the assumption of breach

Jeffrey J. Guy

linkedin.com/in/jjguy    guy@carbonblack.com    @jjguy
Education

Case Western Reserve University
1995 - 1999

Career

ManTech International Corporation
1999 - 2005

JOHNS HOPKINS UNIVERSITY
2008 - 2010

2005 - 2012

Twelve years serving as a targeted attacker
My threat model:

1: TARGETED
2: NOT
compromise is inevitable
detection always fails
“We need to acknowledge once and for all that our networks will be penetrated.”

RSA Executive Chairman Art Coviello, RSA Conference, Feb 2012

Wednesday, August 7, 13
Compromise in seconds, data exfil starts in minutes, detection in months, remediation in weeks at $341k in forensics costs.

THIS IS UNSUSTAINABLE
The difficulty is not so much in developing new ideas, as in escaping from the old ones.

John Maynard Keynes
1935

Implications
Problem of Inductive Reasoning

threat modeling
"The man who has fed the chicken every day throughout its life at last wrings its neck instead... The fact something has happened a number of times causes animals and men to expect it will happen again. Thus our instincts cause us to believe the sun will rise tomorrow, but we may be in no better position than the chicken which unexpectedly has its neck wrung." Bertrand Russell

Nassim Taleb
The Black Swan
How do you assess likelihood?
How do you assess likelihood?

Are you the farmer or the chicken?
Look outward, not inward.

(1) incentives

(2) barriers
Look outward, not inward.

1) incentives
2) barriers
   a) technical
   b) legal
   c) time
Look outward, not inward.

(1) incentives

(2) barriers

(a) technical

(b) legal

(c) time
Look outward, not inward.

you have not been compromised only because no one has tried.

(b) (c) legal

time
For every thousand hacking at the leaves of evil, there is one striking at the root.

Thoreau
Typical resource allocation

- Protect: 90%
- Detect: 10%
- Respond: 0%
- Recover: 0%

Attackers will always gain toehold
Detection efficacy minimal against targeted attacks
Few detection alternatives available
Typically ad-hoc
Few technical products exist
Protect  Detect  Respond  Recover

Typical resource allocation

90%  10%  0%  0%

Shift resources to the right

Required resource allocation

60%  20%  10%  10%
Phishing and Zero day attack

A handful of users are targeted by two phishing attacks; one user opens Zero day payload (CVE-02011-0609)

Back door

The user machine is accessed remotely by Poison Ivy tool

Lateral movement

Attacker elevates access to important user, service and admin accounts, and specific systems

Data gathering

Data is acquired from target servers and staged for exfiltration

Exfiltrate

Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider
A handful of users are targeted by two phishing attacks; one user opens a Zero day payload (CVE-02011-0609).

The user machine is accessed remotely by Poison Ivy tool.

Attacker elevates access to important user, service and admin accounts, and specific systems.

Data is acquired from target servers and staged for exfiltration.

Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider.

detection focus
<table>
<thead>
<tr>
<th>Detection Focus</th>
<th>seconds to minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing and Zero day attack</td>
<td>Back door</td>
</tr>
<tr>
<td>A handful of users are targeted by two phishing attacks, one contains Zero day payload (CVE-02011-0609)</td>
<td>The user machine is accessed remotely by Poison Ivy tool</td>
</tr>
<tr>
<td>Attacker elevates access to important user, service and admin accounts, and specific systems</td>
<td>Data is acquired from target servers and staged for exfiltration</td>
</tr>
<tr>
<td>Data is exfiltrated via encrypted files over ftp to external, compromise machine at a hosting provider</td>
<td>Exfiltrate</td>
</tr>
</tbody>
</table>
detection focus

seconds to minutes
weeks to years

Exhilarate
Gathering
Data
Lateral

Weeks to Years

---

Wednesday, August 7, 13
Detection of the moment of compromise is necessary but insufficient. Full Spectrum Detection is required.
Response
2.6 Recommendations

The key recommendations presented in this section for organizing a computer security incident handling capability are summarized below.

- **Establish a formal incident response capability.** Organizations should be prepared to respond quickly and effectively when computer security defenses are breached. FISMA requires Federal agencies to establish incident response capabilities.

- **Create an incident response policy.** The incident response policy is the foundation of the incident response process, which serves as a consideration for the resources and technologies used.

<table>
<thead>
<tr>
<th>Incident Analysis Hardware and Software</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digital forensic workstations</strong> and/or backup devices to create disk images, preserve log files, and save other relevant incident data</td>
</tr>
<tr>
<td><strong>Laptops</strong> for activities such as analyzing data, sniffing packets, and writing reports (see discussion below table)</td>
</tr>
<tr>
<td><strong>Spare workstations, servers, and networking equipment, or the virtualized equivalents</strong>, which may be used for many purposes, such as restoring backups and trying out malware</td>
</tr>
<tr>
<td><strong>Blank removable media</strong></td>
</tr>
<tr>
<td><strong>Portable printer</strong> to print copies of log files and other evidence from non-networked systems</td>
</tr>
<tr>
<td><strong>Packet sniffers and protocol analyzers</strong> to capture and analyze network traffic</td>
</tr>
<tr>
<td><strong>Digital forensic software</strong> to analyze disk images</td>
</tr>
<tr>
<td><strong>Removable media</strong> with trusted versions of programs to be used to gather evidence from systems</td>
</tr>
<tr>
<td><strong>Evidence gathering accessories</strong>, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions</td>
</tr>
</tbody>
</table>
This is still reactionary incident response

filesystem forensics is lowest common denominator

Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions.
What is the technical preparation for compromise?

- **Establish a formal incident response capability.** Organizations should be prepared to respond quickly and effectively when computer security defenses are breached. FISMA requires Federal agencies to establish incident response capabilities.

---

**Packet sniffers and protocol analyzers** to capture and analyze network traffic

**Digital forensic software** to analyze disk images

**Removable media** with trusted versions of programs to be used to gather evidence from systems

**Evidence gathering accessories**, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions
process creation, file writes, registry writes, network traffic, binary copies
Preparation is not just procedural.

Sensor up! NetSA Network Situational Awareness

Wednesday, August 7, 13
Assessments
Requirement 11: Regularly test security systems & processes.  
Requirement 11.2: Quarterly Vulnerability Assessments  
Requirement 11.3: Annual Penetration Test

Consensus Audit Guidelines

Critical Control 4: Vulnerability Assessments  
Critical Control 20: Penetration Tests

HIPAA

§ 164.308(1)(ii)(A): accurate...assessment of...vulnerabilities

GBLA

§ 501(b): maintain an on-going risk assessment program

Network Pen Tests
Vuln Assessments

Wednesday, August 7, 13
Vulnerability Assessments

Compromise Assessments
Is there an existing compromise we’ve missed?

Network Penetration Tests

Intrusion Exercises
Do my detection and response procedures work?

Wednesday, August 7, 13
Information security through my lens

Inevitability of compromise

Assumption of breach

Protectionism blinds us to new ideas.
Compromise is Inevitable. Assume breach.

Invest in detection, response & recovery

Establish network situational awareness

Remember
questions

Jeffrey J. Guy

Wednesday, August 7, 13