

Emerging Threats:

Lenny Zeltser

Security Consulting Manager, SAVVIS
Senior Faculty Member, SANS Institute
Handler, SANS Internet Storm Center

A dramatic landscape featuring a long, straight road that stretches from the foreground towards a distant horizon. The road is flanked by large, intense flames that appear to be rising from the ground, creating a sense of fire and conflict. The sky above is filled with dark, heavy clouds, adding to the ominous atmosphere. The overall scene suggests a path leading into a dangerous or war-torn environment.

Attackers and defenders are
locked in an arms race



's position has a
few disadvantages





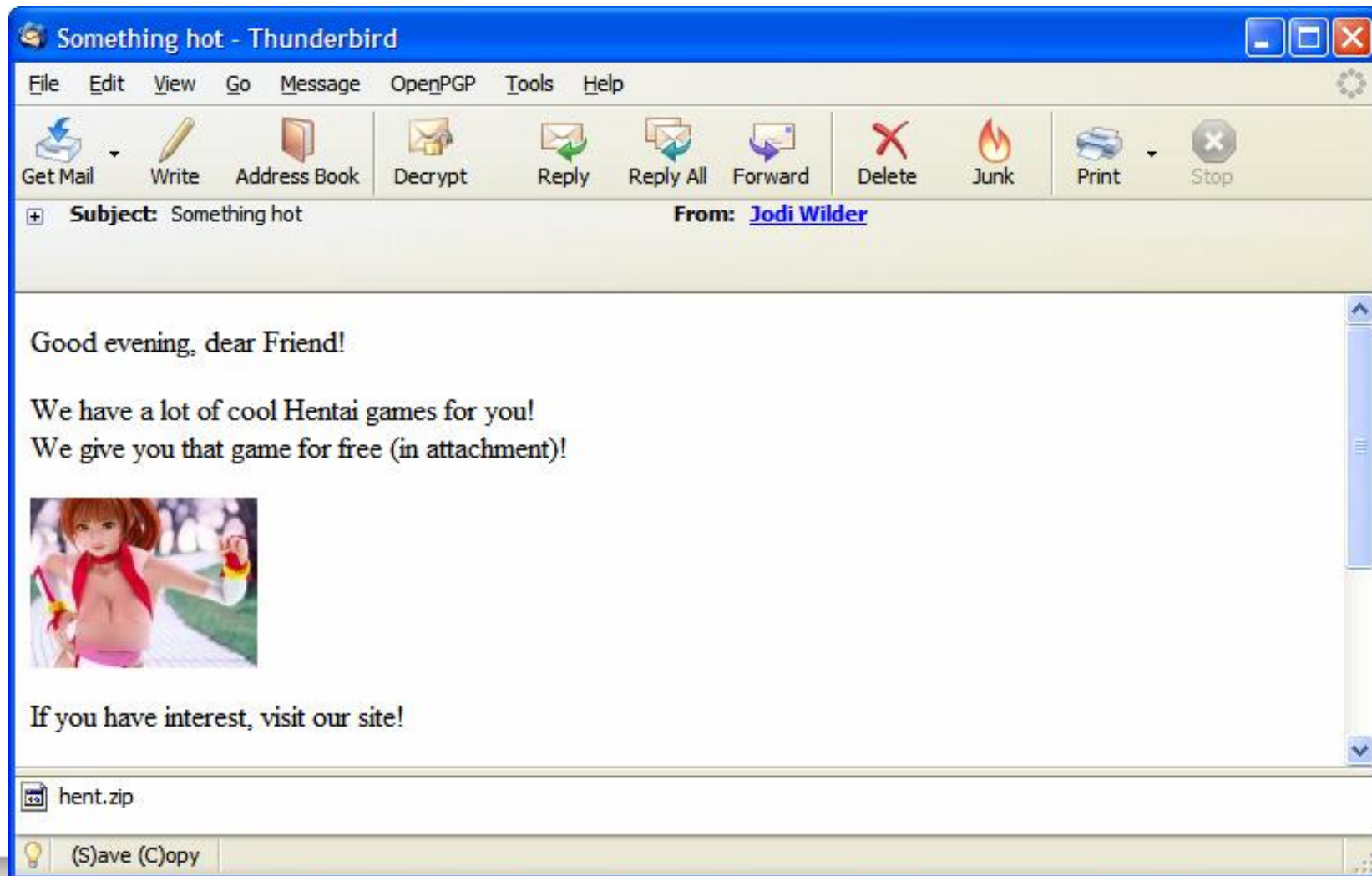
stay abreast
of the threat
landscape

to
keep up
with the
race

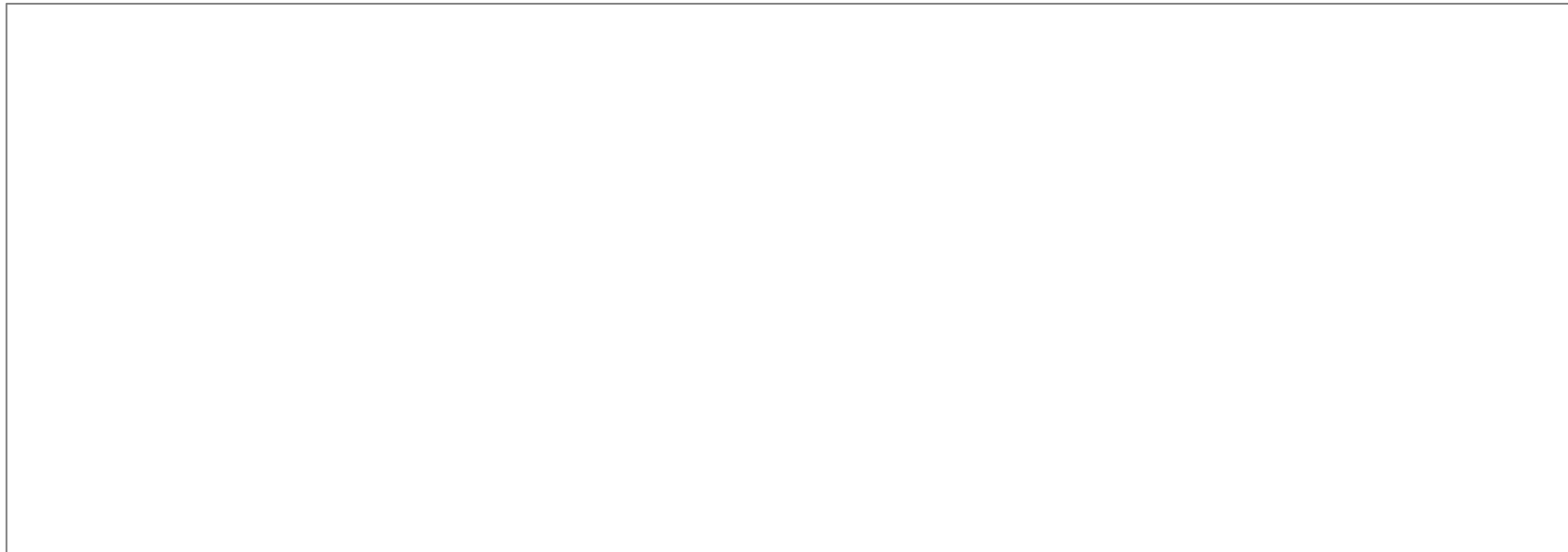


INFORMATION **SECURITY** DECISIONS

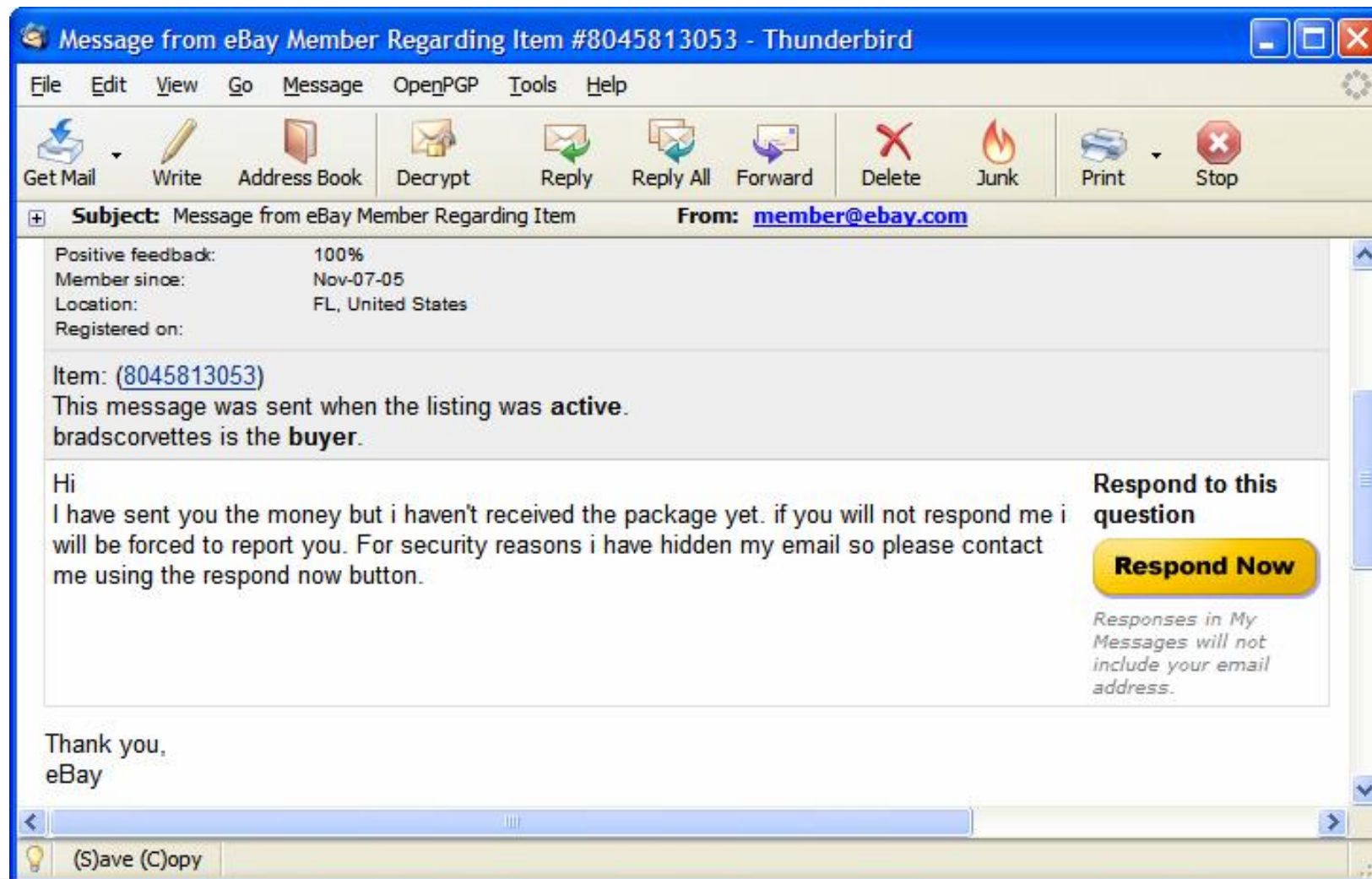
Trick the victim into installing malware



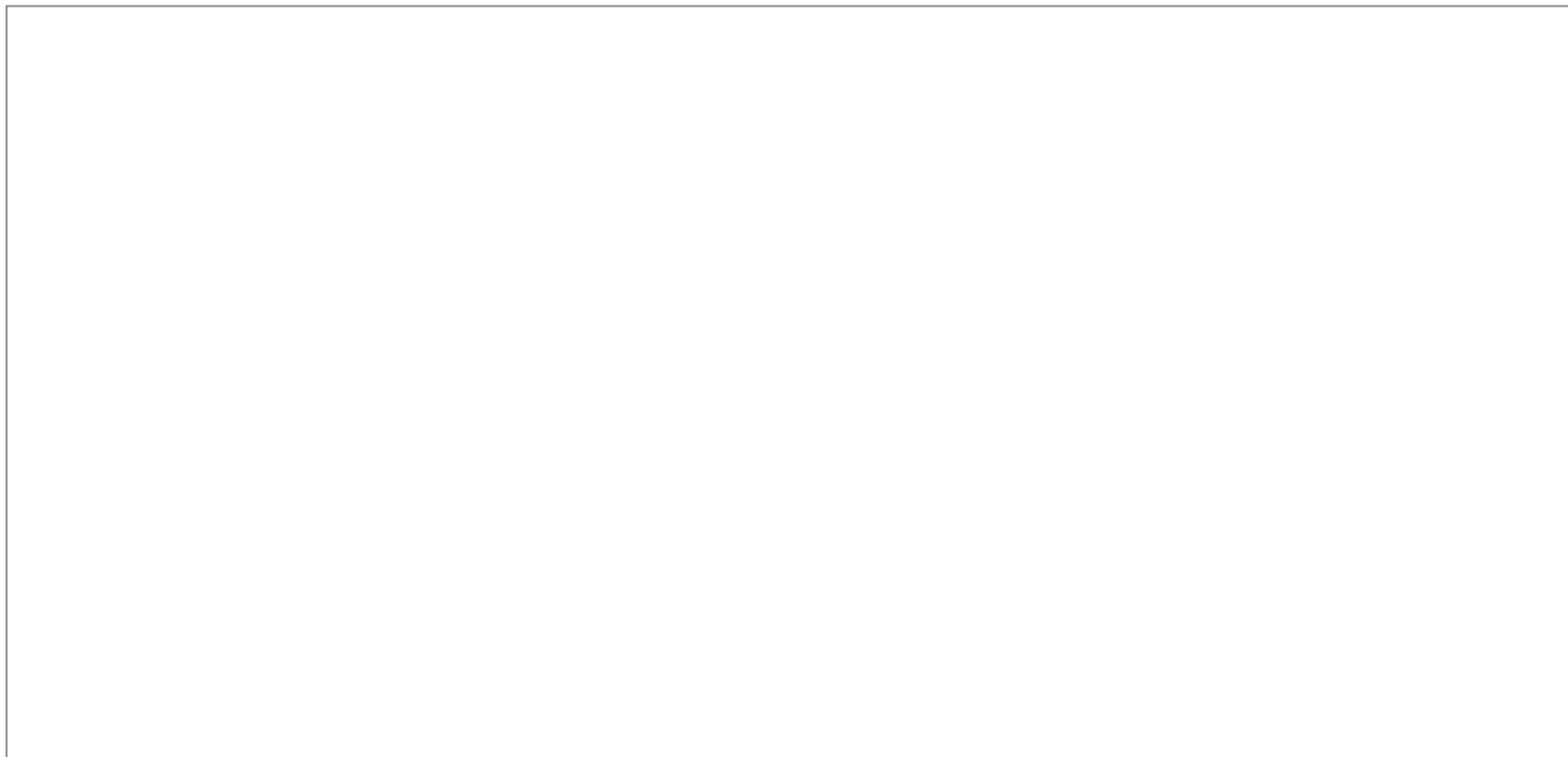
Defraud the victim through



Prey on users of auction Web sites



Phish VoIP access by



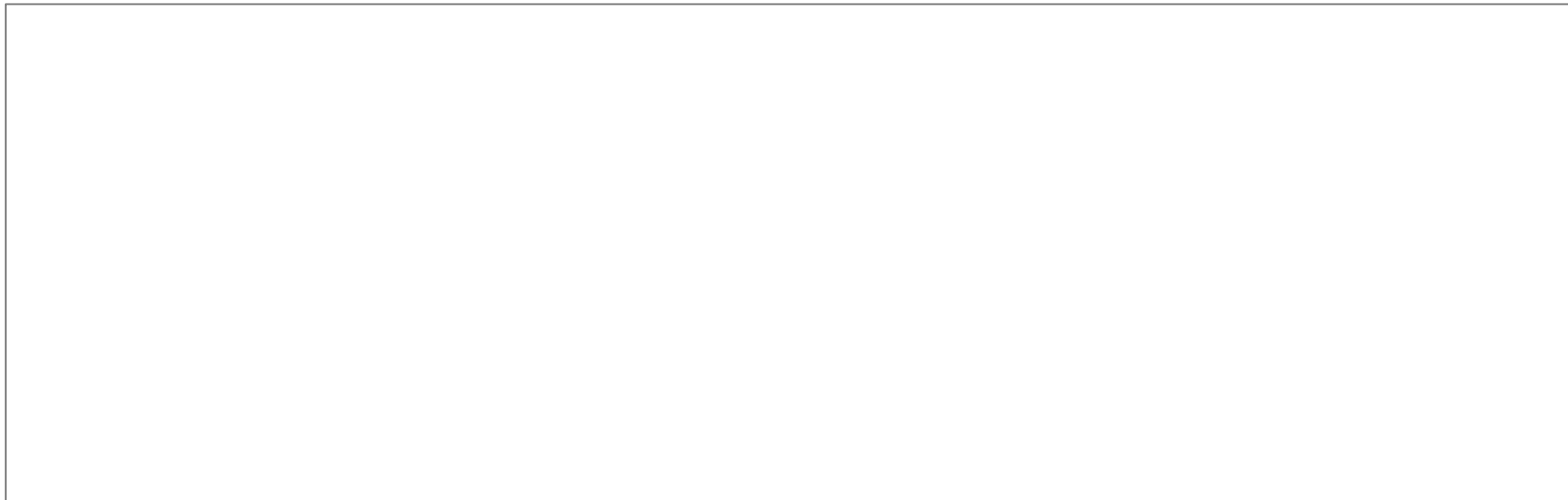
-factor authenticating to banking Web sites via phishing

Your SiteKey:



If you don't recognize your personalized SiteKey,
don't enter your Passcode.

Pursue email access by sites



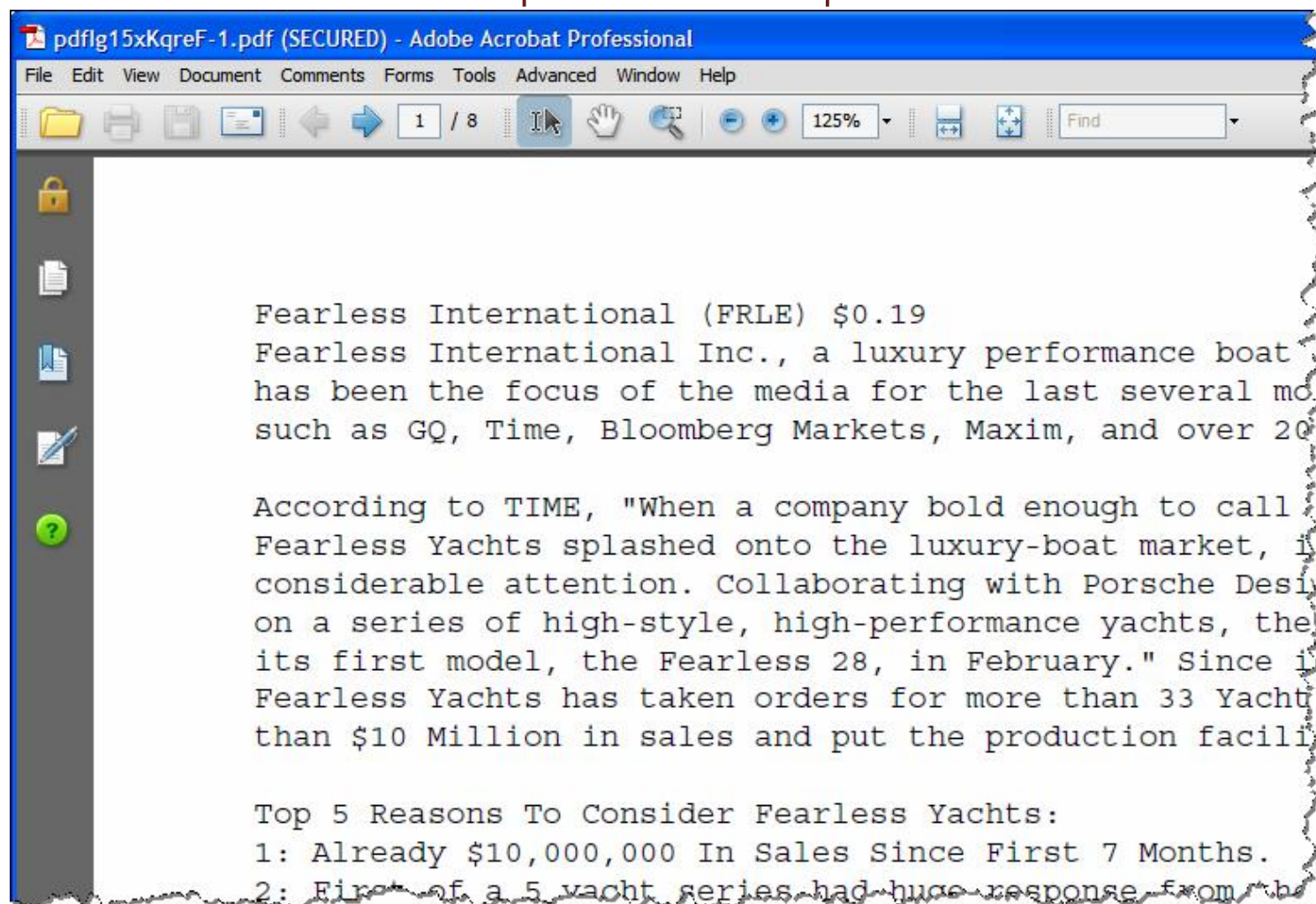
Passwords for emails and same...



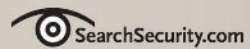
...

PayPal, e-Gold, etc.


Drive up the stock price via pump-and-dump techniques







INFORMATION SECURITY DECISIONS



The Storm worm
modern bot

Self-propagating: Adapts its techniques

Profit-driven: Spam for pump-and-dump

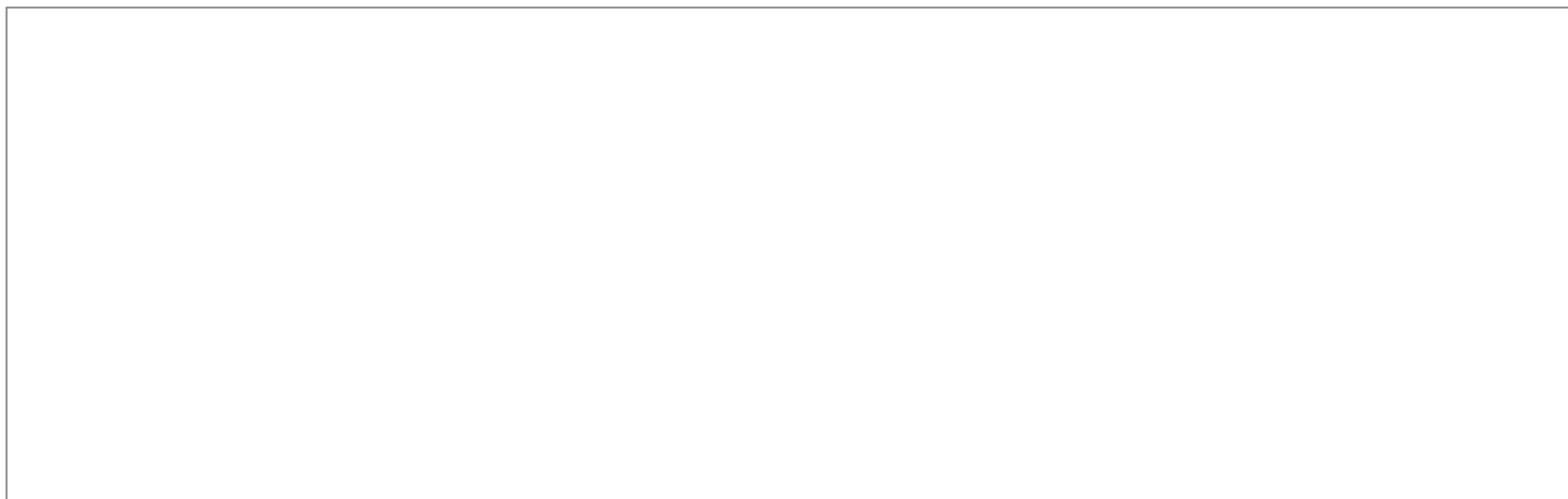
Resilient: P2P and Fast-Flux





Attackers have become very aggressive
in defending their enterprises via

highly active



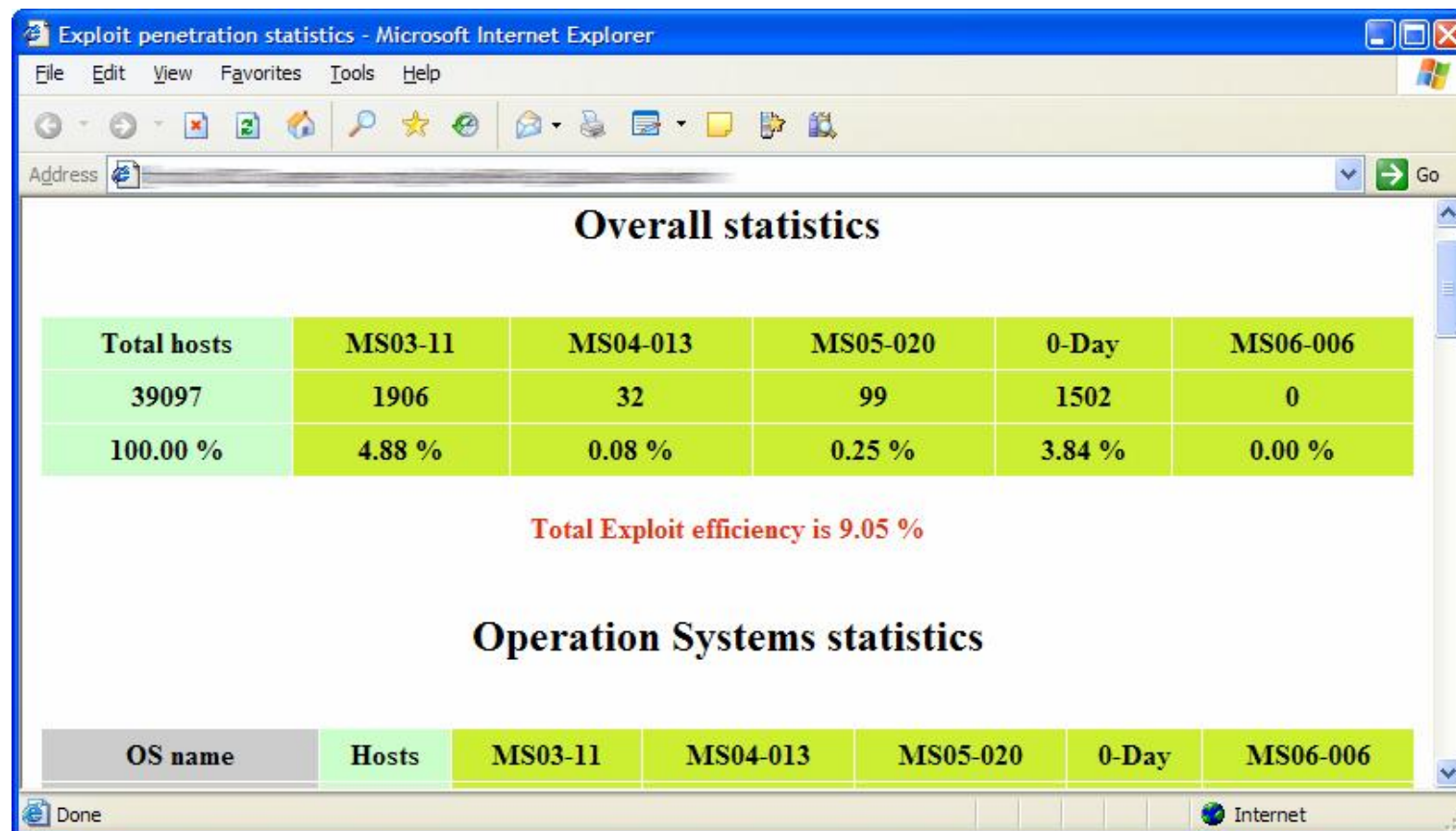


INFORMATION **SECURITY** DECISIONS



Drive-by infections target browser vulnerabilities of Web site visitors

Client-
automate such campaigns



Client-side attacks are growing in popularity

Exploits
Auxiliaries
Payloads
Console
Sessions
About

Internet Explorer COM CreateObject Code Execution (2)

Internet Explorer COM CreateObject Code Execution

Please enter all of the required options and press 'Launch Exploit' to continue.

CURRENT CONFIGURATION - [CHANGE PAYLOAD](#)

EXPLOIT	windows/browser/ie_createobjec
TARGET	Automatic
PAYLOAD	generic/shell_reverse_tcp

STANDARD OPTIONS

SRVHOST	Required
The local host to listen on. (type: address)	<input type="text" value="66.232.30.57"/>
SRVPORT	Required
The local port to listen on. (type: port)	<input type="text" value="80"/>
URIPATH	

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print

Live PoC scanner

Host to scan:

192.168.1.217

Ports:

21,22,25,80,81,110,135,139,143,445,548

[Start Scan](#)

21 22 25 80 81 110

135: OPEN

139 143

445: OPEN

548 445

network reconnaissance



Create a Filter

[Hide filter options](#)

Choose search criteria - Specify the criteria you'd like to use for determining what to do with a message as it arrives. Use "Test Search" to see which messages would have been filtered using these criteria.

From:

Has the words:

To:

Doesn't have:

Subject:

☐ Has attachment

[Show current filters](#)

Cancel

Test Search

Next Step »

Attackers are targeting flaws in applications

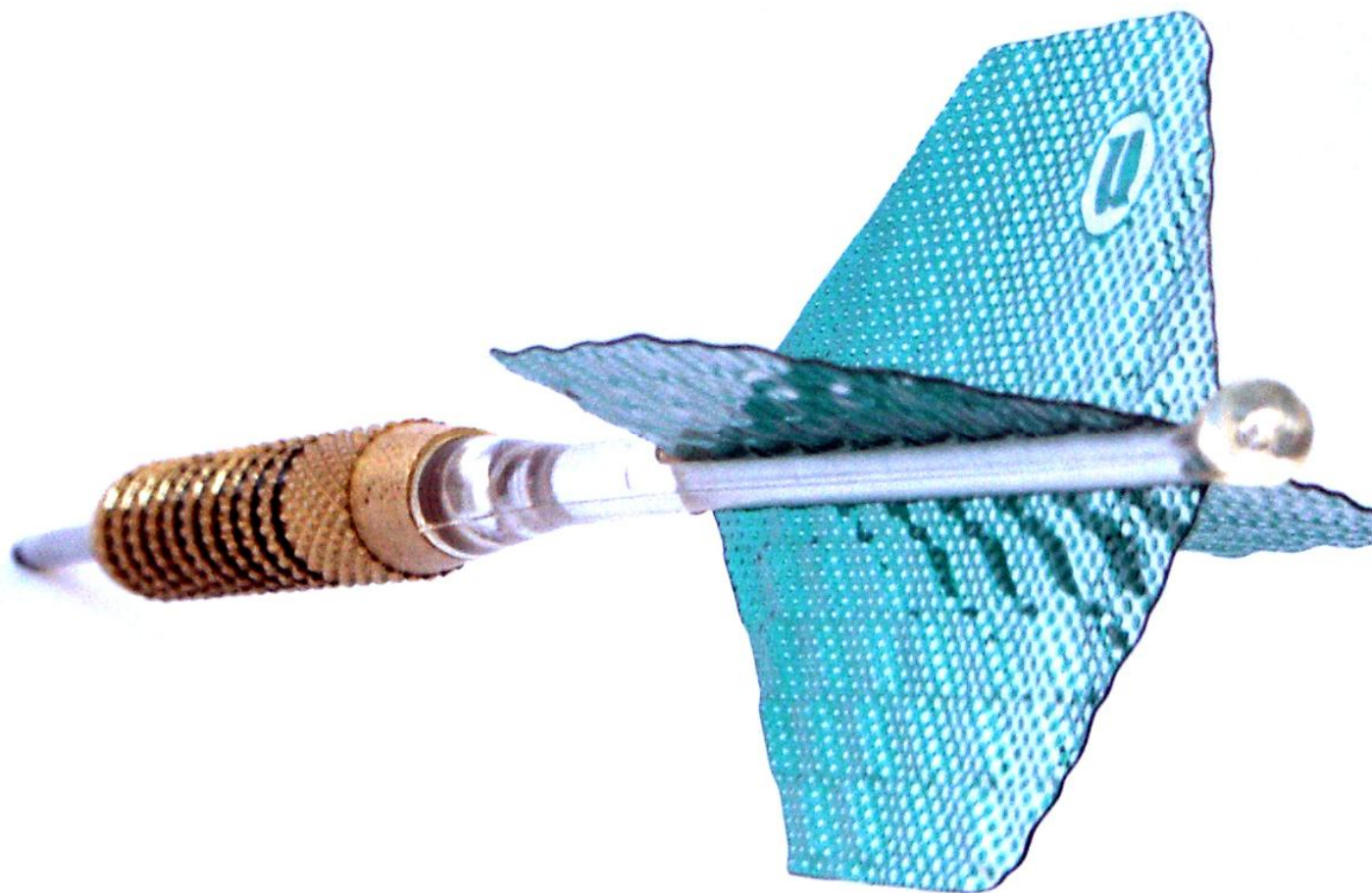


INFORMATION **SECURITY** DECISIONS

targeted with zero-day exploits



hope see again.doc





Attackers
pursued

to harvest
documents

How may we help you?

[About Us](#)

[Rates](#)

[Loans](#)

[Accounts](#)

[Membership](#)

[Services](#)

[Resource Center](#)

Web Home Teller
and **FREE Online Bill Pay**
for personal accounts

Account Number

PIN



[Learn More](#) | [Forgot PIN?](#)



**Pick up
a great
auto loan.**

Apply online!

[click here >>](#)

Need help?

Call 812-855-7823

Toll Free 888-855-MYCU

Quick Links

What's New @ IUCU

Now is a great time to save!

9-Month Certificate @ 5.25% APY—Learn more

**Featured
Rates**

**Auto Loan Rates
as low as**

[Contact Us](#) | [Apply for a Loan](#) | [Become a Member](#) and more

 **6.00%**
APR

IU students pre-phishing via a prior attack



August 23, 2007

5 Clock Tower Place
Suite 500
Maynard, MA 01754
1-800-MONSTER

Dear Monster Customer:

Recently, a malicious software, known as Infostealer.Monstres, was used to gain unauthorized access to the Monster resume database. Regrettably, some of the contact information that was captured included your name, address, telephone number and email address.

As we move forward, I want to reassure you: We are taking swift and decisive action to address this situation and to leverage all of our resources, so we can implement a long-term remedy and protect the data that job seekers like yourself entrust to us. In fact, Monster Worldwide already has identified and shut down a rogue server that was accessing and collecting job seeker contact information through the use of compromised, legitimate employer-client log-in credentials.

At the same time, I ask that you remain alert for counterfeit "phishing" emails that may appear to come from Monster asking you to download software. Monster will NEVER ask you to download any software, "tool" or "access agreement" in order to use your Monster account.

© 2007 Monster Worldwide, Inc. All rights reserved. Monster, the Monster logo and "Your Future. Our Passion." are trademarks of Monster Worldwide, Inc. All other trademarks are the property of their respective owners.

A photograph of a person walking away from the camera in a dark, narrow tunnel. A bright light source from the front casts a long, dark shadow of the person onto the wet, reflective floor. The floor is covered in water droplets, creating a shimmering effect. The walls of the tunnel are dark and textured.

The attackers
better
organized and
equipped

learning and sharing





fend against these trends?

Email – The Gateway to Fraud

Bots –

Web – The Ecosystem for Malware

Targets – Precision in Execution



Lenny Zeltser

www.zeltser.com

lenny.zeltser@savvis.net