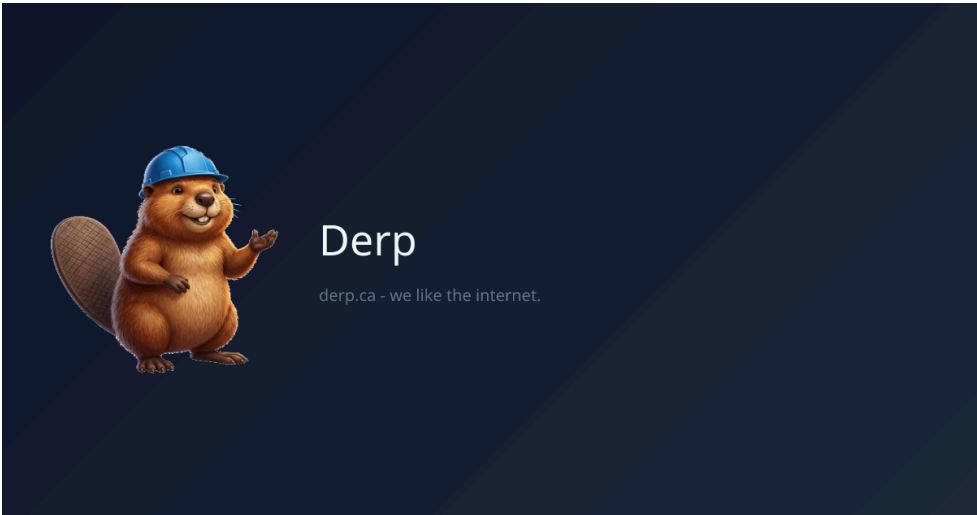


Remcos Banking Fraud via Three Autolt Persistence Chains

derp.ca/research/remcos-autoit-persistence

Kirk

February 24, 2026



malwareremcosautoitincident-responsepurehvincbanking-fraud

Three parallel persistence chains survived every cleanup attempt. Each one impersonates a legitimate business application, installs itself in %LocalAppData% under a professional-sounding directory name, and registers a scheduled task that respawns the payload every few minutes. Two of them deliver Remcos v7.0.1 Pro configured to screenshot Canadian banking portals every five seconds. The third delivers PureHVNC.

This is the fourth post in the [SERPENTINE#CLOUD](#) breach analysis series, following [PureLogs](#), [PureCrypter](#), and [Violet RAT](#). Where those posts covered the Python-based loader chain and its payloads, this one covers the Autolt-based persistence layer that kept everything alive.

Tria.ge and VT refresh (2026-02-26)

We submitted the full Remcos and UrbanEco payload set to Tria.ge on 2026-02-26 and refreshed VirusTotal detections.

SHA-256	Tria.ge	Score	Family
85b6e2db29ee84d25cc2d942fb181581279b87176880790fda0c3c60d9186ee2	https://tria.ge/260226-nwx3acw3g	10	remcos
378b201a0979aff7182edca69148269c9c6685064cac5b7cdcc98375af2fd123	https://tria.ge/260226-nwx3acw3h	10	remcos
29648ce421e80a3d573bdae593d86c53343933373b400c8ce781dd22fbc82176	https://tria.ge/260226-nwxj1acw4a	10	remcos
739a238220890cb4d65d8f696f9f73bb9390ef526875b2136e3bba6b03c7040a	https://tria.ge/260226-nwxvcsw4b	7	--
e3074f9377f4d4b3d3140486cc0cfc5b4b00e583fdc583b716609713ff8e9307	https://tria.ge/260226-nwx55acw4c	3	--
9e709cf922e02bca148866fc84dc783c39e2f51adea4f9179fdd7a1381331fc9	https://tria.ge/260226-nwv1rscw3e	1	--
656775d0dae805523711e08cd4e5882d0f10ec5105acb5ca5da373ccf6759392	https://tria.ge/260226-nwxbjacw3f	1	--

SHA-256	Tria.ge	Score	Family
f8147fb707e8cf6c4f0323eb81d695ffb3a4b14ee4dbb87147750db114c5a165	https://tria.ge/260226-nwyfwscw4d	1	--

Three chains, three payloads

Chain	Directory	Scheduled task	.a3x script	Decoder function	Payload
EcoOptimize	%LocalAppData%\EcoOptimize Solutions\	Cancellation, Involved	r.a3x	MYERSCOMPLAINTS	Remcos x64 PE
WealthWise	%LocalAppData%\WealthWise Analytics Inc\	QuantifyPro	X.a3x	MOMSMEN	Remcos x64 PE
UrbanEco	%LocalAppData%\UrbanEco Innovations\	EcoMap	Q.a3x	TUBECAREFUL	PureHVNC (.NET)

All three chains use the same interpreter binary: `Singer.pif`, a renamed copy of `AutoIt3.exe`.

Artifact	SHA-256	VT	Tria.ge
Singer.pif (Autolt3.exe)	881619a47b62b52305d92640cc4d4845a279c23a5a749413785fc8fcb0fdf7fb	3/76	--
r.a3x (EcoOptimize)	9e709cf922e02bca148866fc84dc783c39e2f51adea4f9179fdd7a1381331fc9	3/76	https://tria.ge/260226-nw1rscw3e (score 1)
EcoOptimize packed PE	656775d0dae805523711e08cd4e5882d0f10ec5105acb5ca5da373ccf6759392	Not indexed	https://tria.ge/260226-nwbbjacw3f (score 1)
EcoOptimize Remcos PE	85b6e2db29ee84d25cc2d942fb181581279b87176880790fda0c3c60d9186ee2	29/76	https://tria.ge/260226-nwwx3acw3g (score 10, remcos)
WealthWise Remcos PE (packed)	378b201a0979aff7182edca69148269c9c6685064cac5b7cdcc98375af2fd123	31/76	https://tria.ge/260226-nwwx3acw3h (score 10, remcos)
WealthWise Remcos PE (unpacked)	29648ce421e80a3d573bdae593d86c53343933373b400c8ce781dd22fbc82176	44/76	https://tria.ge/260226-nwxjlcw4a (score 10, remcos)
UrbanEco Q payload (encrypted)	f8147fb707e8cf6c4f0323eb81d695ffb3a4b14ee4dbb87147750db114c5a165	3/76	https://tria.ge/260226-nwyfwscw4d (score 1)
UrbanEco .NET crypter (Oktszoqyxp.exe)	739a238220890cb4d65d8f696f9f73bb9390ef526875b2136e3bba6b03c7040a	41/76	https://tria.ge/260226-nwxcscw4b (score 7)
UrbanEco PureHVNC (Efjzzebatj.dll)	e3074f9377f4d4b3d3140486cc0cfc5b4b00e583fdc583b716609713ff8e9307	29/76	https://tria.ge/260226-nwx55acw4c (score 3)

The persistence mechanism: Autolt BYOI

The technique is **Bring Your Own Interpreter**. `Singer.pif` is a legitimate, Authenticode-signed copy of `Autolt3.exe` (3/76 on VirusTotal at refresh time). Because the interpreter itself is clean, antivirus has to detect the compiled script -- a `.a3x` file containing obfuscated control flow and encoded payloads.

Script obfuscation

Each `.a3x` script uses the same pattern: a decoder function with a unique name, control flow flattening through nested loops, and dash-separated decimal encoding for string constants. The decoder function name varies per chain -- MYERSCOMPLAINTS, MOMSMEN, TUBECAREFUL -- but the algorithm is identical. Each dash-separated token is converted to a character code and reassembled into a string.

Payload extraction pipeline

```
Singer.pif (AutoIt3.exe)
→ .a3x compiled script
→ Decoder function extracts hex string from $VARIABLE
→ RC4 decrypt (unique key per chain)
→ LZNT1 decompress
→ PE payload
→ Process hollowing into child process
```

The Remcos chains (EcoOptimize, WealthWise) hollow into `TapiUnattend.exe` -- a legitimate Windows binary in `System32`. The PureHVNC chain (UrbanEco) hollows into `RegAsm.exe`, a .NET Framework binary, because PureHVNC requires the CLR.

Scheduled task persistence

Each chain registers Windows scheduled tasks with benign-sounding names. EcoOptimize uses two tasks (`Cancellation` and `Involved`), both triggering via `wscript.exe` every 5 minutes. WealthWise uses `QuantifyPro`. The tasks call back to the persistence directory where `Singer.pif` and the `.a3x` script sit, restarting the chain if it dies.

On one compromised machine, Defender detected `QuantifyPro.bat` (the WealthWise chain) 3,560 times across two days. Every ~69 seconds the scheduled task respawned the process, Defender killed it, and the task spawned it again. Defender couldn't remove the scheduled task itself.

Remcos v7.0.1 Pro -- banking fraud configuration

The EcoOptimize Remcos config contains 58 fields extracted from an RC4 + LZNT1 encrypted SETTINGS resource. The RC4 key is embedded in the PE's resource section. After decryption and decompression, the config is 2,467 bytes.

C2 infrastructure

Nine domains, all on port 4056 with **mutual TLS**:

#	Domain	Port	TLS
1	homoney177.duckdns.org	4056	Yes
2	homoney177.food	4056	Yes
3	homoney177.click	4056	Yes
4	homoney177.shop	4056	Yes
5	homoney177.strangled.net	4056	Yes
6	homoney17.duckdns.org	4056	Yes

#	Domain	Port	TLS
7	homoney1.duckdns.org	4056	Yes
8	homoney1.mooo.com	4056	Yes
9	homoney17.twilightparadox.com	4056	Yes

Three base names ([homoney1](#), [homoney17](#), [homoney177](#)) spread across five DDNS and domain providers -- DuckDNS, Afraid.org FreeDNS ([mooo.com](#), [strangled.net](#), [twilightparadox.com](#)), and cheap gTLDs ([.food](#), [.click](#), [.shop](#)). This layout gives cross-provider fallback when domains are removed.

As of 2026-02-26, the three DuckDNS entries still resolve to [91.219.238.167](#) (ServerAstra, Budapest HU), the three FreeDNS entries resolve to [127.0.0.2](#) sinkholes, and the three paid TLD entries are NXDOMAIN.

Mutual TLS with ECC P-256

Both the client certificate and server certificate are embedded in the config. Both are self-signed ECC P-256 with ECDSA-SHA256 signatures, valid from 1970-01-01 to 2090-12-31 -- the epoch-to-far-future range that Remcos generates by default. The client's private key is also embedded, meaning anyone who extracts the config can impersonate the bot to the C2 server.

Certificate	SHA-256 fingerprint
Client cert	dd492c49a69c45f21c47d41c87d6656d1b8c270e7f493affd728e03afb4c5a4b
Server cert	48d2265b561fb58e4864f9c3eee263eb6fcb858c53f2c630ac0d9c0ab1c7b410
Client private key (d)	91b4f6454440320d8fcfb08c721ef3925c39742ba3953dfbe376e0d382b4e60c

The banking keyword list

Remcos can trigger targeted screenshots when a window title matches a keyword. The EcoOptimize config has this enabled with 62 keywords and a 5-second capture interval. When the victim opens a banking portal, Remcos starts screenshotting every 5 seconds until the window closes.

Canadian banks (9 keywords): [royal](#), [rbc](#), [bmo](#), [scotia](#), [Desjardins](#), [cibc](#), [EasyWeb](#), [tdbank](#), [td](#)

US banks (3): [wellsfargo](#), [truist](#), [chase](#)

Payment processors (15): [paytrace](#), [shopify](#), [square](#), [visa](#), [master](#), [amex](#), [globalgateway](#), [firstdata](#), [nuvei](#), [merchant](#), [american express](#), [paypal](#), [Venmo](#), [Google Pay](#), [bitpay](#)

Crypto wallets (17): [vanguard](#), [fidelity](#), [atomic](#), [ledger](#), [crypto](#), [wallet](#), [ledger live](#), [password phrase](#), [exodus](#), [atomic wallet](#), [exodus wallet](#), [meta](#), [meta mask](#), [trust](#), [trust wallet](#), [blockchain](#)

Payment form fields (11): [cvv](#), [csc](#), [pin](#), [security code](#), [cvc](#), [Expiration date](#), [payment method](#), [payment option](#), [card number](#), [security question](#), [security phrase](#)

General financial (7): [quickbook](#), [adp](#), [intuit](#), [bank](#), [credit union](#), [credit](#), [debit](#)

The list is heavily weighted toward Canadian banks. Every major one is covered by name. [EasyWeb](#) is TD Bank's online banking portal -- targeting the portal name rather than just the bank name catches the actual session.

Screenshots and keylogger

Screenshots land in `%PROGRAMFILES%\Spotify\` as JPEG files named `wnd_YYYYMMDD_HHMMSS.jpg`. The keylogger writes to `spotify.dat` inside `%APPDATA%\ledger spotify\`. The keylogger runs in mode 1 -- all windows, not just targeted ones -- with no file size limit and no encryption. Everything is disguised as Spotify data.

We recovered 402 banking screenshots from the `Spotify/` folder on one of the compromised workstations. They are not HVNC captures -- they are Remcos targeted screenshots triggered by the 62-keyword filter, captured every 5 seconds while the victim browsed banking portals.

Config summary

Field	Value
Version	Remcos v7.0.1 Pro
Campaign ID	With SC
Mutex	Rmc-i8364b-6EJSJD
HWID	32E72218F60ECBCC34247ED29838BD98
Install filename	remcos.exe
Install directory	Remcos in %APPDATA% (hidden)
Keylog file	spotify.dat in %APPDATA%\ledger spotify\
Keylog mode	1 (all windows)
Screenshot folder	Spotify in %PROGRAMFILES%
Screenshot trigger	62 keywords, 5-second interval
Audio folder	MicRecords in %LOCALAPPDATA%
Persistence	HKCU + HKLM Run keys

Config evolution -- same operator, refined targeting

WealthWise delivers a second Remcos build. Field-by-field comparison: 54 of 58 config fields are byte-identical between EcoOptimize and WealthWise. Four fields differ.

The four differences

Field	EcoOptimize	WealthWise
C2 list	9 servers, port 4056	10 servers, port 4057
Mutex	Rmc-i8364b-6EJSJD	Rmc-i8364b-9TU31H
Keywords	62	50
HWID	32E72218F60ECBCC34247ED29838BD98	4CB274427DD8A8917007E4F7ADA6E41E

Everything else is identical: campaign ID (`With SC`), install filename (`remcos.exe`), keylog file (`spotify.dat`), screenshot folder (`Spotify`), keylogger root directory (`ledger spotify`), audio folder (`MicRecords`), all boolean flags, all directory assignments. Same operator, same Remcos builder template, incremented for a second deployment.

Identical TLS certificates

The strongest same-operator evidence: both configs embed the same client certificate, the same server certificate, and the same ECC private key. The SHA-256 fingerprints match byte-for-byte:

- Client cert: `dd492c49...afb4c5a4b` (identical)
- Server cert: `48d2265b...ab1c7b410` (identical)
- Private key d-value: `91b4f645...82b4e60c` (identical)

These certificates were generated once in the Remcos builder and reused across both configs. Sharing the private key means both Remcos instances authenticate to the same C2 infrastructure with the same identity.

C2 expansion

WealthWise increments the port from 4056 to 4057, keeps all 9 original domains, and adds one new domain: `yrem472hd.duckdns.org`. This is the only domain that breaks the `homoney` naming pattern. The random-style name suggests the operator was testing a second naming convention.

Keyword reduction: 62 to 50

WealthWise drops 12 keywords. The removals fall into two categories:

Crypto wallet brands removed (10): `exodus`, `atomic wallet`, `exodus wallet`, `meta`, `meta mask`, `trust`, `trust wallet`, `blockchain`, `bitpay`, and a duplicate `atomic` entry.

TD Bank keywords removed (2): `tdbank`, `td`.

Generic crypto terms (`crypto`, `wallet`, `ledger`) survived. The specific wallet app names (Exodus, MetaMask, Trust Wallet, Atomic Wallet) were cut. And while `tdbank` and `td` were removed, `EasyWeb` -- TD's online banking portal -- was retained. The operator still targets TD customers. They just stopped matching on the bank name and kept only the portal name.

The keyword changes show a narrower target set: specific wallet app names were removed, and bank matching shifted toward portal names rather than brand names. The result is a move from broad crypto-plus-banking monitoring to focused banking fraud.

UrbanEco -- PureHVNC, not Remcos

The third Autolt chain doesn't deliver Remcos. It delivers PureHVNC through five layers of nesting:

```
Singer.pif (AutoIt3.exe)
  → Q (.a3x, TUBECAREFUL decoder)
    → RC4 + LZNT1 → 0ktszoqyrp.exe (.NET AES crypter, 331 KB)
      → AES-256-CBC + GZip → Efjzzebatj.dll (PureHVNC, 790 KB)
        → Assembly.Load + reflective invoke
```

The first two layers match the Remcos chains: Autolt interpreter loads the compiled script, the script decodes and RC4-decrypts the hex payload, LZNT1 (Windows native compression) decompresses it. But instead of a Remcos PE, the output is a 32-bit .NET assembly -- `0ktszoqyrp.exe`, an AES crypter.

Cracking the .NET crypter

IL disassembly of `0ktszoqyrp.exe` revealed two base64-encoded values loaded via `ldstr`:

Parameter	Base64	Hex
AES-256 key	<code>0+vTjfNxTAUtnLSPyNd5zRPnPCLOizfCh+wp5q2/hSI=</code>	<code>3bebd38df3714c052d9cb48fc8d779cd13e73c22ce8b37c287e5a9e6adbf85</code>
AES IV	<code>4oEV6XwpX/PtkgUSmaymbA==</code>	<code>e28115e97c29c7f3ed92051299aca66c</code>

The crypter decrypts an embedded blob with AES-256-CBC, strips a 4-byte size prefix, GZip-decompresses the result, and calls `Assembly.Load()` to reflectively load the inner assembly. The inner assembly is invoked via `InvokeMember("WriteIsolatedWriter")` on the type `Efjzzebatj.IO.StaticWriter`.

PureHVNC -- not Remcos

The inner payload is `Efjzzebatj.dll`, a 790 KB .NET assembly. The namespace is `PureHVNC_Lib` with subnamespaces for `UserManagement`, `ContextManagement`, `Processing`, `Structures`, `Providers`, `Networking`, and `Messaging`. This is PureHVNC -- the hidden VNC client from the PureCoder MaaS ecosystem.

Config extraction via Mono reflection (load the assembly, call `TestFunction()` to initialize, read `ActiveProvider` fields):

Field	Value
Family	PureHVNC
Assembly	Efjzzebatj.dll
Size	790,016 bytes
Compiled	2025-07-24 12:15:39 UTC
Campaign	JULY 24
Mutex	3ddc38f1ccff
Install path	%APPDATA%
Port	6757/tcp
TLS cert CN	Zwfweyag

The 9 C2 domains:

#	Domain
1	nhvncpure.duckdns.org
2	nhvncpure.click
3	nhvncpure.shop
4	nhvncpure.sbs
5	nhvncpureybs.duckdns.org
6	nhvncpurekfl.duckdns.org
7	nhvncpure.twilightparadox.com
8	nhvncpure1.strangled.net
9	nhvncpure2.mo00.com

Infrastructure convergence

These 9 **nhvncpure** domains, port 6757, and TLS certificate CN **Zwfweayg** are not new. They are the exact same C2 configuration we extracted from the **PureLogs** inner RAT (Qdjlj.dll) via protobuf config key 1690109058. Same 9 domains. Same port. Same TLS certificate. Same mutex format.

Component	Delivery chain	C2 domains	Port	TLS CN
PureLogs (Qdjlj.dll)	Python/Donut loader	9x nhvncpure*	6757	Zwfweayg
PureHVNC (Efjzzebaj.dll)	Autolt/UrbanEco	9x nhvncpure*	6757	Zwfweayg

Two different PureCoder tools -- an information stealer and a hidden VNC client -- sharing the same C2 infrastructure, delivered through two completely independent loader chains. The Python-based Donut chain delivers PureLogs. The Autolt-based BYOI chain delivers PureHVNC. Both phone home to the same 9 domains on the same port with the same TLS certificate.

The setup gives the operator redundancy. If the Python chain is removed, the Autolt chain survives. If the Autolt persistence is removed, the Python chain can redeploy. The **nhvncpure** infrastructure backs both paths -- one C2 backend for the PureCoder toolkit.

The three Autolt chains together give the operator:

1. **EcoOptimize** -- Remcos banking screenshots (port 4056, **homoney** C2)
2. **WealthWise** -- Remcos banking screenshots (port 4057, **homoney** C2)
3. **UrbanEco** -- PureHVNC hands-on-keyboard access (port 6757, **nhvncpure** C2)

Two for passive surveillance, one for active control -- all three surviving reboots through scheduled tasks that AV can't kill.

Indicators of compromise

File hashes (SHA-256)

Artifact	Hash	VT	Tria.ge
Singer.pif (Autolt3.exe)	881619a47b62b52305d92640cc4d4845a279c23a5a749413785fc8fcb0fdf7fb	3/76	--
r.a3x (EcoOptimize script)	9e709cf922e02bca148866fc84dc783c39e2f51adea4f9179fdd7a1381331fc9	3/76	https://tria.ge/260226-nwv1rscw3e (score 1)
EcoOptimize packed PE	656775d0dae805523711e08cd4e5882d0f10ec5105acb5ca5da373ccf6759392	Not indexed	https://tria.ge/260226-nwwbjacw3f (score 1)
EcoOptimize Remcos PE	85b6e2db29ee84d25cc2d942fb181581279b87176880790fda0c3c60d9186ee2	29/76	https://tria.ge/260226-nwx3acw3g (score 10, remcos)
WealthWise Remcos PE (UPX packed)	378b201a0979aff7182edca69148269c9c6685064cac5b7cdcc98375af2fd123	31/76	https://tria.ge/260226-nwx3acw3h (score 10, remcos)
WealthWise Remcos PE (unpacked)	29648ce421e80a3d573bdae593d86c53343933373b400c8ce781dd22fbc82176	44/76	https://tria.ge/260226-nwxjacw4a (score 10, remcos)
UrbanEco Q payload (encrypted)	f8147fb707e8cf6c4f0323eb81d695ffb3a4b14ee4dbb87147750db114c5a165	3/76	https://tria.ge/260226-nwyfwscw4d (score 1)

Artifact	Hash	VT	Tria.ge
UrbanEco .NET crypter (Oktszoqyyp.exe)	739a238220890cb4d65d8f696f9f73bb9390ef526875b2136e3bba6b03c7040a	41/76	https://tria.ge/260226-nwxcscw4b (score 7)
UrbanEco PureHVNC (Efjzzebatj.dll)	e3074f9377f4d4b3d3140486cc0cfc5b4b00e583fdc583b716609713ff8e9307	29/76	https://tria.ge/260226-nwx55acw4c (score 3)
EcoOptimize Remcos config	20443e8b4bc3e5b6fdd2cb582c4230791905c9088f05ae618d076de3bb1b45d1	--	--
WealthWise Remcos config	40aa28c73cf1865bda0aba28708abe4dfb6c83d4f9fd123f719d9a0490050db1	--	--

Remcos C2 domains (homoney)

Domain	Port	Chain
homoney177.duckdns.org	4056, 4057	EcoOptimize, WealthWise
homoney177.food	4056, 4057	EcoOptimize, WealthWise
homoney177.click	4056, 4057	EcoOptimize, WealthWise
homoney177.shop	4056, 4057	EcoOptimize, WealthWise
homoney177.strangled.net	4056, 4057	EcoOptimize, WealthWise
homoney17.duckdns.org	4056, 4057	EcoOptimize, WealthWise
homoney1.duckdns.org	4056, 4057	EcoOptimize, WealthWise
homoney1.mooo.com	4056, 4057	EcoOptimize, WealthWise
homoney17.twilightparadox.com	4056, 4057	EcoOptimize, WealthWise
yrem472hd.duckdns.org	4057	WealthWise only

As of 2026-02-26, homoney177.duckdns.org, homoney17.duckdns.org, and homoney1.duckdns.org still resolve to 91.219.238.167. The three FreeDNS domains resolve to 127.0.0.2 sinkholes and .food/.click/.shop are NXDOMAIN.

PureHVNC C2 domains (nhvncpure)

Domain	Port	Chain
nhvncpure.duckdns.org	6757	UrbanEco
nhvncpure.click	6757	UrbanEco
nhvncpure.shop	6757	UrbanEco

Domain	Port	Chain
nhvncpure.sbs	6757	UrbanEco
nhvncpureybs.duckdns.org	6757	UrbanEco
nhvncpurekfl.duckdns.org	6757	UrbanEco
nhvncpure.twilightparadox.com	6757	UrbanEco
nhvncpure1.strangled.net	6757	UrbanEco
nhvncpure2.mo00.com	6757	UrbanEco

As of 2026-02-26, the non-DuckDNS nhvncpure entries (.click, .shop, .sbs, twilightparadox.com, strangled.net, mo00.com) are expired or removed in the current resolution set.

TLS certificate fingerprints (SHA-256)

Certificate	Fingerprint	Context
Remcos client cert	dd492c49a69c45f21c47d41c87d6656d1b8c270e7f493affd728e03afb4c5a4b	ECC P-256, both Remcos configs
Remcos server cert	48d2265b561fb58e4864f9c3eee263eb6fcb858c53f2c630ac0d9c0ab1c7b410	ECC P-256, both Remcos configs
PureHVNC TLS cert	CN=Zwfweayg	RSA-4096, SHA512withRSA

Mutexes

Mutex	Context
Rmc-i8364b-6EJSJD	EcoOptimize Remcos
Rmc-i8364b-9TU31H	WealthWise Remcos
3ddc38f1ccff	UrbanEco PureHVNC

File system artifacts

Path	Context
%LocalAppData%\EcoOptimize Solutions\	EcoOptimize persistence directory
%LocalAppData%\WealthWise Analytics Inc\	WealthWise persistence directory
%LocalAppData%\UrbanEco Innovations\	UrbanEco persistence directory
%APPDATA%\Remcos\	Remcos install directory (hidden)

Path	Context
%APPDATA%\ledger spotify\spotify.dat	Keylog file
%PROGRAMFILES%\Spotify\	Banking screenshot folder
%LOCALAPPDATA%\MicRecords\	Audio recording folder

Scheduled tasks

Cancellation, Involved (EcoOptimize), QuantifyPro (WealthWise), EcoMap (UrbanEco)

The persistence backbone

The Autolt chains are the persistence backbone of this campaign. The Python-based loader chain delivers the payloads. The Autolt chains keep them alive. Every other component -- [PureLogs](#), [PureCrypter](#), [Violet RAT](#) -- can be redeployed through these three scheduled tasks.

The config diffing proves single-operator control. Two Remcos builds with 54/58 identical fields, identical TLS certificates including the private key, and a mutex naming pattern (Rmc-i8364b-*) that changes only the random suffix. The keyword evolution from 62 to 50 shows active refinement -- the operator watching what works and trimming what doesn't.

The UrbanEco discovery closes the infrastructure loop. PureHVNC delivered through Autolt shares exact C2 configuration with PureLogs delivered through Python. Two independent delivery mechanisms, two different PureCoder tools, one backend.

Kirk

I like the internet. Want to get in touch? ·