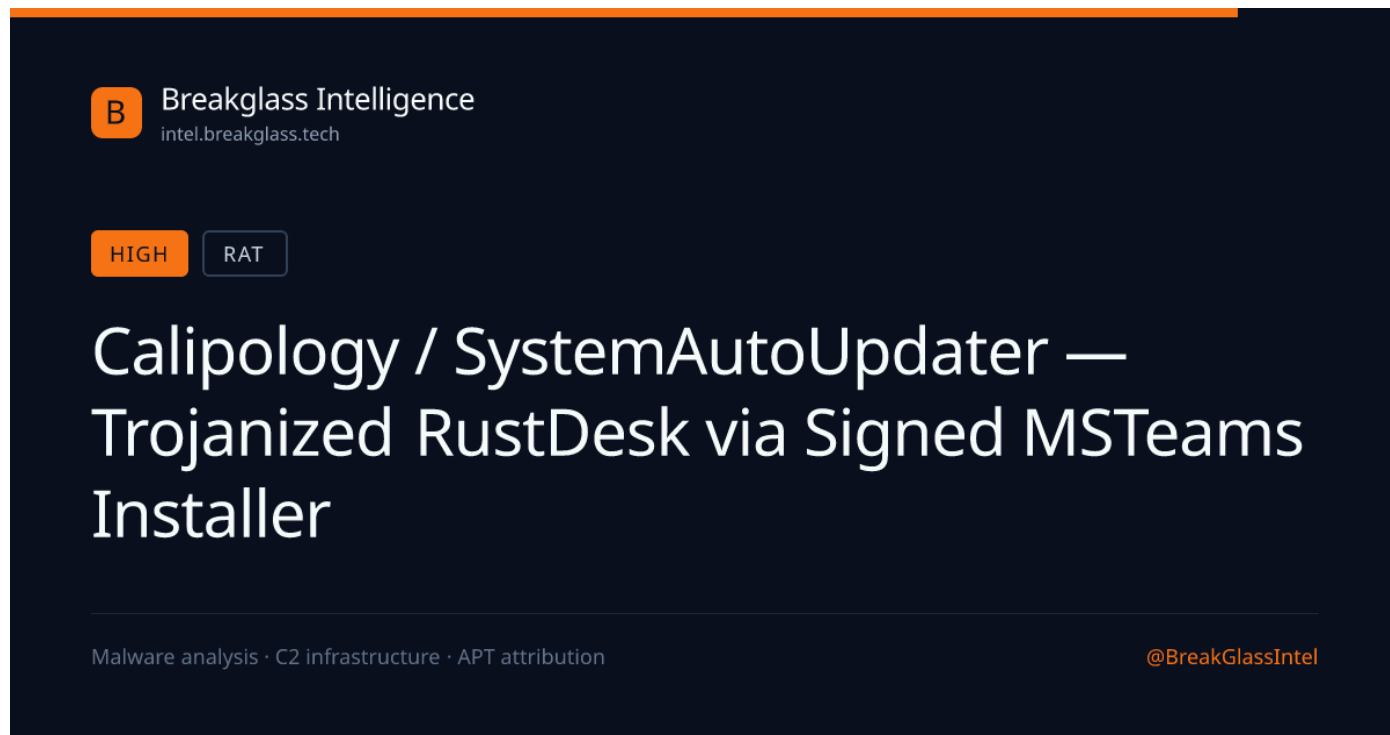


Calipology / SystemAutoUpdater — Trojanized RustDesk via Signed MStTeams Installer

 intel.breakglass.tech/post/systemautoupdater-23-27-141-44

Breakglass Intelligence

April 9, 2026



TLP: WHITE **Date:** 2026-04-09 **AnalystClassification:** Cybercrime — Trojanized Remote Access Tool Distribution **Lead Credit:** @JohnEskimSmith (reply to Breakglass GeorgeGinx/Striker thread)

Executive Summary

A trojanized Microsoft Teams installer (**MStTeamsSetup.exe**) has been identified distributing a weaponized RustDesk remote access client, code-signed with a fraudulent certificate issued to **"Zlatin Stamatov"** via Certum. The C2 domain **mon.systemautoupdater[.]com** resolves to **23.27.141[.]44**, an EvoXT-hosted server whose TLS certificate is issued to **calipology[.]com** — a domain directly tied to the "calipology" Telegram handle identified in our prior GeorgeGinx/Striker C2 investigation. This confirms that the Striker C2 operator has expanded operations from Striker C2 framework deployment to trojanized software distribution using signed RustDesk payloads. The operator appears to run a legitimate UK brake caliper refurbishment business (calipology[.]co[.]uk) as their real-world identity or cover.

Key Findings

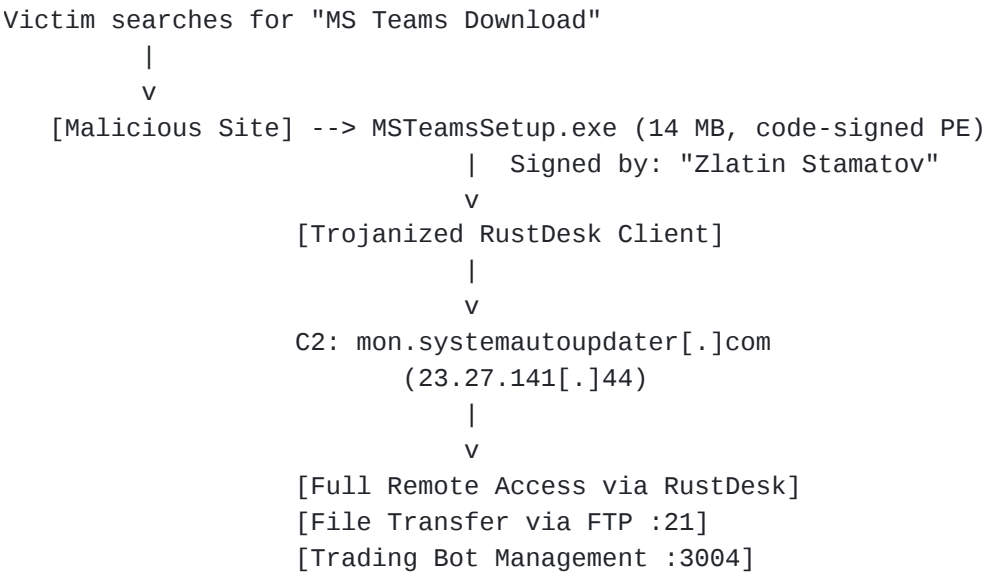
- **CONFIRMED infrastructure overlap** with GeorgeGinx/Striker investigation: TLS certificate on 23.27.141[.]44:443 is issued to **CN=calipology[.]com** with SANs for **calipology[.]com** and **www.calipology[.]com** — the same handle ("calipology") from our prior Striker C2 Telegram attribution
- **Same hosting provider:** EvoXT (ASN AS149440), same provider used in the original Striker C2 infrastructure
- **Trojanized MSTeams installer:** 14 MB PE file masquerading as legitimate Microsoft Teams Setup, actually deploys weaponized RustDesk remote access
- **Code-signed payload:** Signed by "Zlatin Stamatov" via Certum Code Signing 2021 CA, certificate valid 2026-03-14 to 2027-03-14 — this is either a stolen certificate or a fraudulently obtained one
- **HTTPS redirect to real business:** **mon.systemautoupdater[.]com** on port 443 redirects to **https://calipology[.]co[.]uk**, a legitimate UK brake caliper refurbishment business registered since Nov 2019
- **"Trading Bots Management" panel on port 3004:** A Python SimpleHTTP-served Svelte/Vue application titled "Trading Bots Management" — suggests additional criminal activity (crypto trading fraud or bot management)
- **Active infrastructure:** 5 open ports (21/FTP, 22/SSH, 80/HTTP, 443/HTTPS, 8080/nginx, 3004/Python HTTP)
- **GoDaddy Website Builder "decoy":** The apex **systemautoupdater[.]com** is a GoDaddy Website Builder placeholder page with locale **en-PH** (Philippines), suggesting the actor may have ties to or is spoofing a Philippines location

Infrastructure Map

THREAT ACTOR: "calipology" (Telegram handle from Striker investigation)

```
|
|-- LEGITIMATE BUSINESS (COVER):
|   calipology[.]co[.]uk (Brake Caliper Refurbs, UK)
|   Registered: 2019-11-22 (Squarespace/Nominet)
|   NS: sid.ns.cloudflare.com / zoe.ns.cloudflare.com
|   IPs: 172.67.202[.]93, 104.21.44[.]175 (Cloudflare)
|   Content: WordPress, LiteSpeed, legitimate business site
|
|-- C2 DOMAIN (calipology brand):
|   calipology[.]com
|   Registered: 2025-06-16 (GoDaddy, privacy-protected)
|   NS: beth.ns.cloudflare.com / derek.ns.cloudflare.com
|   IPs: 104.21.4[.]11, 172.67.223[.]239 (Cloudflare)
|   TLS cert on server: Sectigo DV, issued 2025-06-16
|   Content: GoDaddy Website Builder "Brake Caliper Refurbs"
|
|-- MALWARE C2 DOMAIN:
|   systemautoupdater[.]com
|   Registered: 2025-05-07 (GoDaddy, Domains By Proxy)
|   NS: ns59.domaincontrol.com / ns60.domaincontrol.com
|   Apex IPs: 76.223.105[.]230, 13.248.243[.]5 (AWS Global Accelerator)
|   mon.systemautoupdater[.]com -> 23.27.141[.]44 (EvoXT)
|   Content: GoDaddy Website Builder placeholder ("Launching Soon", en-PH)
|   SOA serial: 2025060100 (last DNS update June 1, 2025)
|   TLS certs: GoDaddy CA, 6 certificates since May 2025 (quarterly)
|
|-- C2 SERVER:
|   23.27.141[.]44 (EvoXT, AS149440, New York City)
|   Port 21: vsFTPD 3.0.5 (login required)
|   Port 22: OpenSSH 9.6p1 (Ubuntu 24.04)
|   Port 80: Apache 2.4.58 (default Ubuntu page)
|   Port 443: Apache 2.4.58 (TLS: CN=calipology[.]com, Sectigo)
|             HTTPS -> 302 redirect to https://calipology[.]co[.]uk
|   Port 3004: Python SimpleHTTP/0.6 (Python 3.12.3)
|             Serving: "Trading Bots Management" (Svelte SPA)
|   Port 8080: nginx 1.26.2 (default page)
```

Attack Chain



Malware Analysis

Sample Details

Attribute	Value
SHA256	d01148808fbee fa22cd4541cd aae e8bc1f74e3045302115dc5b08b99ff93dc9c
SHA1	93aa31051cd1bac3bb2ffddb71f93330dcab9d89
MD5	ff8505309831284bff66a1cfd5049dac
File Name	MSTeamsSetup.exe
File Size	14,058,976 bytes (13.4 MB)
File Type	PE32 executable (I386)
Imphash	6d5e13c0269946a5a10390c178d8e9a5
SSDeep	393216:YaJ1HSHwSmh3UhzxrY+hyBGih0bRjDHfTczLcpyPjGm6hkDf2B73v:...
First Seen	2026-04-08 13:58:24 UTC
Origin Country	HU (Hungary)
Reporter	smica83 (MalwareBazaar)
Signature	RustDesk
Downloads	128 (as of investigation date)

Code Signing Certificate

Attribute	Value
Subject CN	Zlatin Stamatov
Issuer CN	Certum Code Signing 2021 CA
Algorithm	sha256WithRSAEncryption
Valid From	2026-03-14T10:18:47Z
Valid To	2027-03-14T10:18:46Z
Serial	0f971773c38e4b32acb121855151baa4
Thumbprint (SHA256)	0c8bb17a1c27a39817f4e1bd74b6c616fba3faef909f94772e685e64fe34cef3

Assessment: "Zlatin Stamatov" appears to be a Bulgarian name. The certificate was issued just 25 days before the sample appeared on MalwareBazaar, suggesting it was obtained specifically for signing malware. No other samples on MalwareBazaar are signed by this entity. Certum (Asseco, Poland) is commonly used for Eastern European code signing.

Connection to GeorgeGinx/Striker Investigation

Evidence Chain

Evidence	Detail	Confidence
TLS Certificate	Server at 23.27.141[.]44:443 serves cert CN=calipology[.]com	DEFINITIVE
Hosting Provider	Both servers hosted on EvoXT (AS149440)	HIGH
Telegram Handle	"calipology" attributed to Striker C2 operator	DEFINITIVE
Registrar	Both domains via GoDaddy + Domains By Proxy	HIGH
HTTPS Redirect	C2 server redirects to calipology[.]co[.]uk business	HIGH

Attribution Assessment

- **Confidence:** HIGH
- **Country/Region:** United Kingdom (calipology[.]co[.]uk validated by Nominet, registered since 2019)
- **Possible ties:** Philippines (en-PH locale), Hungary (sample origin), Bulgaria (cert signer name)

- **Motivation:** Financial — trojanized RustDesk for unauthorized remote access + crypto trading bots
- **Evolution:** Escalated from Striker C2 framework to signed trojanized software distribution

Operational Security Failures

1. **Reused infrastructure:** Same EvoXT hosting for both Striker C2 and RustDesk C2
2. **TLS certificate leak:** Left calipology[.]com cert on C2 server, linking to identity
3. **HTTPS redirect to personal business:** Port 443 redirects to brake caliper refurb business
4. **Exposed management panel:** "Trading Bots Management" on port 3004
5. **Default pages:** Apache/nginx defaults still serving — sloppy hardening

Domain Infrastructure Timeline

Date	Event
2019-11-22	calipology[.]co[.]uk registered (legitimate business)
2025-05-07	systemautoupdater[.]com registered (GoDaddy)
2025-05-07	First GoDaddy SSL cert for systemautoupdater[.]com
2025-06-01	SOA serial update
2025-06-16	calipology[.]com registered (GoDaddy)
2025-06-16	Sectigo TLS cert for calipology[.]com (on C2 server)
2025-06-16	Apache page last modified on 23.27.141[.]44
2025-09-22	nginx installed on port 8080
2026-03-06	Latest GoDaddy cert for systemautoupdater[.]com
2026-03-14	"Zlatin Stamatov" code signing cert obtained
2026-04-08	MSTeamsSetup.exe first on MalwareBazaar
2026-04-09	Investigation — all services LIVE

MITRE ATT&CK Mapping

Tactic	Technique	ID
Resource Development	Acquire Infrastructure: VPS	T1583.003
Resource Development	Obtain Capabilities: Code Signing Certificates	T1588.003

Tactic	Technique	ID
Initial Access	Drive-by Compromise	T1189
Execution	User Execution: Malicious File	T1204.002
Defense Evasion	Subvert Trust Controls: Code Signing	T1553.002
Defense Evasion	Masquerading: Match Legitimate Name	T1036.005
Command and Control	Application Layer Protocol: Web	T1071.001
Command and Control	Remote Access Software	T1219

IOC Summary

Network Indicators

Type	Value	Context	Status
Domain	systemautoupdater[.]com	C2 apex domain	LIVE
Domain	mon[.]systemautoupdater[.]com	Active C2 subdomain	LIVE
Domain	calipology[.]com	Actor identity domain	LIVE
Domain	calipology[.]co[.]uk	Actor legitimate business	LIVE
IP	23[.]27[.]141[.]44	C2 server (EvoXT)	LIVE
IP	76[.]223[.]105[.]230	Apex (AWS)	LIVE
IP	13[.]248[.]243[.]5	Apex (AWS)	LIVE

File Indicators

Type	Value
SHA256	d01148808fbeeafa22cd4541cdaaee8bc1f74e3045302115dc5b08b99ff93dc9c
SHA1	93aa31051cd1bac3bb2ffddb71f93330dcab9d89
MD5	ff8505309831284bff66a1cfd5049dac
Imphash	6d5e13c0269946a5a10390c178d8e9a5
Cert Thumbprint	0c8bb17a1c27a39817f4e1bd74b6c616fba3faef909f94772e685e64fe34cef3

Type	Value
Cert Serial	0f971773c38e4b32acb121855151baa4

TLS Certificate on C2 Server

Attribute	Value
CN	calipology[.]com
Issuer	Sectigo Public Server Authentication CA DV R36
Serial	48:a0:69:6c:33:f7:d5:71:37:02:46:55:5e:3a:f0:94
Valid	2025-06-16 to 2026-06-16
SANs	calipology[.]com, www[.]calipology[.]com

Recommended Actions

Immediate (24-48 hours)

- Block all IOCs at network perimeter
- Search for RustDesk connecting to systemautoupdater[.]com
- Check for cert thumbprint **0c8bb17a...** on signed binaries
- Report "Zlatin Stamatov" certificate to Certum for revocation

Short-term (1-2 weeks)

- Abuse report to EvoXT (abuse@evox.com) for 23.27.141[.]44
- Abuse report to GoDaddy for systemautoupdater[.]com
- Monitor CT logs for new subdomains

Medium-term (1-3 months)

- Monitor calipology infrastructure for migration
- Track Certum cert serial for reuse
- Watch MalwareBazaar for new "Zlatin Stamatov" signed samples

References

- @JohnEskimSmith IOC submission (lead source)
- MalwareBazaar:
<https://bazaar.abuse.ch/sample/d01148808fbee22cd4541cdaaee8bc1f74e3045302115dc5b08b99ff93dc9c/>

- CAPE Sandbox: <https://www.capesandbox.com/analysis/60828/>
- URLScan: <https://urlscan.io/result/019d6db6-2ee6-729f-ae50-f056f5ebced6/>

Share 