

Forum:[Hack Forums](#)

Thread: [Baldwin Killer - \[Cheap\] AV/EDR killer - Windows \ Private method \ FUD](#)

Governor - April 26, 2025, 6:22 pm

Contact

? First message via PM

? Telegram Support Bot [@baldwin_support_bot](#)

? Session:

059e7ac97fd4339a895a820732a7c5ae4db4c4952f11680f89609ab0fc230bc110

? Tox:

3195033635C16B8FF1D3926B879C3B71E519F04F95D87CE19E25B5AFF29ADC48CB67DB1D5A
F5

Hi all!

We present to you a project that began to be developed back in 2024. After a huge number of tests and improvements, it is finally ready, below are the main principles of its operation:

? How does Baldwin Killer work ([Click to View](#))

How does Baldwin Killer work

We use a vulnerable driver, through which we locate the ETHREAD structure via parsing, in it we patch the Previous Mode parameter, then with access to read and write kernel memory we find SeValidateImageData, patch it, and after that we can load any unsigned driver.

Then we load our own driver Killer, which parses EPROCESS to get a list of active processes, compares them with antivirus names, and if there are matches, it kills them.

Next, it uses PsSetLoadImageNotifyRoutine and creates monitoring of new process creation — in this monitoring it checks the names of all new processes, and if the name matches an antivirus name, it blocks its loading.

This way it prevents the antivirus from functioning properly.

Then the driver launches your payload and sets up autoloader if required.

There is support for the following antiviruses Windows 10 Defender

Windows 11 Defender

Bitdefender

Avast

ESET NOD32

Kaspersky

Dr.WEB

? However, additional antiviruses may be added upon your request

Additional functionality:

Your payload can either be dropped to disk and run as a process, or loaded into the memory of another process
Auto startup - Boots the killer in the early stages of system startup, and kills antiviruses even before full initialization, also running your Payload

UAC bypass - The new bypass method found by us personally is completely undetectable, has not been used anywhere before. Bypasses the standard UAC level of protection

Ring0 rootkit - All actions of the killer will be completely hidden, your payload will be completely hidden from the task dispatcher, explorer and similar utilities, and startup will also be completely hidden if you have it. (Rootkit bypasses PatchGuard entirely)

Smart screen bypass - Bypassing Smartscreen via DLL SideLoading

Custom additional functionality comes for an additional fee

i At the moment, all additional functionality is FUD for all antiviruses listed in the list. If you need custom functionality, just ask us.

Why us? [\(Click to View\)](#)

Most killers use a driver that provides IOCTLs, through which processes can be killed directly. This is the simplest method that doesn't require writing your own driver or anything like that. You can just use ready-made code from GitHub, and for the most part, killers simply use well-known drivers discovered by other people. This method is very simple, but such killers don't last long.

We use a completely different approach. We use a driver we found ourselves, which wasn't previously known and works on a different principle, allowing us to load our own driver that can hide itself and kill antivirus processes even before they appear in the system, by setting a callback on the process creation function. This allows the killer to remain undetected much longer and work much more effectively than others.

? Base Price: 300\$

Auto startup: + 40\$

UAC bypass: + 50\$

Ring0 rootkit: + 150\$

????? Smart Screen ?????? DLL sideloading: + 40\$

The guarantor is mandatory for the transaction!!

? First message via PM

? Telegram Support Bot [@baldwin_support_bot](#)

? Session:

059e7ac97fd4339a895a820732a7c5ae4db4c4952f11680f89609ab0fc230bc110

? Tox:

3195033635C16B8FF1D3926B879C3B71E519F04F95D87CE19E25B5AFF29ADC48CB67DB1D5A
F5

[Video: <https://vimeo.com/1076989227>]

(If the video is not available, please contact me)

? ???????????? / Affiliate Program! ?
10% commission for every customer you bring

Contract:

[contract=tid]Start Contract[/contract]

bigcriminal1337 - April 27, 2025, 4:02 am

You can sell it for 10x the price if you work EDR's. just saying. Good luck, rare to see good quality.
Any reason why u not mention S1, Cortex, Sophos? Legality?

Governor - April 27, 2025, 5:32 am

(Apr 27, 2025 04:02 AM)bigcriminal1337 Wrote: [\[CITE\]](#) You can sell it for 10x the price if you work EDR's. just saying. Good luck, rare to see good quality.

Any reason why u not mention S1, Cortex, Sophos? Legality?

Hello, thank you for your message. This is the first version of the killer and I tested it with ESET and other antiviruses and released it as soon as possible. However, due to the threads on xss and the exploit, we received so many messages in a short time that we didn't have time to test more

antiviruses and shoot videos.
It will come soon!

bigcriminal1337 - April 27, 2025, 5:34 am

(Apr 27, 2025 05:32 AM)Governor Wrote: [\[CITE\]](#) Hello, thank you for your message. This is the first version of the killer and I tested it with ESET and other antiviruses and released it as soon as possible. However, due to the threads on xss and the exploit, we received so many messages in a short time that we didn't have time to test more antiviruses and shoot videos.

It will come soon!

Exactly the forums that will pay you, 3-4k per license for EDR kill, however do note, that all this people are involved with "RA".

Do you support win server 2008 and above?

Good luck.

Governor - April 27, 2025, 5:40 am

(Apr 27, 2025 05:34 AM)bigcriminal1337 Wrote: [\[CITE\]](#) Exactly the forums that will pay you, 3-4k per license)

Good luck.

Unfortunately, this is not a licensed program, but a one-time service. This is necessary to protect the kernel driver and prevent its patches. The whole project uses 0days, 0day driver and 0day UAC bypass, which we found ourselves

bigcriminal1337 - April 27, 2025, 5:48 am

(Apr 27, 2025 05:40 AM)Governor Wrote: [\[CITE\]](#) Unfortunately, this is not a licensed program, but a one-time service. This is necessary to protect the kernel driver and prevent its patches. The whole project uses 0days, 0day driver and 0day UAC bypass, which we found ourselves

You use 0days to avoid patch guard? Pretty neat. What about old OS? Win7, 2008 server etc.

Are you manually mapping the second driver?

Governor - April 27, 2025, 6:21 am

(Apr 27, 2025 05:48 AM)bigcriminal1337 Wrote: [\[CITE\]](#) You use 0days to avoid patch guard? Pretty neat. What about old OS? Win7, 2008 server etc.

Are you manually mapping the second driver?

on old version it won't work, at least need win 10 1809

yes, we mapping it

GOLLUM - April 27, 2025, 5:35 pm

hide that window i think will be better