

Forum:[Hack Forums](#)

Thread: [PSA: New Malware/Trojan Variant Found](#)

sticksdev - September 10, 2022, 5:51 pm

As of just a few minutes ago, one of my open VMs got hit with a bait discord account on said VM.

The DM was one of those "Fake Image" scams, however, this one was actually an *image*. So I downloaded and opened, nothing seemed to happen until

I was immediately logged out of my discord account and machine account, and the machine rebooted.

Instantly infected with some sort of RAT or Trojan. No popups, just a reboot and disabling of the AV's I had on the system (Malwarebytes, Windows Defender) - it seems to be a common strain of Image Malware. But I don't know.

The file was deleted Apon rebooting. I am monitoring this VM and have isolated it. Will post updates here.

Connection was made to forgin noIP address, it is calling home - Traffic itself is hard to detect and I can't find where it's buried itself at.

(Sep 10, 2022 05:51 PM)sticksdev Wrote: [\[CITE\]](#) As of just a few minutes ago, one of my open VMs got hit with a bait discord account on said VM.

The DM was one of those "Fake Image" scams, however, this one was actually an *image*. So I downloaded and opened, nothing seemed to happen until

I was immediately logged out of my discord account and machine account, and the machine rebooted.

Instantly infected with some sort of RAT or Trojan. No popups, just a reboot and disabling of the AV's I had on the system (Malwarebytes, Windows Defender) - it seems to be a common strain of Image Malware. But I don't know.

The file was deleted Apon rebooting. I am monitoring this VM and have isolated it. Will post updates here.

Connection was made to forgin noIP address, it is calling home - Traffic itself is hard to detect and I can't find where it's buried itself at.

Me and @source@ were talking about it, however the VM suddenly rebooted again after we blocked the home server IPs, VM was dead. OS wiped.

Be very careful.

Origin file is a loader. Self-Delete when reboot as mentioned.

Bastille - September 11, 2022, 12:51 am

Hello,

I'm sorry to hear you experienced that ?

What was the OS of your VM ?
Was Malwarebytes free or paid version ?
Can you still download the image ? I would like to take a look at it for malware analysis
What did you use to check the traffic ? Wireshark ?
Are you into security ?

Kr0n0s - September 11, 2022, 5:14 am

This sounds exactly what a person with no knowledge in IT sec trying to spread panic on a blog post or news, no detailed information, no details, no origin info, very stupid motive, effort required / benefit ratio, sounds implausible and whats better than anything, no proofs in the end, it magically wiped itself out.

By the way, if the 'picture' was really using some kind of 0day, they would be using it to hack binance staff or any other company that has to open pictures on the machine to answer tickets/support, or sold to Zerodium (C.A.B. frontface) for somewhere i believe 500k/1 million for such vulnerability, they will never use it on a random on discord.

sorry but i think you're either lying or just can't differentiate between a picture and some other similar extension, i hope you prove me wrong.

sticksdev - September 11, 2022, 9:02 am

(Sep 11, 2022 12:51 AM)Yseurk Wrote: [\[CITE\]](#) Hello,

I'm sorry to hear you experienced that ?

What was the OS of your VM ?
Was Malwarebytes free or paid version ?
Can you still download the image ? I would like to take a look at it for malware analysis
What did you use to check the traffic ? Wireshark ?
Are you into security ?

1. Windows 10 (10.0.19043 21H1)
2. Free
3. Like I said in the post, the VM was trashed, could have been the file, could have been something else that was transmitted.
4. Wireshark + Firewall traffic from the cloud server itself
5. Yes, It is something I am learning.

(Sep 11, 2022 05:14 AM)Kr0n0s Wrote: [\[CITE\]](#) This sounds exactly what a person with no knowledge in IT sec trying to spread panic on a blog post or news, no detailed information, no details, no origin info, very stupid motive, effort required / benefit ratio, sounds implausible and whats better than anything, no proofs in the end, it magically wiped itself out.

By the way, if the 'picture' was really using some kind of 0day, they would be using it to hack binance staff or any other company that has to open pictures on the machine to answer tickets/support, or sold to Zerodium (C.A.B. frontface) for somewhere i believe 500k/1 million for such vulnerability, they will never use it on a random on discord.

sorry but i think you're either lying or just can't differentiate between a picture and some other similar extension, i hope you prove me wrong.

Hey, I appreciate your response, thanks for taking some time out of your day to write such a detailed response, but I want to reiterate:

1. This happened extremely quickly. I was away for most of the automated stuff but I only interacted with the file and then left to go do something and I came back

to a dead VM after we blocked it's home server.

2. I can understand how this can sound "noobish" and fake, but I assure you that I was trying my best to share what I had found using the information I had gathered and what I had available at the time of posting.

3. Also please bare in mind that I am still learning more and more about this field everyday - so I am bound to make mistakes.

Once again, thanks for you reply and criticism. I appreciate it.

(Sep 11, 2022 08:57 AM)Dyne Wrote: [\[CITE\]](#) Hello,

Please forward me the .exe or photo if you can recover it from the discord account and/or elsewhere.

It is likely a .lnk which produces a fetched decoy.

It is unlikely you were sent a 0day via discord, this seems like an awful waste for a multiple hundred thousand dollar exploit.

Hope I can help you out with this.

I agree with some of the comments here that it might be a spoofed metadata which makes it "appear" as a image, however it's just an exactable hiding under it. I am trying to recover the account but it's been locked.

I will post any updates if there is more to come. Thanks.