

Silver Fox Wraps ValleyRAT in ZPAQ and a ByteDance Binary: A Telegram Chinese Language Pack MSI Lure

 intel.breakglass.tech/post/silverfox-valleyrat-telegram-chinese-langpack-zpaq-bytedance-ctg

Breakglass Intelligence

April 8, 2026

BREAKGLASS INTELLIGENCE

Threat Intelligence & Security Research

intel.breakglass.tech

@BreakGlassIntel

TL;DR

On **April 8, 2026**, a weaponized MSI installer disguised as a Telegram Chinese language pack — [点击安装中文语言包a.msi](#) — surfaced on MalwareBazaar (reported by **CNGaoLing**). The sample delivers **ValleyRAT** with a kernel-mode rootkit and employs a six-stage infection chain built around a legitimate **zpaqfranz** decompression binary used as a LOLBin, a **ByteDance/TikTok** elevation service binary used as a DLL sideloading host, and a vulnerable **wnBios** BIOS driver used via BYOVD for physical memory access.

Runtime, tooling, AV-targeting logic, and infrastructure all match **Silver Fox APT** (also tracked as SwimSnake, The Great Thief of Valley, UTG-Q-1000, Void Arachne) — a Chinese-nexus cybercrime crew extensively documented by Fortinet, Forescout, Qi'anxin, and others. The C2 [118.107.43.65:5040](#) is hosted by **CTG Server Ltd** (Hong Kong), the same bulletproof hosting network repeatedly tied to this actor.

What this report adds to the public record:

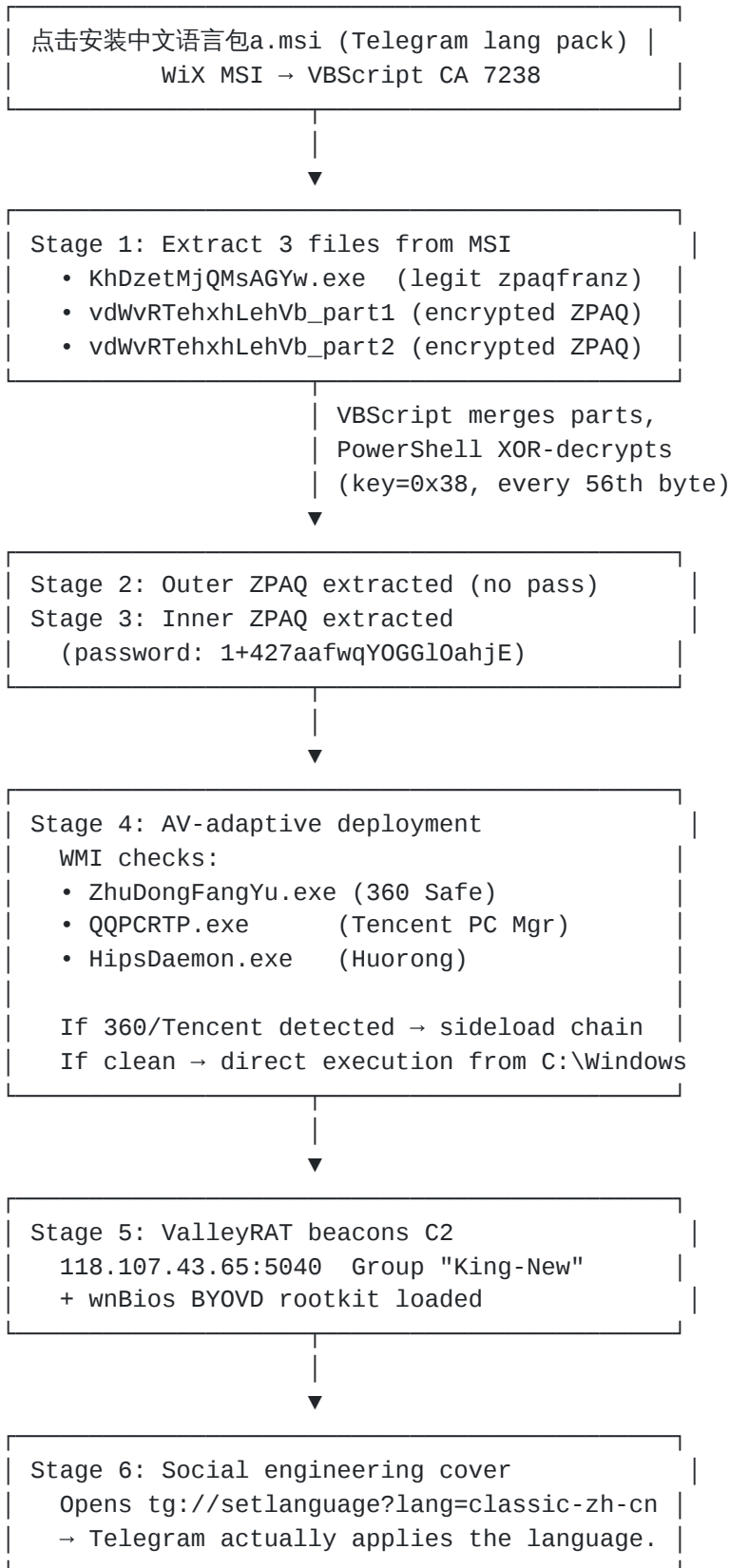
- Documents a fresh Silver Fox delivery chain using **ZPAQ compression** (via the legitimate [zpaqfranz](#) v60/v63.2 binary) as a LOLBin packer — an uncommon choice in malware that sidesteps 7-Zip/WinRAR signatures
- Details DLL sideloading via a **ByteDance SodaMusicLauncher.exe** (AppShell Elevation Service) binary — abuse of a signed binary from one of China's largest tech companies
- Captures the operator identifier **King-New** and campaign tag **mEGLoIEgCfaQ** from the ValleyRAT runtime configuration string
- Provides the active C2 and CTG Server bulletproof netblock for defenders

Hat tip to [CNGaoLing](#) for the sample on MalwareBazaar. If you've published prior reporting on this cluster, operator handle, or tooling variant and we missed it, please [reach out](#) — we'll update and credit.

The Sample

Property	Value
Filename	点击安装中文语言包a.msi ("Click to Install Chinese Language Pack a")
SHA256	8b3a49e89932a7c371ceca9ecbc6c0151e38dc97c191f7a0aa92a8baa8b6e8ab
MD5	89e11f8b8f81a0a111bc99ba631ca85d
File Type	MSI Installer (WiX Toolset 3.14.1.8722)
File Size	4,710,400 bytes (4.49 MB)
Product Name	IssueAccentRequest
Created	2026-03-24 10:32 UTC
First seen on MalwareBazaar	2026-04-08 06:45 UTC
Reporter	CNGaoLing
MB Tags	Gh0stRAT, MSI, SilverFox, ValleyRAT

Six-Stage Infection Chain



The MSI sets `ARPSYSTEMCOMPONENT=1` to hide from Add/Remove Programs and runs its VBScript custom action at sequence 4001 (right after file extraction) as SYSTEM via type 7238 (deferred, no impersonation).

The ZPAQ LOLBin Angle

The packer of choice here is **ZPAQ**, an archival format with a journaling option that is almost never seen in malware. The dropper ships a signed, legitimate copy of `zpaqfranz` (v60/v63.2, 3.7 MB) renamed to `KhDzetMjQMsAGYw.exe` and uses it as a LOLBin to extract two nested archives — one unkeyed, one password-protected (`1+427aafwqY0GG10ahjE`).

The point of using `zpaqfranz` instead of `7z.exe` or PowerShell's `Expand-Archive` is to sidestep the large body of static and behavioral detections that key on 7-Zip and WinRAR extraction by malware droppers. Defenders should treat `zpaqfranz.exe` execution outside of backup/developer workstations as high-signal.

ByteDance `SodaMusicLauncher.exe` Sideloaded

When the VBScript detects **Qihoo 360** or **Tencent PC Manager** running, it pivots into a quieter execution mode: instead of dropping the ValleyRAT binary directly into `C:\Windows\`, it deploys a DLL sideloading chain using a **legitimate ByteDance binary**.

Property	Value
File	<code>SodaMusicLauncher.exe</code>
Signer	Beijing Microlive Vision Technology Co., Ltd. / Beijing Bytedance Network Technology Co., Ltd.
Role	ByteDance AppShell Elevation Service
Service Name	<code>AppShellElevationService</code>
Registry Key	<code>SOFTWARE\ByteDance\AppShell</code>
CLSID	<code>{63C34537-A073-440B-A889-8BFDCCCE724F3}</code>

The actor drops malicious `powrprof.dll` and `wsc.dll` next to this binary so that loading either DLL (triggered by the ByteDance binary's normal startup) gives them code execution inside a trusted, signed process context. The choice of a ByteDance binary is operationally interesting — signed binaries from Chinese tech majors are almost always allowlisted on Chinese-market endpoints, including the very 360/Tencent products Silver Fox is trying to evade.

A `launcher_config.json` configures persistence under `SingMusice`:

```
{"app_name": "SingMusice", "cur_path": "/", "run_name": "SodaMusicLauncher"}
```

ValleyRAT Runtime Configuration

The ValleyRAT binary is a **Nim-compiled PE64** (MinGW GCC 15.1.0, 711,168 bytes) with a `.rdata` section entropy of 7.98 — consistent with an encrypted configuration / shellcode blob. The embedded configuration string is underscore-delimited:

```
SEJLPw8_IssueAccentRequest_GjdLUhqZIJJB_mEGLoIEgCfaQ_LocateHighlightTensorFlow_118.107.43.65_King-New_eRMqYUTL_1_TriggerMonitorStudioOne_.exe
```

Field	Value
Campaign ID	mEGLoIEgCfaQ
C2 IP	118.107.43.65
Operator Group	King-New
Kernel driver	eRMqYUTL
Persistence dir	TriggerMonitorStudioOne

A second Nim binary, `DesignAccent.exe` (Nim 2.2.6, MinGW GCC 15.1.0), is deployed as a scheduled task. It imports `httpclient`, `httpcore`, `base64`, `sha256`, `jpeg`, `png`, and `simd` — the image modules are consistent with either steganographic C2 or screenshot capability. Its C2 URL is not stored in plaintext; the `.rdata` entropy is 7.75.

wnBios BYOVD Kernel Rootkit

The dropper ships `pagmuAYJrRPZXvMRuTwfEPWXMkKHbP` — a 23,352-byte kernel driver whose PDB path gives it away:

```
c:\winddk\7600.16385.1\wincor\wnbios1.2.0.0\amd64\wnBios.pdb
```

This is **wnBios 1.2.0.0**, a legitimate Wincor Nixdorf BIOS access driver whose `MmAllocateContiguousMemory`, `MmGetPhysicalAddress`, and `ZwMapViewOfSection` primitives provide arbitrary physical memory read/write — the classic BYOVD toolkit for disabling kernel-mode security products, patching PatchGuard callbacks, and hiding processes or files. The `eRMqYUTL.sys` blob alongside it (1.16 MB, entropy 8.00) is encrypted shellcode loaded by this driver at runtime.

C2 Server — 118.107.43.65 on CTG Server Ltd

Property	Value
IP	118.107.43.65
Open ports (external)	5040/tcp (C2), 139/tcp (NetBIOS)
OS	Microsoft Windows
Provider	CTG Server Ltd (Hong Kong)
Netblock	118.107.40.0/21
Abuse	cs.mail@ctgserver.com
Registrant	BGP Consultancy Pte Ltd (Singapore)

The C2 IP has no reverse DNS and no Shodan/InternetDB surface — the operator is actively filtering passive scanners. Only the custom C2 port and NetBIOS are visible externally. CTG Server / RACKIP has been documented repeatedly as a preferred bulletproof host for Silver Fox operations, and the adjacent 118.107.47.0/24 subnet hosts a separate multi-tenant cybercrime block (91pronFree k3s microservice farm, Taiwan lottery gambling networks, solxnk.com DeFi scam platform, and a Nacos service registry with default creds leaking the entire internal architecture).

Attribution — Silver Fox, High Confidence

Evidence	Detail
Infrastructure	CTG Server Ltd (HK) — recurrent Silver Fox hoster
Tooling trifecta	ValleyRAT + BYOVD rootkit + DLL sideloading
AV targeting	Specific Chinese AV enumeration (360/Tencent/Huorong)
Lure theme	Telegram Chinese language pack — matches the actor's pattern of impersonating popular Chinese-language software (Teams, Zoom, Signal, Taiwan tax)
Signed host	ByteDance binary abuse — pattern of using legitimate Chinese tech company binaries
Operator tag	King-New — possible operator or campaign cluster identifier

Silver Fox is a dual-purpose Chinese-nexus crew operating in the murky intersection of cybercrime and state-aligned espionage. Known targets span Chinese-speaking populations across China, Taiwan, Hong Kong, Singapore, Malaysia, Japan, the Philippines, Thailand, Vietnam, and India.

Detections & Hunting

1. **Block** `118.107.43.65` at the perimeter. If operationally feasible, block `118.107.40.0/21` (CTG Server bulletproof netblock).
2. **Hunt** for process names `GjdLUhqZIJJB.exe`, `SingMusice.exe`, `DesignAccent.exe`.
3. **Alert** on MSI installations with VBScript custom actions (type 7238) spawning PowerShell.
4. **Alert** on `zpaqfranz.exe` execution outside known developer/backup workstations.
5. **Monitor** service creation of `AppShellElevationService` with non-standard binary paths.
6. **Monitor** for `tg://setlanguage` URI handlers invoked by non-Telegram processes.
7. **Hunt** for kernel driver load events where the image path contains `wnBios` or matches the PDB `wnbios1.2.0.0`.

MITRE ATT&CK

T1566.002 · T1204.002 · T1218.007 · T1059.005 · T1059.001 · T1053.005 · T1574.002 · T1068 · T1036 · T1027 · T1497.001 · T1014 · T1070 · T1057 · T1082 · T1571 · T1071.001

IOCs

SHA256

8b3a49e89932a7c371ceca9ecbc6c0151e38dc97c191f7a0aa92a8baa8b6e8ab 点击安装中文语言包a.msi

Network

118.107.43.65:5040	ValleyRAT C2 (CTG Server Ltd, HK)
118.107.40.0/21	CTG Server Ltd bulletproof netblock

Runtime identifiers

mEGLoIEgCfaQ	Campaign ID
King-New	Operator group
IssueAccentRequest	MSI product name / install dir
TriggerMonitorStudioOne	Persistence directory
AppShellElevationService	Sideloaded service name
1+427aafwqYOGG10ahjE	Inner ZPAQ archive password
0x38	XOR key

Targeted AV processes

ZhuDongFangYu.exe	Qihoo 360 Active Defense
QQPC RTP.exe	Tencent PC Manager
HipsDaemon.exe	Huorong HIPS

Share 

Related Reports

[high](#)

[Multi-RAT Operation Dismantled: WaterHydra APT Nexus, Five AES Keys Recovered, and Live C2 Infrastructure Mapped Across Three Continents](#)

[3/7/2026](#)