Cyber Crime and Cyber Forensics for Criminal Law Practitioners

Steven Chabinsky
General Counsel and Chief Risk Officer, CrowdStrike

Presented 20 May 2014, Continuing Legal Education & Training, U.S. Court of Appeals for the Armed Forces
Today’s Agenda

4:00pm – 5:00pm

• Defining “Cyber”
• Exploring the Cyber Threat Actor Landscape
• Legal Considerations for Search and Seizure
• Overview of Computer Forensics
• Q&A – if we don’t have time for all questions, contact me:
  – Steve.Chabinsky@CrowdStrike.com

1 Hour Goal: General Knowledge, Specific Resources
Defining “Cyber”
and
Exploring the Cyber Threat Actor Landscape
Cyber: What is it?

• The military is becoming 100% reliant upon vulnerable technologies to:
  – Communicate, whether internally, with government partners, or with the public (email, VoIP, social media, websites)
  – Store sensitive information up to the Top Secret level, as well as unclassified data about personnel.
  – Procuring/Delivery of products and services (think USTRANSCOM for starters)
  – Manufacture equipment, many of these products also contain computer chips (including biomedical devices)
  – Control industrial systems, including critical infrastructure
Exploring the Cyber Threat Actor Landscape

<table>
<thead>
<tr>
<th>WHO?</th>
<th>WHAT?</th>
<th>Where/When?</th>
<th>HOW?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spies</td>
<td>Confidentiality</td>
<td>“Everything, All the time”</td>
<td>Remote Access</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>-the Eagles</td>
<td>Close Access</td>
</tr>
<tr>
<td></td>
<td>Availability of information and Technology enabled systems</td>
<td>Life in the Fast Lane</td>
<td>Insider Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Supply Chain</td>
</tr>
<tr>
<td>Criminals</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warriors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terrorists</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Why? If you’re the bad guy, why not?!?
What’s a System? It’s not just “data”

- Industrial Control Systems
  - Stuxnet
  - Aurora Generator Test
- Transportation
  - Hacking cars!
- Biomedical Devices
  - Hacking insulin injection pumps!
  - VPOTUS’s Pacemaker?
Costly cyberespionage on 'relentless upward trend'

Defense Security Service report says attacks were up 75% in one year, with new focus on space and military technology

by Taylor Armerding, CSO

December 18, 2012

Cyberespionage is nothing new. So a report from the U.S. government says attacks were up 75% in one year, with a new focus on space and military technology, is not a surprise. But it is a reminder of how serious the threat is.

DSS Director Stanley L. Sims said it is more of the same, but with better tools. "The tools of the trade are more sophisticated, and the threat is more widespread," he said.

While the percentage of attacks from different regions of the world has remained steady, the percentage of attacks from China has increased significantly.

"Cyberespionage is not just an issue for the United States, it is a global problem," Sims said. "It is necessary to address this threat with a coordinated global effort."
PRC actors remain the world’s most active and persistent perpetrators of economic espionage.

But, the Russians and others also are in the economic espionage game.

Source: http://www.crowdstrike.com/global-threat/
Organized Cybercrime:

Graphic by: Brian Krebs

Source: http://krebsonsecurity.com
Organized Cybercrime:

Source: http://krebsonsecurity.com
Cybercrime: Really is Organized

10 specializations in organized cyber crime:

1. Coders/Programmers
2. Distributors/Vendors
3. Techies
4. Hackers
5. Fraudsters
6. Hosters
7. Cashers
8. Money Mules
9. Tellers
10. Leaders
Cyber Terrorism

Oxford Study: compiled a list of 404 members of violent Islamist groups

Engineers are strongly over-represented among graduates in violent Islamic groups
Cyber War?

• Alleged Russian use in conflicts with Estonia (2007) and Georgia (2008)

• Alleged North Korean DDoS against U.S. and South Korea (2009)

• Alleged U.S. use of Stuxnet in nuclear enrichment standoff with Iran (discovered 2010)
Legal Considerations for Search and Seizure
USDOJ CCIPS: The Experts

Great Free Resources available at www.cybercrime.gov
Searching & Seizing Computers

Source www.cybercrime.gov

Over 200 pages long (plus best Appendix ever!)

• Searching **Without** a Warrant
• **Searching With** a Warrant
• Preserving and Obtaining stored data from special 3rd parties (18 USC § 2703)
  • Electronic Communication Service
  • Remote Computing Service
• Surveillance (18 USC § 3121; 18 USC § 2511)
  • Pen Register/Trap & Trace (incl. cell-site)
  • Full Content
• Evidence
  • Authentication
Searching **With a Warrant**

Source: [www.cybercrime.gov](http://www.cybercrime.gov)

- Search Strategy
- Drafting Affidavits, Applications, and Warrants
  - Describing what is to be seized with particularity
  - The need for imaging and off-site examination
  - Keeping your options open for search techniques
  - Delayed notification requirements
  - Potential need for multiple warrants
- Forensic Analysis: legal aspects
  - Two-Stage search
  - Commingled records
  - Use of forensic software in analysis
  - Changing focus/Need for new warrant
  - Time limitations
  - Rule 41(f) Inventory
- Special rules: Privacy Protection Act (journalists/authors); 28 CFR § 59.4(b) regulations relating to doctors, lawyers, clergy.
Q: Why are some federal law enforcement investigative authorities located in the “Crimes” part of Title 18 of the United States Code, rather than in the “Criminal Procedure” part?
What are Computer Crimes?

Source: www.cybercrime.gov

- Computer Fraud & Abuse Act (18 USC § 1030)
- Wiretap Act (18 USC § 2511)
- Pen/Trap (18 USC § 3121)
- Stored Communications (18 USC § 2701)
- Identity Theft (18 USC § 1028)
- Access Device Fraud (18 USC § 1029)
- Spam (18 USC § 1037)
- Wire Fraud (18 USC 1343)
- Communication Interference (18 USC § 1362)
18 USC 1029: Access Devices (passwords)

• Prohibits certain activities relating to the use, production, or trafficking in access devices with intent to defraud:

– an access device refers to any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)
18 USC 1030: National Security Information

1030(a)(1) Summary (Felony)

1. Knowingly access computer without or in excess of authorization
2. obtain national security information
3. reason to believe the information could injure the U.S. or benefit a foreign nation
4. willful communication, delivery, transmission (or attempt) OR willful retention of the information
18 USC 1030: Unauthorized Access

1030(a)(2) Summary (Misl.)
1. Intentionally access a computer
2. without or in excess of authorization
3. obtain information
4. from
   financial records of financial institution
   or consumer reporting agency
   OR
   the U.S. government
   OR
   a protected computer

(Felony)
5. committed for commercial advantage or private financial gain
   OR
   committed in furtherance of any criminal or tortious act
   OR
   the value of the information obtained exceeds $5,000
18 USC 1030: USG Computers and Fraud

**1030(a)(3) Summary (Misd.)**
1. Intentionally access
2. without authorization
3. a nonpublic computer of the U.S. that was exclusively for the use of U.S. or was used by or for U.S.
4. affected U.S. use of computer

**1030(a)(4) Summary (Felony)**
1. Knowingly access a protected computer without or in excess of authorization
2. with intent to defraud
3. access furthered the intended fraud
4. obtained anything of value, including use if value exceeded $5000
18 USC 1030: Causing Damage

Summary of (a)(3)(A):
1. Knowingly cause transmission of a program, information, code, or command
2. intentionally cause damage to a protected computer without authorization

Summary of (a)(3)(B):
1. Intentionally access a protected computer without authorization
2. recklessly cause damage
3. cause loss

Summary of (a)(3)(C):
1. Intentionally access a protected computer without authorization
2. cause damage
3. cause loss

Felony
3. resulting in loss of $1,000 or during 1 year
   - modifies medical care of a person
   - causes physical injury
   - threatens public health or safety
   - damages systems used by or for government entity for administration of justice, national defense, or national security
   - damages affect 10 or more protected computers during 1 year
# 18 USC 1030: Penalties

<table>
<thead>
<tr>
<th>Offense</th>
<th>Section</th>
<th>Sentence*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtaining National Security Information</td>
<td>(a)(1)</td>
<td>10 (20) years</td>
</tr>
<tr>
<td>Accessing a Computer and Obtaining Information</td>
<td>(a)(2)</td>
<td>1 or 5 (10)</td>
</tr>
<tr>
<td>Trespassing in a Government Computer</td>
<td>(a)(3)</td>
<td>1 (10)</td>
</tr>
<tr>
<td>Accessing a Computer to Defraud &amp; Obtain Value</td>
<td>(a)(4)</td>
<td>5 (10)</td>
</tr>
<tr>
<td>Intentionally Damaging by Knowing Transmission</td>
<td>(a)(5)(A)</td>
<td>1 or 10 (20)</td>
</tr>
<tr>
<td>Recklessly Damaging by Intentional Access</td>
<td>(a)(5)(B)</td>
<td>1 or 5 (10)</td>
</tr>
<tr>
<td>Negligently Causing Damage &amp; Loss by Intentional Access</td>
<td>(a)(5)(C)</td>
<td>1 (10)</td>
</tr>
<tr>
<td>Trafficking in Passwords</td>
<td>(a)(6)</td>
<td>1 (10)</td>
</tr>
<tr>
<td>Extortion Involving Computers</td>
<td>(a)(7)</td>
<td>5 (10)</td>
</tr>
</tbody>
</table>

* The maximum prison sentences for second convictions are noted in parentheses.
Computer Forensics
Forensics: Complicated enough to start with . . .
NW3C Training Approach: Break it into 4 Tiers...
NW3C Training Approach: Break it into 4 Tiers...
NW3C Training Approach: Break it into 4 Tiers...
NW3C Training Approach: Break it into 4 Tiers.

- Conduct full on-scene examinations using mobile computer forensics laboratory
- Conduct live examinations to preserve volatile memory and defeat countermeasures
- Serve as subject matter experts for police department and courts
- Conduct strategic research and tactical advanced data recovery in fixed laboratory
- Examine exotic media and multiple operating systems
- Obtain certification in all major forensic software tools
Closing Thoughts
Cybercrime and Cyber Forensics

• Cybercrime is here to stay
  – Harms to confidentiality, integrity, and availability will increasingly impact military administrative matters, logistics, defenses, and warfighting functions.

• Cyber investigations and forensics
  – Are increasingly required for internal personnel matters
  – Are increasingly required for criminal and espionage investigations
  – May be required to properly *categorize and attribute* acts of terrorism and war
Thank you for your service!

Steve.Chabinsky@CrowdStrike.com

(202) 870-1442

Follow me on ☀️: @StevenChabinsky