

Marketing Security

through

FUD, Findings, Futures, and Friends

caveat emptor: This material is furnished as-is. The author makes no warranties of any kind, including, but not limited to fitness for purpose, merchantability, exclusivity, or freedom from patent, trademark, or copyright infringement. The findings, interpretations, and conclusions expressed herein are those of the author and do not necessarily reflect the views of any employers, past or present. Use of any product names, images, or trademarks in this material is not intended in any way to infringe on the rights of the trademark holder, nor is it intended to positively or negatively endorse any product or solution. Permission is granted for free usage of all or portions of this document, including derived works, provided proper acknowledgement is given.

June 2008

Prentice Kinser, CISSP-ISSAP

1

Marketing Security - Maturity

**Level 1 - Fear,
Uncertainty, and
Doubt (FUD)**

ie. scare tactics

**Level 2 – Findings
Driven (audits,
incidents, etc)**

ie. opportunism

**Level 3 – Future
Focused**

ie. integrated with mature
architecture disciplines

Level 4 – Populism

ie. wholistic, positive,
friendly, fun – each
employee becomes a
security advocate

Maturity Level 1 - Fear, Uncertainty, and Doubt (FUD)

Level 1 - Fear, Uncertainty, and Doubt (FUD)

“...all things being equal, buyers would rather take the chance that the attack won't happen than suffer the sure loss that comes from purchasing the security product ... Security is fundamentally a negative sell. One solution is to stoke fear. Fear is a primal emotion, far older than our ability to calculate trade-offs. And when people are truly scared, they're willing to do almost anything to make that feeling go away”

(Bruce Schneier, CRYPTO-GRAM, June 15, 2008, <http://www.schneier.com/crypto-gram.html>)

Level 1 - Fear, Uncertainty, and Doubt (FUD) - examples

“Hackers have used so-called “phishing” efforts to trap online users into Man-in-the-Middle (MITM) schemes by spoofing financial institution websites ... In early December 2007, a Russian-German hacker gang looted commercial bank accounts in four countries using a custom-built Trojan deployed in place by expertly crafted and extremely focused phishing attacks ... To further compound these complex phishing attacks, a new variant has been added called “silentbanker.” Unlike conventional cyber-banking frauds in which bank clients are steered to a bogus website, silentbanker software uses the genuine bank website and is able to manipulate the user’s account without the client’s knowledge ... Since late 2007, silentbanker has targeted more than 400 banks worldwide”

(Source: CIA Cyber-Intelligence Note, 19 March 2008, *Online Hacking Attacks Threaten U.S. Banking and Financial Institutions*, http://www.businessweek.com/pdfs/2008/0816_online_attacks.pdf)

A recent analysis of the Google Blacklist of phishing websites indicates that 25% of those that are operational target online banking

(Source: <http://portal.spidynamics.com/blogs/msutton/archive/2007/01/04/A-Tour-of-the-Google-Blacklist.aspx>)

Level 1 - Fear, Uncertainty, and Doubt (FUD) - examples

Threats are trending back to external: organized crime, state sponsored terrorism, and hactivism. Script kiddies are less of a problem now than they were in the past – now the focus is on revenue generation.

(Source: Jerry Martin (www.team-cymru.org) talk given at ISSA Chapter Meeting 4/9/08)

Military officials have long believed that "it's cheaper, and we kill stuff faster, when we use the Internet to enable high-tech warfare," says a top adviser to the U.S. military on the overhaul of its computer security strategy. "Now they're saying, 'Oh, shit.'"

(Source: BusinessWeek cover story April 10, 2008, *The New E-spionage Threat*, http://www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm)

Level 1 - Fear, Uncertainty, and Doubt (FUD) - examples



Get ready for even harder to recognize virus/phishing e-mails. (auto-spear-phishing)

Current: E-mail spreads as fast as possible.

Better (Future?): Smart Worms will use Targeted e-mail.

User sends valid e-mail:

```
From: Alice
To: Bob
Subject: Meeting
```

Hey Bob:

we will have a meeting tomorrow at 2:00pm.

5 min later, bot sends followup:

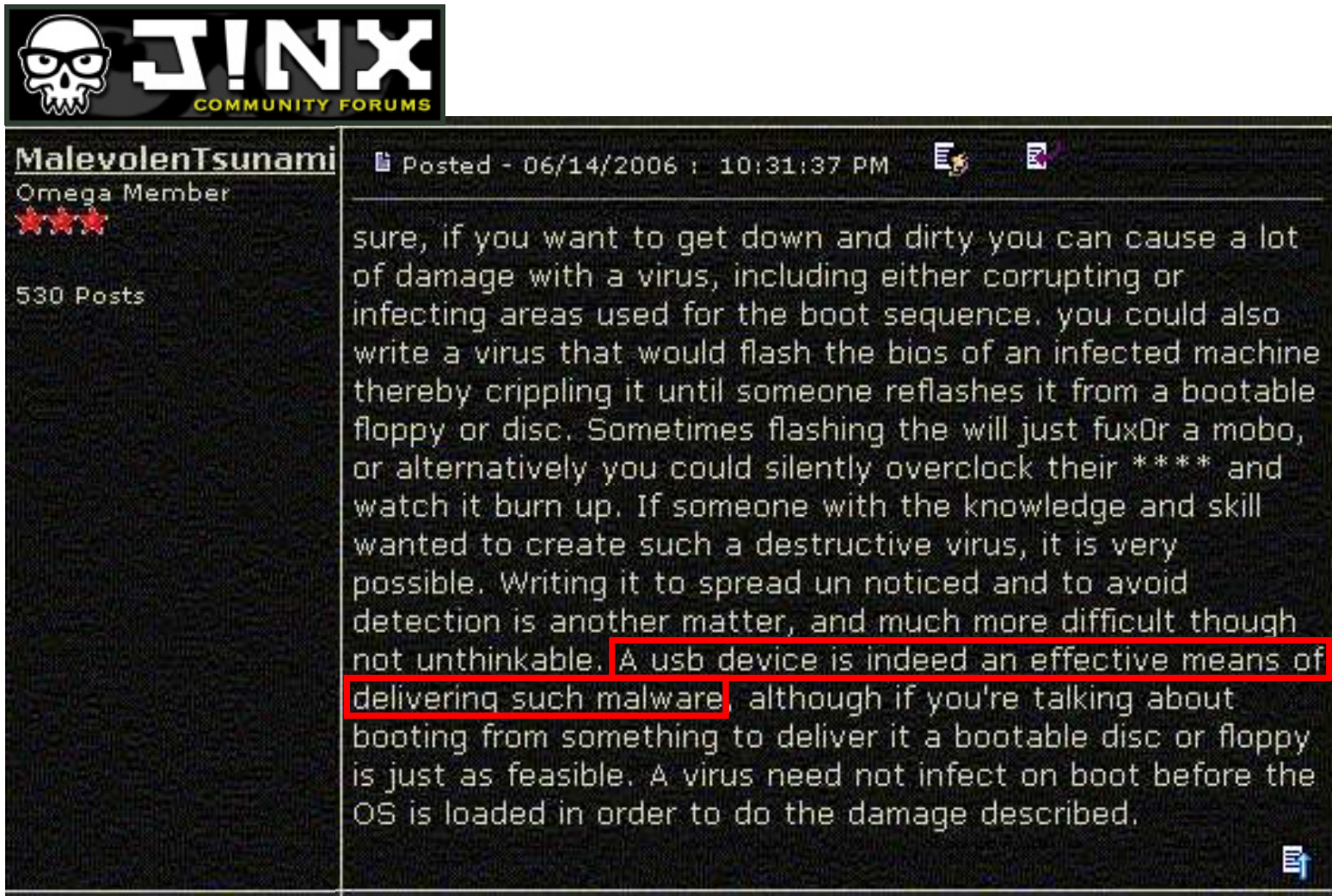
```
From: Alice's Bot
To: Bob
Subject: Meeting
```

Sorry, I forgot to attach this document to my e-mail.

Alice

(from <http://isc.incidents.org/presentations/sansfire2006keynote.pdf>)

Level 1 - Fear, Uncertainty, and Doubt (FUD) - examples



J!NX
COMMUNITY FORUMS

MalevolentTsunami
Omega Member
★★★★
530 Posts

Posted - 06/14/2006 : 10:31:37 PM

sure, if you want to get down and dirty you can cause a lot of damage with a virus, including either corrupting or infecting areas used for the boot sequence. you could also write a virus that would flash the bios of an infected machine thereby crippling it until someone reflashes it from a bootable floppy or disc. Sometimes flashing the will just fuxOr a mobo, or alternatively you could silently overclock their **** and watch it burn up. If someone with the knowledge and skill wanted to create such a destructive virus, it is very possible. Writing it to spread un noticed and to avoid detection is another matter, and much more difficult though not unthinkable. **A usb device is indeed an effective means of delivering such malware**, although if you're talking about booting from something to deliver it a bootable disc or floppy is just as feasible. A virus need not infect on boot before the OS is loaded in order to do the damage described.

Maturity Level 2 - Findings Driven

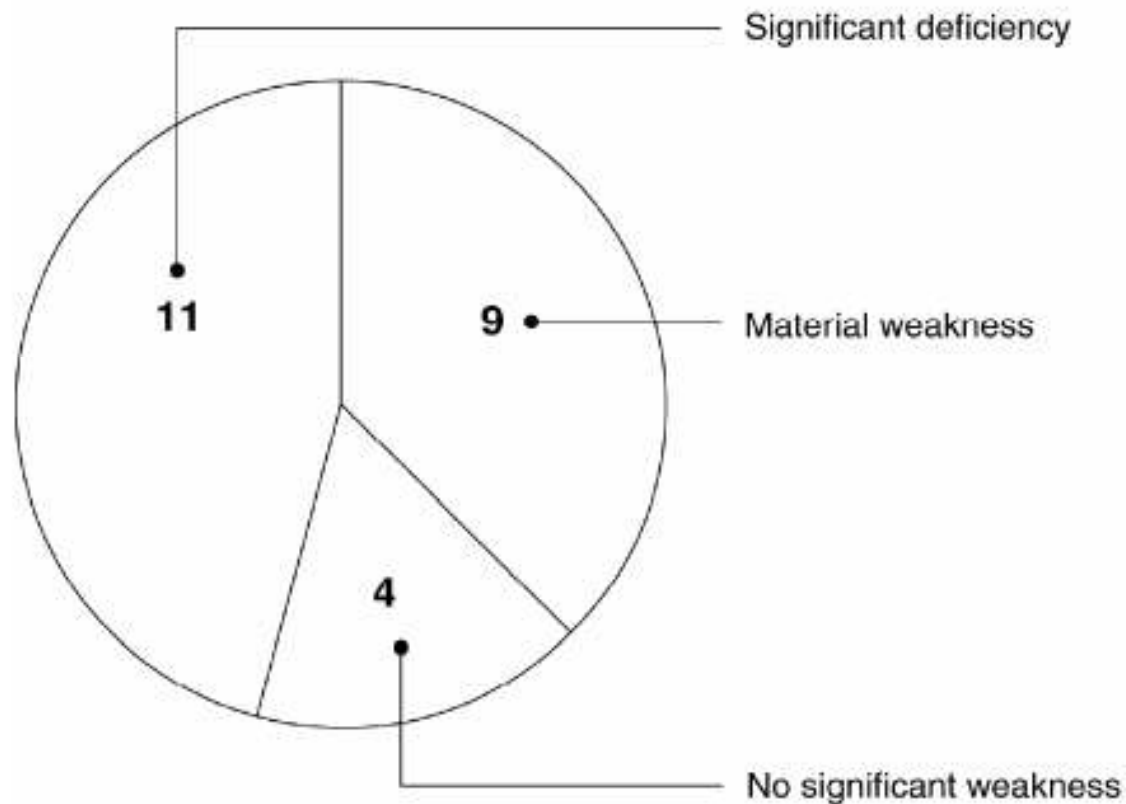
June 2008

Prentice Kinser, CISSP-ISSAP

9

Level 2 - Findings Driven – FISMA Example

Figure 5: Number of Major Agencies Reporting Significant Deficiencies in Information Security

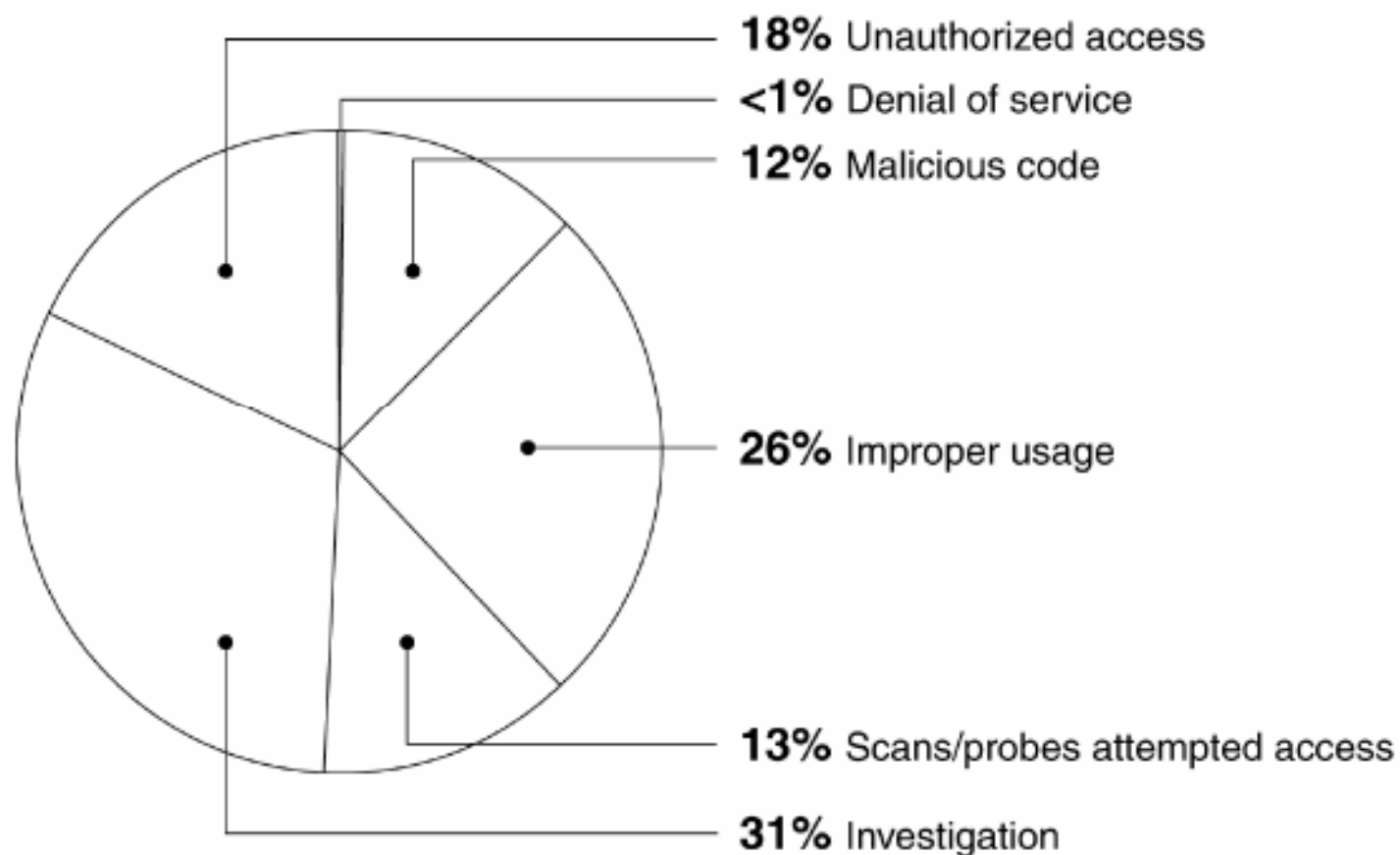


Source: GAO analysis of agency performance and accountability reports for FY2007.

Progress Reported, but Weaknesses at Federal Agencies Persist, Statement of Gregory C. Wilshusen Director, Information Security Issues, March 12, 2008 <http://www.gao.gov/new.items/d08571t.pdf>

Level 2 - Findings Driven - US-CERT example

Figure 8: Percentage of Incidents Reported to US-CERT in FY07



Source: GAO analysis of US-CERT data.

Progress Reported, but Weaknesses at Federal Agencies Persist, Statement of Gregory C. Wilshusen Director, Information Security Issues, March 12, 2008 <http://www.gao.gov/new.items/d08571t.pdf>

Maturity Level 3 – Future Focused

June 2008

Prentice Kinser, CISSP-ISSAP

12

What's wrong with FUD and Audit Findings?

Though effective, fear mongering is not very ethical. The better solution is not to sell security directly, but to include it as part of a more general product or service. Your car comes with safety and security features built in and it should be the same with computers and networks.

(Bruce Schneier, CRYPTO-GRAM, June 15, 2008, <http://www.schneier.com/crypto-gram.html>)

Example – selling Two-Factor Authentication as a “Customer Experience” benefit

Consumers Respond Well to Two-Factor Authentication

Bank Info Security – May 23, 2007

Excerpt

Online banking consumers are proving to be far more accepting of strong authentication than industry pessimists predicted—in spite of the fact that most of them are unaware of the new regulation.

A recent consumer banking poll conducted by Javelin Research on behalf of Authentify found that 90 percent of consumers would prefer security over convenience or felt neutral about the choice. Over half of those consumers who do not bank online said that the main concern that kept them from transacting online was security.

More than one in five of these consumers were completely unaware of the FFIEC guidance or any requirements for banks to move away from the insecure username and password model, which means that they welcome changes without their banks even having to use the regulations as an ‘excuse’ for the inconvenience.

Source: Javelin Strategy and Research

Example – selling advanced messaging vs. “Secure eMail”

“A healthy chunk of today's 20-something workers prefer IM to email, Skype to the traditional telephone, and file-sharing networks to photo albums. For data storage, they might choose the iPod over the flash drive; for meetings, Second Life over in-person encounters; and for computing, smart phones and laptops over desktops.”

(SC Magazine, *The Next Generation*, April 01, 2008,
<http://www.scmagazineus.com/The-next-generation/article/108410/>)

Example – selling advanced messaging vs. “Secure eMail”

“...a user’s computer is now no longer a single device, but rather a virtual amalgamation of various devices (e.g., a PC, a laptop, a personal digital assistant [PDA], and a cell phone), each of which provides a channel into information and processes. Users assume that the channels are segmented views of an integrated system. The enterprise’s stark reality is that this is not actually true.”

(Burton Group, *Content and Collaboration Strategies VantagePoint 2008–2009*, v1.0, 10 June 2008, <http://www.burtongroup.com/Client/Research/Document.aspx?cid=1392>)

Maturity Level 4 – Populism

June 2008

Prentice Kinser, CISSP-ISSAP

17

Example - empower the populace, and they will empower you (note the focus on “Do’s”, not “Don’ts”)

Ruin a pickpocket's day

Pickpockets love crowds. Take precautions to protect your valuables:

- Use a purse with a secure clasp. Keep the purse close to your body and your hand on the clasp.
- Carry your wallet inside your coat or side trouser pocket, never in your rear trouser pocket. Also, place a rubber band around your wallet to feel resistance if it is removed from your pocket.
- Beware of loud arguments or commotions that may be staged to distract you while your pocket is picked.
- If your pocket is picked, yell out immediately to warn others. Don't be afraid to shout. Tell the train or bus operator, and request the police.
- Avoid standing near train car doors to lessen your chance of being crowded or bumped by others. If you're jostled in a crowd, a pickpocket may be responsible.

From http://www.wmata.com/metrorail/metrorail_safety.cfm

Example – encourage “Perspective Taking”

When you watch this short video, try to imagine the vision-impaired individual as representing your business, the leader-dog as your security team, and the dangerous environment as your threat surface.

Metro_Madness-56k.wmv

From http://www.wmata.com/riding/leader_dogs.cfm

Levels of Maturity – **complimentary building blocks, not mutually exclusive**

Level 1 - Fear, Uncertainty, and Doubt (FUD)

ie. scare tactics

Level 2 – Findings Driven (audits, incidents, etc)

ie. opportunism

Level 3 – Future Focused

ie. integrated with mature architecture disciplines

Level 4 – Populism

ie. wholistic, positive, friendly, fun – each employee becomes a security advocate