



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

Malware Purported To Disable Antivirus Products On Windows Systems

Untested threat actor “mkdele” advertised malware that they claim will disable different antivirus products on machines running Windows, on the Russian language Deep Web forum xss[.]is. The actor claims the malware works with systems running Windows 7 through 11 (64-bit architecture only) without software dependencies. The actor specified the malware is obfuscated to avoid being detected as malicious by most antivirus products. They also noted that operators need to establish administrator privileges before running the malware on the target machine. Once the code is executed, the actor claims the malware will automatically disable various antivirus products, including:

- Microsoft Defender
- Kaspersky
- Norton
- Avast
- BitDefender

After antivirus protection is disabled, the actor claims that operators can freely run malicious payloads on the target machine until the system is rebooted or even after startup, depending on the build of the malware they purchased.

The actor is asking \$600 USD for a single build of the malware with persistence until reboot, and \$1,300 USD for three builds of the malware that will allegedly maintain persistence after startup.

The actor required escrow for payment, indicating they are more likely to have what they claim.

Original post from
threat actor “mkdele”
advertising their
malware to disable
antivirus products

Malware Purported To Disable Antivirus Products Cont.

Disable Antivirus | Win7&10&11 | 100%FUD | Private Stub

mkdele · Четверг в 11:02

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

+ Новая сделка



mkdele

CD-диск

Пользователь

Регистрация: 18.07.2019

Сообщения: 13

Реакции: 2

Четверг в 11:02

Hello guys

I'm selling a program for disabling antivirus software, which disables most antivirus .
Windows Defender/Kaspersky/avast etc..

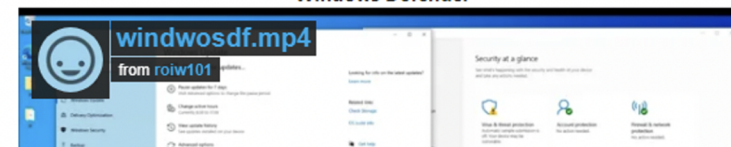
I have tested more than a dozen and all were successful.

The program achieves the effect of disabling the antivirus through the exploit.
you can literally start any program you want

Customization is accepted, if you need other functions just contact me.

Demo video:

Windows Defender



Service Creates New Cryptocurrencies For Fraud

Untested threat actor “Redon1” advertised their service to create new cryptocurrencies powered by a variety of blockchains on the Russian language Dark Web forum exploit[.]in. Threat actors can use these cryptocurrencies in different fraud schemes.

One scheme highlighted by the threat actor is to create a new cryptocurrency and widely promote it on multiple platforms to create exaggerated publicity to lure in would-be investors. Once customers have purchased the new coin, the threat actor can blacklist a customer’s crypto wallet. This would prevent the customer from selling or refunding their money, leaving the threat actor with the profits of the sale. The actor indicated a user can specify their own transaction fees allowing them to take larger amounts of money from victims. Although the actor did not specify a price for their service, they said they would split the profits generated from the sales of the new currencies they create.

Despite their lack of credibility on the forum, the actor accepts the use of escrow service for payment, increasing the likelihood that they can create new cryptocurrencies on different blockchains.



Original post from threat actor "Redon1" announcing their service to create new cryptocurrencies for fraud

Service Creates New Cryptocurrencies For Fraud Cont.

R

I can create your Token [BSC - ETH]

By Redon1, 19 hours ago in [Job] - search, execution of work

Follow

Start new topic

Reply to this topic

Redon1

megabyte

R

Paid registration

58 posts

Joined

04/26/20 (ID: 103365)

Activity

dpyroe / other

Posted 19 hours ago

Report post

Hello Exploit Brothers.

I come with a new thread that i can create Tokens [coins ... like Shiba inu , Safemoon , BabydogeCoin , and many of many more] especially if you look to scam on it.

i can add a blacklist function , when your token is active... you can blacklist manually every buyer and they can't sale.

you can set any fee [your desire] .

you will have your own marketing wallet that you will receive reward in bnb/eth after every sale .

and many of many other functions can add !

ready to use guarantor as service or i can work first ... you can just pay amount what will took to build it into ethereum/binance smartchain.

for more info - PM.

Increased Exploits For RCE Vulnerability In Spring Cloud Function

More threat actors are developing exploits for a newly discovered remote execution code (RCE) vulnerability in the Spring Cloud Function by VMware. ZeroFox anticipates this could lead to a potential increase in attacks carried out against cloud services that use the widely deployed Spring Cloud Framework.

In early April 2022, ZeroFox researchers observed the untested actor “WhiteRabbit” looking for proof-of-concepts (POCs) to exploit this vulnerability, tracked as CVE 2022-22963, on the English language Dark Web forum “KickAss”.

The vulnerability allows threat actors to remotely execute code on affected servers by creating malicious HTTP header requests. Affected versions of the Spring Cloud Function include:

- 3.1.6
- 3.2.2
- Older, unsupported versions

The well-regarded threat actor and administrator “NSA” quickly replied to the actor’s original post, sharing different exploits that are already publicly available for the vulnerability. ZeroFox researchers have observed other threat actors sharing additional POCs in response to similarly interested threat actors.

Original post from
threat actor
"WhiteRabbit" looking
for proof-of-concepts
(POCs) to exploit the
new vulnerability in
Spring Cloud Function

Exploits For Vulnerability In Spring Cloud Function Cont.

RCE 0-day Vulnerability found in Spring Cloud (SPEL)



WhiteRabbit
Purchased Member
progress: 33%

Posts: 41
Threads: 5
Reputation: 0

PM Find Rate

This might be bigger than log4j:
<https://www.cyberkendra.com/2022/03/rce-...cloud.html>

Trying to find the poc

Follow the white rabbit



NSA
NSA
★★★★★
founder

Posts: 5,587
Threads: 1,385
Reputation: 201

<https://nsfocusglobal.com/spring-cloud-f...ity-alert/>

POC
<https://github.com/Pizz33/Spring-Cloud-Function-SpEL>

<https://github.com/hktalent/spring-spel-0day-poc>

Don't worry, we don't spy on you - much