Jun 11, 2015 · 20 min read

Learn How to Hack a Computer, Server, or Plane Within A Week

Doom DOS Code

- *Any actions and/or activities related to the material contained within this page is solely your responsibility. The misuse of the information provided can result in criminal charges brought against the person(s) in question. The author will not be held responsible in the event that any criminal charges be brought against any individuals misusing the information and/or breaking the law.*
- *All the information provided on this page is for* ***educational purposes only****. This content and its author is in no way responsible for any misuse of this security knowledge based on penetration testing, ethical hacking, and whitehat hacking.*
- *By continuing you agree to the following: you shall not misuse the information to gain unauthorized access. However, you may try out these hacks and interception techniques on your own computer,*

server, car, or plane at your own risk within a simulated environment. ***Performing hack attempts (without permission) on computers that you do not own is illegal.***

The Benefit of Learning How to Hack

What average users perceive as digital locks on their private data is often nothing more than a half-open door waiting to be walked into.

By understanding exactly how blackhat hackers gain access to target machines, similar to how thieves gain access to homes, engineers will develop better "locks" and average users will remember to "lock their doors" more often. After all, locks are useless without the knowledge on how they work and why they should always be utilized.

For example, those that believe that an antivirus suite is enough to protecting their computer should think again. Antivirus suites are not unsinkable ships, and those that believe them to be are likely to be completely oblivious to how viruses spread, how unpatched exploits result in breaches, and other fundamental knowledge tin keeping digital data safe.

. . .

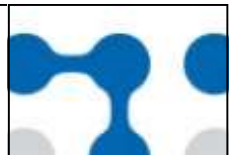
> *"The overall costs of identity theft to the American economy is estimated to reach $100 billion annually, and the cost globally is easily in the hundreds of billions of dollars."*

A hacker stole $50k from my bank account.

Two weeks ago I came to work, pretty stressed about our new Tribe at Boost, which starts on February 2nd, but we were...

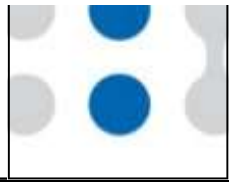
medium.com

US Government's HR Department Has Been Hacked, Government Employee Data Leaked | Techdirt



The US government keeps insisting that companies should be giving it information in order to help the government block...

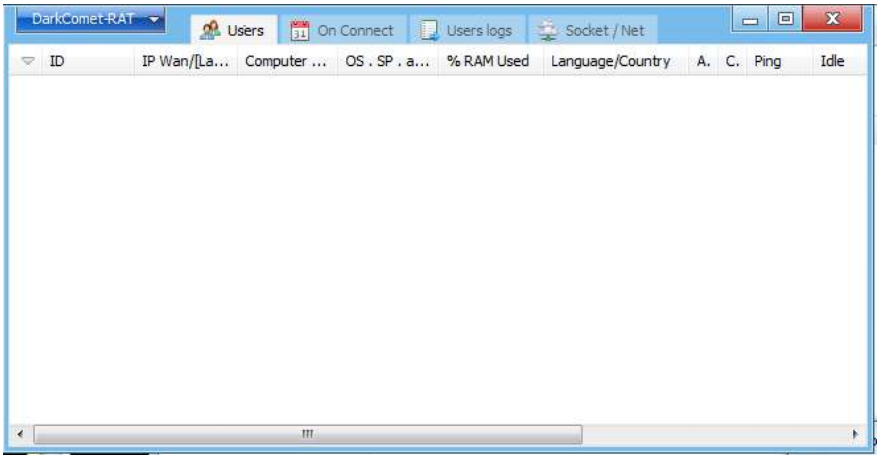
www.techdirt.com



. . .

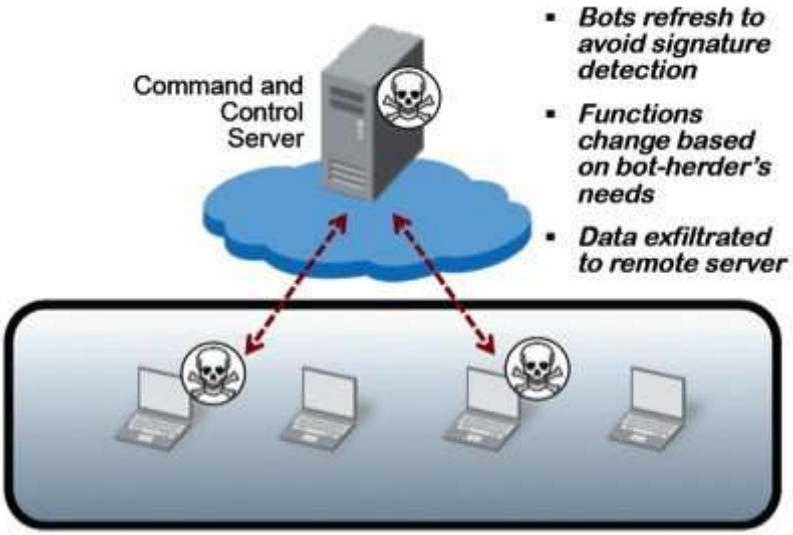
How To Create a Virus That You Can Use to Monitor and Control Infected Computers

Creating a virus is as simple as creating a Word document. I wish I was kidding. Take a look for yourself at one of the most popular virus creation software for hackers:



DarkComet-RAT

DarkComet allows a hacker to create a connection between an infected machine and his own machine in a virtual manner. It gives him the same control over a computer as it would if he plugged in a monitor and keyboard.



What is a botnet?

A virus also lets a hacker track every single keystroke of an infected machine, activate available microphones and cameras, and install further backdoor exploits to maintain permanent access.

Create Your Own Virus Within an Hour

1. Download DarkComet-Rat 5.31 from here. This is the most recent version that can build a live virus. (New versions have had the feature stripped by its developer after he grew sad over the fact that his tool made it possible for Syrian activists to be tracked after their machines were infected).

2. Follow this resource step by step to create a virus file. You can even morph your virus into photo or PDF document, which will open properly even as the infection takes control of the computer.

3. Move the infected file to your desired target (that you own or have written permission to infect) via a USB, file-sharing service, or emailing.

4. Run the infected file.

5. Check to see if the infection has connected the target machine to your control panel.

6. Play sounds on the target machine, view its screen, read its keystrokes, upload files to it, download files from it, and test

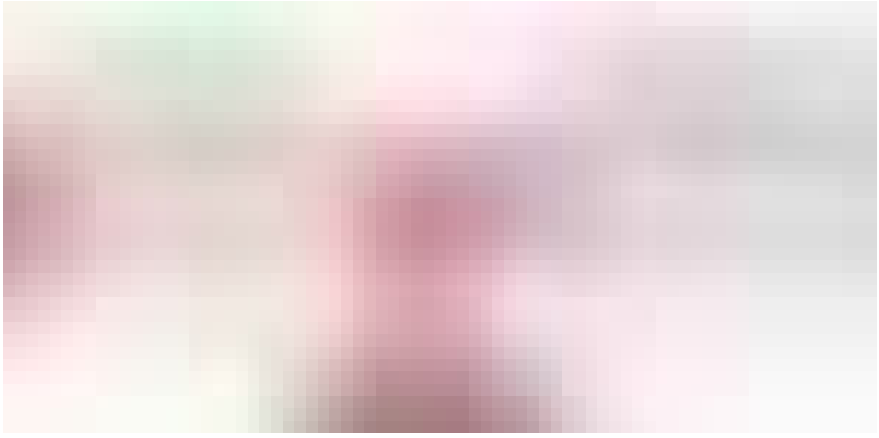
virtually every single feature available in the control panel to familiarize yourself with how much it would suck if someone infected you with one of these simple, yet nasty, digital parasite.

. . .

Hiding a Virus Effectively

The steps above will fail if the target machine has an antivirus program installed on it. Do not worry though. You can still gain access to your test machine regardless of how updated the antivirus program on it is.

To do so, you will need access to something called a Fully Undetectable (FUD) Crypter. These programs take an infected file and make its contents obscure in a way which seems normal to an antivirus program.



What is a FUD Crypter

If a virus program looks like a dog for example, and an infected file is held within a completed puzzle, a crypter takes that puzzle and breaks it up. Then it leaves instructions for itself on how to build the puzzle back up, all under the nose of an antivirus program. By the time the puzzle is built, the infection has spread across the computer, and the antivirus will have missed it all while trying to make sense of the randomly encrypted virus it doesn't know how to make sense of.

Simply "Googling it," ceases to be an effective way to get hacking tools through the internet. A Google search for "virus crypter" will land you

hundreds of results for the most overused crypters known to virtually every single antivirus research lab in the world.

None of the crypters that show up on Google will be adequate in hacking a system with an antivirus program.

What you need to Google to get a decent virus crypter is "hack forums." Below are two forums that will likely do:

- hackforums.net
- leakforums.org

Make an account to view the private threads, keep a lookout for recent crypters, and be ready to shell out anywhere from $10–100 per week to the developer of your desire crypter. This fee will fund his work as he keeps it updated and undetected by antivirus programs.

From there you'll likely be met with the crypter's custom guide. Simply load your infected virus into your crypter, using whatever instructions are available, and let it do its magic. The end result will be a fully hidden virus which antivirus programs shouldn't detect.

If you want to test how good of a job you crypter did,then use a service such as this one to test your completed virus. You can use VirusTotal.com if you want but they send infected files to over 50 malware laboratories as soon as your gains access to one of their test machines.

Sending files to VirtusTotal and letting your fellow hack forum acquaintances and crypter developer know that you have done so will likely get you cursed, banned, and hacked for being a "complete and total f**king noob" that made the fully undetected crypter fully detected within a matter of hours.

Spreading a Virus

Viruses are spread through various ways. It depends what the objective of the hacking at hand is.

If the objective is to steal the wallets of Bitcoin holders, then a little research on the internet could help you pinpoint one of the 150 Bitcoin stealing trojans and couple it up with your infected file. From

there, it could be spread through file-sharing services where users look for free music, movies, and software such as thepiratebay.se and other locations.

You would be surprised at how many owners of Bitcoins valued at thousands of dollars are unaware of basic security protocols. We're talking about above-average users, holding thousands of dollars on their computer, not knowing how to setup a basic thing such as 2-step verification or antivirus sandboxing for unknown files.

A virus could also be spread using a USB which is setup to autorun a file when inserted into a computer, without having to access the keyboard or mouse.

Some people that create viruses do so in order to control thousands of computers and to send bogus information to servers to take them offline. This process is known as a denial of service attack (DDOSing). They spread viruses through torrents and other public downloads as well.

Some people that create viruses do so in order to make use of the hardware of infected targets to crack passwords through brute-force attempts, and to even mine Bitcoins and then sell them. They use similar mass virus spreading techniques. You'd be surprised at how many people will turn off their antivirus program in order to use a video game cheat program, or other "crack," as instructed by the person who made it.

> *Your antivirus program will pick up that the cheat program is trying to modify your video game while it's running. Thus, it will get rid of the file and mark it as a virus. This is normal. Do not worry (average user), just turn off your antivirus program and then run the cheat program again. It will do it's job (and most of the time, it will do a little bit more). -Typical virus spreading message*

Other people that create viruses may have the intent of identity theft, sextortion, and various other nefarious purposes. They are capable of

bending software to their will, and they will not stop using every excuse and illusion possible to make opening a virus sound reasonable.

For the purposes of this page, the ways to spread a crypted virus are not important. What's important is understanding that there are thousands of people around the world who spend their entire lives using hack forum resources and learning how to get what they want no matter what the cost is. What's important is understanding that we all could benefit from using a small fraction of our time protecting ourselves against such exploits and vulnerabilites.

A growing majority of viruses have also begun to encrypt the data of their targets, making it inaccessible until a ransom has been paid using a virtual and anonymous cryptocurrency. Such viruses are known as ransomware and besides preventing their infection, nothing can recover lost data if the software encrypts the files of a target machine. Even policemen have had to shell over the money to recover their ransomed files this year.

Police chief: "Paying the Bitcoin ransom was the last resort"

Ransomware comes of age with unbreakable crypto, anonymous payments. A small town police department just outside of...

arstechnica.com

In the end, if a hacker wants access to your identity, your data, or extortion money, nothing will stop them but the safeguards you set in place for your digital home. That's the most important take away for any computer or technology users.

Those that actually want to learn how to spread viruses: the hack forums are always up and online to access.

It's fortunate that we have the internet today to educate people how to do things. Learning how to hack is a beautiful skill, as is lock-picking, which can help develop better security methods and other innovations.

Unfortunately, people may use such knowledge for wrong reasons. Such as invading homes and stealing items, such as hacking into systems and stealing data, or such as building bombs and blowing up property.

> *A couple of years later, I got into trouble again—this time it was far more serious. A local kid made a bomb and blew up a $20,000 haystack. His mother called the fire department so that they could talk to her son about fire safety, and they asked him how he learned to build the bomb. No surprises for guessing what he said—he learned it from Harper Reed, of course. And so, agents from the Bureau of Alcohol, Tobacco and Firearms came over with their badges and their guns, and began questioning me. It was very intimidating. But I soon realized that these people don't know about bulletin boards, or even the Internet. They thought I was some major information source, telling kids all over Greeley how to build bombs. But I had just told the kid about an anarchist website, and he'd found the information himself. -Harper Reed, Medium*

Knowledge is power. Do you want the power to protect yourself from hackers?

Scanning and Hacking into Computers Directly

If "digital doors" are left ajar, then we can expect that those who intend to steal from within will develop a way to scan for them.

In the same way that a thief might go around trying to open doors in a neighborhood until he finds one that is left open, and then set up a plan to come back and take what's within, hackers work in the same way.

A virus is simply one way which a computer may be compromised. There exists entire operating systems such as BackTrack and Kali, which hold thousands of vulnerabilities for hacking systems and

compromising data. They also let hackers scan thousands of ports, access points, and backdoors left wide open within computers.

Running BackTrack and Kali on your computer is as easy as visiting the respective websites, downloading a file, and loading it onto a USB.

Then when your computer boots up simply tap the ESC or F1–12 keys until you reach a prompt that allows you to boot into the operating system you have burned onto the USB.

From there, hacking into computers and iPhones is as easy as sitting down with your computer/laptop, connecting to a WiFi network that other devices are connected to, and clicking a few buttons.

Hacking Windows 8 using Kali and Armitage (a click-to-hack solution that virtually anyone with a mouse and keyboard can use).

Hacking the most recent iPhone model, with the most recent firmware, using Backtrack 5.

For further information on using click-to-hack solutions such as Armitage, refer to their readily available PDF "get in through the backdoor."

After a hacker gains access to a system they can inject a virus to maintain their access even after the target leaves the WiFi network the compromise took place in. A compromised target can also be used to hack into other systems, and if the hacker covers his tracks well it can be difficult to tell who really did the hacking at hand.

Every time you sit down in a Starbucks and begin to use the free and public WiFi, you could become infected or even used as a proxy in hacking other systems. Likewise goes for using any unsecured access point.

Actually, that's not accurate since even your secured home's WiFi could be cracked in.

Hacking WiFi Passwords

Kali and Backtrack both have security solutions for cracking WEP and WPA passwords. They accomplish this by recording data that is sent between the WiFi access points and devices that have been authenticated already.

After recording enough data patterns begin to emerge that brute-force cracking can identify in order to determine the WiFi access point's

password.

If you need a verbal step by step guide in doing this, please refer to the video below which utilizes the Kali operating system:

To make sure that you can properly record WiFi packets sent over the air, and that your range is increased so that you may do so from a distance or even a van, look into a $30 antenna such as the one below:

Spoofing WiFi Networks

Spoofing WiFi involves the use of a hacking operating system, or a hacking device, to pretend that your equipment is the WiFi access point. This will cause devices that are connected to a WiFi network to connect to your device instead of the access point.

Then your device connects the victims to the internet. Since the hacker acts as a bridge between every piece of information that travels to and from surveilled targets, it lets them save everything.

It also lets hackers redirect victims to their own sign in pages. If a victim is connected to a spoofed network for example, they could visit Facebook.com and the password they type in goes directly to the hacker. After the password is captured the victim will be directed to the actual Facebook page, where they will enter their password one more time and sign in properly.

Hackers that are really advanced will know how to pass the username and password from their fake pages directly to Facebook, so that the user is able to sign in the very first time and not notice that a single thing is off.

If you want to learn how to spoof Facebook, through a few keystrokes and mouse clicks using Kali, watch the video below:

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through

If you want to buy a device which will automatically spoof WiFi networks to save intercepted information, then you can always look into the Pineapple Mark V.

If you want to create a spoofed Facebook webpage that saves that passwords that are typed in and then redirects to the proper page, you may follow the resource posted below:

NavTechno

As we all want to hack our friend facebook account,and want to read all his personal things. Today i m gonna teach you...

navtechno.blogspot.com

Social Engineering

Social engineering is one of the simplest ways to comprise a target system. This method of hacking refers to deceiving people so that they give over information and system/building access without knowing any better:

> *If a company hires us for a social engineering engagement, typically they want us to get in and get to their back-up tapes, or into the data in their document room.*

> *Let's say I am posing as a fire inspector. The first thing I will have besides my badge and uniform is a walkie-talkie, like all firemen. Outside, we'll have our car guy. The guy that sits in the car, and basically his job in the beginning is to send chatter through to our walkie-talkies. We will have a recording of all that chatter you'll hear on walkie-talkies. He sits in the car and plays it and sends it through to our walkie-talkies.*

> *While I'm talking with the person who has been assigned to us, my partner knows his job is to immediately wander away from us. So, my partner will immediately walk off. In most cases our escort will say "Can you come back here? I need to keep you guys together." We say "Sure, sorry." But really that means nothing to us. All it means is that we keep doing it until she gives up. My partner will wander off two or three times more times and get warned until she finally stops and gives up. She just thinks he's a fireman and thinks "Let's just let him do what he needs to do."*

> *-How to rob a back: a Social Engineering Walkthrough*

Two years ago I found a simple vulnerability in Gmail that makes it easy to compromise accounts via social engineering. It simply requires a target's Gmail address and inputting it into the "forgot password" form.

If the target has a phone number on file for recovering their account if they forget their password, then Gmail will provide the last two numbers of the phone number it has recorded. It will also not send a recovery code until you click “send recovery code.”

At that moment, if you know the target (and have permission to access their email account) and their phone number matches to the one Google has on file, let them know that you’re inviting them to a beta Google product and that Google will send them a verification code via their phone.

Click “send recovery code” on the recovery form, and then ask the target for the code. The text they receive states“Your Google verification code is…” It does not state “Your Google password recovery code is…” This is a big flaw on Google’s part which they have not yet fixed. Users will often give this code up, not knowing how important it is that they do not share it with anyone.

Hotmail does not have this problem. Their recovery texts clearly state that the following code is used for password recovery.

Around the time I found out about the Gmail exploit and began using it on my friends, one of them got me back by coming up with his own method of comprising my account password: a simple video recording. While typing my password into a school computer at blazing speed, with him standing over my shoulder, he used his phone to record every keystroke that I typed into the computer. It was genius and I was furious that he gained access to my account, with such an exploit having never once occured to me in my life.

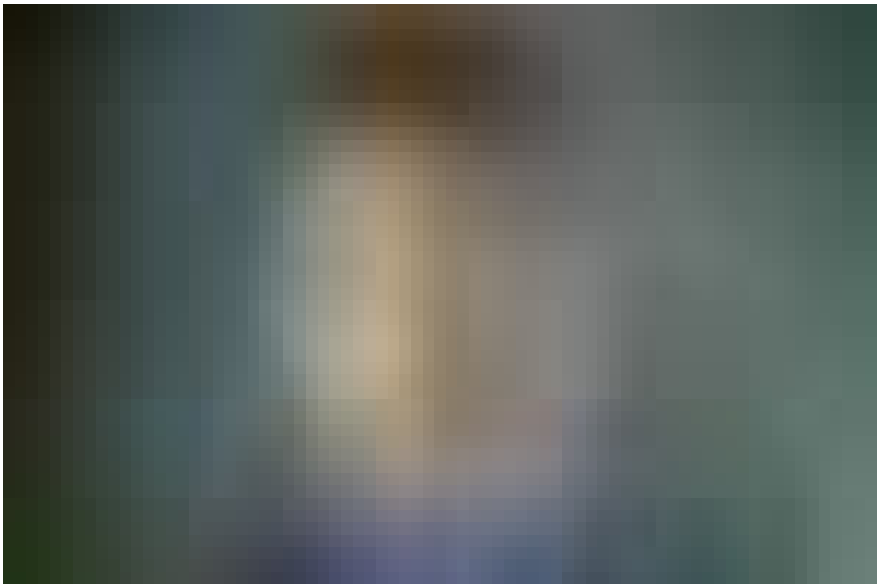
Hackers that discover software, hardware, or social engineering exploits will often not share their discovery for free. They sell these exploits for top-dollar to customers that are in need of unused and working hacks.

Through social engineering one might also make use of technology, such as an email spoofer, to send emails from an address that they do not have access to (such as contact@johnappleseed.com). Sometimes email clients will report that something is off with these spoofed emails. But in my experience, they never do.

Through social engineering, one might also call others from numbers that they do not own. This service makes it easy to connect two phone numbers together and record the conversations that follow. Connecting restaurants together and calling people from 666–666–6666 can be fun for some. But using this tool, you can also call people from their friends' and coworkers' numbers if you have access to them.

I once called a shipping service, without spoofing my number, and asked them to let "the customer" pick up his package from the LaserShip facility instead of letting the shipping process finish (due to concerns over negative reviews about how LaserShip employees throw boxes). After suppling the tracking number and apologizing for making the call from my personal device since the outbound call center was closed for Sunday, the representative on the other end followed my instructions. At the LaserShip facility, I was took out my ID but the worker said it wasn't necessary.

It was a bit shocking to learn that if someone lived in the area, and had access to my tracking number for an expensive package, that they could have easily social engineered picking it up. Mind you, there were cameras at the facility but that's when a pornstache comes into play.



Portnstache, Orange is the New Black

If you think anyone is going to be able to track down a stolen computer or camera after such a shipping social engineering method is used, then think again.

Hardware Hacking

The USB Rubber Ducky costs about $40 and lets you create exploits that run upon USB insertion without the need for computer interaction.

There are also gadgets that let you put them into the back of computers and then connect keyboard USB cables into them to record every keystroke:

Spy Gadgets - The KeyShark USB keystroke recorder

Check out the KeyShark USB keystroke recorder. The KeyShark can be connected to a keyboard to record every single...

www.geeky-gadgets.com

- Portable—move it from computer to computer.
- Installs in seconds—Just plug it in.
- Uses no system resources. Truly runs in the background.
- Works with all PC operating systems with USB keyboards.
- Data is retained even during system lock-ups and power outages.
- No Software to learn. Use in conjunction with programs you already know.
- Fully undetectable and can store over a years worth of data. 4MB internal memory.
- Records password and every keystroke ever pressed including special characters

Even the most digitally secure system can fall prey to a hacker that uses another mode of attack, such as social engineering or direct hardware hacking.

Keep your eyes peeled for viruses, odd phone calls, unknown computer devices, and other tomfoolery that hackers may use to gain access to your data.

Hacking Planes, Trains, Ships, and Cars

If you followed along and created some viruses using the information laid above (and have seen for yourself how easy it is to hack software and hardware), then you might be asking if it's just as easy to hack planes, trains, and cars.

I wish I was kidding, but it is.

However, it will take more than a week if you want to find your own exploits rather than simply following along to hacking guides. Before you can hack automobiles and transportation systems you'll need to master the things outlined below:

- Linux essentials
- Linux networking
- Basic security testing with Kali
- Hacking: The Art of Exploitation
- The Fat-Free Guide to Network Security Scanning
- SSH Mastery
- Hacking and Penetration with Low Power Devices
- Practical Reverse Engineering
- Learning The Bash Shell
- Command Line Kung Fu
- Learning Perl

After you master every topic outlined, you'll be able to follow along with the information that details exactly how transportation hacking works:

This embedded content is from a site that does not comply with the Do Not Track (DNT) setting now enabled on your browser.

Please note, if you click through and view it anyway, you may be tracked by the website hosting the

Note: Joke about hacking live planes at your own expense and responsibility. That sort of funny business (which is more known as terrorist threats) will not be so funny with the FBI and DOD(even if you're a security penetration tester).

Chris Roberts
@Sidragon1

Follow

Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone ? :)

Feds Say That Banned Researcher Commandeered a Plane | WIRED

A security researcher kicked off a United Airlines flight last month after tweeting about security vulnerabilities in...

www.wired.com

Hacking Nuclear Facilities

Oh boy. You really want to learn how to hack don't you?

You can download the Stuxnet source code available here. It is the world's first weapon made entirely out of code which targeted an Iranian nuclear power plant. It is also extremely advannced, caused real damage, and almost started World War III.

This is not an exaggeration, and once again, I wish that I was kidding. It's just that average computer users and citizens are not aware of Stuxnet's existence and what the use of it sets a precedent for (nothing good that is).

Since the source code for it is available, anyone with a keyboard, a mouse, and a few years of programming knowledge can modify it to their own needs and spread it further.

I'm not sure if hackers have ever thought of their work as a "pass it on" sort of endeavor. But it definitely has a lot of similarities.

To learn more about Stuxnet you may watch the short documentary below:

Expanding Your Knowledge

Hackers will use any resources and knowledge available to get into the places that they want to get into. If you are a criminal and want to get into something, the only thing stopping you is a Google search or a hack forum search.

There are thousands around the world that make a living out of using their hacking knowledge for personal gain, and at times just for

entertainment.

The good however, is that there are also hackers who share their exploits with security experts so that they may be patched up. Google for one seems to be slow at patching simple things such as automated text messages.

As engineers and software developers catch up with hackers, average users can expand their own knowledge of security protection to insure that what's important to them is safe. They should never rely on locks, doors, and antivirus programs provided by "security professionals" as being enough. Rather, they should trust their own intuition after gaining enough knowledge to be able to tell the difference between knowing something and not knowing something.

An article is coming soon on protecting your "digital home," from hackers.

Follow me on Medium or subscribe to my newsletter for future updates. Thanks for reading.

. . .

A Fascinating Book

Whitehat hackers and average users alike will benefit from reading The Art of Intrusion. It is a beautifully written book that shares stories of whitehat, greyhat, and blackhat hacker endeavors.

Trolling Scammers

In addition to virtual machines setup using VirtualBox being extremely useful for setting up simulated machines and computers for hacking, they are also useful for trolling call-center virus removal scammers. One time I setup a Windows XP machine and wasted hours of a scammer's time, only to tell him that he was being trolled. It seems that there are hackers out there with more time on their hands than mine that get back at these people for scamming old and gullible people into paying them for useless services, as well as for essentially installing viruses on their computers:

Scammed

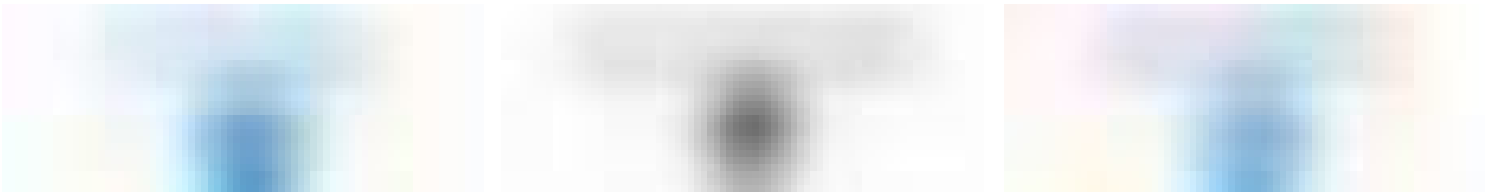
Some of America's poorest people are being targeted by cyber-scammers. Can an errant hacker find the culprits?

medium.com

Mastering BackTrack and Kali

The best resource I know of that will teach professional penetration testing techniques is SecurityTube.com. They also offer a virtual simulation network for testing hacks on, as well as hacking competitions.

•••



-