

Forum:[Hack Forums](#)

Thread: [\[0DAY EXPLOIT \]](#) [\[DL & EXEC \]](#) [\[AUTO-SPREAD \]](#) [\[FUD \]](#) [\[PRIVATE \]](#) [\[3 COPIES ONLY \]](#)

CashoutArtist - May 3, 2019, 10:12 am

This is a range scanner based exploit where you are able to simply silently drop your stub and execute it.

3 Copies:
\$850 BTC
\$950 BTC
\$1.2k BTC

Have it all for yourself: (Released only to you and no one else)
\$2.4k BTC0

Proof:

<https://vimeo.com/334094944>

Password: hf2019k

For more information about this vulnerability PM me.

If you are actually interested in buying (Must show proof of funds), Send me a pm to receive a demo in live screenshare.

[contract=tid]Start Contract[/contract]

aternoted - May 3, 2019, 11:11 am

(May 3, 2019 10:45 AM)The Hammer Wrote: [\[CITE\]](#) So this is fully autopilot and I set a range of IPs and my stub is injected? Why does it cost so much?

It's 0Day exploit, meaning it is developed by himself lol He only have the exploit, no one knows it. In the market 0days is expensive lol

CashoutArtist - May 3, 2019, 11:30 am

(May 3, 2019 10:45 AM)The Hammer Wrote: [\[CITE\]](#) So this is fully autopilot and I set a range of IPs and my stub is injected? Why does it cost so much?

(May 3, 2019 11:11 AM)aternoted Wrote: [\[CITE\]](#) It's 0Day exploit, meaning it is developed by himself lol He only have the exploit, no one knows it. In the market 0days is expensive lol

Yes, fully autopilot, a python script. You just place the download for the stub and it will be injected and executed in to a range of IPs. It by passes the security of the server (exploit in security, thus exploit) and has not been used yet (thus 0day) and it being to private and unknown as it was developed by me is the reason it is so expensive.

Psychedelic. - May 3, 2019, 11:37 am

how many bots can i get with this?

Zorb - May 3, 2019, 11:53 am

(May 3, 2019 11:37 AM)Jasonfaps Wrote: [\[CITE\]](#) how many bots can i get with this?

This. And how many are windows 8+? Not worth it is the bots are all gonna be shitty windows 2003

int - May 3, 2019, 12:18 pm

w10_exploit.py

bots that show up arent even windows 10

nice1

Psychedelic. - May 3, 2019, 1:58 pm

(May 3, 2019 12:18 PM)int Wrote: [\[CITE\]](#) w10_exploit.py

bots that show up arent even windows 10

nice1

Wait, you're right. Seems fishy.

int - May 3, 2019, 2:01 pm

(May 3, 2019 01:58 PM)Jasonfaps Wrote: [\[CITE\]](#) Wait, you're right. Seems fishy. 7 day old account, I don't trust

Psychedelic. - May 3, 2019, 2:02 pm

(May 3, 2019 02:01 PM)int Wrote: [\[CITE\]](#) 7 day old account, I don't trust

Same, this does seem scammy. I doubt anyone is really going to buy this without any vouches and such a high price.

CashoutArtist - May 3, 2019, 5:07 pm

(May 3, 2019 11:37 AM)Jasonfaps Wrote: [\[CITE\]](#) how many bots can i get with this? Thousands to hundreds of thousands

(May 3, 2019 11:53 AM)Ridd3n Wrote: [\[CITE\]](#) This. And how many are windows 8+? Not worth it is the bots are all gonna be shitty windows 2003 No, watch the proof. Last is a windows 8

(May 3, 2019 12:18 PM)int Wrote: [\[CITE\]](#) w10_exploit.py

bots that show up arent even windows 10

nice1 w_10 does not stand for windows 10

(May 3, 2019 01:58 PM)Jasonfaps Wrote: [\[CITE\]](#) Wait, you're right. Seems fishy. Read above

(May 3, 2019 02:01 PM)int Wrote: [\[CITE\]](#) 7 day old account, I don't trust Check my other thread. Then go check dispute database. Scammers are all 1 year + old accounts.

(May 3, 2019 02:02 PM)Jasonfaps Wrote: [\[CITE\]](#) Same, this does seem scammy. I doubt anyone is really going to buy this without any vouches and such a high price. Do you even know what 0 day means. If you think I am scammy, check my other thread, high cost method and near 10 sold. Made near 1k BTC just from that 4-6 days.

More info:

w_10 means its version 10 of the exploit derp. Its just a file name.

As I said, if you are actually interested, I can provide LIVE SCREENSHARE for this.

Riddick - May 3, 2019, 5:27 pm

Is it just me or is the password for the video link incorrect?

CashoutArtist - May 3, 2019, 5:30 pm

(May 3, 2019 05:27 PM)Mirage Wrote: [\[CITE\]](#) Is it just me or is the password for the video link incorrect?

It works , type it in...admin

Lombaraspine - May 3, 2019, 5:33 pm

No its not admin Imfao thats the wrong pw

Vanilla - May 3, 2019, 5:37 pm

guy is retarded. whats the PW lol

CashoutArtist - May 3, 2019, 5:40 pm

(May 3, 2019 05:27 PM)Mirage Wrote: [\[CITE\]](#) Is it just me or is the password for the video link incorrect?

(May 3, 2019 05:33 PM)Lombaraspine Wrote: [\[CITE\]](#) No its not admin Imfao thats the wrong pw

(May 3, 2019 05:37 PM)Vanilla Wrote: [\[CITE\]](#) guy is retarded. whats the PW lol

Sorry about that, currently re uploading video. It has some breaks. Will update you in a few minutes!

Porn - May 3, 2019, 6:07 pm

Sorry, that password was incorrect. Please try again.

CashoutArtist - May 3, 2019, 6:19 pm

(May 3, 2019 05:27 PM)Mirage Wrote: [\[CITE\]](#) Is it just me or is the password for the video link incorrect?

(May 3, 2019 05:33 PM)Lombaraspine Wrote: [\[CITE\]](#) No its not admin Imfao thats the wrong pw

(May 3, 2019 05:37 PM)Vanilla Wrote: [\[CITE\]](#) guy is retarded. whats the PW lol

(May 3, 2019 06:07 PM)Porn Wrote: [\[CITE\]](#) Sorry, that password was incorrect. Please try again.

New link is

<https://vimeo.com/334094944>

Password: hf2019k

Vanilla - May 3, 2019, 6:40 pm

I love people who resell Eternal Blue!

BTC - May 3, 2019, 6:48 pm

(May 3, 2019 06:40 PM)Vanilla Wrote: [\[CITE\]](#) I love people who resell Eternal Blue!

This is exactly what I thought when I first saw this.

Got to love the Mac also ? Very stylish, anybody who uses Mac must be extremely technologically advanced

Good luck with your sales bro

CashoutArtist - May 3, 2019, 6:48 pm

(May 3, 2019 06:40 PM)Vanilla Wrote: [\[CITE\]](#) I love people who resell Eternal Blue!

This is not eternal blue. Eternal blue is absolute shit and FYI, eternal blue doesn't hit jack shit even after 10 minutes of running. I suppose you might want to do a little research before you start making claims. I provide live screenshare as well.

(May 3, 2019 06:48 PM)BTC Wrote: [\[CITE\]](#) This is exactly what I thought when I first saw this.

Got to love the Mac also ? Very stylish, anybody who uses Mac must be extremely technologically advanced

Read above.

Furthermore:
Eternal Blue:

Mine:

Vanilla - May 3, 2019, 7:10 pm

(May 3, 2019 06:48 PM)CashoutArtist Wrote: [\[CITE\]](#) This is not eternal blue. Eternal blue is absolute shit and FYI, eternal blue doesn't hit jack shit even after 10 minutes of running. I suppose you might want to do a little research before you start making claims. I provide live screenshare as well.

Read above.

Furthermore:
Eternal Blue:

Mine:

i can change a console interface print command with no coding knowledge lol. you just put in a good ip range lol

CashoutArtist - May 3, 2019, 7:16 pm

(May 3, 2019 07:10 PM)Vanilla Wrote: [\[CITE\]](#) i can change a console interface print command with no coding knowledge lol. you just put in a good ip range lol

The exploit uses a HMValidateHandle technique to bypass ASLR, after exploitation, it downloads and executes a file in the target system. It can scan 200k ips per each minute.

Upon execution CreateWindowEx sends the message WM_NCCREATE to the window when it's first created. By using the SetWindowsHookEx function, it is possible to set a custom callback that can handle the WM_NCCREATE message right before calling the window procedure. Then simply by leveraging a HMValidateHandle technique utilized to bypass ASLR we can deploy a file and execute it in the system trough a base64 encoded shellcommand.

Eternal Blue goes through the SMB PROTOCOL

Vanilla - May 3, 2019, 7:19 pm

(May 3, 2019 07:16 PM)CashoutArtist Wrote: [\[CITE\]](#) The exploit uses a HMValidateHandle technique to bypass ASLR, after exploitation, it downloads and executes a file in the target system. It can scan 200k ips per each minute.

Upon execution CreateWindowEx sends the message WM_NCCREATE to the window when it's first created. By using the SetWindowsHookEx function, it is possible to set a custom callback that can handle the WM_NCCREATE message right before calling the window procedure. Then simply by leveraging a HMValidateHandle technique utilized to bypass ASLR we can deploy a file and execute it in the system trough a base64 encoded shellcommand.

Eternal Blue goes through the SMB PROTOCOL

this cracks me up just talking abt win api functions. wont work with me ?

CashoutArtist - May 3, 2019, 7:23 pm

(May 3, 2019 07:19 PM)Vanilla Wrote: [\[CITE\]](#) this cracks me up just talking abt win api functions. wont work with me ?

Go read about the CVE, not my fault you know nothing about building exploits. Now please, if you have nothing to contribute, your opinion was pretty clear, just leave the thread.

Vanilla - May 3, 2019, 7:42 pm

(May 3, 2019 07:23 PM)CashoutArtist Wrote: [\[CITE\]](#) Go read about the CVE, not my fault you know nothing about building exploits. Now please, if you have nothing to contribute, your opinion was pretty clear, just leave the thread.

if its a cve then its not a 0day dude

CashoutArtist - May 3, 2019, 7:59 pm

(May 3, 2019 07:42 PM)Vanilla Wrote: [\[CITE\]](#) if its a cve then its not a 0day dude

Just no comment. First, go read CVE and learn about exploits as you have some half baked information. I suggest you properly learn about what you are going on about and then comeback. Suggest you not to argue on a topic upon which you have no matter as it clearly can be seen that YOU ARE NOT INTERESTED for PURCHASING.

TCP - May 3, 2019, 8:51 pm

(May 3, 2019 07:59 PM)CashoutArtist Wrote: [\[CITE\]](#) Just no comment. First, go read CVE and learn about exploits as you have some half baked information. I suggest you properly learn about what you are going on about and then comeback. Suggest you not to argue on a topic upon which you have no matter as it clearly can be seen that YOU ARE NOT INTERESTED for PURCHASING.

By 0day we commonly mean a vulnerability never discovered before, which is not this case

CashoutArtist - May 3, 2019, 9:13 pm

(May 3, 2019 08:37 PM)Vanilla Wrote: [\[CITE\]](#) Dwc guysFurther posts will be regarded as sales trashing. You should read the rules once again.

(May 3, 2019 08:51 PM)DNA Wrote: [\[CITE\]](#) By 0day we commonly mean a vulnerability never discovered before, which is not this case

Yes, this is a 0 day sir. Never been put out. MAYBE 2-3 days old max.

Quick Hit from the appraisers group will be recieveing a live screenshare session soon, he will post some further information about this.

MaximumPain - May 3, 2019, 9:30 pm

(May 3, 2019 11:30 AM)CashoutArtist Wrote: [\[CITE\]](#) Yes, fully autopilot, a python script. You just place the download for the stub and it will be injected and executed in to a range of IPs. It by passes the security of the server (exploit in security, thus exploit) and has not been used yet (thus 0day) and it being to private and unknown as it was developed by me is the reason it is so expensive.

To everyone else reading: DWC.

Your joking i certainly hope right? If you have A 0DAY FOR WINDOWS YOU WOULD NOT BE SELLING THIS FOR CHEAP. YOU WOULD BE GOING TO A BUG BOUNTY SITE OR SOMETHING SIMILAR AND SELLING THERE. ???

What are you saying?

"it was developed by me" - Can you explain the bug? And how you managed to bypass various protections??? ?

Please tell us is this a 0day? Or no and that there is a CVE associated with this bug?

Also he has only been here for 8 days. please work carefully to those interested.

CashoutArtist - May 3, 2019, 9:41 pm

(May 3, 2019 09:30 PM)MaximumPain Wrote: [\[CITE\]](#) To everyone else reading: DWC.
Your joking i certainly hope right? If you have A 0DAY FOR WINDOWS YOU WOULD NOT BE SELLING THIS FOR CHEAP. YOU WOULD BE GOING TO A BUG BOUNTY SITE OR SOMETHING SIMILAR AND SELLING THERE. ???

What are you saying?

"it was developed by me" - Can you explain the bug? And how you managed to bypass various protections??? ?

Please tell us is this a 0day? Or no and that there is a CVE associated with this bug?

Pricing:

This is mainly for servers, nothing like a torrent 0-Day (Sold for 11k on Dream 8 months ago).

Read the past 2 pages, not going keep re-explaining the same thing over and over again.

\$850-1.2k for 3 copies is a fairly good price.

\$2.4k for a private is cheap as well, but if I list this at for a whole coin, who will actually buy it.
Common marketing sense, I don't think you have ever sold a 0 day exploit.

Why would I report it to bug bounty? No thanks bro, even after I sell it, I still have my own personal uses of this.

There is someone else selling a 0 DAY cheaper then me buddy. \$500 at his end. The user M L T is also selling a 0 DAY, go post this same post on there please :D

Off topic unprofessionalism:

Exploit: In your mind a "bug". Ok.

Vulnerability: "bypass various protections" Ok.

0 Day: "CVE associated" Ok.

From the above, it is assumed you have a IQ <80.

From the rules of HF and words of Xerotic himself: "It is not up to you to decide who is legitimate, there is a contract system in place. You can research members there before a deal so it isn't your responsibility to harass a member on their sales thread."

MaximumPain - May 3, 2019, 9:46 pm

(May 3, 2019 09:41 PM)CashoutArtist Wrote: [\[CITE\]](#) Pricing:

This is mainly for servers, nothing like a torrent 0-Day (Sold for 11k on Dream 8 months ago).

Read the past 2 pages, not going keep re-explaining the same thing over and over again.

\$850-1.2k for 3 copies is a fairly good price.

\$2.4k for a private is cheap as well, but if I list this at for a whole coin, who will actually buy it.
Common marketing sense, I don't think you have ever sold a 0 day exploit.

Why would I report it to bug bounty? No thanks bro, even after I sell it, I still have my own personal uses of this.

There is someone else selling a 0 DAY cheaper then me buddy. \$500 at his end. The user M L T is also selling a 0 DAY, go post this same post on there please :D

Off topic unprofessionalism:

Exploit: In your mind a "bug". Ok.

Vulnerability: "bypass various protections" Ok.

0 Day: "CVE associated" Ok.

From the above, it is assumed you have a IQ <80.

MLT I know is not a scammer. Lol? I said if it is not a 0day and that if there is a CVE let me know it. Can you not comprehend? So it is for servers. Alright. So do you know sir, how much this would go for? ?

Quit bluffing and either show valid proof or explain yourself here. (1.2k\$ for 3 copies? YOUR JOKING RIGHT? FOR A WINDOWS SERVER 0DAY LMAO, I WOULD LOVE TO KNOW WHICH UNIVERSE YOU BELONG TO BECAUSE CLEARLY WE ARE NOT IN THE SAME ONE)

"I don't think you have ever sold a 0 day exploit." I dont think you know if i did or did not lmao so hush child. ? Clearly I can tell you never have. So do tell me sir, exactly, what is the bug type?

CashoutArtist - May 3, 2019, 9:49 pm

(May 3, 2019 09:46 PM)MaximumPain Wrote: [\[CITE\]](#) MLT I know is not a scammer. Lol? I said if it is not a 0day and that if there is a CVE let me know it. Can you not comprehend? So it is for servers. Alright. So do you know sir, how much this would go for? ?

Quit bluffing and either show valid proof or explain yourself here. (1.2k\$ for 3 copies? YOUR JOKING RIGHT? FOR A WINDOWS SERVER 0DAY LMAO, I WOULD LOVE TO KNOW WHICH UNIVERSE YOU BELONG TO BECAUSE CLEARLY WE ARE NOT IN THE SAME ONE)

"I don't think you have ever sold a 0 day exploit." I dont think you know if i did or did not lmao so hush child. ? Clearly I can tell you never have. So do tell me sir, exactly, what is the bug type?

I told Vanilla to read the basics of CVE because he has no clue what he is talking about. Please take this to pm.

MaximumPain - May 3, 2019, 10:04 pm

(May 3, 2019 09:49 PM)CashoutArtist Wrote: [\[CITE\]](#) I told Vanilla to read the basics of CVE because he has no clue what he is talking about. Please take this to pm.I have taken this to PM and do not think you will reply any further. ?

Quote:It can scan 200k ips per each minute.

bullshit lol... Sure I guess "it can". I bet "it can" also fly.

Im done talking. Either provide me with accurate details (im not asking exactly where the bug is, im asking for details so i can ask you more in depth questions)

HmValidateHandle can leak kernel addresses but it still just doesn't match up at all with everything else that's said by you.

CashoutArtist - May 3, 2019, 10:07 pm

(May 3, 2019 10:04 PM)MaximumPain Wrote: [\[CITE\]](#) I have taken this to PM and do not think you will reply any further. ?

bullshit lol... Sure I guess "it can". I bet "it can" also fly.

Im done talking. Either provide me with accurate details (im not asking exactly where the bug is, im asking for details so i can ask you more in depth questions)

HmValidateHandle can leak kernel addresses but it still just doesn't match up at all with everything else that's said by you.

Sent you more buddy, check again

stdio - May 3, 2019, 10:37 pm

(May 3, 2019 07:23 PM)CashoutArtist Wrote: [\[CITE\]](#) Go read about the CVE, not my fault you know nothing about building exploits. Now please, if you have nothing to contribute, your opinion was pretty clear, just leave the thread.

Selling 0day then claiming its a CVE.

I can review this in detail if you are willing but you gotta come straight.

Regards

CashoutArtist - May 3, 2019, 10:39 pm

(May 3, 2019 10:37 PM)Homi Wrote: [\[CITE\]](#) Selling 0day then claiming its a CVE.

I can review this in detail if you are willing but you gotta come straight.

Regards

He mentioned eternal blue, I told him go read the cve on eternal blue and then compare it to what I said, don't understand why people are misunderstanding it.

stdio - May 3, 2019, 10:47 pm

(May 3, 2019 10:39 PM)CashoutArtist Wrote: [\[CITE\]](#) He mentioned eternal blue, I told him go read the cve on eternal blue and then compare it to what I said, don't understand why people are misunderstanding it.

People here cannot just trust a new account popping outta nowhere with a 0 day.

you need reviews before people can trust your stuff :)

Good luck

CashoutArtist - May 3, 2019, 11:03 pm

(May 3, 2019 10:47 PM)Homi Wrote: [\[CITE\]](#) People here cannot just trust a new account popping outta nowhere with a 0 day.

you need reviews before people can trust your stuff :)

Good luck

Yea, a few users told me this as well, check out my other products. I own some large products, google my hosting service.

packofmidgets - May 4, 2019, 8:49 am

(May 3, 2019 11:03 PM)CashoutArtist Wrote: [\[CITE\]](#) Yea, a few users told me this as well, check out my other products. I own some large products, google my hosting service.

are you selling those other products for as much as this ? If not then you can probably see how someone would have an issue taking your word from a \$100 product sale versus your \$1k product sale. I am not sales trashing as I do not know if this is legit or not but I am going to try and help you understand why everyone here is going to assume you are scamming. If someone sold 1000 items of a \$1-\$10 product then said I have a \$1000 product it would be easy for someone to simply use the low cost items to prepare for a exit scam. It has been done many times in the past. All the users are trying to state is that if you want to sell it then you should give a vouch copy to someone with rep that they trust since they do not trust you. This is not tor where you can be completely anonymous and sell stuff for that kind of price with no rep. Here we use a rep system and you do not have any to offer for a sale this big. And I have sold 0days i the past and I can tell you now that you could easily get \$80,00+ for a 0day that you claim to have. People will try to prove you are fake on principal mainly because your price is shit for something you claim to have and the other thing would be because others have tried to do this and failed which means they will not think you of all ppl (a nobody on there site) could come up with it yourself with them never hearing of you before. Please think about this and think about what I have said. I am not sales trashing but merely trying to help you out. So that being said can you tell me more about this?

CashoutArtist - May 4, 2019, 8:53 am

(May 4, 2019 08:49 AM)packofmidgets Wrote: [\[CITE\]](#) are you selling those other products for as much as this ? If not then you can probably see how someone would have an issue taking your

word from a \$100 product sale versus your \$1k product sale. I am not sales trashing as I do not know if this is legit or not but I am going to try and help you understand why everyone here is going to assume you are scamming. If someone sold 1000 items of a \$1-\$10 product then said I have a \$1000 product it would be easy for someone to simply use the low cost items to prepare for a exit scam. It has been done many times in the past. All the users are trying to state is that if you want to sell it then you should give a vouch copy to someone with rep that they trust since they do not trust you. This is not tor where you can be completely anonymous and sell stuff for that kind of price with no rep. Here we use a rep system and you do not have any to offer for a sale this big. And I have sold 0days i the past and I can tell you now that you could easily get \$80,00+ for a 0day that you claim to have. People will try to prove you are fake on principal mainly because your price is shit for something you claim to have and the other thing would be because others have tried to do this and failed which means they will not think you of all ppl (a nobody on there site) could come up with it yourself with them never hearing of you before. Please think about this and think about what I have said. I am not sales trashing but merely trying to help you out. So that being said can you tell me more about this?Quick Hits from the appraiser group will be giving a review soon. He will provide further infomation. No point to explain to the time wasters posting in my thread.

Also a 0 fay is 0 day because it is private, more hands it goes through the less valuable it becomes.

BTC - May 4, 2019, 10:26 am

(May 3, 2019 09:13 PM)CashoutArtist Wrote: [\[CITE\]](#) Yes, this is a 0 day sir. Never been put out. MAYBE 2-3 days old max.

(May 3, 2019 07:23 PM)CashoutArtist Wrote: [\[CITE\]](#) Go read about the CVE, not my fault you know nothing about building exploits.

It is very odd, you seem to contradict yourself here.

Quote:A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software).

[https://en.wikipedia.org/wiki/Zero-day_\(computing\)](https://en.wikipedia.org/wiki/Zero-day_(computing))

Could you clear this up for me, by chance? is it perhaps you mislabeled this as a zero day? Or you possibly are confused what a CVE is?

If you could clear my confusion that would be great. I think it is possibly just your terminology that is misrepresented, and if you could be more clear as to what this actually is...that would be great. I get too confused when you flip flop between it being public CVE and zero day... cause if it's a zero day then there is absolutely no way you can "Go read about the CVE" as you stated yourself. That just definition-ally contradicts the term you have classified as in your title, as well thread.

CashoutArtist - May 4, 2019, 10:48 am

(May 4, 2019 10:26 AM)BTC Wrote: [\[CITE\]](#) It is very odd, you seem to contradict yourself here.

[https://en.wikipedia.org/wiki/Zero-day_\(computing\)](https://en.wikipedia.org/wiki/Zero-day_(computing))

Could you clear this up for me, by chance? is it perhaps you mislabeled this as a zero day? Or you possibly are confused what a CVE is?

If you could clear my confusion that would be great. I think it is possibly just your terminology that is misrepresented, and if you could be more clear as to what this actually is...that would be great. I get too confused when you flip flop between it being public CVE and zero day... cause if it's a zero day

then there is absolutely no way you can "Go read about the CVE" as you stated yourself. That just definition-ally contradicts the term you have classified as in your title, as well thread.

See, I mentioned for Vanilla to read the CVE for eternal blue and crosscompare it to how my 0 day works. He didn't know what he was rambling on about. My 0 day isn't in the CVE lol.

BTC - May 4, 2019, 10:53 am

(May 4, 2019 10:48 AM)CashoutArtist Wrote: [\[CITE\]](#) See, I mentioned for Vanilla to read the CVE for eternal blue and crosscompare it to how my 0 day works. He didn't know what he was rambling on about. My 0 day isn't in the CVE lol.

Ohh okay , makes sense, with the context of the post originally it lead me to believe that you referenced your exploit.

CashoutArtist - May 4, 2019, 10:55 am

(May 4, 2019 10:53 AM)BTC Wrote: [\[CITE\]](#) Ohh okay , makes sense, with the context of the post originally it lead me to believe that you referenced your exploit.

Ahh, I see many people misunderstood that, vanilla mentioned that exploits have nothing involved with win api so I told him refer the CVE as the CVE actually provides really good information. If you want to learn about exploits and vulns, its really good to learn from previous ones and it helps in finding new ones in my opinion. But was just trying to show him the technical aspects are completely different.

LanMan - May 4, 2019, 11:21 am

(May 3, 2019 07:16 PM)CashoutArtist Wrote: [\[CITE\]](#) The exploit uses a HMValidateHandle technique to bypass ASLR, after exploitation, it downloads and executes a file in the target system. It can scan 200k ips per each minute.

Upon execution CreateWindowEx sends the message WM_NCCREATE to the window when it's first created. By using the SetWindowsHookEx function, it is possible to set a custom callback that can handle the WM_NCCREATE message right before calling the window procedure. Then simply by leveraging a HMValidateHandle technique utilized to bypass ASLR we can deploy a file and execute it in the system trough a base64 encoded shellcommand.

Eternal Blue goes through the SMB PROTOCOL

You just quoted the details step by step about the Local priv escalation vuln CVE-2019-0859

<https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/>

So there is no technical detail about your Oday, if its really one.

BTC - May 4, 2019, 11:23 am

(May 4, 2019 11:21 AM)LanMan Wrote: [\[CITE\]](#) You just quoted the details step by step about the Local priv escalation vuln CVE-2019-0859

<https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/>

So there is no technical detail about your Oday, if its really one.

Damn nice catch! I tried copy score and other plagiarism tests but did not uncover anything. This is a straight rip-off from that post. If you read through it literally is word for word WTF

CashoutArtist - May 4, 2019, 11:24 am

(May 4, 2019 11:21 AM)LanMan Wrote: [\[CITE\]](#) You just quoted the details step by step about the Local priv escalation vuln CVE-2019-0859

<https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/>

So there is no technical detail about your Oday, if its really one.

Its not the same as this. It is has the same first step for the custom callback message, but further

than that it is all different. Not going into any more detail because at that point I am giving the vuln away.

(May 4, 2019 11:23 AM)BTC Wrote: [\[CITE\]](#) Damn nice catch! I tried copy score and other plagiarism tests but did not uncover anything. This is a straight rip-off from that post. If you read through it literally is word for word WTF

Will be getting this vouched by Quick Hit anyways lol. Dw about that :)

BTC - May 4, 2019, 11:29 am

Your Words:

Quote:Upon execution CreateWindowEx sends the message WM_NCCREATE to the window when it's first created.

Quote:HMValidateHandle technique utilized to bypass ASLR

Quote:By using the SetWindowsHookEx function, it is possible to set a custom callback that can handle the WM_NCCREATE message right before calling the window procedure.

From Article:

Quote:using the well-known HMValidateHandle technique to bypass ASLR.

Quote:CreateWindowEx sends the message WM_NCCREATE to the window when it's first created

Quote:By using the SetWindowsHookEx function, it is possible to set a custom callback that can handle the WM_NCCREATE message right before calling the window procedure.

Source: <https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/>

CashoutArtist - May 4, 2019, 11:31 am

(May 4, 2019 11:29 AM)BTC Wrote: [\[CITE\]](#) Your Words:

From Article:

Source: <https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/>

Source: <https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/>

As i quoted you before, I said I learned vulns and exploiting from the CVE itself. If you learn from it, and you have a good base, you can slightly alter a previous 0 day and create a new one with time.

(May 4, 2019 10:55 AM)CashoutArtist Wrote: [\[CITE\]](#) Ahh, I see many people misunderstood that, vanilla mentioned that exploits have nothing involved with win api so I told him refer the CVE as the CVE actually provides really good information. If you want to learn about exploits and vulns, its really good to learn from previous ones and it helps in finding new ones in my opinion. But was just trying to show him the technical aspects are completely different.

BTC - May 4, 2019, 11:32 am

(May 4, 2019 11:31 AM)CashoutArtist Wrote: [\[CITE\]](#) As i quoted you before, I said I learned vulns and exploiting from the CVE itself. If you learn from it, and you have a good base, you can slightly alter a previous 0 day and create a new one with time.

You plagiarized and copy / pasted from this article. That is far different from learning from the CVE itself. You matched WORD FOR WORD. That is no coincidence, you plagiarized.

CashoutArtist - May 4, 2019, 11:33 am

(May 4, 2019 11:32 AM)BTC Wrote: [\[CITE\]](#) You plagiarized and copy / pasted from this article. That is far different from learning from the CVE itself. You matched WORD FOR WORD

Bro, you just plagiarize checked it and you couldn't find it "facepalm", obviously terms are not going to change lol. And it doesn't matter. I will get a review from Quick Hits of the Appraiser group in the

coming time. Stop spamming my thread lol. This also isn't a homework assignment, don't think I am getting any grades for this lol.

(May 4, 2019 11:23 AM)BTC Wrote: [\[CITE\]](#) Damn nice catch! I tried copy score and other plagiarism tests but did not uncover anything. This is a straight rip-off from that post. If you read through it literally is word for word WTF

BTC - May 4, 2019, 11:36 am

(May 4, 2019 11:33 AM)CashoutArtist Wrote: [\[CITE\]](#) Bro, you just plagiarize checked it and you couldn't find it "facepalm"

That is because this article would not have appeared in any copy score tests given the fact it was released less than a month ago. Regardless, your reply was word for word copied from that article. I am not spamming your thread, I am just confused as to why you lie to us in your replies. Seems you don't even know what you are selling or have your own words to back up your claims, considering you are copy / pasting other people's work in attempts to sell to users here on the forum. That is wrong in my books

If you copy / paste it makes me think you just copy / paste the exploit itself ?

LanMan - May 4, 2019, 11:37 am

(May 4, 2019 11:24 AM)CashoutArtist Wrote: [\[CITE\]](#) Its not the same as this. It has the same first step for the custom callback message, but further than that it is all different.

(May 3, 2019 07:16 PM)CashoutArtist Wrote: [\[CITE\]](#) And execute it in the system trough a base64 encoded shellcommand."After a successful exploitation, the exploit executed PowerShell with a Base64 encoded command." from article.

You only gave the CVE details word for word then, nothing else ? what about the RCE part of it ? I hope you have a very solid voucher to sell this without any backups claims.

CashoutArtist - May 4, 2019, 11:40 am

(May 4, 2019 11:36 AM)BTC Wrote: [\[CITE\]](#) That is because this article would not have appeared in any copy score tests given the fact it was released less than a month ago. Regardless, your reply was word for word copied from that article. I am not spamming your thread, I am just confused as to what you are selling. Seems you don't even know considering you are copy / pasting other people's work in attempts to sell to users here on the forum. That is wrong in my books

Its just a explanation. I learned from the CVE itself...am I supposed to make up half baked shit like vanilla? Cmon now lol. I didn't copy and paste it either rofl. I actually know it and know how that one works. So basically the initial part is the same for about the first 3 steps up until the function id, originally the function id would be set to 0 and data sets can be altered and information can be injected. Here, we(me and my partner) used a different way to bring about injection. Simple as it is. Reason I am not selling it for THOUSANDS. Its not a full blown out fresh 0 day, but it is still a new and working viable 0day.

(May 4, 2019 11:37 AM)LanMan Wrote: [\[CITE\]](#) "After a successful exploitation, the exploit executed PowerShell with a Base64 encoded command." from article.

You only gave the CVE details word for word then, nothing else ? what about the RCE part of it ? I hope you have a very solid voucher to sell this without any backups claims.

Will do buddy, as I mentioned 10+ times. The user Quick Hits will be reviewing this. Waiting for him. Already posted video proof, don't really understand why people keep going on about technical aspects, not going to tell you details about the vuln before you show any interest in purchasing.

BTC - May 4, 2019, 11:42 am

(May 3, 2019 07:16 PM)CashoutArtist Wrote: [\[CITE\]](#) By using the SetWindowsHookEx function, it is possible to set a custom callback that can handle the WM_NCCREATE message right before calling the window procedure.

^^ Those are your words

This is from [article](#) vvv

Quote:By using the SetWindowsHookEx function, it is possible to set a custom callback that can handle the WM_NCCREATE message right before calling the window procedure.

CashoutArtist - May 4, 2019, 11:44 am

(May 4, 2019 11:42 AM)BTC Wrote: [\[CITE\]](#) ^^ Those are your words

This is from article vvv

Yes. I never said I didn't refer the article lol. Anyways, ima head to bed, be back in 5-6 hours.

BTC - May 4, 2019, 11:46 am

(May 4, 2019 11:44 AM)CashoutArtist Wrote: [\[CITE\]](#) Yes. I never said I didn't refer the article lol. Anyways, ima head to bed, be back in 5-6 hours.

(May 4, 2019 11:36 AM)BTC Wrote: [\[CITE\]](#) If you copy / paste it makes me think you just copy / paste the exploit itself ?

So is your exploit same as this one or modified version you are saying? Because they look exact same as the one publicly written in this article and already analyzed by Kaspersky

A zero-day and public exploit are very different is my only reasoning. I only buy zero-days as I am avid renter for past 5 years of my life, but if it's based from a public exploit then it's definon-ally not a zero day.

Perhaps if you could clear up all this plagiarism and fact it matches a public exploit, with proper reasoning then I would be considering purchasing your exploit ? Thanks. Eager to hear your response.

?rescent - May 4, 2019, 11:48 am

Guys... I don't think this guy is a skid... I've talked to him for awhile and he knows what he is talking about, he's nice and has showed me some stuff.

CashoutArtist - May 4, 2019, 11:51 am

(May 4, 2019 11:46 AM)BTC Wrote: [\[CITE\]](#) So is your exploit same as this one or modified version you are saying? Because they look exact same as the one publicly written in this article and already analyzed by Kaspersky

A zero-day and public exploit are very different is my only reasoning. I only buy zero-days as I am avid renter for past 5 years of my life, but if it's based from a public exploit then it's definon-ally not a zero day.The exploit posted in the CVE was a 0 day lol. I used it for reference in comparison to eternal blue. ONLY the first 3 initial steps are the same. I will not release any further information post custom callback information. Simple as it goes.

(May 4, 2019 11:48 AM)?rescent Wrote: [\[CITE\]](#) Guys... I don't think this guy is a skid... I've talked to him for awhile and he knows what he is talking about, he's nice and has showed me some stuff. Thanks buddy! Hopefully we can work something out soon :D

BTC - May 4, 2019, 11:54 am

(May 4, 2019 11:51 AM)CashoutArtist Wrote: [\[CITE\]](#) The exploit posted in the CVE was a 0 day lol. This is where I am confused...I sell zero days for past half decade now, and have never heard of someone use the term so lightly. It was a zero-day but no longer is a zero day exploit.

Okay so the first 3 steps of your exploit are ripped from public exploit, and then you plagiarized your responses straight from a public article. Can you clear this up for me so I, as well others, can feel comfortable with purchasing?

<http://imgtfy.com/?q=define+zero-day>

<http://imgtfy.com/?q=define+CVE>

CashoutArtist - May 4, 2019, 11:55 am

(May 4, 2019 11:54 AM)BTC Wrote: [\[CITE\]](#) This is where I am confused...I sell zero days for past half decade now, and have never heard of someone use the term so lightly. It was a zero-day but no longer is a zero day exploit.

Okay so the first 3 steps of your exploit are ripped from public exploit, and then you plagiarized your responses straight from a public article. Can you clear this up for me so I, as well others, can feel comfortable with purchasing?

Pming you jabber, if you are interested in purchasing..we will talk there.

BTC - May 4, 2019, 11:56 am

(May 4, 2019 11:55 AM)CashoutArtist Wrote: [\[CITE\]](#) Pming you jabber, if you are interested in purchasing..we will talk there.

Spoiler [\(Click to View\)](#)

I handle all transactions on-site and using off-site chat services for transactions is frowned upon for obvious reasons ? This is the second time now you try to convince me to talk with you off-site. I do not do that. I stated it last time we spoke and will state it again. I do not want to speak with you if not on the forum itself. Thanks.

No problem if you are going to sleep, I will await your response as I was seriously interested in this product until the uncovering truth of your plagiarism.

CashoutArtist - May 4, 2019, 11:57 am

(May 4, 2019 11:56 AM)BTC Wrote: [\[CITE\]](#) I handle all transactions on-site and using off-site chat services for transactions is frowned upon for obvious reasons ? This is the second time now you try to convince me to talk with you off-site. I do not do that.

Read pm, obvio? We are not trading off site, we are discussing offsite. Not pming or publically posting about a 0 day. Common sense.

BTC - May 4, 2019, 12:00 pm

(May 4, 2019 11:57 AM)CashoutArtist Wrote: [\[CITE\]](#) Read pm, obvio? We are not trading off site, we are discussing offsite. Not pming or publically posting about a 0 day. Common sense.

(May 4, 2019 11:56 AM)BTC Wrote: [\[CITE\]](#) I do not want to speak with you if not on the forum itself.I ask you questions about your product multiple times, you ignore me and try to persuade to speak on different platforms.

I will stop responding at this point, given you only want to prove your authenticity of the exploit off-site and fail to do so onsite, not worth the risk to me. If you can not say what you need to say on the forum then it's worrying. Good day, and goodbye.

LanMan - May 4, 2019, 12:03 pm

Okay so this CVE was patched recently:

<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0859>

And this driver exploit doesn't affect XP OS so how come you got a XP infected ?

Anyway this is all about the public local privilege escalation cve. We have no info what so ever about the RCE, the most pricy kind of 0days. And a 0day RCE for 2k ? you can add 2 more zero if you really have that.

BTC - May 4, 2019, 12:04 pm

(May 4, 2019 12:03 PM)LanMan Wrote: [\[CITE\]](#) And a 0day RCE for 2k ? you can add 2 more zero if you really have that.

My thoughts exactly, I sell zero-days for past half decade and rent them, this is an absurd price for what is being claimed. Nothing to back up these claims other than plagiarized answered copy/pasted from public articles about public exploits that have been patched. ?

CashoutArtist - May 4, 2019, 12:04 pm

(May 4, 2019 12:00 PM)BTC Wrote: [\[CITE\]](#) I ask you questions about your product multiple times, you ignore me and try to persuade to speak on different platforms.

I will stop responding at this point, given you only want to prove your authenticity of the exploit off-site and fail to do so onsite, not worth the risk to me. Good day, and goodbye.

I suggest you wait for a review then. Thanks for your time and have a good day! I gave you my partners contact as I am going offline, that is all. If YOU do not want to take an initiative, then it is not my fault. Good day mate.

BTC - May 4, 2019, 12:06 pm

(May 4, 2019 12:04 PM)CashoutArtist Wrote: [\[CITE\]](#) I suggest you wait for a review then. Thanks for your time and have a good day! I gave you my partners contact as I am going offline, that is all. If YOU do not want to take an initiative, then it is not my fault. Good day mate.

I asked you multiple questions in regards to your product. You responded to my questions by saying to speak on Jabber, then give me the Jabber ID of your "partner" and expect me to take the initiative to further question different people about the same questions I had already asked you in regards to your product being sold on this platform? No.

Anything you say on Jabber can be said on-site. There is no need for Jabber. Answer my questions here, or in PM on HackForums, not on different platform.

CashoutArtist - May 4, 2019, 12:06 pm

(May 4, 2019 12:03 PM)LanMan Wrote: [\[CITE\]](#) Okay so this CVE was patched recently:

<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0859>

And this driver exploit doesn't affect XP OS so how come you got a XP infected ?

Anyway this is all about the public local privilege escalation cve. We have no info what so ever about the RCE, the most pricy kind of 0days. And a 0day RCE for 2k ? you can add 2 more zero if you really have that.

If you want more info, check BTC's post. My partners jabber is there, contact him. I am going offline. I already told you that it is not the exact same various times.

BTC - May 5, 2019, 11:14 pm

I still have interest in this product.

By the way is nice to see you again [GLWS88!](#)

Didn't think I would match your Discord from this profile to your last profile here on the forums did ya? ;)

Before purchasing, I would appreciate you to clear up the plagiarism claims made against you for this product, so I can feel comfortable in knowing what is being sold.

Also can you respond to the deal dispute posted quite some time ago? You have been online many times since, I am unsure why you have not responded. It makes me very worried as I am still trying to purchase some exploits to rent.

<https://hackforums.net/showthread.php?tid=5966978>

k1ng0fn0th1ng - May 6, 2019, 8:34 am

Is this the same or similar thing as "hackforums.net/showthread.php?tid=5965338"?
What versions of Windows does it work on?

BTC - May 9, 2019, 5:18 am

(May 6, 2019 08:34 AM)k1ng0fn0th1ng Wrote: [\[CITE\]](#) Is this the same or similar thing as "hackforums.net/showthread.php?tid=5965338"?
What versions of Windows does it work on?

Yes this is evidently the same exploit only a different GUI. This has been public for some time now, to the best of my knowledge. Given the replies to the thread, and plagiarism it is hard to believe otherwise.

investlom - May 14, 2019, 7:16 pm

No review yet for this products?

Cooooool - May 14, 2019, 7:44 pm

(May 14, 2019 07:16 PM)investlom Wrote: [\[CITE\]](#) No review yet for this products?
At least make a slight effort to read the thread and its entirety. It's a scam, there is no RCE Zero-Day for 2K, we're all gonna die some day, and we are tiny and meaningless.

Remember:

Reality is an illusion, the universe is a hologram, buy gold, byeeeeeeeeeeeeeeeeee!

CashoutArtist - May 14, 2019, 8:07 pm

(May 14, 2019 07:44 PM)Cooooool Wrote: [\[CITE\]](#) At least make a slight effort to read the thread and its entirety. It's a scam, there is no RCE Zero-Day for 2K, we're all gonna die some day, and we are tiny and meaningless.

Remember:

Reality is an illusion, the universe is a hologram, buy gold, byeeeeeeeeeeeeeeeeee!
Its not a scam derp, already sold this to 0dayguys.