

Forum:[Hack Forums](#)

Thread: [NtKiller - Kernel Level EDR Killer \(Advanced Persistence \ UAC BYPASS \ ROOTKIT\)](#)

NTKSoftware - April 1, 2026, 6:09 am

Hello everyone. This thread has been translated to english since it was only available in russian. If you find any mistakes, please report it ?

? NtKiller is an advanced tool for termination of antiviruses, EDRs and any other security solutions.
?

We started development of the software in June, 2025 and first releases were done on other forums in December, 2025

Default Antivirus list:Windows Defender 10

Windows Defender 11

Trend Micro Home

ESET Home

Kaspersky

Avast

Norton

AVG

Malwarebytes

Bitdefender

Dr. Web

Advanced solutions:ESET for small Business

ESET Protect / Endpoint Advanced (Company) (Aggressive mode)

Bitdefender GravityZone (EDR / Aggressive mode)

Trend Micro Trend Vision One (Aggressive mode)

Microsoft Defender for Business

Custom Solutions:

Anything can be killed in theory. Contact us for more details.Antiviruses

EDR

Software Firewall

Anticheats

Anything else

Default Functionality:Silent termination of "Default" and "Advanced" solutions

Support of HVCI/VBS / Memory Integrity

Advanced persistence (Antiviruses are terminated at launch, so your payload remains undetected the entire time of your operation)

Strong Anti Debugging and Analysis

Customization of "Default Functionality" is possible. Contact is for more details.

Additional Modules:UAC Bypass - for all levels of UAC (unknown vulnerability, Windows 7-11 26H1, Windows server 2012-2025 x64.)

NtKiller Rootkit (ring3, ring0 is not developed anymore)

Media:

[ESET Protect / Endpoint Advanced \(aggressive setting\)](#)

[Windows 11 25H2 Pro Defender](#)

You may report of the videos do not work. They are often taken down.

SupportMail: support@ntkiller.pro

Jabber: ntkiller@exploit.im
Tox:
B394E68715120FBC9AD1C4AA78B567B520EE3ABF947DCA206CD51241A75F2801F646FA8CB
7CA
Session: 0583d054aa78b235f86811b2fc7df4de67f898b064d8ec5ad4d54b36a655286456
Telegram: @ntkiller (please beware of scams)

Pricing

Current pricing model is individual, price will be decided on request.
We will not give out unlimited builds

FAQ

Q: What is the advantage of NtKiller?

A: A regular crypt cannot fully bypass detection at runtime: first, a standard crypt cannot pass dynamic analysis, second, eventually the crypt will be discovered after signature databases are updated - it's only a matter of time. In contrast, NtKiller works differently: it terminates the target solution (antivirus, EDR, etc.), so the solution simply does not have enough time to detect your payload. Thus your payload can be executed on systems even with advanced AVs that analyze program behavior.

Q: Is NtKiller compatible with Cobalt Strike or another C2 framework?

A: Yes, NtKiller can be launched directly from Cobalt Strike (or used to deploy a Cobalt Strike beacon). It works the same with any other C2 framework.

Q: I only want to kill the solution without any payload

A: Yes, this is possible. We have two modes of operation. In the first case, we only kill the solution. In the second case, we kill the solution and then launch your payload.

Q: When will you issue a refund?

A: We offer refunds only if the product and/or its additional functionality does not work on most supported systems. Customers have the right to request a refund within three days of receiving the product. After this period, no refunds will be issued.

Q: Which versions of Windows are supported?

A: Windows 7-11, Windows server 2012-2025 x64.

Q: What can be a payload?

A: Any exe file. If you need to run a specific payload (DLL, shellcode, powershell script), please let us know.

[contract=tid]Start Contract[/contract]

News:

<https://cybersecuritynews.com/threat-actors-advertised-ntkiller-malware-on-dark-web/>

<https://gbhackers.com/ntkiller-malware/>

<https://prevent-ransomware.com/blog/hidden-malware-ntkiller-threatens-antivirus-and-edr-defenses-in-2026>

<https://cyberpress.org/ntkiller-malware/>

<https://diamatix.com/dark-web-ntkiller-antivirus-edr-bypass/>

Wrote you on telegram

NTKSoftware - April 1, 2026, 4:06 pm

(Apr 1, 2026 09:37 AM)EiderZ Wrote: [\[CITE\]](#) Wrote you on telegram
Hi, I don't think your message went through.

NTKSoftware - April 4, 2026, 5:59 am

Hello everyone, Tox server online again:

B394E68715120FBC9AD1C4AA78B567B520EE3ABF947DCA206CD51241A75F2801F646FA8CB
7CA

Stanley - April 12, 2026, 4:48 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Madam - April 13, 2026, 4:43 am

Does it bypass SentinelOne?