Threats and Attacks

Security Components Recap

- Asset – tangible or intangible i.e. equipment, data, reputation etc…
- Vulnerability - a weakness in the organization or network exploited to cause a security incident
- Exploit – the means that a vulnerability is leveraged
- Threat - the intention of a threat actor to exploit a vulnerability
- Threat Vector – the delivery method used to deliver or execute the exploit
- Risk – the potential the likelihood and impact (or consequence) of an actor exercising a vulnerability
- Control - a procedure or system put in place to mitigate risk

Malware

- Adware & Spyware
- Viruses & worms
- Ransomware and Crypto-Malware
- Trojans & RAT
- Rootkit
- Keylogger
- Bots/botnet
- Logic bomb
- Backdoor

Adware and Spyware

Adware

- Advertising-supported software that generates revenue by displaying adverts
- Uses cookies to deliver targeted adverts

Spyware

- Similar to a trojan however the software itself provides some function other than the malicious software

Viruses and Worms

Virus

- Malicious software
- Propagated through user action
- Contains a payload

Worm

- A type of virus that can propagate through systems on a network without user action

Ransomware and Crypto-Malware

- Uses some form of encryption to lock a user out of a system
- User is required to pay to gain access to their data
- Typically delivered through phishing emails

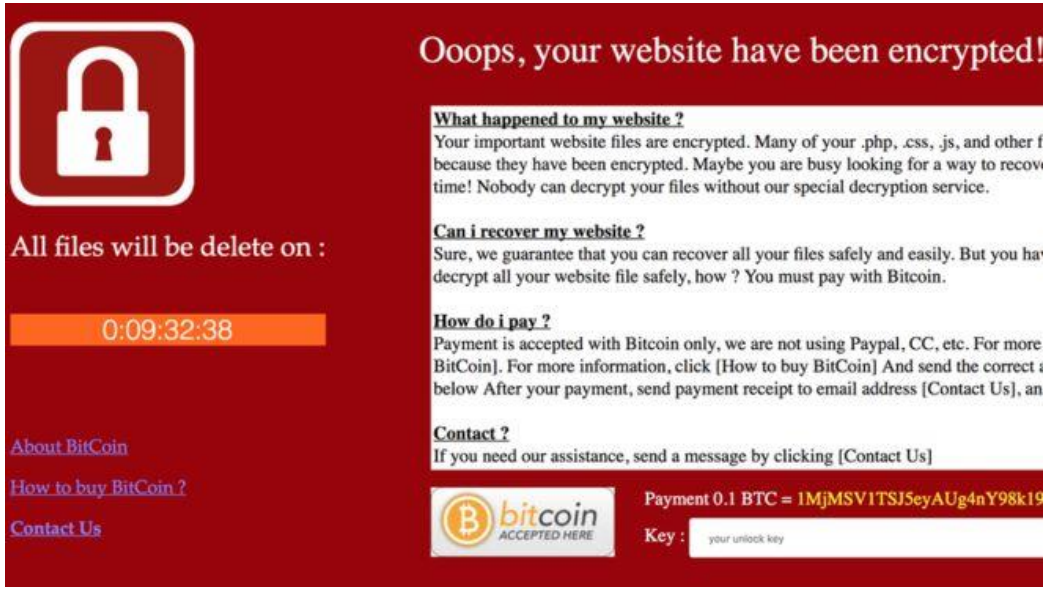


Image Source: https://www.bbc.com/news/technology-43877677

Trojans and RATs

Trojan

- Malicious software that appears useful that the user willingly installs
- Usually target user information - passwords

RAT

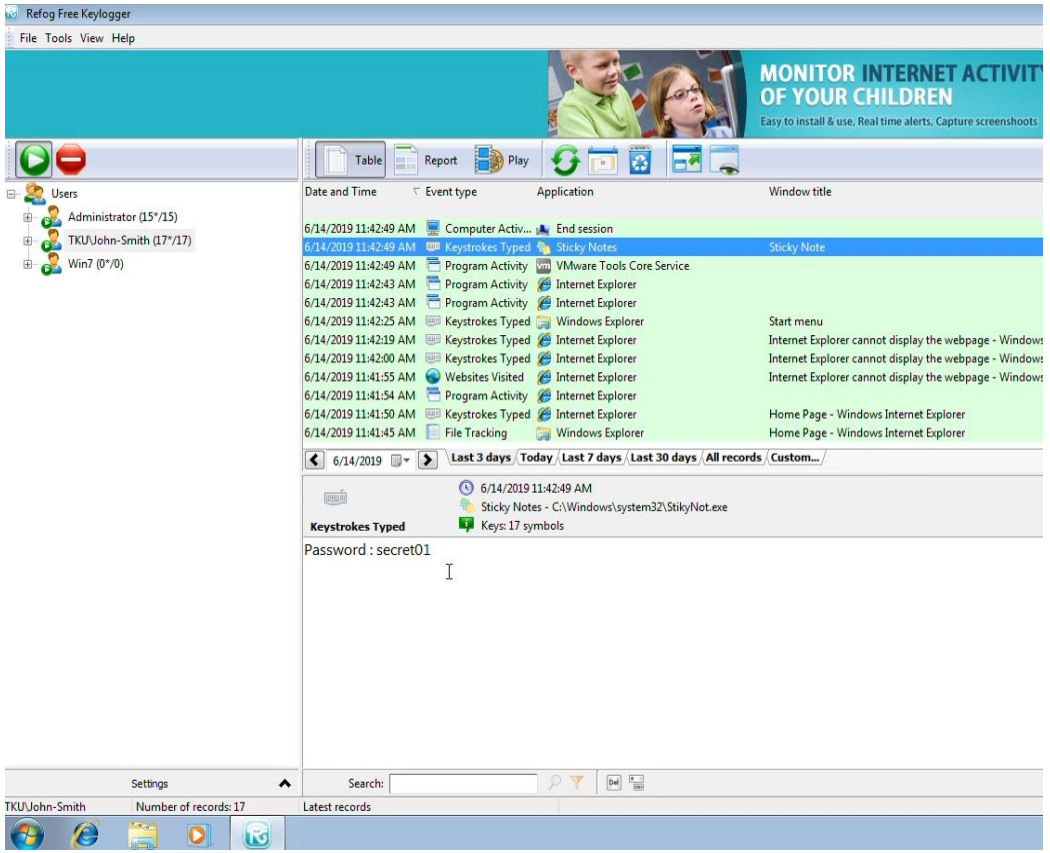
- Remote Access Trojan / Remote Administration Tools
- Give a remote user control over an infected system

Rootkits

- Malware that infects the operating system
- Difficult to detect and remove

Keyloggers

- A specific form of spyware
- Software that record user interaction – primarily keystrokes
- Often can collect other forms of information such as screenshots
- Bypasses encryption and authentication controls



Bots and Botnets

- Distributed malware attack
- Implement (Distributed) Denial of Service (DoS/DDoS)
- Target other machines to join the botnet

Logic Bombs

- Malicious software that set to execute at a certain time
- Usually a result of a malicious or disgruntled insider

Backdoor

- An entry point to an application or operating system
- Once a hacker gains access to a system a backdoor is used to maintain access to the system
- Vulnerability testing is used to identify backdoors

Vulnerabilities

Common Vulnerabilities

- Memory safety
  - Buffer overflow
  - Heap spraying
  - Unauthorized code execution
- Unvalidated input
- Race conditions
- Access-control problems
- Weaknesses in authentication, authorization, or cryptographic practices
- Insecure data
  - Storage
  - Transit

Malware Prevention

Host Security

- Anti-malware
  - Update and scan regularly
  - Enable real-time protection
  - Filter email / IM / websites / privacy protection
- Data Execution Prevention (DEP)
- Address Space Layout Randomization (ASLR)
- File Integrity Check
- Data Loss Prevention
- Application Whitelisting
- Firewall
- Intrusion Detection

User Security

- Restrict system privileges
- User training and awareness
- Professional practice - keep up-to-date with threats

Monitoring

- System log analysis
- Continuous monitoring
- Internal and external IT auditing

Data Loss Risk Mitigation

- Disaster Recovery Plan
- Disk mirroring
  - RAID mirroring - https://www.seagate.com/au/en/manuals/network-storage/business-storage-nas-os/raid-modes/
- Replication
  - File
  - Database
- File backup
  - Format - tape, cloud,
  - Frequency – daily, weekly, monthly
- System imaging