How has the APT changed the way we approach network forensics?

Charles Smutz

Network Forensics Panel

SanS 4n6 and IR Summit

About Panelist

Name	Charles Smutz
Background	Sysadmin, Networking, C&A
Current Job	Lead Software Developer
Employer	Lockheed Martin CIRT
Education	Pursuing PhD at GMU

How APT has changed Net 4n6

- What
  - Threat/Campaign vs. Vulnerability/Attack Focus
- When
  - Increase in frequency of attacks
  - Historical Perspective
- How
  - Processes, Techniques, Tools

What: Threat/Campaign vs. Vulnerability/Attack Focus

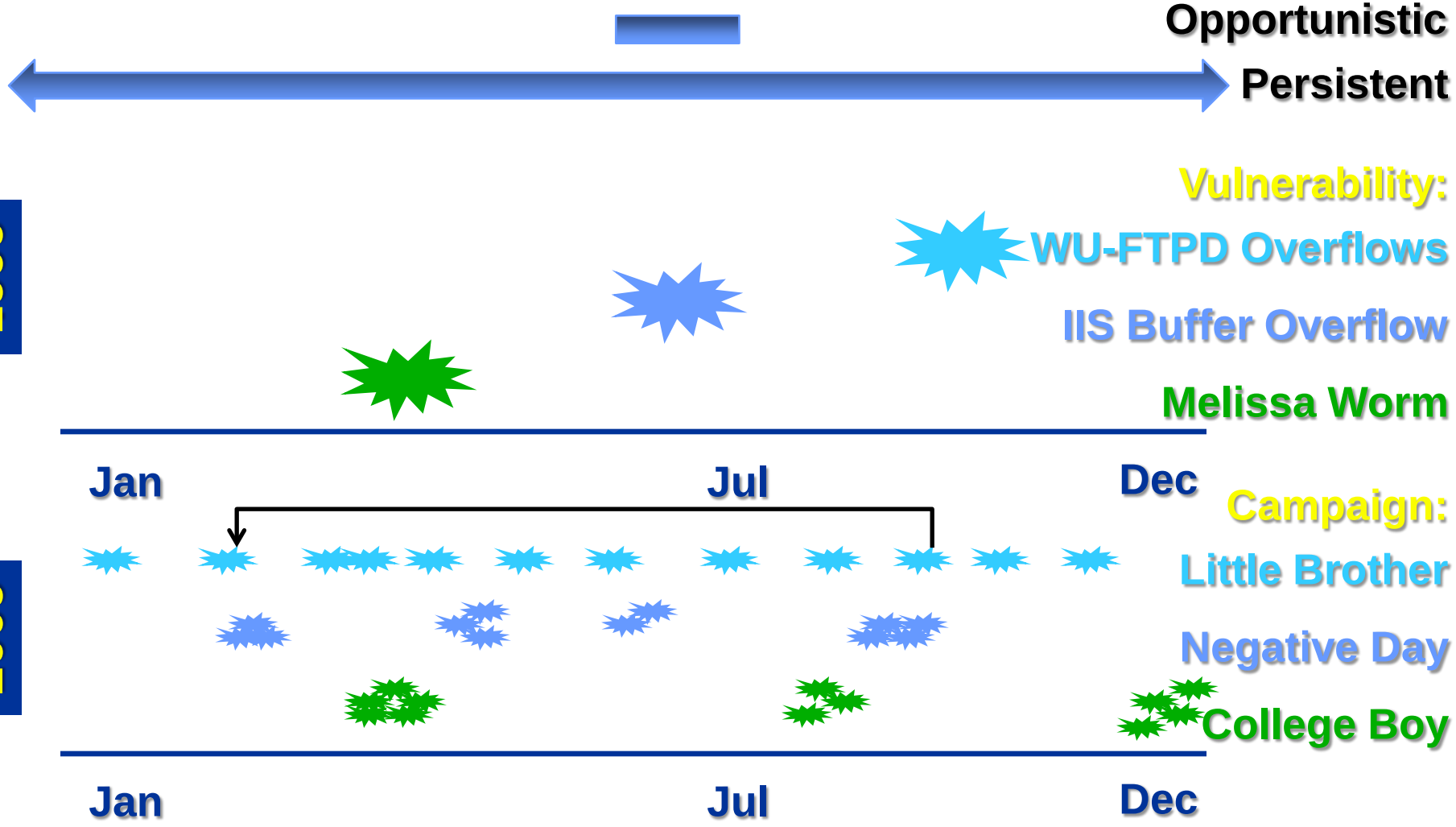
```
From: spoofed@partner.com
Received: from open.relay.com
([10.10.10.10]) by mx.company.com
Received: from now.bad.com
([172.16.1.1]) by mx.relay.com
Date: Thu, 17 Jun 2010 12:03:41
-0700 (PDT)
Message-Id: <1.1.2.3.5.8@mailer>
X-Mailer: SillyMailer v3.14
Subject: All your Base are belong
to us

Please review attached.

Edward Spoofed
Spoofed Inc.
301-867–5309
```

```
InfoKey: Creator
InfoValue: Acrobat PDF Printer
InfoKey: Author
InfoValue: TK421
InfoKey: Producer
InfoKey: ModDate
InfoValue: D:20100616+08'00'
PdfID1: 8d23f593e67be992ff3470d
PdfID0: 798f9d8e3966ac586a61dc0
```

```
for(fqchp=0;fqchp<inxnh;fqchp++)
  {dnysj[fqchp]=dtkrx + hjnoa;}
if(ingmh){hsbsd();hsbsd();try
  {this.media.newPlayer(null);}
  catch(e) {}hsbsd();}
```

```
<Obfuscated Embedded Malware>
```

When: More Frequent, Historical



How: Processes, Techniques, Tools

- **What**
  - **Threat Focused 4n6**
- **When**
  - **Frequent, Rapid Analysis**
  - **Long Term Knowledge/Intelligence Management**

If existing tools don't do what you need, you may have to build your own

Charles Smutz

charles.smutz@lmco.com

Personal Blog:
http://smusec.blogspot.com