Malware: Types, Impact, and Famous Attacks

Introduction

Any software designed to damage, take advantage of, or harm computer systems, networks, or devices is referred to as malware. Malware comes in a variety of forms, each with unique features and effects. This paper examines the many kinds of malware, their effects, and a thorough examination of a well-known malware attack: The WannaCry.

Malware Types and Their Effects

1. Viruses

Malware that attaches itself to a trustworthy application or file and expands to other files or systems when it is run is called a virus.

Impact: Viruses have the ability to quickly spread via networks, corrupt files, and slow down systems.

Example: The "ILOVEYOU" virus, which pretended to be an email attachment of a love letter, infected millions of computers in 2000.

2. Worms

Worms are self-replicating malware that spreads throughout networks without the need for human intervention.

Impact: They may spread payloads like ransomware, overburden systems, and use bandwidth.

Example: The "Conficker" worm (2008) used flaws in Windows OS to infect millions of PCs worldwide.

3. Trojan Horses

Trojan horses appear as trustworthy software but are actually dangerous programs. They do not multiply themselves, in contrast to viruses.

Impact: They have the ability to download more malware, open backdoors for attackers, and steal confidential information.

Example: The Zeus Trojan (2007) caused large financial losses by targeting banking information.

4. Ransomware

In order to recover a victim's files, ransomware encrypts them and requests payment, typically in bitcoin.

Impact: It has the potential to completely destroy businesses, resulting in lost data, financial damages, and interruptions in operations.

Example: WannaCry (2017) demanded Bitcoin payments from over 200,000 systems in 150 countries.

5. **Spyware**
   Spyware illegally tracks user behavior and gathers private data without permission.
   Impact: It can result in identity theft, compromise privacy, and steal credentials.
   Example: Pegasus Spyware (2016) targeted journalists and activists, extracting data from smartphones.

6. **Adware**
   Often included with free software, adware shows unwanted advertisements.
   Impact: It causes system lag, interferes with user experience, and may result in other malware outbreaks.
   Example: 250 million machines were infected by Fireball Adware (2017), which used browser hijacking to show advertisements.

7. **Rootkits**
   Attackers can get administrative control over a system while remaining undetected thanks to rootkits.
   Impact: They make it possible for system manipulation, data theft, and persistent access.
   Example: The Sony BMG Rootkit (2005) was integrated into CDs to stop copying, but it also led to security flaws.

The Well-Known WannaCry Malware Attack

Summary

In May 2017, the ransomware assault known as WannaCry took place. It took advantage of an issue in Microsoft Windows known as EternalBlue, which was reportedly created by the National Security Agency (NSA) of the United States and made public by the hacker collective Shadow Brokers.

How It Operated

1. **Infection:** WannaCry spread via taking use of the EternalBlue vulnerability in unpatched Windows PCs or by sending phishing emails.

2. **Encryption:** After entering a system, it used RSA and AES encryption to make files unreadable.

3. **Demand for Ransom:** In order to decipher the ransom note, 300–600 Bitcoin were required.

4. **Propagation:** The worm spread quickly by searching the same network for weak systems.

Effects

- **Global Reach:** The issue impacted more than 200,000 PCs across 150 countries.

- **Important Sectors:** Governmental organizations, corporations, and hospitals experienced disruptions. The National Health Service (NHS) in the UK was badly affected, with appointments and procedures being canceled.

- **Financial Losses:** Over $4 billion in damages are estimated.

Reduction

- Microsoft issued emergency updates for Windows XP and other unsupported systems.
- A security researcher found a kill switch, which slowed the spread.

Flowchart: WannaCry Attack Process

```
[Start] --> [Phishing Email or Exploit EternalBlue] --> [Infection]
[Infection] --> [Encrypt Files] --> [Display Ransom Note]
[Encrypt Files] --> [Scan Network for Vulnerable Systems] --> [Spread to Other Systems]
[Display Ransom Note] --> [Demand Bitcoin Payment] --> [End]
```

Conclusion

Malware is a serious danger to people, businesses, and governments. Implementing successful cybersecurity solutions requires an understanding of the many types of malware and their effects. The significance of regular software updates, user knowledge, and strong security procedures is underscored by the WannaCry attack.

References with URLs

1. Symantec (2017) - WannaCry: The ransomware worm that shook the world
   URL: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack
2. Microsoft Security Blog (2017) - Customer Guidance for WannaCrypt Attacks
   URL: https://www.microsoft.com/security/blog/2017/05/12/customer-guidance-for-wannacrypt-attacks/
3. Kaspersky Lab (2020) - What is Malware? Types and Examples
   URL: https://www.kaspersky.com/resource-center/threats/malware
4. BBC News (2017) - NHS cyber-attack: GPs and hospitals hit by ransomware
   URL: https://www.bbc.com/news/health-39899646