**Knowing Your Enemy**

**Two types of Bugs**

Known

* Patch available

Unknown

* Zero Days
* No patch

**www.Exploit-db.com** is a database of known exploits across different platforms

* Most exploits on here are known exploits so will most likely have patches available
* However, not all machines are patched

Certain exploits form 2016 and 2017 still haven’t been patched on certain windows machines and are still open to exploitation

**Malware**

* **Macro** **virus**
  + A virus that is activated or let out when a file is opened
* **Stealth** **virus**
  + Virus that tries to trick antivirus software by intercepting its request to the OS and provide incorrect information
* **Polymorphic** virus
  + Make varied operational copies of itself
  + May have no parts remaining identical between infections making it difficult to detect directly using signatures and anti-virus software
* **Self-garbling virus**
  + Modify parts of its own code so that it doesn’t match predefined AV signature
* **Bots & Zombies**
  + Hacked devices under the control of a hacker
  + Compromised machine can be added to a bot network
* **Worms**
  + Virus that spreads from on machine to another
* **OS Rootkits**
  + Worst to get
  + Embedded in to kernel of OS so its existence is hidden completely from the OS
* **Firmware rootkits**
  + Malware on hard drives firmware
  + Even formatting drive and reinstalling OS wont shift this
  + This is NSA, GCHQ level malware
* **Keyloggers**
  + Log key inputs
* **Trojans**
  + Programs that appear to be one thing but are actually malware
* **Remote Access Tools (RATs)**
  + Remote tools to allow access to your machine
* **Ransomware**
  + Covertly encrypts all the user’s files with a key only the hacker has
  + A ransom message is then sent to the user to request funds in order to decrypt the files
* **Malvertisement**
  + Online advertisements that are infected with malware
  + Script will be executed that then starts a cascade of other scripts until eventually malware is downloaded and presented to the user
  + Due to the chain of scripts in different changing locations, its hard for the website provider to know that the advertisement is bad

Other variations of malware

* Spyware
* Adware
* Scareware (trick you into thinking you have a virus top pay for antivirus)
* Browser Hijacking
* Potentially unwanted programmes (PUPs)

**Phishing, Vishing, SMShing**

Typically done through emails or messages that **direct the recipient to a fake site that looks real**

* Relies on social engineering

Emails don’t digitally sign messages sent, so there is authentication of the sender

* No guarantee of who It’s come from
* Emails can be easily spoofed to look like they come from a legitimate source

Spear phishing

* Targeting someone for phishing specifically

**Techniques used**

* **Subdomains and misspelt**
  + http://**www.google.com**.stationx.net
  + trying to convince that google is domain when stationx is real domain
* **IDN homograph attack**
  + Internationalised Domain Name Standard
  + Using letters or fonts that look the same as another letter
  + http://www.goog**1**e .com
* **Hidden URLs**
  + “Click Here”
  + [www.google.com](http://www.google.com) – but actually linked to a different site (the attack site)
  + Right clicking on the Hyperlink and selecting copy link location will allow you to post the real link location
  + Some email clients can have the real domain and java script faked as well so it’s hard to detect
  + You can check the raw HTML through the email client to confirm
* **Covert URL redirect**
  + Cross-site scripting / cross-site request forgery in combination with URL manipulation
  + **Get a link to a real site but the real site is being manipulated**
  + The hacker has found a flaw in the website and uses techniques to manipulate the website and redirect you to fraudulent sites **(open redirects)**
  + **Scripts can be inserted into legit URLs** (reflected cross site vulnerability) and processed
  + These scrips can be executed and do anything like key logger or steal username & password

**Vishing**

* Phone or voice phishing
* People from India pretending to be Microsoft

**SMShing**

* Using text messages to phish
* “Payment to royal mail to receive package”

**Spam & Doxing**

**Spam is any message that you didn’t request**

The barrier to entry to become a spammer is low

* Very small operating costs and hard to hold senders accountable as its relatively easy to hide where the emails are coming from

**Doxing is gathering information on someone and using it to create a threat**

* E.g. releasing the info to the public if an agreement isn’t made

**Social Engineering**

**Scams, Cons, Tricks & Frauds**

Advanced fee fraud- “you’ve won!”

* Pay small fee to receive funds

Claims you owe money on a debt

Claims to recover money from a previous scam for a fee

PC support – “buy the product to get rid of virus”

Fake friend scam – Facebook request

Fake payment on eBay

* Asks seller to send item same day for emergency such as child’s birthday
* Sends fake email from “PayPal” saying the payment has gone through
* Item has already been sent and is too late to intercept

**CPU Hijackers**

**Crypto Mining Malware / Cryptojackers**

**Hijack people’s machines to use their CPU cycles to mine crypto**

Jackers mine crypto on someone else’s machine, getting the crypto rewards for mining without using their own electricity

Can be done via

* Phishing attacks
* Social engineering
* Exploiting a vulnerability to gain access
* Bad app download
* Untrusted code

Also done by websites

* JavaScript based mining tools (which can be injected into websites)
* Browser
* Websites

**How to mitigate this**

* Check CPU processes and make sure the usage isn’t too high from browsers etc.
* Some websites use hidden windows that you may not even be able to see so quitting the app might need to be done to close the website
* Add browser add-ons like NoCoin that prevent coin mining from any site like CoinHive