Managing Enterprise Cybersecurity MIS 4596

Malware Analysis

Unit #18

Agenda

- Computer virus
- Malicious software
- Proliferation of malware
- Malware components
- Anti-malware components
- Best practices for protection

Virus

Virus: attached to a file

1986

Brain virus

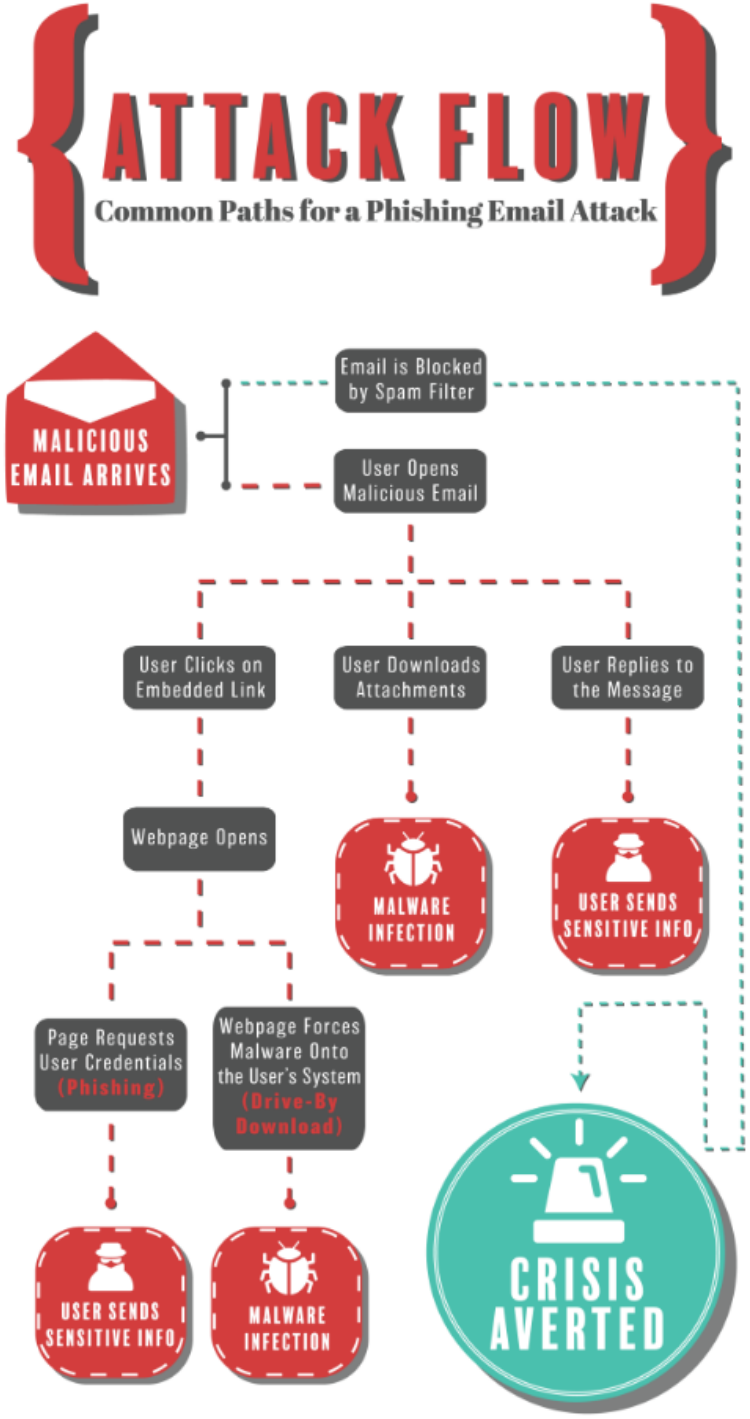
an F-Secure Production

Malicious Software (Malware)

Malware enables unauthorized access to networks for purposes of theft, sabotage, or espionage

- There are many types of malware, many cyberattacks use a combination of several types to achieve their goals
  - Obtain sensitive information (login credentials, credit card data, Social Security numbers, …)
  - Gain unauthorized access to systems
  - Carry out a profit-oriented scheme
- Usually introduced into a network through phishing, attachments, downloads, or may gain access through social engineering or flash drives
- Manual attacks on information systems are less common than the used to be

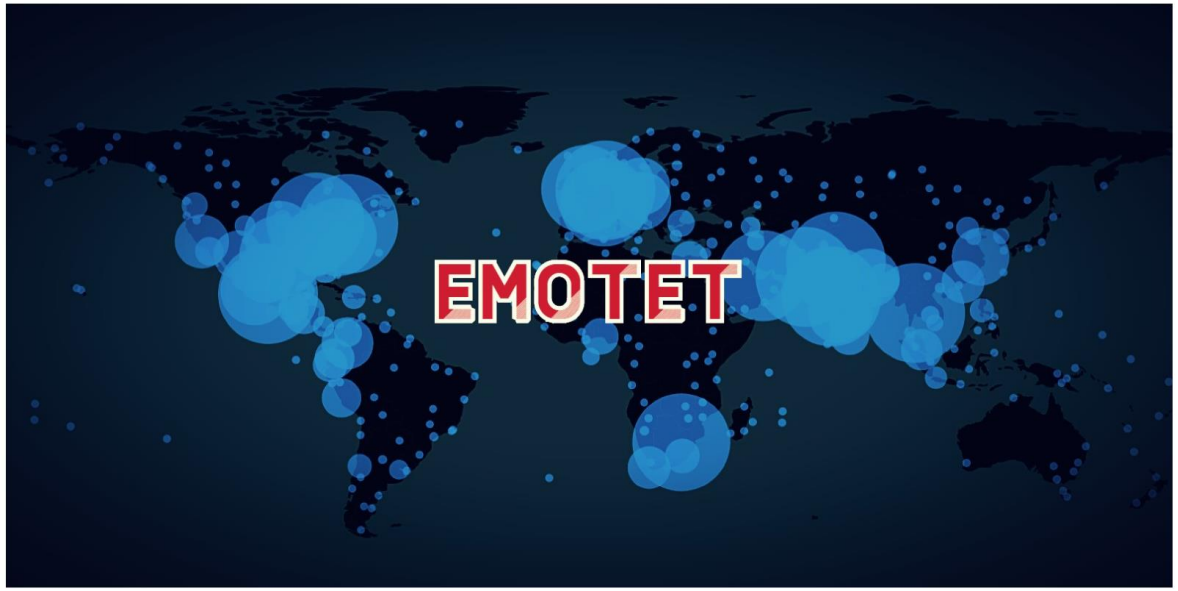
  >95% of all compromises use email as the main attack vector



Types of malware

Type	What It Does	Real-World Example
Ransomware	disables victim's access to data until ransom is paid	RYUK
Fileless Malware	makes changes to files that are native to the OS	Astaroth
Spyware	collects user activity data without their knowledge	DarkHotel
Adware	serves unwanted advertisements	Fireball
Trojans	disguises itself as desirable code	Emotet
Worms	spreads through a network by replicating itself	Stuxnet
Rootkits	gives hackers remote control of a victim's device	Zacinlo
Keyloggers	monitors users' keystrokes	Olympic Vision
Bots	launches a broad flood of attacks	Echobot
Mobile Malware	infects mobile devices	Triada

https://www.crowdstrike.com/epp-101/types-of-malware/



Emotet is a notorious malware distributed through email containing malicious Microsoft Word and Excel document attachments. When users open these documents and macros are enabled, the Emotet DLL will be downloaded and loaded into memory.

Once Emotet is loaded, the malware will sit quietly, waiting for instructions from a remote command and control server.

Eventually, the malware will steal victims' emails and contacts for use in future Emotet campaigns or download additional payloads such as Cobalt Strike or other malware that commonly leads to ransomware attacks.

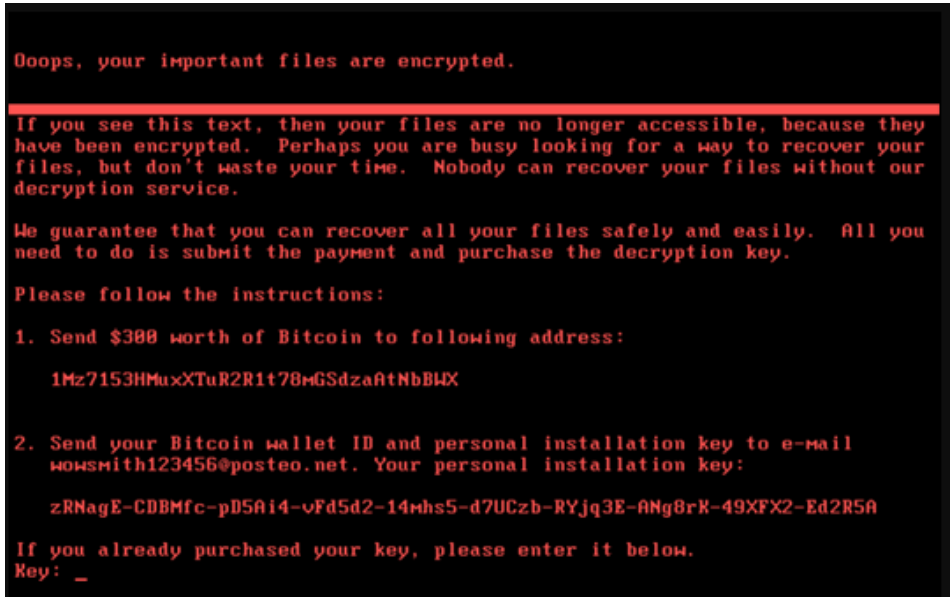
While Emotet has been considered the most distributed malware in the past, it has gradually slowed down, with its last spam operation seen in November 2022. However, even then, the spamming only lasted two weeks.

Emotet returns in 2023

Today, cybersecurity firm Cofense and the Emotet-tracking group Cryptolaemus warned that the Emotet botnet had once again resumed sending emails.

Ransomware

- Software that uses encryption to disable a target's access to its data until a ransom is paid
  - The victim organization is rendered partially or totally unable to operate until it pays
  - There is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly



In 2019 the city of Baltimore was hit by a type of ransomware named RobbinHood which was distributed using the National Security Agency's Eternal Blue hacking tool

- The attack halted all city activities, including tax collection, property transfers, and government email for weeks, and cost the city more than $18 million
- The same type of malware was used against the city of Atlanta in 2018, resulting in costs of $17 million

Fileless Malware

- Does not install anything initially, instead, it makes changes to files that are native to the operating system, such as PowerShell
  - Because the operating system recognizes the edited files as legitimate, a fileless attack is not caught by antivirus software
  - Because these attacks are stealthy, they are up to 10 times more successful than traditional malware attacks

Astaroth is a fileless malware

- When users downloaded the file, a Windows Management Instrumentation (WMI) tool was launched, along with other legitimate Windows tools
- These tools downloaded additional code that was executed only in memory, leaving no evidence that could be detected by vulnerability scanners
- Then the attacker downloaded and ran a Trojan that stole credentials and uploaded them to a remote server

Malware proliferation is directly related to profit hackers can make without being caught

Money making schemes include:

- Compromising systems with botnets for later use in:
  - Distributed denial of service (DDoS) attacks
  - Spam distribution
- Ransomware encrypting users' files with keys that are only given after users pay a ransom
- Spyware collects personal data for resale
- Redirecting web traffic pointing people to a specific product for purchase
- Installing key loggers, which collect financial information for reuse
- Carrying out phishing attacks, fraudulent activities, identity theft, and information warfare

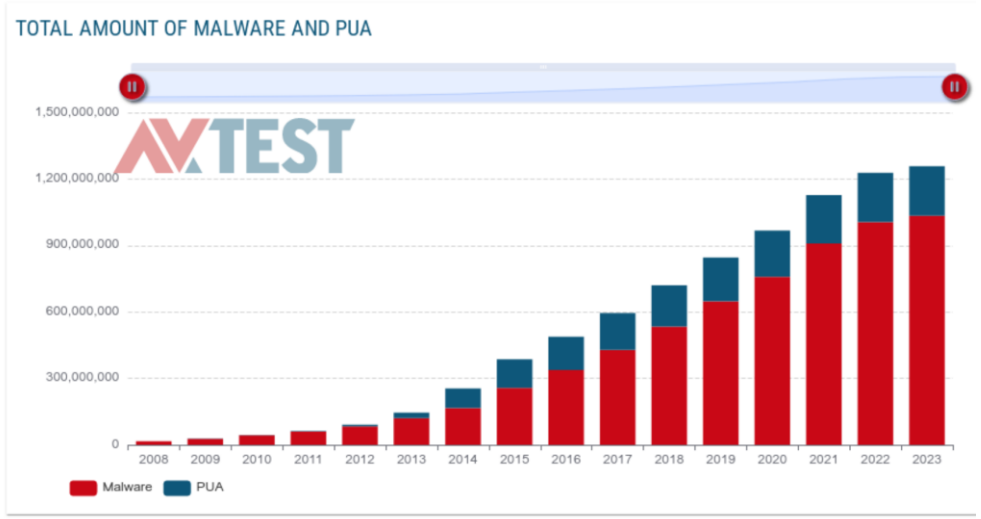
Malware is increasing

AVTest reports over 450,000 new malware and potentially unwanted applications (PUA) identified each day

Main reasons types malware is increasing in quantity and potency:

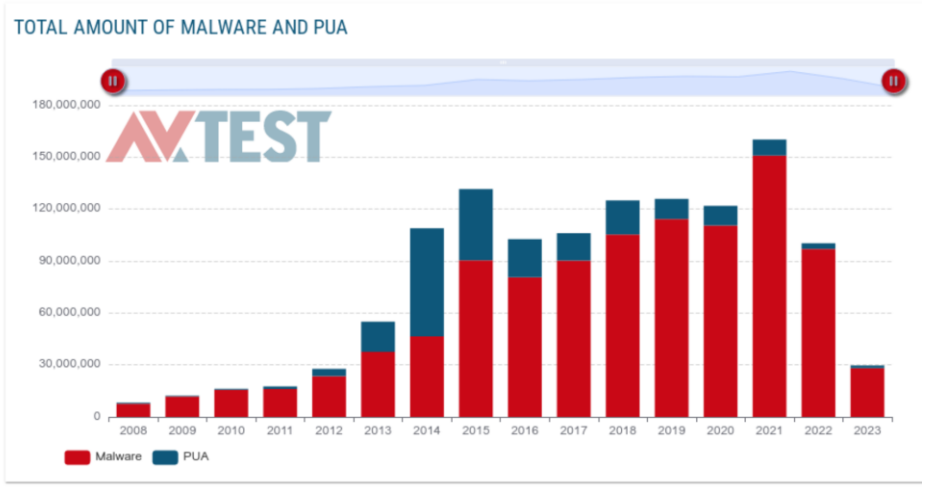
- Homogenous computer environments (Windows, MacOS, Android, iOS) – 1 piece of malware will work on many/most devices
- Everything is becoming a computer capable of being compromised (phones, TVs, game consoles, power grids, medical devices,…)
- More people and companies store all their data in digital format
- Many accounts are configured with too much privilege (i.e. root/administrator access)
- More people who do not understand technology are using it for sensitive purposes (i.e. e-commerce, online banking, …)

Total malware



Source: av-atlas.org

New Malware



Source: av-atlas.org

https://www.av-test.org/en/statistics/malware/

Malware Components

Malware typically has 6 common elements

1. **Insertion** – Installs itself on the victim's computer
2. **Replication** – Copies itself and spreads to other victims
3. **Avoidance** – Uses methods to avoid being detected
4. **Trigger** – An event initiates its payload execution
5. **Payload** - Caries out its function (i.e. exploits a vulnerability to provide access, deletes files, encrypts files, installs a backdoor, …)
6. **Eradication** – Removes itself after its payload is executed

Anti-malware software components

Detection techniques

- Signature-based
- Integrity-based
- Heuristic-based
- Behavior-based

Protection techniques

- Quarantine the file
- Clean the file
- Roll-back to prior version of the file
- Warn the user
- Log the event

Signature-based malware detection

Anti-malware software scans files, e-mail, other data and **compares** them **to a database of signatures** created by the anti-malware vendor

- A malware signature is a sequence of code extracted from the virus that is used to identify the virus
- Can only identify previously identified malware
- Updates to the signatures must be downloaded and applied frequently
- Cannot detect 0-day attacks

Signature-based malware detection avoidance

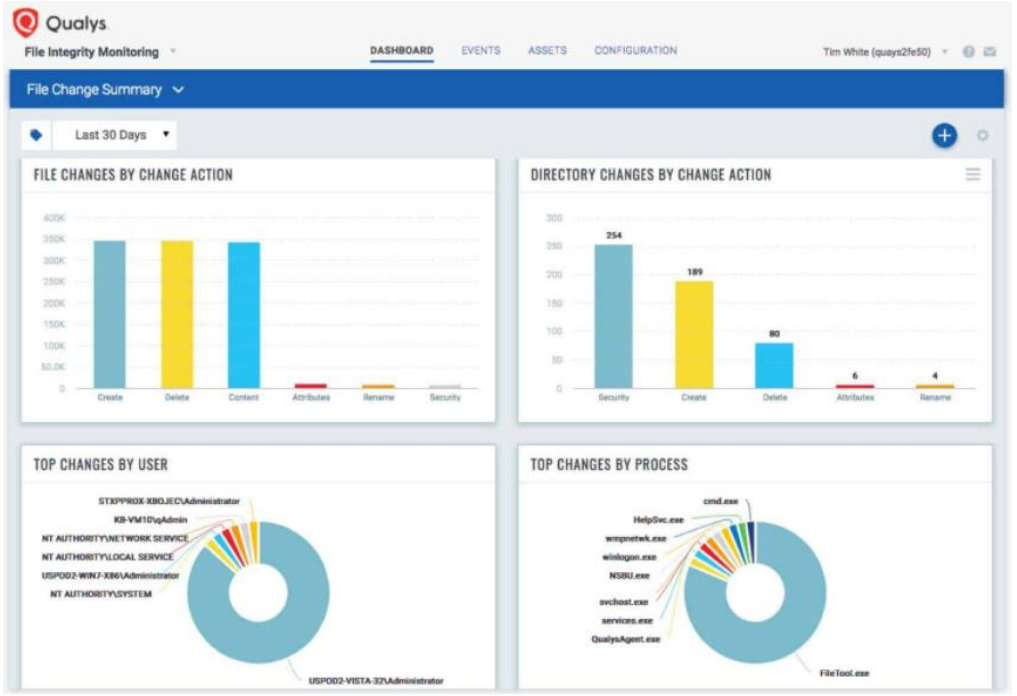
Polymorphic virus has the capability to change its own code to produce thousands of varied operational versions of itself

- Can use different encryption techniques
- Can vary the sequence of their instructions
  - Combining noise or bogus instructions with the useful instructions
  - Using a mutation engine and a random-number generator to change the sequence of their instructions

Multi-part virus distributes its components to different parts of the system

Integrity-based malware detection

- Calculates and stores a hash for each component of the system: operating system files, application files, configuration files, …
- Each new scan of the system calculates a hash for each component and compares it with the stored hash to detect differences
- Detected differences send alters and are flagged as suspect for further analysis



Heuristic-based malware detection

Analyzes the overall structure of the malicious code, evaluating

- Coded logic, instructions, functions and modules
- Data types and structures

Assesses likelihood that the code is malicious by accumulating a scored rating of “suspiciousness”

- Increases as it finds more potentially malicious attributes
- Compared to a threshold, which when crossed the detector identifies the software as malware and the protections are activated

2 types of heuristic malware detection methods

1. Static analysis – Reviewing code without running it
2. Dynamic analysis – Reviewing code as it is running

Behavior-based malware detection

Allows suspicious code to execute within the unprotected operating system, and watches its interaction with the operating system components looking for suspicious activities:

- Writing to Run keys in the Windows Registry or startup files
- Opening, deleting, or modifying files
- Modifying executable logic
- Creating or modifying macros and scripts
- Scripting e-mail messages to send executable code
- Connecting to network shares or resources
- Formatting a hard drive or writing to the boot sector

Anti-malware software components

Detection techniques

- Signature-based
- Integrity-based
- Heuristic-based
- Behavior-based

} ***Proactive techniques able to detect new malware (i.e. 0-day attacks)***

Protection techniques

- Quarantine the file
- Clean the file
- Roll-back to prior version of the file
- Warn the user
- Log the event

Best practices against malware attacks

User Education

Training users on best practices can go a long way in protecting an organization

- How to avoid malware
  - Don’t download and run unknown software
  - Don’t blindly insert “found media” into your computer
- How to identify potential malware
  - Phishing emails
  - Unexpected applications/processes running on a system

https://www.rapid7.com/fundamentals/malware-attacks/

Best practices against malware attacks

Use Reputable Anti-Virus (A/V) Software

- When installed, a suitable A/V solution will detect (and remove) any existing malware on a system, as well as monitor for and mitigate potential malware installation or activity while the system is running. It'll be important to keep it up-to-date with the vendor's latest definitions/signatures.

Ensure Your Network is Secure

- Control access to systems on the organization's network
- Use of proven technology and methodologies—such as using a firewall, IPS, IDS
- Remote access only through VPN—will help minimize the attack "surface" your organization exposes

Regular Website Security Audits

- Scan the organization's websites regularly for vulnerabilities
  - Software with known bugs and server/service/application misconfiguration
  - Detect if known malware has been installed

Create Regular, Verified Backups

- Have regular (i.e. current and automated) offline backup
- Make sure they are verified to be happening on the expected regular basis and are usable for restore operations
  - Old, outdated backups are less valuable than recent ones
  - Backups that don't restore properly are of no value

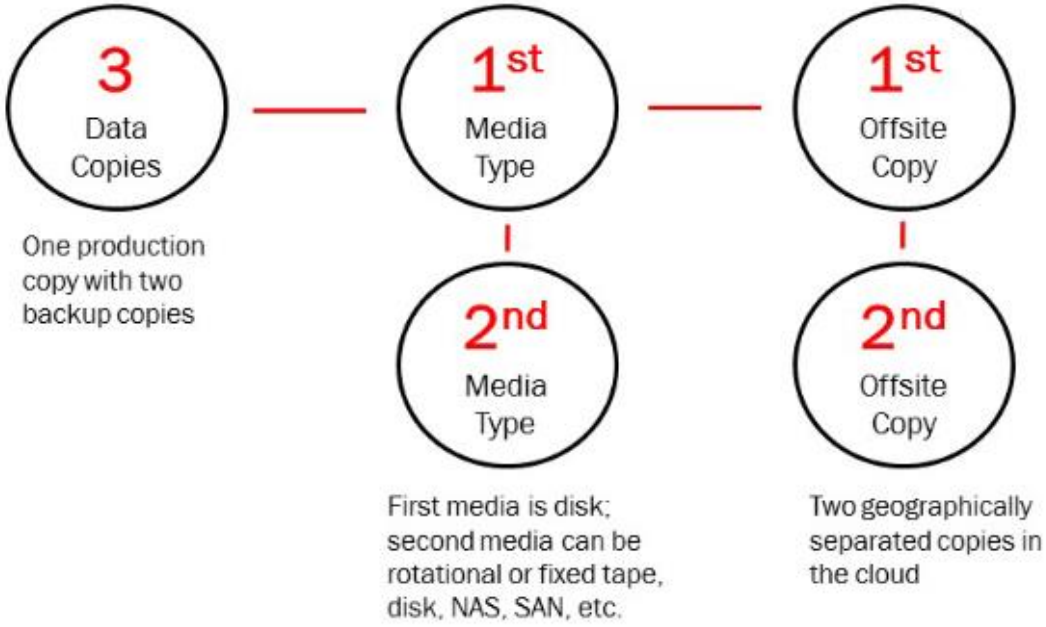
https://www.rapid7.com/fundamentals/malware-attacks/

Mitigation – Backup Best Practice

Three-Two-One rule

- Make 3 copies of all mission critical software and corresponding data in 2 different formats (to run on Linux and Windows machines), with 1 copy stored off-site not connected to any network

Maersk had 50 copies of their mission critical software and corresponding data – all in the same format, all on the network



AV-TEST Awards for Anti- Malware, Botnets, Ransomware and APT groups

Criteria:

- Protection
- Performance
- Usability

Platforms

- Windows
- Android
- MacOS

Agenda

- ✓Computer virus
- ✓Malicious software
- ✓Proliferation of malware
- ✓Malware components
- ✓Anti-malware components
- ✓Best practices for protection