

Forum:[Hack Forums](#)

Thread: [Free Guide to making \\$\\$\\$ with malware](#)

slezer - July 17, 2023, 3:28 pm

Blackhat Guide to starting out & making real money with malware.

Choosing your malware, Making your payload FUD, Spreading, Monetization, Staying Anonymous & Useful Resources.

In this thread I will cover most things a newbie in the malware scene must know before starting out. Feel free to reply to this thread if you have any questions and I'll do my best to help. I also included a list of VPS/RDP server providers, file scanners and RATs / miners at the bottom of the thread.

[\[BLACKHAT\] ALL-IN-ONE RAT MENTORING - SETUP, CRYPTING, SPREADING, MONETIZATION](#)

In case you find this guide helpful and would want to have me answer your questions and teach you, privately and more in depth, my malware mentoring service may be interesting for you. As your mentor, my #1 goal is to help you make a stable source of income using malware & blackhat techniques.

Introduction

The first and most important thing you must keep in mind is your main goal, if your main goal is making money, then keep reading, if not, I can't guarantee this guide will be good for you. A common way of accomplishing this goal with malware nowadays is silent mining. To get a good setup, I recommend you find a RAT/Loader malware that suits your need, my personal setup goes something like this :

I like to use # RAT as my main payload for it's many persistence features that allow you to keep your bots alive for longer times, I then use the auto task feature to execute a UAC bypass of mine that after executes a silent miner. The reason for the UAC bypass is to bypass the administrator rights permission prompt that is required by my miner's settings to work. I personally mine RVN with GPU and XMR with CPU.

The reason you should spread a loader or a RAT with remote file execution features is that having post-infection control on your bots is essential, for example, you don't want to be spreading a silent miner alone, because you will not have the opportunity to maximize the profit from these installs post-execution. On the other side, when spreading a RAT or a loader, you will be able to execute other payloads than, here in this example a silent miner, on your bots. This is key, you want to be able to keep control on your bots.

If you choose to go for a loader, I suggest you buy Amadey Loader, which is sold for 600\$ or Smoke Loader for 400\$ on a forum which I can not mention the name of if I don't want to get warned here. Another great and cheap option I would recommend is # RAT, it has many persistence features to avoid losing your bots and is being sold for fairly cheap. Like I said, good software will

most of the time, be paid. For a free RAT, I suggest using [DcRat](#), it is an open source RAT and tends to be pretty stable.

Making your payload FUD

Now don't go and spread your DcRat executable just yet, your exe needs to be FUD (Fully Undetectable) by antivirus software, or almost, at least. To do this, you can choose to get scammed here by buying a garbage 100\$ public crypter or pay a few hundred dollars and get a better, private crypter. If you don't want to spend that much money on that, I would recommend you use a dropper/shellcode loader, this is probably the most used alternative to crypting. Some people also use LNK/URL "exploits" which are not really exploits, but simple powershell or batch command shortcuts with downloading or memory loading features. To check detections on your payload, you can scroll down to the end of this thread where I included a list of file scanning services that don't distribute results to antivirus companies. Never use VirusTotal, because they share scan results and will end up getting your file even more detected.

Note: Scantime means when an antivirus scans your file before it gets executed, runtime is whether or not antiviruses detect your payload when it gets executed.

Spreading your payload

This is the step where most losers will give up, or decide to buy installs. I'm warning you, spreading is not that easy when you're starting out, but once you get the hang of it, it's smooth sailing. In this section, I will cover a few known spreading methods and the ones I recommend the most.

Before I go any further, I strongly recommend you stay away from bot/install shops, these installs are shared and most people who buy these are already mining on the bots, and their logs are most likely raped to hell and back. So please save your time and stay away from these.

1. Landing Pages

Landing Pages are websites which exist with the sole purpose of spreading malware. They're basically websites offering a fake piece of software which is appealing to download. Landing pages require traffic to function properly, there are many ways to get traffic to a website, such as SEO, Google Ads and YouTube, for example. It is also worth mentioning that most landing pages use WordPress. Landing Pages are pretty much the meta currently in spreading due to the fact that they will spread your payload on autopilot once they receive enough traffic.

2. Advanced YouTube Spreading

YouTube Spreading is known to be oversaturated but with this twist to the classic version of this method, you can get nice amounts of installs. This method implies buying or obtaining in any way YouTube account cookies (cookies are a piece of data that can be used by anyone to log into an account, think of it as a password, kinda.). The channels you get the cookies from need to have at least 1k subscribers, once you have some channel cookies, which I won't cover how to get in this thread, you create a video for a game cheat, for example (if you think of something unique, it will work better) and upload your video on the channels with a link to your payload in the description. Since the channels already have a decent following they will get more exposure statistically.

3. Torrent Spreading

Torrent spreading has been around for the longest times, it is still a thing but has become harder to perform efficiently over time due to measures that have been put in place by torrenting websites. To torrent spread, you will need an account on popular torrent sites such as #, TorrentGalaxy, Torrenting, Demonoid, etc. Ranked accounts on these websites are being sold to make this part easier. When you have a ranked account with the ability to upload in the software / cracked games section, you will need your payload to be FUD to avoid being banned. You then have 2 options, bind your payload to real cracked software from those torrent sites, or make a launcher payload that launches the cracked software's exe and your FUD payload's exe.

Profiting from installs (Monetization)

The first method I would recommend is the most straightforward, silent mining. I would recommend anyone to use this miner: [Unam Sanctam Silent Miner](#), it is free and open source, it has fairly profitable algorithms like Kawpow (RVN) and is the miner with the most persistence, compared to Pure Miner which barely has any, and is being sold. I would not recommend Pure Miner unless you are fine with losing bots. With this method you will need a decent amount of bots to make good profit but I still recommend it when starting because it is the easiest and most simple way to monetize installs. It will give you a good example that silent mining can be very profitable when practiced on a large scale.

The second method I would recommend is harvesting credentials & cookies. For this you will need a stealer. There pretty much isn't any free and reliable stealers I can think of at the moment. Over on the paid side I would recommend Pure Logs if you're starting out. Once you start getting cookies and credentials you can decide to sell them by finding buyers or if you end up getting crypto wallet accounts or something of the sort you can try logging into them and emptying the accounts yourself.

The third method I would recommend requires more experience and a lot of bots but you can make some decent profit from this one if you do it correctly. Using some RATs or specialized tools, you can turn your bots into proxies. You can then sell them as residential proxies. You can choose to create an autobuy website to automate the selling process.

Staying Anonymous (OpSec)

Staying anonymous is a very important thing to keep in mind when doing malware. Unless you want to get federal agents knocking on your door, I strongly believe everyone should use these tips.

First of all, get an actually good VPN; Now don't go and buy [censored] or other dogshit VPNs that keep logs. I personally recommend using [Mullvad VPN](#). Please keep in mind that using a VPN does not automatically make you anonymous, it does far less than that, all a VPN does is 'hide' your IP address & encrypt your internet traffic. This does not necessarily mean nobody can view that traffic. The burden of trust of your traffic shifts from your ISP (Internet Service Provider) to your VPN company. Mullvad has sort of proven that they do not keep logs. Their headquarters in Sweden were raided by police with the goal of finding logs and they left empty handed; here is their [article](#) which covers it more in detail. Mullvad also only costs 5\$ per month (can be paid with cryptocurrency, including Monero) and does not require any of your info to create an account on their site.

I also recommend you don't use Google Chrome or Microsoft Edge. You should use a better option like Firefox or Tor if you want to go wild. Browsers like Chrome and Edge are owned by companies who are known to collect data, which is the reason I would advise against using these.

One of the first things I would also do if I was starting out is buy an RDP from a bulletproof provider and keeping all your malware and compromising files on there. This way, when you need to do get some dirty work done, you can connect to your RDP, connect to your VPN and/or hop on Tor and get your work done, all within your RDP. You should also keep a copy of the files you put in your RDP on a USB drive of yours, so that in the event of your hosting company going down, you wouldn't be absolutely fucked (talking from experience). You should of course keep the files on your USB drive encrypted using a reliable encryption algorithm like AES-256 or ChaCha20.

This is extremely important : You should never connect to your RDP/VPS related to malware/spooky shit under your actual IP address, at least hide your IP with a VPN when connecting to it to avoid linking your IP addresses to these boxes in case of an investigation.

One good thing to take note of is that : Convenience decreases with the more OpSec measures you put in place ; this means that by trying to stay anonymous, you will put in measures that can & will take time off you by : slowing down your internet speeds (by using Tor or a VPN, or both.), 'wasting' time to encrypt files that can be compromising in the case of a police investigation, etc.

Resources (File Scanners, Server Providers, RATs, Silent Miners)

Scanners

<https://websec.nl/scanner> (Scantime) - 40 Antiviruses & Unlimited scans.

<https://avcheck.net/> (Scantime) - 26 Antiviruses & 0.1\$ per scan.

<https://scanner.to/> (Runtime) - 21 Antiviruses & 1\$ per scan.

<https://checkzilla.io/> (Runtime) - 18 Antiviruses & 1\$ per scan.

Server Providers

[Cloak.su](https://cloak.su) - Recommended :)

[Bullethost.net](https://bullethost.net)

[PrivateAlps](https://privatealps.com)

[CrazyRDP](https://crazyrdp.com)

[AnonVM](https://anonvm.com)

RATs & Other Malwares

[Rem cos RAT](#) (Paid) (My personal favorite, albeit it requiring a powerful RDP server)

[Warzone RAT](#) (Paid)

[DcRat](#) (Free & Open Source)

Unam Sanctam Silent Miner (Free & Open Source)

- [Miner Builder](#)

- [Web Panel](#)

Sticky Bot - July 17, 2023, 3:36 pm

Hi, I'm Sticky Bot. The owner of this thread has purchased a Paid Sticky. Hack Forums does not get involved in deals or deal disputes. We do not vouch for the product or the service offered by

members. Please note that all deals are at your own risk. The sticky will expire on 07-31-2023. If you or a loved one are interested in buying a sticky please visit this page: [Buy Sticky](#). For more information about Paid Stickies you can read our [Help Doc](#).

DramaKing - July 18, 2023, 6:37 am

(Jul 17, 2023 03:28 PM)slezer Wrote: [\[CITE\]](#) Beginner's Guide to starting out & making money with malware.

Covers: Choosing your malware, Making your payload FUD, Spreading & Monetization.

I have thought about writing this and selling it as an e-book for a long time and I figured I would do it and make it free, since as a beginner, I would've found this information very helpful. Please keep in mind that all the information I have provided here comes from my personal experience. You might also want to check out my signature if you need any help, resources or services related to this thread. Most of the things I will cover in this thread, I can help you with. You can message me on [Telegram](#) or on here if you need help with anything.

Feel free to reply to this thread if you have any questions and I'll do my best to help.

Choosing your malware *Must Read*

The first and most important thing you must decide when starting out with malware is : what is the main malware you want to spread? The answer to this question is fairly simple, if you have money, buy a loader and spread that. If you're just starting out and/or don't want to invest money into tools just yet, use a RAT and set it up on an RDP, which should only cost a few dollars. Before I get any deeper you must know that malware is not for poorons, some tools on the market go for thousands of dollars.

The reason you should spread a loader or a RAT with remote file execution features is that having post-infection control on your bots is essential, for example, you don't want to be spreading a silent miner alone, because you will not have the opportunity to maximize the profit from these installs post-execution. On the other side, when spreading a RAT or a loader, you will be able to execute other payloads than, here in this example a silent miner, on your bots.. This is the key, you want to be able to keep control on your bots.

If you choose to go for a loader, I suggest you buy Amadey Loader, which is for sale for 600\$ on a forum which I can not mention the name of if I don't want to get warned here. Like I said, malware is not for poorons. For a free RAT, I suggest using [DcRat](#), it is open source and pretty stable from my experience.

Making your payload FUD

Now don't go and spread your shitty DcRat executable just yet, your exe needs to be FUD (Fully Undetectable) by antivirus software, or almost, at least. To do this, you can choose to get scammed here by buying a garbage 100\$ public crypter or pay a few hundred dollars and get a better, private crypter. If you don't want to spend that much money on that, I would recommend you use a simple downloader program which can add exclusions to Windows Defender, this way you could at least bypass Windows Defender. If you need help with that, you can message me here or on Telegram which is on my profile.

To test detections on your payload, I suggest using these websites:

Scantime means when an Antivirus scans your file before a victim executes it, Runtime means

when a victim executes your payload, will the Antivirus be able to stop it from infecting them.

<https://antiscan.me/> (Scantime) - 4 free scans per day, can be bypassed using Tor.

<https://scanner.to/> (Runtime) - Paid.

Spreading your payload

This is the step where most losers will give up, I am warning you, spreading is not that easy when you are starting out, but once you get the hang of it, it's smooth sailing from here. In this section I will cover a few known spreading methods and the ones I recommend the most.

1. Landing Pages

Landing Pages are websites which exist with the sole purpose of spreading malware. They're basically websites offering a fake piece of software which is appealing to download. Landing pages require traffic to function properly, there are many ways to get traffic to a website, such as SEO, Google Ads and YouTube, for example. It is also worth mentioning that most landing pages use WordPress. Landing Pages are pretty much the meta currently in spreading due to the fact that they will spread your payload on autopilot once they receive enough traffic.

2. Advanced YouTube Spreading

YouTube Spreading is known to be oversaturated but with this twist to the classic version of this method, you can get nice amounts of installs. This method implies buying or obtaining in any way YouTube account cookies (cookies are a piece of data that can be used by anyone to log into an account, think of it as a password, kinda.). The channels you get the cookies from need to have at least 1k subscribers, once you have some channel cookies, which I won't cover how to get in this thread, you create a video for a game cheat, for example (if you think of something unique, it will work better) and upload your video on the channels with a link to your payload in the description. Since the channels already have a decent following they will get more exposure statistically.

Profiting from installs (Monetization)

The first method I would recommend is the most straightforward, silent mining. For poorons, you can use [Unam Sanctam Silent Miner](#), which is free and open source. For people willing to pay I would recommend Pure Miner. With this method you will need a decent amount of bots to make good profit but I still recommend it when starting because it is the easiest and most simple way to monetize installs. It will give you a good example that silent mining can be very profitable when practiced on a large scale.

The second method I would recommend is harvesting credentials & cookies. For this you will need a stealer. There pretty much isn't any free and reliable stealers I can think of at the moment. Over on the paid side I would recommend Pure Logs if you're starting out. Once you start getting cookies and credentials you can decide to sell them by finding buyers or if you end up getting crypto wallet accounts or something of the sort you can try logging into them and emptying the accounts yourself.

The third method I would recommend requires more experience and a lot of bots but you can make some decent profit from this one if you do it correctly. Using some RATs or specialized tools, you can turn your bots into reverse proxies. You can then sell these proxies as residential proxies. You can choose to create an autobuy website to automate the selling process.

This pretty much sums it up, if you guys want me to go more in detail about a specific part of this guide, let me know. And again, if you need help with anything, feel free to message me here or on

Telegram and I will be glad to help :)

Number 3 is something that I've considered, but how would you sell access to a reverse proxy? Wouldn't it need to be reconfigured every time someone new used it?

sheedok - July 18, 2023, 6:40 am

Youtube spam works very well.

I see it on YT. YT doesn't care at all..

Any tutorial about YT cookies and such things?

How to get them and so on..

slezer - July 18, 2023, 9:49 am

(Jul 18, 2023 06:37 AM)DramaKing Wrote: [\[CITE\]](#) Number 3 is something that I've considered, but how would you sell access to a reverse proxy? Wouldn't it need to be reconfigured every time someone new used it?

Yes, it would probably need to have its config changed everytime someone different uses it, but normally people have an automated website, which rents the proxies at a certain price, per day and users need to refill their balance to pay for the proxies. It's definitely over on the advanced side of monetization techniques.

(Jul 18, 2023 06:40 AM)sheedok Wrote: [\[CITE\]](#) Youtube spam works very well.

I see it on YT. YT doesn't care at all..

Any tutorial about YT cookies and such things?

How to get them and so on..

I am not aware of any tutorials on that, to be honest. You would have to look for a vendor on forums, maybe make some posts asking people if they know anybody who can sell you YouTube cookies.

DramaKing - July 18, 2023, 10:46 am

(Jul 18, 2023 06:40 AM)sheedok Wrote: [\[CITE\]](#) Youtube spam works very well.

I see it on YT. YT doesn't care at all..

Any tutorial about YT cookies and such things?

How to get them and so on..

Grab the Cookies folders from browser data locations.

slezer - July 18, 2023, 11:38 am

(Jul 18, 2023 10:46 AM)DramaKing Wrote: [\[CITE\]](#) Grab the Cookies folders from browser data locations.

This is a good idea, but you would need a stealer & this would require mass spreading, which kind of defeats the purpose of trying to start spreading for the first time with that method.

DramaKing - July 18, 2023, 1:48 pm

(Jul 18, 2023 11:38 AM)slezer Wrote: [\[CITE\]](#) This is a good idea, but you would need a stealer & this would require mass spreading, which kind of defeats the purpose of trying to start spreading for the first time with that method.

I assume that you're saying that to promote paid software. You don't NEED a special hacking program to read the SQLite3 database file where cookies are stored. However, I did confirm that Chrome at least encrypts the Cookies files with AES256-GCM and encrypts the encryption key with DPAPI. So it would be really hard without either a tool like Nirsoft ChromeCookiesView or desktop access.

slezer - July 18, 2023, 2:10 pm

(Jul 18, 2023 01:48 PM)DramaKing Wrote: [\[CITE\]](#) I assume that you're saying that to promote paid software. You don't NEED a special hacking program to read the SQLite3 database file where cookies are stored. However, I did confirm that Chrome at least encrypts the Cookies files with AES256-GCM and encrypts the encryption key with DPAPI. So it would be really hard without either a tool like Nirsoft ChromeCookiesView or desktop access.

You said it yourself, it's hard to decrypt the cookies file in Chrome without remote access, so why waste your time with that when you can get a paid tool that does it automatically. I also don't know how my reply promotes paid software in any way.

I don't think you understood what I meant. To get these cookies, you need bots, and if you're starting out and don't have any, where are you getting your cookies from? This comes back to what I was saying, you will probably need to find a vendor to get your first cookies.

PMMR - July 20, 2023, 1:23 pm

Great tutorial! Thanks for making it free.

slezer - July 20, 2023, 2:55 pm

(Jul 20, 2023 01:23 PM)duerme Wrote: [\[CITE\]](#) Great tutorial! Thanks for making it free.

You're welcome, I'm glad you found it useful. Let me know if I should elaborate on some specific topics.

ParasyteMaxim - July 21, 2023, 9:31 am

Great thread, very informative. How many installs are you going to need in order to hit \$100 days with miners?

slezer - July 21, 2023, 11:04 am

(Jul 21, 2023 09:31 AM)ParasyteMaxim Wrote: [\[CITE\]](#) Great thread, very informative. How many installs are you going to need in order to hit \$100 days with miners?

Depends which currency you are mining. It varies a lot from currency to currency depending on many factors.

(Jul 21, 2023 09:44 AM)shatter Wrote: [\[CITE\]](#) Nice tutorial on how to end up on a list. I should probably add an OpSec part xD

DramaKing - July 21, 2023, 12:32 pm

(Jul 21, 2023 09:31 AM)ParasyteMaxim Wrote: [\[CITE\]](#) Great thread, very informative. How many installs are you going to need in order to hit \$100 days with miners?

I'm guessing, but it would be around 100-1000 to start.

slezer - July 21, 2023, 12:44 pm

(Jul 21, 2023 12:32 PM)DramaKing Wrote: [\[CITE\]](#) I'm guessing, but it would be around 100-1000 to start.

There's pretty much no way of getting 100\$ per day with 100 online bots; I'd say 300 minimum.

DramaKing - July 21, 2023, 12:57 pm

(Jul 21, 2023 12:44 PM)slezer Wrote: [\[CITE\]](#) There's pretty much no way of getting 100\$ per day with 100 online bots; I'd say 300 minimum.

Yeah, that's more realistic as a best case scenario. The bots could be the latest and greatest gaming machines, or they could be used for digital signage.

slezer - July 21, 2023, 2:22 pm

(Jul 21, 2023 12:57 PM)DramaKing Wrote: [\[CITE\]](#) Yeah, that's more realistic as a best case scenario.

The bots could be the latest and greatest gaming machines, or they could be used for digital signage.

True. If you have 100 Threadripper CPUs mining for you, it could be 100% possible to make much more than 100\$ USD per day but that's almost impossible.

nvidiageek - July 21, 2023, 5:16 pm

(Jul 21, 2023 02:22 PM)slezer Wrote: [\[CITE\]](#) True. If you have 100 Threadripper CPUs mining for you, it could be 100% possible to make much more than 100\$ USD per day but that's almost impossible.

So I presume the average joe case would be around 15-20\$ a day?

slezer - July 21, 2023, 7:39 pm

(Jul 21, 2023 05:16 PM)nvidiageek Wrote: [\[CITE\]](#) So I presume the average joe case would be around 15-20\$ a day?

Average joe? Pretty much anyone that doesn't have down syndrome can make 200+ \$USD per day if you learn how to spread properly. Theres no limit as to how much money you can make with malware either; more bots = more money.

Added OpSec & Terminology.

ParasyteMaxim - July 22, 2023, 11:20 am

Tell us more please slezer, can you give a run down of costs for poors and people with a few quid? Im getting into sec in a big way now that ive been forced out of easy web dev work by gpt

slezer - July 22, 2023, 11:31 am

(Jul 22, 2023 11:20 AM)ParasyteMaxim Wrote: [\[CITE\]](#) Tell us more please slezer, can you give a run down of costs for poors and people with a few quid? Im getting into sec in a big way now that ive been forced out of easy web dev work by gpt

I included links for malwares which are open source on GitHub.

B3RS3RK - July 24, 2023, 12:34 pm

Nice tutorial. So all of this can, hypothetically, be started for under \$50?

slezer - July 25, 2023, 12:04 pm

(Jul 24, 2023 12:34 PM)B3RS3RK Wrote: [\[CITE\]](#) Nice tutorial. So all of this can, hypothetically, be started for under \$50?

Well yeah, but your payload won't be FUD, because you need a crypter or an AV bypass.

DarkKnightDumno - July 25, 2023, 8:50 pm

mmf typed up a whole essay, aint tryna read allat

slezer - July 25, 2023, 9:20 pm

(Jul 25, 2023 08:50 PM)DarkKnightDumno Wrote: [\[CITE\]](#) mmf typed up a whole essay, aint tryna read allat

I'm not obligating you to read my thread. I'm simply trying to help people :)

plug1N - July 26, 2023, 12:14 am

I'm glad I came across a helpful person like you on this forum, my websta.

I will try all the methods and ask you on the parts I can't

thanks sensei ?

DarkKnightDumno - July 26, 2023, 10:26 pm

(Jul 25, 2023 09:20 PM)slezer Wrote: [\[CITE\]](#) I'm not obligating you to read my thread. I'm simply trying to help people :)
ik you good bro, im not tryna insult you or anything :)

liwenyuan - July 29, 2023, 4:00 am

???VPN????????????,????????????????????????????????

slezer - July 29, 2023, 5:38 am

(Jul 29, 2023 04:00 AM)liwenyuan Wrote: [\[CITE\]](#)

???VPN????????????,????????????????????????????????

Please speak English on here.

liwenyuan - July 29, 2023, 9:54 am

Hi, I'm from China. I will go to college soon, and now I have two choices: 1. to learn and develop knowledge and become a social animal in the future. 2. Become what you say, but can you have a normal job in this line of work. It feels illegal. What do you think of this

slezer - July 29, 2023, 9:56 am

(Jul 29, 2023 09:54 AM)liwenyuan Wrote: [\[CITE\]](#)

??,????????????????,????????:1.????????,????????2.????????,??

I put your text through Google Translate and you do have an interesting point. I know a lot of people who do this and still have a job, and it's not like you're straight up scamming people.

deraive - July 29, 2023, 4:39 pm

thanks really a lot man

slezer - July 30, 2023, 5:07 pm

(Jul 29, 2023 04:39 PM)deraive Wrote: [\[CITE\]](#) thanks really a lot man

You're welcome, let me know if you have any questions.

Cortex101 - July 30, 2023, 9:12 pm

Nice tutorial bro, really appreciate it

slezer - July 30, 2023, 9:17 pm

(Jul 30, 2023 09:12 PM)Cortex101 Wrote: [\[CITE\]](#) Nice tutorial bro, really appreciate it

I'm glad my guide helped you. As always, let me know if you have any questions.

Sticky Bot - July 31, 2023, 4:00 pm

Hi, I'm Sticky Bot. The owner of this thread has purchased a Paid Sticky. Hack Forums does not get involved in deals or deal disputes. We do not vouch for the product or the service offered by members. Please note that all deals are at your own risk. The sticky will expire on 08-28-2023. If you or a loved one are interested in buying a sticky please visit this page: [Buy Sticky](#). For more information about Paid Stickies you can read our [Help Doc](#).

BELG - August 3, 2023, 4:38 am

[quote="slezer" pid='62030663' dateline='1689632882']

Beginner's Guide to starting out & making money with malware.

Covers: Choosing your malware, Making your payload FUD, Spreading, Monetization, OpSec & Terminology in malware.

Thanksss a lott this is really good

slezer - August 3, 2023, 4:50 am

(Aug 3, 2023 04:38 AM)BELG Wrote: [\[CITE\]](#) Thanksss a lott this is really good
I'm glad my guide helped you. Let me know if you have any questions.

BELG - August 3, 2023, 4:55 am

(Aug 3, 2023 04:50 AM)slezer Wrote: [\[CITE\]](#) I'm glad my guide helped you. Let me know if you have any questions.

Oh i can use this with the Metasploit payload right?

slezer - August 3, 2023, 7:25 am

(Aug 3, 2023 04:55 AM)BELG Wrote: [\[CITE\]](#) Oh i can use this with the Metasploit payload right?
What exactly are you refering to in the guide?

TheEasyPeasy - August 5, 2023, 4:52 am

Great thread, very informative

butu - August 16, 2023, 3:33 am

Great and thanks alot ,It is very useful for me as beginner.

itzarima - August 21, 2023, 3:47 pm

it seems intresting...

Gurdji - August 22, 2023, 3:06 pm

such a nice guide thank you

463n7 - August 24, 2023, 8:51 pm

This was really good, thanks for posting this up. Especially for people like me that are new to this side of things!

Aschen - August 25, 2023, 1:06 am

Interesting guide, ty vm

Taway2842 - August 25, 2023, 11:35 pm

thank you nice guide

JamesChoe - August 26, 2023, 6:09 am

Thanks for this really detailed post

anihil - August 26, 2023, 11:50 am

Great thread, very informative , i will add to my stuff

Sticky Bot - September 8, 2023, 9:55 am

Hi, I'm Sticky Bot. The owner of this thread has purchased a Paid Sticky. Hack Forums does not get involved in deals or deal disputes. We do not vouch for the product or the service offered by members. Please note that all deals are at your own risk. The sticky will expire on 10-06-2023. If you or a loved one are interested in buying a sticky please visit this page: [Buy Sticky](#). For more information about Paid Stickies you can read our [Help Doc](#).

r2die2 - September 11, 2023, 4:36 am

Hi thanks for the tutorial realy hard to know where to start. This realy helped give me a better

understanding, but are there any other rats that you could recommend that have a lifetime payment or cheaper full year plan. I can afford warzone rat but would be nice to have a lifetime payment instead.

eesdasdwac - September 11, 2023, 6:27 pm

ehhhhhhhhhehhhhhhhhehhhhhhhhehhhhhhh [warn]

Mystic - September 17, 2023, 6:22 am

Can i use Proton vpn? or does it keep logs?

what rdp should i buy and use? and how do i even use a rdp on a rat i never knew of this and where do i find these loaders and so on?

Trephy - September 19, 2023, 1:08 pm

Thanks for sharing man, appreciate it!

slezer - September 19, 2023, 2:26 pm

(Sep 17, 2023 06:22 AM)Mystic Wrote: [\[CITE\]](#) Can i use Proton vpn? or does it keep logs?

what rdp should i buy and use? and how do i even use a rdp on a rat i never knew of this and where do i find these loaders and so on?

I recommend you use Mullvad VPN, it's only 5\$ per month and can be payed with Monero.

I personally use Bullethost.net for my VPS and RDP servers, never had a problem with them.

You can simply browse the forum here and you'll most likely find sales thread for some loaders.

I think I'm going to add a list of RATs, Loaders, VPNs, server providers, etc.

Mystic - September 20, 2023, 10:18 am

(Sep 19, 2023 02:26 PM)slezer Wrote: [\[CITE\]](#) I recommend you use Mullvad VPN, it's only 5\$ per month and can be payed with Monero.

I personally use Bullethost.net for my VPS and RDP servers, never had a problem with them.

You can simply browse the forum here and you'll most likely find sales thread for some loaders.

I think I'm going to add a list of RATs, Loaders, VPNs, server providers, etc.

i have crypter and it has a .bat loader function but i dont now how to use it its private i got it for free tho and i have the source code for it can you show me how to use the .bat loader function cause it put in on a scantime and it bypass all of it but when i run it does not work

fluxd - September 22, 2023, 4:39 pm

What is the typical detection / removal time frames for your infected hosts, on avg ofc.

Also looking into DcRat it seems the repo has been archived is there an active fork to target, or does this need a new dev... I happen to know my way around c#.

Would love to talk more on the setup / config seems really interesting.

slezer - September 22, 2023, 5:00 pm

(Sep 22, 2023 04:39 PM)fluxd Wrote: [\[CITE\]](#) What is the typical detection / removal time frames for your infected hosts, on avg ofc.

Also looking into DcRat it seems the repo has been archived is there an active fork to target, or does this need a new dev... I happen to know my way around c#.

Would love to talk more on the setup / config seems really interesting.

DcRat is still working as of today, but its starting to get relatively old, if you can make your own fork, go for it! There is no typical removal time, it all depends on your malware's persistence, Warzone RAT, for example has much more persistence which allows you to keep bots for longer.

asyn - September 23, 2023, 8:17 am

Thanks for your sharing [warn]

Sticky Bot - February 17, 2024, 11:13 pm

Hi, I'm Sticky Bot. The owner of this thread has purchased a Paid Sticky. Hack Forums does not get involved in deals or deal disputes. We do not vouch for the product or the service offered by members. Please note that all deals are at your own risk. The sticky will expire on Mar 17, 2024. If you or a loved one are interested in buying a sticky please visit this page: [Buy Sticky](#). For more information about Paid Stickies you can read our [Help Doc](#).

Mooooookie - February 17, 2024, 11:20 pm

Just read your write up, and I must say, it was well written and had some good information in it. Actually motivated me to want to learn more about this field. Silent mining is something that has always taken my interest somewhat. How many installs would you need to make approx \$1k a month from silent mining?

slezer - February 18, 2024, 7:47 pm

(Feb 18, 2024 12:20 AM)Mooooookie Wrote: [\[CITE\]](#) Just read your write up, and I must say, it was well written and had some good information in it. Actually motivated me to want to learn more about this field. Silent mining is something that has always taken my interest somewhat. How many installs would you need to make approx \$1k a month from silent mining?

First of all, thanks for the words and I'm glad it motivated you to start out.

1000\$ divided by 30 days is 33\$, which means you must earn 33\$ per day by mining to reach your goal. This is entirely possible, and I would consider this as a great goal to start. It's generally hard to estimate how many installs you would need to reach a goal since mining profits depend entirely on your victim's computer specs (CPU & GPU). To give you a rough number, I'd say you'd need around 200 gaming PC bots, online at all times to make that much per day. But again, this is a very rough estimate.

Mooooookie - February 19, 2024, 3:15 am

(Feb 18, 2024 08:47 PM)slezer Wrote: [\[CITE\]](#) First of all, thanks for the words and I'm glad it motivated you to start out.

1000\$ divided by 30 days is 33\$, which means you must earn 33\$ per day by mining to reach your goal. This is entirely possible, and I would consider this as a great goal to start. It's generally hard to estimate how many installs you would need to reach a goal since mining profits depend entirely on your victim's computer specs (CPU & GPU). To give you a rough number, I'd say you'd need around 200 gaming PC bots, online at all times to make that much per day. But again, this is a very rough estimate.

Nice. I like the way you broke it down into how much will be needed per day, as it makes the goal feel more easily achievable. This is something I can actually see myself doing. I just recently registered a business, so am a little busy at the moment getting things setup with that, but I'm definitely going to add this to my list of things to do. You sound like you know what you're talking about, and will make an effort to reach out to you once I'm ready for some proper guidance. How much funds do you think I should set aside for a project like this?

slezer - February 19, 2024, 6:29 am

(Feb 19, 2024 04:15 AM)Mooooookie Wrote: [\[CITE\]](#) Nice. I like the way you broke it down into how much will be needed per day, as it makes the goal feel more easily achievable. This is something I can actually see myself doing. I just recently registered a business, so am a little busy at the moment getting things setup with that, but I'm definitely going to add this to my list of things to do. You sound like you know what you're talking about, and will make an effort to reach out to you once

I'm ready for some proper guidance. How much funds do you think I should set aside for a project like this?

Good luck with your business, I genuinely hope that works out for you ;)

As for how much to set aside for this kind of project, it really depends on how big you want to go; if you simply want to try this out with some decent tools, there's a lot of really good open source RATs and silent miners you can use for free.

In my mentoring service, I make use of these tools so the only thing you'd have to pay for is the mentoring part which will include a big setup guide I'm writing at the moment, along with all the spreading material you'll need.

If this works well and you decide to go bigger, you can easily switch to better paid tools over time.

kmokl - February 22, 2024, 11:33 am

thank you so much my family needs some money

JMuRWaZE - February 26, 2024, 7:11 pm

Does this require high-performance computer?

antX - February 26, 2024, 8:03 pm

Thank you for your work here the format clean.

Cyb3rAlb - February 27, 2024, 6:16 am

thanks for making this free ,really

loki958 - February 27, 2024, 6:32 am

Im very new to hacking so i wanted to know.

1. how do i actually control the rat and the silent miners i have ready, is there a specifi program i need and how will i track all my bots

slezer - February 28, 2024, 6:05 pm

(Feb 27, 2024 07:32 AM)loki958 Wrote: [\[CITE\]](#) Im very new to hacking so i wanted to know.

1. how do i actually control the rat and the silent miners i have ready, is there a specifi program i need and how will i track all my bots

RATs let you control all the bots directly in their server application. As for silent miners, some work like RATs and some are web based and have a web panel where you can see all your infected bots.

majhoul33 - February 29, 2024, 1:58 pm

thank you very much

ikele - March 2, 2024, 7:55 am

(Jul 17, 2023 03:28 PM)slezer Wrote: [\[CITE\]](#) Blackhat Guide to starting out & making real money with malware.

Choosing your malware, Making your payload FUD, Spreading, Monetization, Staying Anonymous & Useful Resources.

In this thread I will cover most things a newbie in the malware scene must know before starting out. Feel free to reply to this thread if you have any questions and I'll do my best to help. I also included a list of VPS/RDP server providers, file scanners and RATs / miners at the bottom of the thread.

very interesting ty

Draps - March 9, 2024, 11:42 pm

Just learning, this helps a lot!

gr0wth - March 10, 2024, 12:26 pm

Thank you for sharing, just a question regarding mullvad. Have you used any of their servers that are rented? I'm assuming based off the guide we're supposed to use servers that are owned by them

slezer - March 10, 2024, 8:16 pm

(Mar 10, 2024 12:26 PM)gr0wth Wrote: [\[CITE\]](#) Thank you for sharing, just a question regarding mullvad. Have you used any of their servers that are rented? I'm assuming based off the guide we're supposed to use servers that are owned by them

Well if you're paranoid, yeah, strictly use servers that are owned by them.

proboysasa - March 11, 2024, 8:05 am

Sir, this post as unlocked already so I don't need to reply for read. But I m still want to reply and want to say thank you for giving this information. And love you sir. Thanks brother

NyxCoder - March 11, 2024, 3:44 pm

Thanks for sharing bro, appreciate it

Frychi - March 18, 2024, 3:07 pm

Awesome! Thank you for your response, all the best!

griffon99 - March 18, 2024, 4:13 pm

Thanks, i am new here and this is really interesting.

Do you think this would work if the endpoints were fully patched? I imagine UAC bypass means the endpoints have to have vulns that are unpatched against

jakajaka - March 18, 2024, 6:12 pm

I am trying to download quasar but windows defender is yelling at me how do I bypass that?

SIM-5504527 - March 23, 2024, 6:36 pm

Thank you for the informative thread, still taking notes from this.

Sticky Bot - March 30, 2024, 3:35 pm

Hi, I'm Sticky Bot. The owner of this thread has purchased a Paid Sticky. Hack Forums does not get involved in deals or deal disputes. We do not vouch for the product or the service offered by members. Please note that all deals are at your own risk. The sticky will expire on Apr 27, 2024. If you or a loved one are interested in buying a sticky please visit this page: [Buy Sticky](#). For more information about Paid Stickies you can read our [Help Doc](#).

GuySensei - April 4, 2024, 1:32 pm

great post thanks. I loved mullvad.

StealthCoder1337 - April 4, 2024, 6:14 pm

Thanks for the post. Got me a step closer to setting up my own botnet. Are there any other opensource RAT alternatives aside from DCRat?

slezer - April 4, 2024, 7:07 pm

(Apr 4, 2024 06:14 PM)StealthCoder1337 Wrote: [\[CITE\]](#) Thanks for the post. Got me a step closer to setting up my own botnet. Are there any other opensource RAT alternatives aside from DCRat? There's AsyncRAT, but aside from these two I don't know any other good open source ones.

dolly - April 4, 2024, 11:35 pm

how much take time to start earn money from this?

nikkisolis - April 6, 2024, 5:28 am

Great guide good on you m8

Whackawhathathwatawathwak - April 10, 2024, 1:09 pm

I saw N-o-r-d was audited, they don't seem to log

FocusZero - April 17, 2024, 4:03 am

Thanks man, great tutorial. I've one project that I'm working on so this post changed my mind how to execute first few steps. tyyy <3

JDH1217 - April 17, 2024, 1:32 pm

How would you recommend going about constructing a landing page and advertising or making sure it gets traffic?

Raven_666 - April 18, 2024, 1:36 am

You're better off breaching companies than this method, and it would be free

slezer - April 18, 2024, 4:43 am

(Apr 18, 2024 01:36 AM)Raven_666 Wrote: [\[CITE\]](#) You're better off breaching companies than this method, and it would be free

This is a guide for malware, not for breaching companies, and no, it would not be free.

dubbstaap77 - April 21, 2024, 5:32 am

nice guide thanks 4 this

TGHB - April 22, 2024, 12:46 pm

It's cool that you took the time to share this post

Tocx - April 28, 2024, 1:54 pm

W tutorial thanks brotha

Stanley - May 5, 2024, 5:07 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

endovenoso-Krf - May 6, 2024, 9:15 am

i'm interested in?

Tocx - May 7, 2024, 12:36 am

number 3 is interesting

uluda88 - May 20, 2024, 4:16 am

A good tutorial for newbs like me, thanks.

gleesh6 - May 21, 2024, 7:48 pm

can you mentor me im looking for help with someone who has experience