

Emerging Internet Security Threats in 2009

Lenny Zeltser

Senior Faculty Member, SANS Institute
Security Consultant, Savvis

Attackers and defenders are locked in an arms race.





The defender's position has a few disadvantages.

Social Engineering – The Foot in the Door

Attackers may gain the victim's trust by posing as a friend.

"I am now in United Kingdom on urgent business, I was robbed at my hotel...

Sorry i did not inform you about my traveling. I need you to **lend me with a sum of 1000 Dollars** urgently so that i can travel back home"

Yes, people have lost money through this scam.

“Woman Wires \$4K Abroad In Facebook Scam

ST. LOUIS -- A Missouri woman was tricked into wiring about \$4,000 to someone in England after receiving faked messages from a friend on Facebook asking for help, police said Wednesday.”

Source: The Associated Press

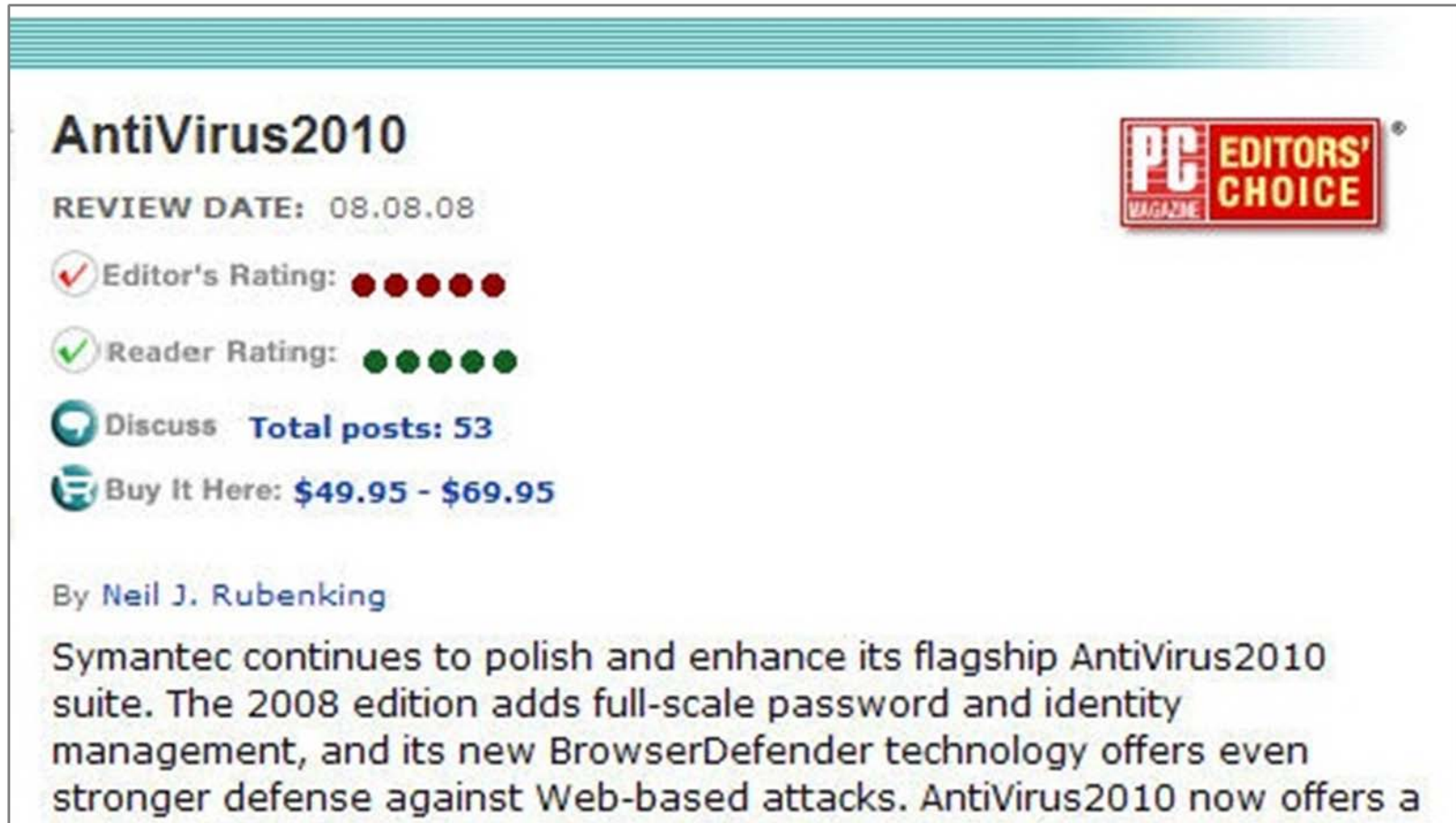
Scammers may employ the phone (VoIP) to lower the victim's guard.

"Dear MasterCard customer,

... we will never ask for personal account information via email or web pages... Please **call us immediately** at (615) 348-6681"


"We regret to inform you that we had to lock your account access. **Call** (567) 258-5114 to restore your bank account."

Malware may spoof product reviews.



AntiVirus2010

REVIEW DATE: 08.08.08



✓ Editor's Rating: ●●●●●

✓ Reader Rating: ●●●●●

Discuss **Total posts: 53**

Buy It Here: **\$49.95 - \$69.95**

By [Neil J. Rubenking](#)

Symantec continues to polish and enhance its flagship AntiVirus2010 suite. The 2008 edition adds full-scale password and identity management, and its new BrowserDefender technology offers even stronger defense against Web-based attacks. AntiVirus2010 now offers a

Source: Bleeping Computer

Malicious sites may customize the message based on your location.



REUTERS

Powerful explosion burst in New York this morning.

At least 12 people have been killed and more than 40 wounded in a bomb blast near market in New York. Authorities suggested that explosion was caused by "dirty" bomb. Police said the bomb was

The line between criminal physical and virtual worlds is fading.

PARKING VIOLATION

This vehicle is in violation of
standard parking regulations.

To view pictures with information
about your parking preferences,
go to **HORRIBLEPARKING.COM**

So What?

- **Your customers are being socially-engineered.**
- **Your employees, too.**
- **Increase awareness, but assume it will fail.**
- **Monitor and defend accordingly.**

Web – The New Operating System

Attackers continue to compromise websites via SQL injection.

```
Cookie: ref=ef';DECLARE @S VARCHAR(4000);SET  
@S=CAST(0x4445434C4152452040542076617263686172283  
23535292C404320766...
```

SQL encoded; delivered as a cookie;
targeted IE zero-day

Malicious sites may interact with victims' web applications.

CSRF

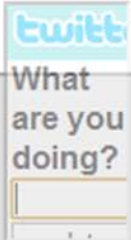
- Crafted links submit GET requests to authenticated applications.

Clickjacking

- The true destination of the click is the targeted link or button on the invisible frame.

Example: Proof-of-concept clickjacking for Twitter

Do you have a tiny face?



Yes

No

Exploit kits automate infection campaigns.



ZoPack

El-Fiesta

IcePack

Neosploit

AdPack

... and many others

Victims are targeted via malicious and obfuscated Flash ads.

```
movie 'advertisement.swf' {  
  frame 1 {  
    function () {  
      for (;;) {  
        for (;;) {  
          for (;;) {
```

ADVERTISEMENT



**NO Commissions
and NO Charges**

EASYFOREX™**LEARN MORE** 

HOME

THE MAGAZINE

INTERNATIONAL EDITION



▼ LOGIN / REGISTER

Newsweek

SEARCH SITE

WEB

Cover
Subscribe now
best onl

Attackers are paying more attention to social networking sites.

Secret video by

Rate: ★★★★★ 24 ratings **Views:** 941

From:
Joined: 1 year ago
Videos: 5

[Subscribe](#)

Added: **August 09, 2007** ([more info](#))

Embed: [Customize](#)

```
<object width="425" height="344"><param name="n
```

► **More From:**

▼ **Related Videos**

Your version of Flash player is out of date.
Please download this update.

[Download](#)

“LOL. You’ve been caught on hidden

So What?

- **Focus on strengthening your web applications.**
- **Make it hard to target your users via your application.**
- **Consider whether your developers actually care about security, though.**

Malware – Pursuing Data and Computing Power

Malware is a component of many data breaches.

Malware captured transitions that were not encrypted in transit.

Source: Heartland Payment Systems

Man planted malware to crash point-of-sale servers of retail companies.

Source: Department of Justice

10 Days of Torpig

Data Type	Number of Items
Mailbox account	54,000
Email address	1,200,000
Form data	12,000,000
Windows password	1,200,000
Other accounts	900,000

The Tigger trojan was indicative of feature-packed malware.

Deactivates debuggers

Disables anti-virus tools

Rootkit runs in safe mode

Takes screenshots

Captures passwords, cookies, certs

Sniffs the network

Observes browsers

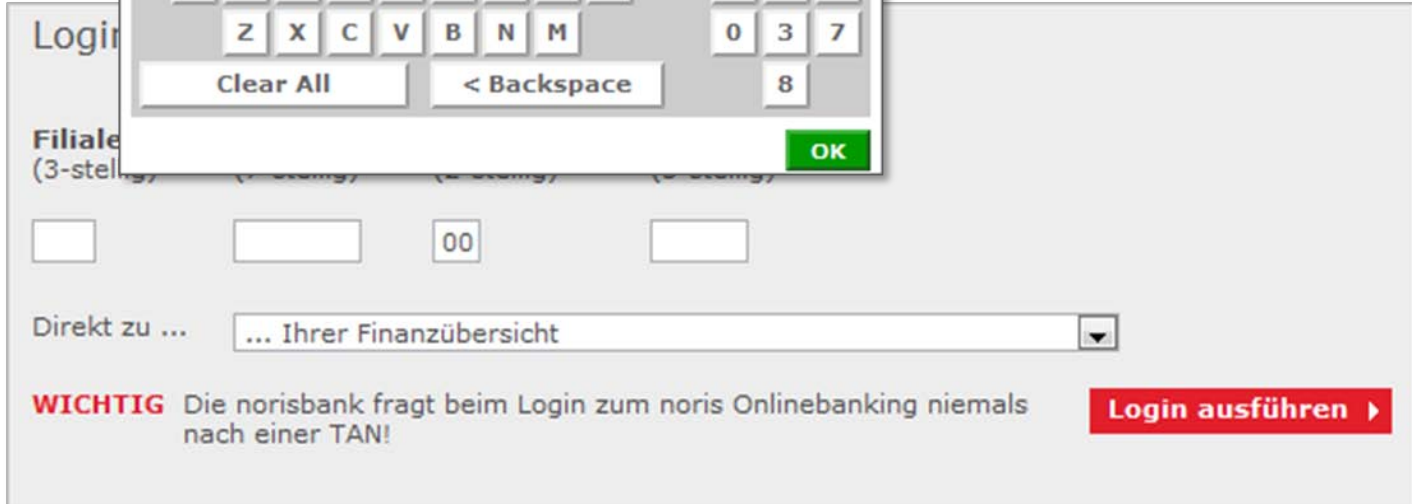
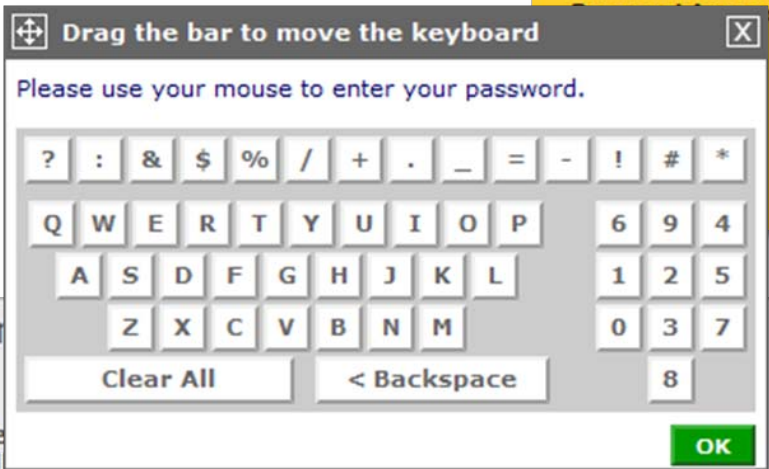
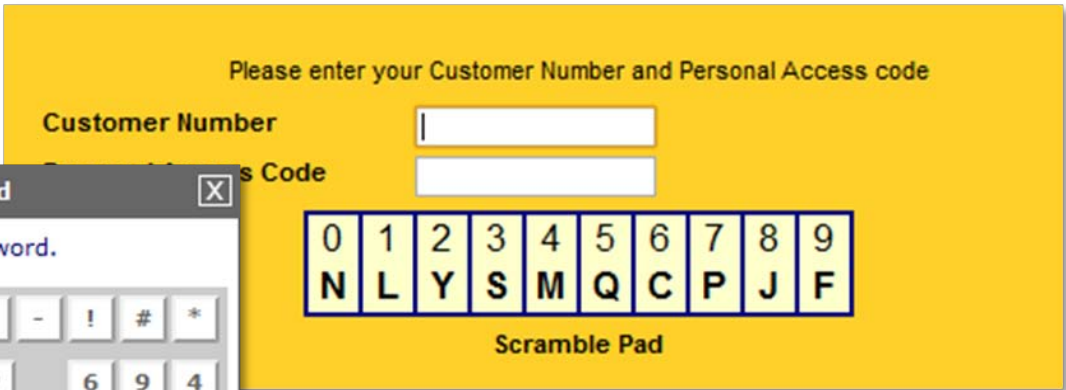
Logs keystrokes

Opens a backdoor

Removes other malware

Source: Michael Hale Ligh

A Limbo 2 trojan intercepted 2-factor auth and virtual keys.



Another trojan harvested one-time password card contents.

S.F.F. Confirme o Cartão De Segurança.

	1	2	3	4	5	6	7	8	
A	111	111	111	111	111	111	111	111	A
B	222	222	222	222	222	222	222	222	B
C	333	333	333	333	333	333	333	333	C
D	444	444	444	444	444	444	444	444	D
E	555	555	555	555	555	555	555	555	E
F	666	666	666	666	666	666	666	666	F
G	777	777	777	777	777	777	777	777	G
H	888	888	888	888	888	888	888	888	H

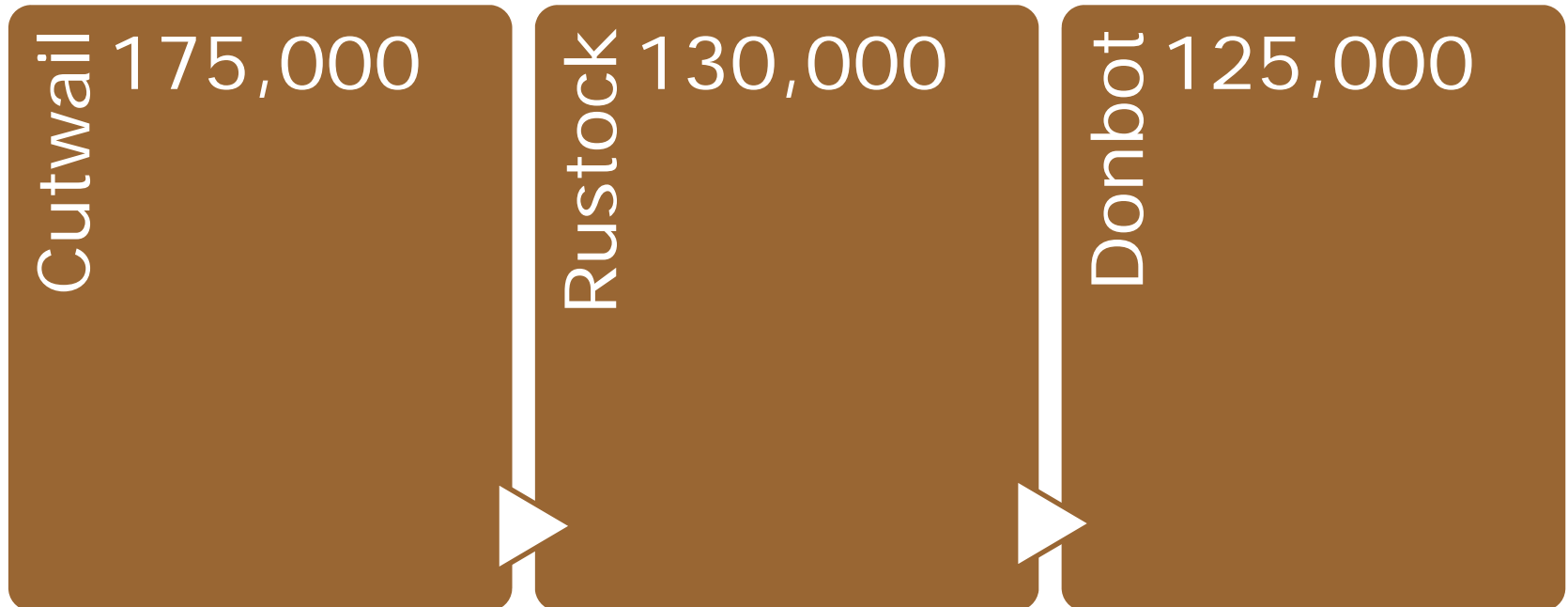
Microsoft Internet Explorer



Prezado Cliente, no momento estamos em manutenção. Para sua segurança, acesse nosso site dentro de algumas horas.

OK

Botnets offer crimeware-as-a-service (CaaS) for Spam, DDoS, etc.



Source: SecureWorks

Numerous entities offer malware installation services.

Victim's Location	Price per 1,000 installs
Asia	\$12
Europe	\$40
USA	\$140
Italy	\$150
Canada	\$200
UK	\$220

Price Source: InstallsForYou

So What?

- **Reassess the strength of your web app's authentication process.**
- **Understand what other process weaknesses malware may target.**
- **Consider scenarios where attackers have more computing power than you.**

Targets – Precision in Execution

Zero-day exploits target organizations.

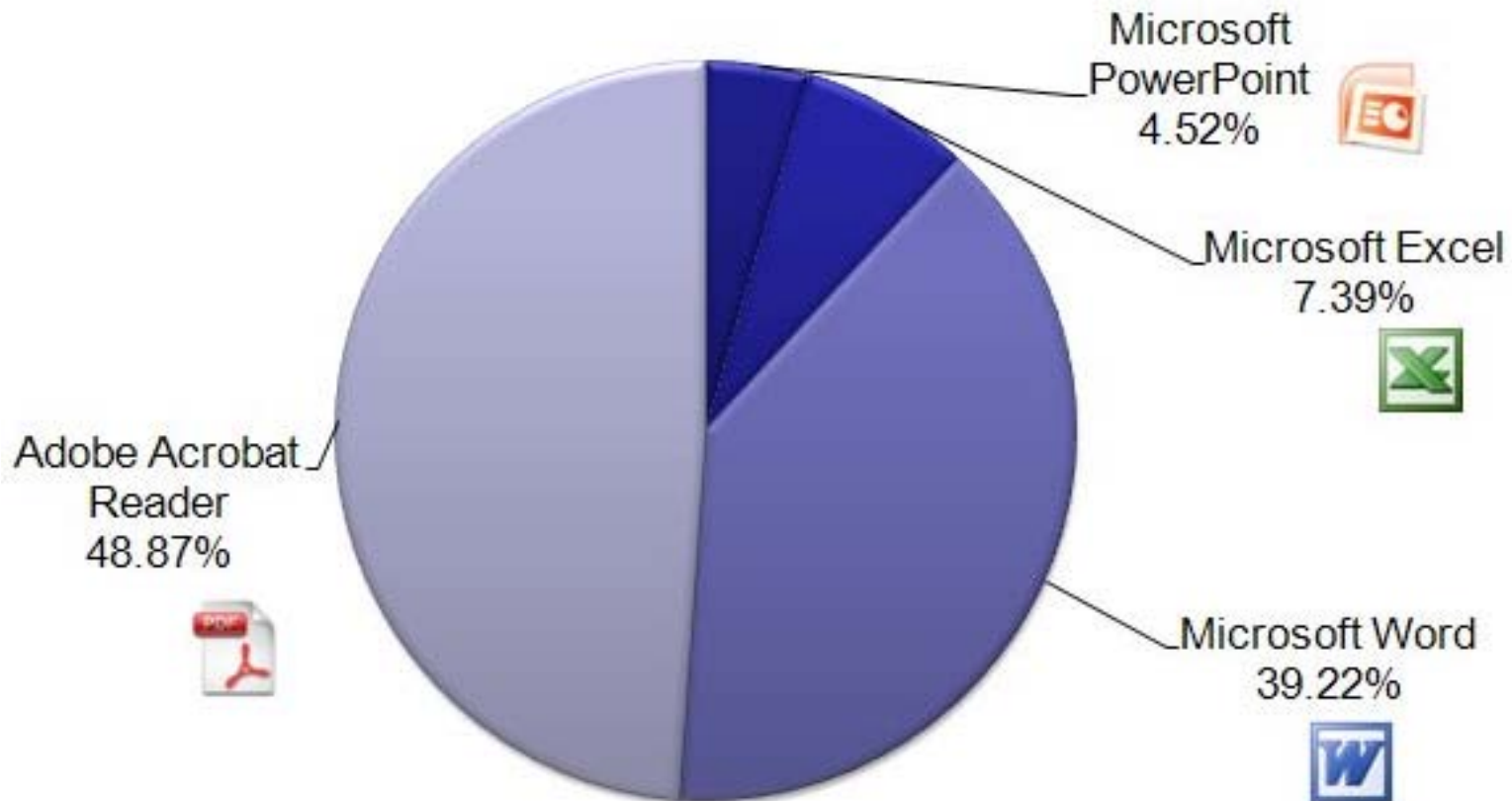
“public reports of a vulnerability in Microsoft Office Excel ... We are aware only of limited and **targeted attacks...**”

Source: Microsoft

“A critical vulnerability has been identified in Adobe Reader 9 and Acrobat 9 and earlier versions. ... **this issue is being exploited.**”

Source: Adobe

Targeted Applications in 2009



Attacks against pro-Tibet groups carried malicious attachments.

Spoofered as if from a trusted source.

ROWMAN & LITTLEFIELD
1-800-462-6420 • www.rowmanlittlefield.com

CHINA'S TIBET?
Autonomy or Assimilation
By Warren W. Smith, Jr.

**Order today
and SAVE
50% !***

"Warren Smith deserves a prize for this work. He has presented a clear-eyed, well-informed, and penetrating analysis of China's blatantly colonial policy in Tibet. If you want to understand the realities of the Tibet question, this book is a must read. You'll never again hear the oft-repeated phrase "China's Tibet" in quite the same way." —Robert Thurman, Columbia University

"This is a landmark study of China's efforts to fully subsume Tibet and to rewrite Tibetan history to conform to this official reality. Smith's dispassionate, critical, and detailed account makes clear China's goal of complete assimilation and the futility of the Dalai Lama's policy to seek some kind of

CHINA'S TIBET?
AUTONOMY OR ASSIMILATION

1 of 3



Executives at a
Swedish company
targeted via
spoofed emails.

Provided a
backdoor to
the attacker

Installed the Poison
Ivy trojan.



Fully controlled the
infected system.

Attackers targeted accounting and financial systems.

“Web-based commercial **EFT origination applications are being targeted** ... to circumvent online authentication methods. Illicitly obtained credentials can be used to initiate fraudulent ACH transactions and wire transfers...

Source: FDIC

So What?

- **Consider how your organization will detect a targeted attack.**
- **How will you respond to it?**
- **Combine the targeted scenario with social engineering and malware facets.**

Money – Commercialization of Threats

Spam fuels the Internet criminal economy.

Fast payouts, high degree of security... These are few reasons why **Golden Gate casino** is

Discounts and perfect prices only for you. Forget about problems with **ON line pharmacy!**

No experience required. Limited **homeworker opportunity.**

Try Fatblaster, product with natural herbal ingredients which do all work of fat burning for

Marketplace for stolen data is very active.

I'm a legit **drop for items** in US, you can trust me 100%, i also can **cashout**

Selling **Cvv2 & Full info** (US) - (FR) | Selling Host Hacked | Webmail | Selling **Fast VPN**

Spam All Banks UK / US

Selling **logins** good RDP / VNC

Marketplace for stolen data and malware is quite healthy.

Goods and Services	Prices
Bank accounts	\$10-\$1,000
Credit cards	\$0.40-\$20
Full identities	\$1-\$15
Email passwords	\$4-\$30
Proxies	\$1.50-\$30
Scams	\$2.5-\$50/week for hosting
Mailers	\$1-\$10

Price Source: Symantec

Extortion makes money and can take many forms.



Extortion occurred on social networking sites.

"A 16-year-old boy from Clackamas County, Ore., is accused of taking over the MySpace Facebook pages of two young women he knew and promising to **return control if they sent him nude pictures** of themselves."

Source: ABC News

Ransomware in the browser



Если рекламный модуль был вами установлен, но вы решили отказаться от подписки, то вам достаточно отправить смс на короткий номер, указанный ниже. Полученный код позволит вам удалить информер.

- 1 информер удалится автоматически через 30 дней.
- 2 бесплатный доступ к порно - видео архивам.
- 3 служба технической поддержки.

Чтобы удалить информер, отправьте смс с текстом **87654** на номер **9800**.

введите код, полученный в ответном смс

отправить

ВОЙТИ НА САЙТ



An extortionist demanded \$10 mil for 8 mil patient records.

"I have your shit! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. ... For \$10 million, I will gladly send along the password."

Source: WikiLeaks

Extortionists may launch DDoS attacks via botnets.



Example: A demand placed on a European gambling company (50,000 DNS requests/sec).

So What?

- **Consider how you will respond to an extortion demand.**
- **Will you pay up? Do you have law enforcement contacts?**
- **How likely are attackers to outspend you to get what they want?**



The attackers are organized and well-equipped.



The defenders need to keep learning
and sharing.





How does your security posture fend against these trends?

Social Engineering – The Foot in the Door

Web – The New Operating System

Malware – Pursuing Data & Computation

Targets – Precision in Execution

Money – Commercialization of Threats

Thought Exercise

Assume you're
compromised.

How will you detect,
respond, contain?





Lenny Zeltser

www.zeltser.com

twitter.com/lennyzeltser

lenny.zeltser@savvis.net

Thanks to our Sponsors



[Product trial download page](#)



[Free Whitepaper: Reduce shopping cart abandonment. Increase revenue.](#)