Crimeware and Botnets

Ben Zhao, Blasé Ur, David Cash
November 16, 2018
CS 232/332
Internet Crime as a Financial Ecosystem

As the Internet evolved, so did cybercrime...

- Liberal “slide borrowing” from C. Wilson @ NEU
- Most content from recent papers by Savage/Voelker et al.
Malware, Spyware, Adware, Ransomware, Trojans, RATs, Bots…

CRIMEWARE
Structure of the Underground

- Bulletproof Hosting
- Pay-per-Install and Exploit-as-a-Service
- Botnets
- Stolen Account Credentials
- Credit Card and Bank Account Theft
- DDoS and Ransomware Extortion
- Blackhat SEO
- Spam
- Click Fraud and Ad Injection
- Bitcoin Mining
- Carders, Cashiers, and Money Mules
- Phishing
- Pharma
- Counterfeit Goods
- Fake Anti-virus
- Malware Attachments
- Zero-day Development
- Crimeware Development
- Click Fraud and Ad Injection
- Bitcoin Mining
- Malware Attachments
Types of Crimeware

• Concealment and control
  – Trojans, backdoors, root kits

• Infection and propagation
  – Viruses and worms

• Stealing and spying
  – Spyware, keyloggers, screen scrapers

• Profit
  – Dialers, scareware, ransomware, ad injection and clicking, droppers, crypto currency mining, credential and account theft, …

• Botnets

Note
A given piece of crimeware may exhibit multiple types of behavior!
Trojans

• Software that appears to do something useful
  – A game
  – An e-card
  – A needed video codec
  – A browser toolbar

• But actually harms the system in some way
  – Malicious activity is often masked
  – User only sees the “advertised” functionality
Backdoors

• Malware that opens a secret entry point into a system

• Many possible implementations
  – Create a specific user account with a predefined password
  – Enable guest access
  – Turn-on existing remote admin functionality (e.g. remote desktop, telnet)
  – Open a listening port and wait for commands

• Trojan + backdoor = Remote Access Trojan (RAT)
  – Common tools used by spies and stalkers
Rootkits

• Tool that gives an attacker continued privilege escalation
  – Typically installed after exploiting the kernel or gaining root privileges
  – Modifies the OS to make privilege escalation permanent

• Emphasis on evasion
  – Rootkit makes itself (and possibly other malware) undetectable
  – Hides processes, files, network sockets
  – In other words: the OS can no longer be trusted

• Very challenging to remove
  – Erasing the OS and reinstall from scratch might work
Types of Rootkits

• User-level rootkit
  – Replaces system utilities like ps, ls, ifconfig, etc.
  – Replaces key system libraries like libc
  – Annoying, but detectable by AV and utils like tripwire

• Kernel-level rootkits
  – Modify or replace key OS kernel functionality
  – Sometimes implemented as a kernel module or device driver
  – Mitigation: kernel-driver signing (required by 64-bit Windows)

• Bootkits
  – Replace the boot loader or Master Boot Record (MBR)
  – Loads before the OS and modifies it as it loads

• Hypervisor-level rootkits, firmware/BIOS rootkits, …
Viruses and Worms

• Virus
  – Self-replicating code that infects other programs
  – When an infected program is run, the virus executes and spreads
  – Very rare today, fallen out of fashion

• Worm
  – Self-replicating program, does not require a host
Worm Considerations

• Vector of infection
  – Infect victim, mail copies to everyone in address book
  – Infect removable drives, e.g. USB keys
  – Infect shared network drives
  – Scan for vulnerable hosts on the internet and exploit them
  – Attempt to crack remote access passwords

• Spreading behavior: slow or fast? Noisy or stealthy?

• Payload
  – Some have no payload, just spread
  – Others are backdoors, bots, spyware, etc.
# Famous Worms

<table>
<thead>
<tr>
<th>Name</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morris Worm</td>
<td>1988</td>
<td>Exploited bugs in sendmail and fingerd, crashed the internet</td>
</tr>
<tr>
<td>ILOVEYOU</td>
<td>2000</td>
<td>Email attachment, estimated $5.5-10 billion in damages</td>
</tr>
<tr>
<td>Code Red</td>
<td>2001</td>
<td>Exploited MS Index Server, infected 340k servers in 14 hours</td>
</tr>
<tr>
<td>Nimda</td>
<td>2001</td>
<td>Used exploits in IE and IIS, spam and network drive infections</td>
</tr>
<tr>
<td>SQL Slammer</td>
<td>2003</td>
<td>Exploited MS SQL Server, entire vulnerable population infected in 10 minutes</td>
</tr>
<tr>
<td>MyDoom</td>
<td>2004</td>
<td>1 million infections, turned into a DDoS botnet</td>
</tr>
</tbody>
</table>
Spyware

• Crimeware that passively observes user w/o their knowledge
  – Surprisingly, often used in personal relationships
• Examples:
  – Keyloggers stealthily record all keystrokes
  – Screen scrapers record everything on the screen
• Often used to steal credentials and accounts
  – Personal information like social security number
  – Bank accounts, credit cards
  – Webmail, social networking, etc.
• Modern examples may record audio or webcam video
  – Often used for extortion
• **Dialers**
  – Old school scam
  – Modem: call expensive 1-900 numbers
  – Cell connection: send SMS to “premium messaging” services

• **Scareware**
  – Fake anti-virus

• **Ransomware**
  – Encrypt the victim’s files, demand payment for the decryption key
  – Often relies on cryptocurrency to avoid banks
  – Likelihood of receiving the key, even if you pay, is not great
$\$$, continues

- **Ad fraud**
  - Inject ads into the users browser, or onto their desktop
  - Surreptitiously click on ads on the attacker’s own website

- **Droppers**
  - Install crimeware from other attackers for a fee
  - Pay-per-install services

- **Crypto currency mining** (coinhive, cryptojacking…)}
Computers don’t just infect themselves…

CRIMEWARE DISTRIBUTION
Building a Botnet

• Botnets are a key enabler of cybercrime
  – Very lucrative to be a botmaster ;)

• How do you build a botnet?
  – Compromise hundreds of thousands of machines
  – Infect them with bot software

• How do you compromise enough machines?
Methods of Compromise

1. Malware email attachments
   - Leverages social engineering
   - Attachment may be a malware program in disguise, or...
   - May leverage an exploit in another piece of software

2. Scanning
   - Connect to servers and probe them for known vulnerabilities
   - Brute force remote access credentials, e.g. SSH

3. Exploiting browser bugs
   - Known as drive-by exploits or drive-by downloads
   - Get the victim to visit a webpage containing exploits
Malware Attachments

- Send spam containing malicious attachments
- Use social engineering to trick users into downloading & opening the attachments

**Misleading Icons and File Extensions**
- funny.jpg
- contract.docx

**Scripting Languages**
- VisualBasic script macros
- Flash and JavaScript

**Exploitable Vulnerabilities**
- Any complex file format can potentially trigger exploitable bugs and contain shellcode

Often enhanced by social engineering and phishing/spear-phishing attacks
Application Exploit Examples

CVE-2016-2334
Heap-based buffer overflow in the ExtractZlibFile method in 7zip and p7zip allows remote attackers to execute arbitrary code via a crafted HFS+ image

CVE-2016-5108
Buffer Overflow in Processing QuickTime IMA Files
Scanning

• Automatically connect to systems & attempt to exploit

• Port scans and fingerprinting
  – Which services are open and what software is running?
  – Port 80/443 – HTTP(S)
  – Port 139/445 – Windows file sharing (SMB; Server Message Block)
  – Now faster by way of ZMap & variants

• Password brute force cracking
  – Port 22 – SSH
  – Port 23 – Telnet
  – Port 3389 – Windows Remote Desktop Protocol (RDP)
Mirai

• First large-scale IoT botnet
  – Released in August 2016, Infected ~500k devices within few days
  – 500Gbps attack targeting Liberia & 1 underwater fiber optic cable
  – 665Gbps attack against Brian Krebs (non-amplified attack!)

• Trivial infection mechanism
  – Hardcoded list of 60 default login/passwds for IoT devices
  – Wireless Access Points (WAPs), IP cameras, Digital Video Recorders (DVRs), etc.

• Writers caught and sentenced Sept 2018
  – 3 twenty-somethings from NJ, PA and LA
  – Rented out slices of their botnet for attacks (incl. one on Krebs)
  – 5 years probation, 2500 hours comm service, $127,000
## Partial Mirai Credential List

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>666666</td>
<td>666666</td>
</tr>
<tr>
<td>888888</td>
<td>888888</td>
</tr>
<tr>
<td>admin</td>
<td><em>(none)</em></td>
</tr>
<tr>
<td>admin</td>
<td>1111</td>
</tr>
<tr>
<td>admin</td>
<td>1111111</td>
</tr>
<tr>
<td>admin</td>
<td>1234</td>
</tr>
<tr>
<td>admin</td>
<td>12345</td>
</tr>
<tr>
<td>admin</td>
<td>123456</td>
</tr>
<tr>
<td>admin</td>
<td>54321</td>
</tr>
<tr>
<td>admin</td>
<td>7ujMko0admin</td>
</tr>
<tr>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>admin</td>
<td>admin1234</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>meinsm</td>
</tr>
<tr>
<td>admin</td>
<td>pass</td>
</tr>
<tr>
<td>admin</td>
<td>password</td>
</tr>
<tr>
<td>admin1</td>
<td>password</td>
</tr>
<tr>
<td>administrator</td>
<td>1234</td>
</tr>
<tr>
<td>administrator</td>
<td>admin</td>
</tr>
<tr>
<td>guest</td>
<td>12345</td>
</tr>
<tr>
<td>guest</td>
<td>guest</td>
</tr>
<tr>
<td>root</td>
<td><em>(none)</em></td>
</tr>
<tr>
<td>root</td>
<td>000000000</td>
</tr>
<tr>
<td>root</td>
<td>1111</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>1234</td>
</tr>
<tr>
<td>root</td>
<td>12345</td>
</tr>
<tr>
<td>root</td>
<td>123456</td>
</tr>
<tr>
<td>root</td>
<td>54321</td>
</tr>
<tr>
<td>root</td>
<td>666666</td>
</tr>
<tr>
<td>root</td>
<td>7ujMko0admin</td>
</tr>
<tr>
<td>root</td>
<td>7ujMko0vizxv</td>
</tr>
<tr>
<td>root</td>
<td>888888</td>
</tr>
<tr>
<td>root</td>
<td>admin</td>
</tr>
<tr>
<td>root</td>
<td>anko</td>
</tr>
<tr>
<td>root</td>
<td>default</td>
</tr>
<tr>
<td>root</td>
<td>dreambox</td>
</tr>
</tbody>
</table>

*The promise of IoT! Imagine what’s coming next?*