Modern Incident Response

Jeffrey J. Guy | 9 Jun 14
jjguy@bit9.com
@jjguy
1999 - 2005
USAF Red/Blue Team

2005 - 2012
Spooky computer stuff

2012 - 2014
Startup 1.0

2014 -
Level up! Startup 2.0
MY THREAT MODEL:

1: OPPORTUNISTIC
2: NOT

DON’T OVERCOMPLICATE THE THREAT
Opportunistic threats sell our **computers**.  
**Goal: breadth** of access.

“Advanced” threats sell our **data**.  
**Goal: precision** of access.
Opportunistic threats sell our computers. Goal: **breadth** of access.

“Advanced” attackers are testing our defenses. Our defenses are **insufficient**.

“Advanced” threats sell our data. Goal: **precision** of access.
COMPROMISE IS INEVITABLE

DETECTION BYPASSED AT WILL
TWO STANDARD “BEST PRACTICES”:

1: ENDPOINT ANTIVIRUS
2: NETWORK IDS
TWO STANDARD “BEST PRACTICES”:
1: ENDPOINT ANTIVIRUS
2: NETWORK IDS
Polymorphism and new delivery mechanisms such as Web-attack toolkits continued to drive up the number of malware variants in common circulation. In 2010, Symantec encountered more than 286 million unique variants of malware.

A growing proliferation of Web-attack toolkits drove a 93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009. Shortened URLs appear to be playing a role here too. During a three-month observation period in 2010, 65% of the malicious URLs observed on social networks were shortened URLs.

This was the average number of identities exposed in each of the data breaches caused by hacking throughout the year.

In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals, there was a sharp rise in the number of reported new mobile operating system vulnerabilities—up to 163 from 115 in 2009.
WHO WRITES THE FIRST SIGNATURE?
**OPPORTUNISTIC**

- **Goal**: Maximize slope.

**“Advanced”**

- **Goal**: Minimize slope.
**OPPORTUNISTIC**

Goal is to maximize slope.

**“Advanced”**

Goal is to minimize slope.
Compromise happens in **seconds**
Data exfiltration starts **minutes** later
It continues **undetected** for **months**
Remediation takes **weeks**
At **$341k** per incident 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

A brief aside
Problem of Inductive Reasoning
"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 our customers assess likelihood of a “real” compromise?
How do our customers assess likelihood of a “real” compromise?

Are they the farmer? Or the chicken?
LOOK OUTWARD, NOT IN

(1) Incentives

(2) Barriers
LOOK OUTWARD, NOT IN

(1) Incentives
(2) Barriers
   (a) Technical
   (b) Legal
   (c) Time
LOOK OUTWARD, NOT IN

(1) Incentives
(2) Barriers
   (a) Technical
   (b) Legal
   (c) Time
LOOK OUTWARD, NOT IN

(1) Incentives
(2) Barriers
(a) Technical
(b) Legal
(c) Time

The only reason a network hasn’t been compromised is because no one has bothered to try.
For every thousand hacking at the leaves of evil, there is one striking at the root.

Thoreau
The assumption of breach is an information security management philosophy.

```

Assumption of Breach
Inevitability of compromise
Failure of detection
“Advanced” attackers
```

"Advanced" attackers
Protection, detection and response as a continuous process.
A growing consensus

“Security...will shift to rapid detection and response capabilities linked to protection systems to block further spread of the attack.”


“Functions organize basic cybersecurity activities at their highest level. These Functions are: Identify, Protect, Detect, Respond, and Recover.”

NIST Cybersecurity Framework for Critical Infrastructure, Feb 2014

Assume the organization is already infected. Change your "incident response" mindset to a "continuous detection and response" process.

Gartner Research Note, Feb 2014
If you’re a CISO,
...and you drink the Kool-Aid,
...what’s next?
If you’re a CISO, …and you drink the Kool-Aid, …what’s next?

“I need an in-house IR team.”
Current IR practices are based largely on external consultant practices.
Current IR practices are based largely on external consultant practices. IR consultants rely heavily on digital forensics.
Current IR practices are based largely on external consultant practices. IR consultants rely heavily on digital forensics.

Digital forensics is not a choice, it’s the lowest common denominator.
The CISO does not have to accept lowest common denominator.
The CISO does not have to accept the lowest common denominator.

The CISO cannot accept the lowest common denominator.
Scenario: You observe network traffic to a known malware C2 server from an internal host.

Goal: *Triage, identify initial infection vector.*
Scenario: You observe network traffic to a known malware C2 server from an internal host.

Goal: *Triage, identify initial infection vector.*

<table>
<thead>
<tr>
<th>Triage review:</th>
<th>Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data acquisition:</td>
<td>Minutes to hours</td>
</tr>
<tr>
<td>Artifact analysis:</td>
<td>Minutes to hours</td>
</tr>
<tr>
<td>Skill required:</td>
<td>Medium to high</td>
</tr>
<tr>
<td>Confidence in result:</td>
<td>Medium</td>
</tr>
</tbody>
</table>
**Scenario:** You observe network traffic to a known malware C2 server from an internal host.

**Goal:** Triage; identify initial infection vector.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Time Frame</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triage review</td>
<td>Minutes to hours</td>
<td>Medium</td>
</tr>
<tr>
<td>Data acquisition</td>
<td>Minutes to hours</td>
<td>Medium to high</td>
</tr>
<tr>
<td>Artifact analysis</td>
<td>Minutes to hours</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Bottom line:**

- Domain SME
- Hours to days *(weeks?)*
- Medium confidence
You observe network traffic to a known malware C2 server from an internal host.

**Scenario:**
Triage, identify initial infection vector.

**Goal:**
- Triage review
- Data acquisition
- Artifact analysis

**Skill required:** Medium to high

**Confidence in result:** Medium

**Bottom line**
a domain SME
hours to days (weeks?)
medium confidence

**Data acquisition:** Minutes to hours

**Artificial analysis:** Minutes to hours

**This happens daily**
The CISO cannot afford to execute continuous response with existing practices.
The CISO cannot afford to execute continuous response with existing practices.

As a result, activity is: ignored, improperly analyzed, or pre-emptively remediated.
the U.S. to cover their tracks, then into their computers in Russia—FireEye spotted them. Bangalore got an alert and flagged the security team in Minneapolis. And then...

Nothing happened.
Compromise happens in seconds
Data exfiltration starts minutes later
It continues undetected for months
Remediation takes weeks
At $341k per incident in forensics costs

THIS IS UNSUSTAINABLE
We are being outclassed.

Incident response must get faster and cheaper.

Compromise happens in seconds
Data exfiltration starts minutes later
It continues undetected for months
Remediation takes weeks
At $341k per incident in forensics costs

THIS IS UNSUSTAINABLE
You better have a vision, you better have a plan, and you better have the passion for getting things done.

Lou Holtz
I don’t have the answers.
I don’t have the answers.

It’s being defined now by PHBs.
I don’t have the answers. It’s being defined now by PHBs. If we don’t get in front of it, they will (try to) define it for us.
Scenario: You observe network traffic to a known malware C2 server from an internal host.

Goal: Triage, identify initial infection vector.

Triage review: Bottom line

Data acquisition: a domain SME

Artifact analysis: hours to days (weeks?)

Skill required: medium confidence

Confidence in result: Medium
Scenario: You observe network traffic to a known malware C2 server from an internal host.

Goal: Triage, identify initial infection vector.

Bottom line: a domain SME hours to days (weeks?) medium confidence

Triage review: Minutes to hours

Data acquisition: Minutes to hours

Artifact analysis: Minutes to hours

Skill required: Medium to high

Confidence in result: Medium

Goal: a junior to mid guy minutes high confidence
Scenario: You observe network traffic to a known malware C2 server from an internal host.

Goal: *Triage, identify initial infection vector.*

<table>
<thead>
<tr>
<th>Triage review:</th>
<th>Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data acquisition:</td>
<td>Minutes to hours</td>
</tr>
<tr>
<td>Artifact analysis:</td>
<td>Minutes to hours</td>
</tr>
<tr>
<td>Skill required:</td>
<td>Medium to high</td>
</tr>
<tr>
<td>Confidence in result:</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Scenario: You observe network traffic to a known malware C2 server from an internal host.

Goal: *Triage, identify initial infection vector.*

<table>
<thead>
<tr>
<th>Triage review:</th>
<th>Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data acquisition:</td>
<td>Minutes to hours</td>
</tr>
<tr>
<td>Artifact analysis:</td>
<td>Minutes to hours</td>
</tr>
</tbody>
</table>

| Skill required:         | Medium to high           |
| Confidence in result:   | Medium                   |
### Scenario:
You observe network traffic to a known malware C2 server from an internal host.

### Goal:
Triage, identify initial infection vector.

### Triage review:

<table>
<thead>
<tr>
<th>Data acquisition</th>
<th>Minutes to hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artifact analysis</td>
<td>Minutes to hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Skill required:</th>
<th>Medium to high</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence in result:</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Yes, I build a product to help.

Our existence is proof of need.

We don’t have a lock on smart folks.
...and we’re not alone.
Parting shots

UNSUSTAINABLE

Lowest common denominator cannot continue.

Any question, in seconds, with a junior guy.

IR != Digital Forensics
“The attacker has the advantage”
“The attacker has the advantage”
“The attacker has the advantage”

...because we give it to him.
QUESTIONS?

Jeffrey J. Guy
jjguy@bit9.com
@jjguy