

Forum:[Hack Forums](#)

Thread: [REG EXPLOIT | WD BYPASS - UAC EXPLOIT TESTS](#)

latencyx - October 26, 2024, 6:24 pm

Hello buddys again,

Recently I've become more and more interested in ways to bypass antivirus software and I come here once again to share my ideas for personal projects^^

I saw on some forums people selling so-called reg droppers with very expensive prices, but their objective is basically this:

Add Exclusion to WD

Little Stub

Chrome Bypass

And have the possibility of being attached to EMAIL.

And I confess, this really caught my attention and I decided to create my own project with these interesting ideas, and I'm here to share it with members who are interested in the subject, what do you think? I saw that it is little explored on HF ^^

Please feel free to provide constructive criticism and debate, after all, we are here to share!

Operation:

Choose your .exe

It will create a .REG that does the following

Booting a ps1 > Uac Bypass > added the C: exclusions > Reading the bytes of your .exe > executing.

[Video: <https://youtu.be/EBNJv2LK1yA>]

If you have any ideas that you want to be implemented, you can send me a PM.?

Bastille - October 26, 2024, 6:36 pm

That's the kind of content I like to see on HF ? I've stumbled upon black hat activities and methods recently (I've spent all my time on the white hat side and didn't pay that much attention to the black), and I have to admit that I like it.

I plan to start playing with RATs and sutff in my homelab soon, I see that you're using Async and many people recommended it. I'll take a try with it too, and will follow your future threads I guess

Is the :

Code Add Exclusion to WDObfuscated ? When I'm doing malware analysis I often see PS command lines adding exclusion path to WD and it's easy to check them

latencyx - October 26, 2024, 6:41 pm

(Oct 26, 2024 06:36 PM)Bastille Wrote: [\[CITE\]](#) That's the kind of content I like to see on HF ? I've stumbled upon black hat activities and methods recently (I've spent all my time on the white hat side and didn't pay that much attention to the black), and I have to admit that I like it.

I plan to start playing with RATs and sutff in my homelab soon, I see that you're using Async and many people recommended it. I'll take a try with it too, and will follow your future threads I guess

Is the :

Code Add Exclusion to WDObfuscated ? When I'm doing malware analysis I often see PS command lines adding exclusion path to WD and it's easy to check them

Hi Bastille! I'm glad you came across this.? I use AsyncRat because, in my opinion, it provides a very stable connection with users, making it useful for my tests.

I've already published the Windows Defender bypass method here on HF so that members can understand a bit of how it works. However, my code is a bit different and isn't obfuscated because I'm testing several functions haha.

woo097878781 - October 27, 2024, 6:24 am

What is the py script you use? I want to try it too, haha

latencyx - October 27, 2024, 7:23 am

(Oct 27, 2024 06:24 AM)woo097878781 Wrote: [\[CITE\]](#) What is the py script you use? I want to try it too, haha

Hi buddy , the .py I'm using is my project. I'm still developing why I want the output to be FUD

woo097878781 - October 27, 2024, 8:16 am

(Oct 27, 2024 07:23 AM)latencyx Wrote: [\[CITE\]](#) Hi buddy , the .py I'm using is my project. I'm still developing why I want the output to be FUD
good I look forward to your completion

latencyx - October 27, 2024, 2:00 pm

Hello friends,

I'm here to bring you the first update of REG EXPLOIT. I've made some nice little changes!

- [*] The system is now web-based
- [*] Updated .reg protection
- [*] Added login system via KEY
- [*] Bot to create new KEYS
- [*] Zip system and adding password to .zip

These are small changes that make a difference. The output is 1/40 Kleenscan (the only empty one is a false positive).

Result:

[Kleenscan result](#)

Demonstration:

[Video: <https://youtu.be/7eTVGgMRX9M>]

Some people ask about the sale, and I started thinking about it, it's something new on the market and interesting, any thoughts on it?

woo097878781 - October 28, 2024, 4:02 pm

(Oct 27, 2024 02:00 PM)latencyx Wrote: [\[CITE\]](#) Hello friends,

I'm here to bring you the first update of REG EXPLOIT. I've made some nice little changes!

- [*] The system is now web-based

- [*] Updated .reg protection
- [*] Added login system via KEY
- [*] Bot to create new KEYS
- [*] Zip system and adding password to .zip

These are small changes that make a difference. The output is 1/40 Kleenscan (the only empty one is a false positive).

Result:

[Kleenscan result](#)

Demonstration:

[Video: <https://youtu.be/7eTVGgMRX9M>]

Some people ask about the sale, and I started thinking about it, it's something new on the market and interesting, any thoughts on it?

I'm interested in how you did it

I combined ps1 with hexadecimal and successfully bypassed WD, but I couldn't create it into REG. It didn't work after creation. It was a bit distressing. :((

latencyx - October 29, 2024, 8:32 am

(Oct 28, 2024 04:02 PM)woo097878781 Wrote: [\[CITE\]](#) I'm interested in how you did it
I combined ps1 with hexadecimal and successfully bypassed WD, but I couldn't create it into REG. It didn't work after creation. It was a bit distressing. :((

It depends a lot on how your code works, and how complex it is. There are many ways to do what I do but few are stable and good, basically what I try to do theoretically is this:

Basically the code I created does the following steps:

REG creates a PS1 and adds it to startup

[User Restarts PC]

.PS1 starts

C: added exclusions

.PS1 executes the bytes of your .exe saving on the PC.

Now it all depends on how you execute it and how well it is done?

Hello everyone,

I'm here to bring you updates on the project, basically I added some features and protections.

[*]Sales panel

[*]Login panel

[*]Update on the .REG obfuscation system

[*]JunkCode system (Making the output more unique)

Here are some screenshots, what do you think of the design?

Sales Panel:

Login Panel:

Obfuscation:

~

Gmail attach:

I'm still thinking about a price, I'm thinking about leaving the price low for the first few days or leaving a promotional code if I sell it.

hoangdoan - October 29, 2024, 6:14 pm

Great dude, good luck.

Have you thought about offering your services?

latencyx - October 30, 2024, 3:40 am

(Oct 29, 2024 06:14 PM)hoangdoan Wrote: [\[CITE\]](#) Great dude, good luck.

Have you thought about offering your services?

I'm thinking about it, but I'm going to improve security and the user panel a little more, I'm going to give access to some members who have a good reputation, I believe there are few providers of the same service as mine, and those that exist charge an absurd amount for just one file, while I sell unlimited access to a number of files

New Update!

I'm still working on the website hosting along with small aspects of our service. Our website is now online but still under construction! I created an infographic for sales. Since I don't have access to the HF market, I'll just share updates of my work here. Curious users can see the new changes and improvements, as well as give ideas for the project. ^^ Of course, if you're a recognized user in the community, feel free to request a test; I'd be happy to send you a test key! [2 Keys free]

[*] Website update for different devices

[*] Domain update

[*] The project has been named Empty Builder (I thought it was interesting xD)

Remember, this project is in its early stages, so any contributions will be greatly appreciated! To the user who comes from HF out of curiosity, mention I give a \$10 discount (Temporary)

For those users who have little knowledge in this area or are interested, contact me, I am willing to help HF members to build a reputation! Everyone is welcome.?

Demonstration:

[Video: <https://www.youtube.com/watch?v=YdANz2YoOTs>]

Soccerdude6000 - October 30, 2024, 7:06 pm

Anyone know any good exploits for MAC os?

latencyx - October 31, 2024, 7:51 am

(Oct 30, 2024 07:06 PM)Soccerdude6000 Wrote: [\[CITE\]](#) Anyone know any good exploits for MAC os?

I believe this is not the best place to ask this, make a topic just for this.

Biggy_Asian - October 31, 2024, 8:19 am

(Oct 26, 2024 06:24 PM)latencyx Wrote: [\[CITE\]](#) Hello buddys again,

Recently I've become more and more interested in ways to bypass antivirus software and I come here once again to share my ideas for personal projects^^

I saw on some forums people selling so-called reg droppers with very expensive prices, but their objective is basically this:

Add Exclusion to WD

Little Stub

Chrome Bypass

And have the possibility of being attached to EMAIL.

And I confess, this really caught my attention and I decided to create my own project with these interesting ideas, and I'm here to share it with members who are interested in the subject, what do you think? I saw that it is little explored on HF ^^

Please feel free to provide constructive criticism and debate, after all, we are here to share!

Operation:

Choose your .exe

It will create a .REG that does the following

Booting a ps1 > Uac Bypass > added the C: exclusions > Reading the bytes of your .exe > executing.

[Video: <https://youtu.be/EBNJv2LK1yA>]

If you have any ideas that you want to be implemented, you can send me a PM.?

Using registry in any kind of way is heavily watched and if I am correct heavily sigged too. IF this was to be used in the wild it would be detected and probably patched insainly easily/quick too. Its alr tho.

latencyx - October 31, 2024, 8:33 am

(Oct 31, 2024 08:19 AM)Biggy_Asian Wrote: [\[CITE\]](#) Using registry in any kind of way is heavily watched and if I am correct heavily sigged too. IF this was to be used in the wild it would be detected and probably patched insainly easily/quick too. Its alr tho.

I've been using this method for about 2 months, I recently came to explore for sale and if it is detected there are thousands of ways to get around it and if it is detected I will bring a quick update,It's just a matter of trying and seeing

Biggy_Asian - October 31, 2024, 8:35 am

(Oct 31, 2024 08:33 AM)latencyx Wrote: [\[CITE\]](#) I've been using this method for about 2 months, I recently came to explore for sale and if it is detected there are thousands of ways to get around it and if it is detected I will bring a quick update,It's just a matter of trying and seeing

Good luck. All I am saying is no one in their right mind is gonna pay 70 for it. I saw that banner you made. I wouldn't even pay 5 for it. But good luck. There's gonna be someone willing to buy anything. Also isn't this on your github?

latencyx - October 31, 2024, 8:46 am

(Oct 31, 2024 08:35 AM)Biggy_Asian Wrote: [\[CITE\]](#) Good luck. All I am saying is no one in their right mind is gonna pay 70 for it. I saw that banner you made. I wouldn't even pay 5 for it. But good luck. There's gonna be someone willing to buy anything. Also isn't this on your github?

the service is not available on github, the only thing I made available was a source that has similarities with mine about Uac Bypass. If you come here to bring non-beneficial criticism there is no need, I fulfill the objective of the service being sold correctly and I believe it is a fair price for what is offered, thank you for the comments.

Biggy_Asian - October 31, 2024, 8:52 am

(Oct 31, 2024 08:46 AM)latencyx Wrote: [\[CITE\]](#) the service is not available on github, the only thing I made available was a source that has similarities with mine about Uac Bypass. If you come here to bring non-beneficial criticism there is no need, I fulfill the objective of the service being sold correctly and I believe it is a fair price for what is offered, thank you for the comments.

If you do not want such criticism do not post such services otherwise expect such. If not me it would be someone else. I get you "think" (I am nearly quoting) its a fair price however I and likely ALOT of other people will almost not see it that way.

Also you say it has similarities however that leads me to have reason to believe it is mostly just that source with some slight changes or non at all.

latencyx - October 31, 2024, 9:01 am

(Oct 31, 2024 08:52 AM)Biggy_Asian Wrote: [\[CITE\]](#) If you do not want such criticism do not post such services otherwise expect such. If not me it would be someone else. I get you "think" (I am nearly quoting) its a fair price however I and likely ALOT of other people will almost not see it that way.

Also you say it has similarities however that leads me to have reason to believe it is mostly just that source with some slight changes or non at all.

Yes friend, I understand your point of view, I am updating the service daily so that it meets users' expectations and that I can charge this amount, however, it has only been 4 days since the start of public development and I am meeting the objectives, I believe There are many other sellers who sell much more expensive products and don't even want to maintain consistency in their updates, etc., I appreciate your comments as it is necessary and believe me I am working to have an efficient product

woo097878781 - November 1, 2024, 1:41 pm

(Oct 30, 2024 03:40 AM)latencyx Wrote: [\[CITE\]](#) I'm thinking about it, but I'm going to improve security and the user panel a little more, I'm going to give access to some members who have a good reputation, I believe there are few providers of the same service as mine, and those that exist charge an absurd amount for just one file, while I sell unlimited access to a number of files

New Update!

I'm still working on the website hosting along with small aspects of our service. Our website is now online but still under construction! I created an infographic for sales. Since I don't have access to the HF market, I'll just share updates of my work here. Curious users can see the new changes and improvements, as well as give ideas for the project. ^^ Of course, if you're a recognized user in the community, feel free to request a test; I'd be happy to send you a test key! [2 Keys free]

[*] Website update for different devices

[*] Domain update

[*] The project has been named Empty Builder (I thought it was interesting xD)

Remember, this project is in its early stages, so any contributions will be greatly appreciated!
To the user who comes from HF out of curiosity, mention I give a \$10 discount (Temporary)

For those users who have little knowledge in this area or are interested, contact me, I am willing to help HF members to build a reputation! Everyone is welcome.?

Demonstration:

[Video: <https://www.youtube.com/watch?v=YdANz2YoOTs>]

Teacher, I have a question for you. I see that the powershell directive in your reg uses base64.

Why doesn't your antivirus software report virus warnings?

I am working on a complex method and it has been successful, but it seems that false positives and blocking seem to be difficult to solve, especially when writing ps1 under Run, it will be blocked.

I used multiple pieces of encrypted malware code and stored them elsewhere in Run for easy recall, assembly, and execution.

Such as: A0-A800 hexadecimal or base64

Call using powershell

Works great but is too complex

latencyx - November 1, 2024, 1:47 pm

(Nov 1, 2024 01:41 PM)woo097878781 Wrote: [\[CITE\]](#) Teacher, I have a question for you. I see that the powershell directive in your reg uses base64.

Why doesn't your antivirus software report virus warnings?

I am working on a complex method and it has been successful, but it seems that false positives and blocking seem to be difficult to solve, especially when writing ps1 under Run, it will be blocked.

I used multiple pieces of encrypted malware code and stored them elsewhere in Run for easy recall, assembly, and execution.

Such as: A0-A800 hexadecimal or base64

Call using powershell

Works great but is too complex

Base64 itself is not the problem; try executing legitimate code through PowerShell, and you will see that there won't be issues. If you have problems with PowerShell, it's because something in your base64 raises suspicion with AMSI. Try to circumvent this by modifying the content of your base64. Feel free to send your code to me privately for me to check.

edit:

I will soon release a .LNK builder here that will also use BASE64 parameters, but it is not intended to bypass WD, it will be free so it may be interesting for studies, I recommend it

woo097878781 - November 1, 2024, 6:05 pm

(Nov 1, 2024 01:47 PM)latencyx Wrote: [\[CITE\]](#) Base64 itself is not the problem; try executing legitimate code through PowerShell, and you will see that there won't be issues. If you have problems with PowerShell, it's because something in your base64 raises suspicion with AMSI. Try to circumvent this by modifying the content of your base64. Feel free to send your code to me privately for me to check.

edit:

I will soon release a .LNK builder here that will also use BASE64 parameters, but it is not intended to bypass WD, it will be free so it may be interesting for studies, I recommend it

Teacher thank you

Your articles are very valuable
You inspire me a lot and I will continue to learn from you.

Nice to communicate with you
If you can share the .LNK builder, I will study it carefully.

latencyx - November 2, 2024, 11:51 am

Hello everyone,

Changelog:

- [*] Updated our login page
- [*] Availability of a Powershell Crypter (Only .ps1) (Free)
- [*] Availability of a Signature Spoofer (Only .exe) (Free)
- [*] Updated our .REG obfuscation (Paid)

Random Scan (1/41):

https://kleenscan.com/scan_result/dc37d6bf168dfec3af2961ff1e384197d3035a075952a937a57dd523e8b45de7

mres - November 3, 2024, 4:40 am

Great product. latencyx even helped me, setting up a RAT for me, and was patiently using his time to learn me a couple of things.

no detection on WD, no smartscreen so its does what it says it does.

latencyx - November 3, 2024, 4:42 am

(Nov 3, 2024 05:40 AM)mres Wrote: [\[CITE\]](#) Great product. latencyx even helped me, setting up a RAT for me, and was patiently using his time to learn me a couple of things.

no detection on WD, no smartscreen so its does what it says it does.

Thank you for your feedback^^

Hreidmar - November 3, 2024, 10:24 am

(Oct 31, 2024 08:35 AM)Biggy_Asian Wrote: [\[CITE\]](#) Good luck. All I am saying is no one in their right mind is gonna pay 70 for it. I saw that banner you made. I wouldn't even pay 5 for it. But good luck. There's gonna be someone willing to buy anything. Also isn't this on your github?

This is HackForums....there will be plenty of people that don't know anything beyond plug&play stuff buying this trying to play Hackermans so let the person open up his store and earn some money.

It's not like he's trying to scam people, in some sense he's selling "convenience" so people that buy this don't have to spend their time learning some basics to do it themselves.

We shall see how much demand there is for it.

latencyx - November 4, 2024, 5:44 am

(Nov 3, 2024 11:24 AM)Hreidmar Wrote: [\[CITE\]](#) This is HackForums....there will be plenty of people that don't know anything beyond plug&play stuff buying this trying to play Hackermans so let the person open up his store and earn some money.

It's not like he's trying to scam people, in some sense he's selling "convenience" so people that buy this don't have to spend their time learning some basics to do it themselves.

We shall see how much demand there is for it.

I find it interesting that you make these comments for guys who sell a single .reg for \$1000, and not

for me who has this entire service for just \$70 lol

Hreidmar - November 5, 2024, 12:49 pm

(Nov 4, 2024 06:44 AM)latencyx Wrote: [\[CITE\]](#) I find it interesting that you make these comments for guys who sell a single .reg for \$1000, and not for me who has this entire service for just \$70 lol
Not sure what kind of comments do you mean, maybe you're misunderstanding my reply to the other poster?

latencyx - November 5, 2024, 12:51 pm

(Nov 5, 2024 01:49 PM)Hreidmar Wrote: [\[CITE\]](#) Not sure what kind of comments do you mean, maybe you're misunderstanding my reply to the other poster?
I'm not talking about your comment, friend, but about some other people lol, I understand your perspective

Bastille - November 6, 2024, 10:56 am

This was initialy a thread about a project, then you started selling your product here, please create a dedicated thread here : [Member Sales Market](#)

Please also read the [Help Docs](#), there are many rules to be aware about when you deal on HF

Thanks