SearchFinancialSecurity.com
INFORMATION SECURITY
FINANCIAL INFORMATION SECURITY DECISIONS

Emerging Internet Security Threats in 2009

Lenny Zeltser

Senior Faculty Member, SANS Institute
Incident Handler, Internet Storm Center
Security Consultant, Savvis

Attackers and defenders are locked in an arms race.

Financial incentives encourage R&D investment in attacks.

Financial firms are at the forefront of the threat landscape... That's where the money is.

Social Engineering – The Foot in the Door

“Con-artists” let victims arrive at the expected conclusion.

“I found your [domain] name for sale on the web. Can you give me a price for the name in the subject line. …

Of course, we must be sure that you are engaging a reputable appraisal company…”

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…

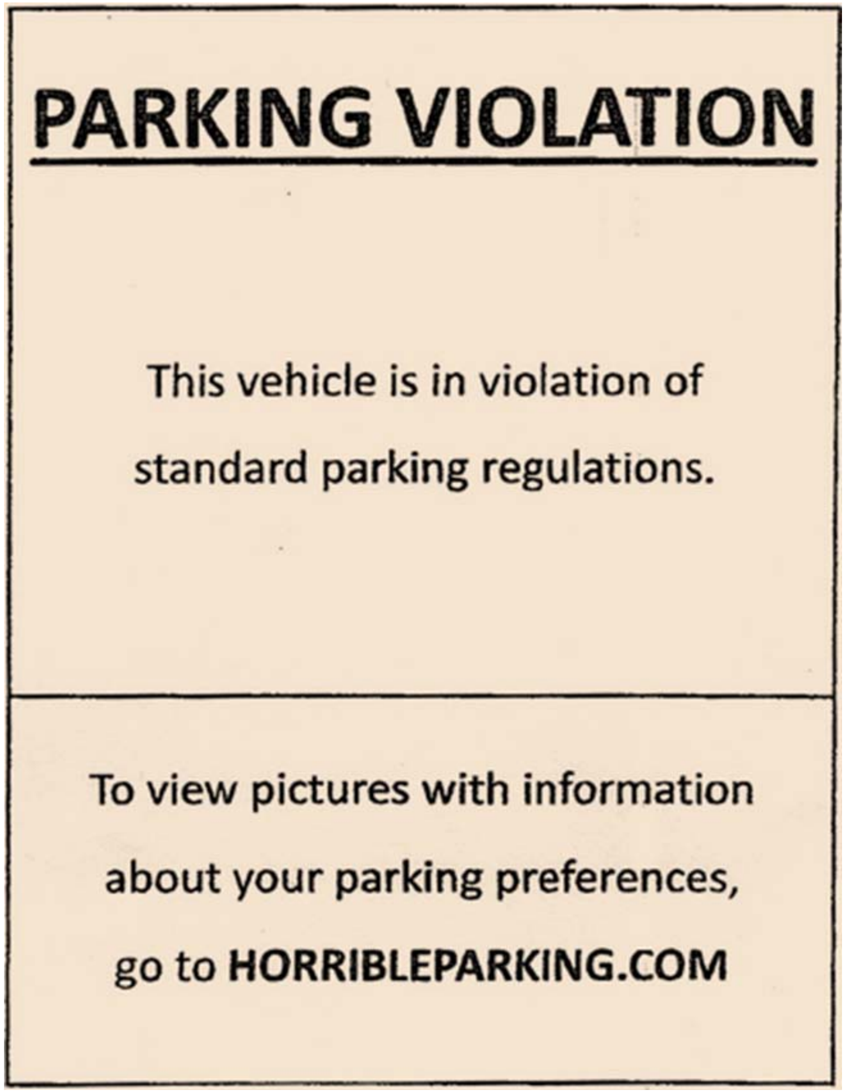
Sorry i did not inform you about my traveling. I need you to lend me with a sum of 1000 Dollars urgently so that i can travel back home”

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."

The line between criminal physical and virtual worlds is fading.

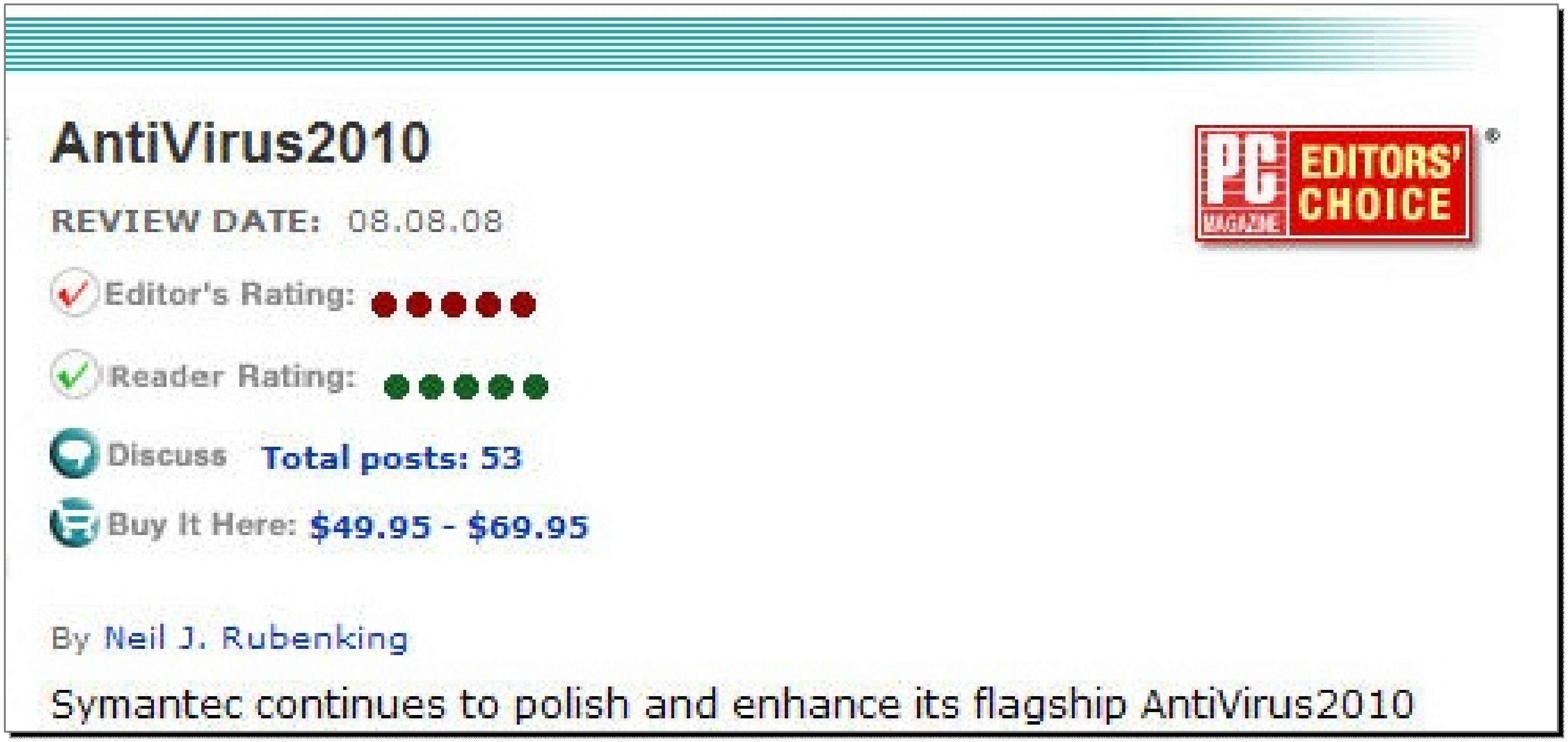


PARKING VIOLATION

This vehicle is in violation of
standard parking regulations.

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

Malware may spoof product review sites to legitimize a fake AV tool.



AntiVirus2010

REVIEW DATE: 08.08.08

Editor's Rating: ●●●●●

Reader Rating: ●●●●●

Discuss Total posts: 53

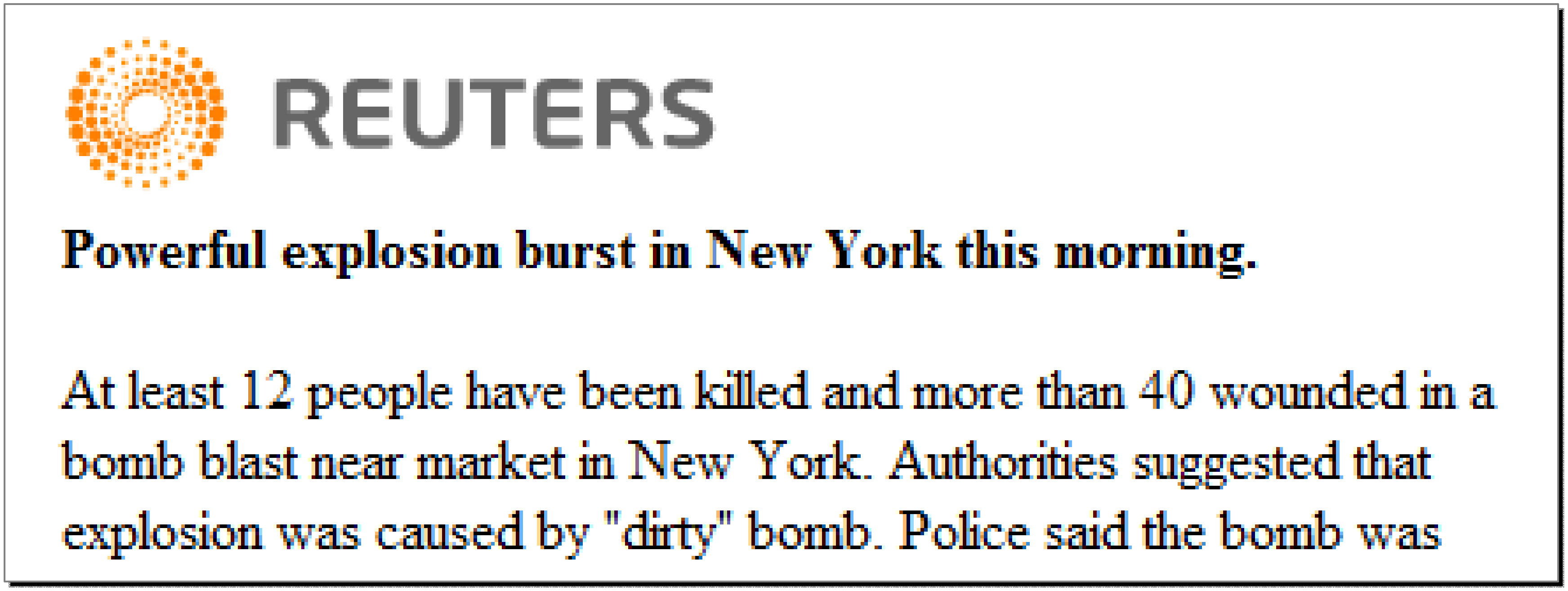
Buy It Here: $49.95 - $69.95

By Neil J. Rubenking

Symantec continues to polish and enhance its flagship AntiVirus2010

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

So What?

- Your customers are being targeted.
- Your employees, too.

- Increase awareness, but assume it will fail.
- Monitor and defend accordingly.

Web – The New Operating System

Attackers 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.

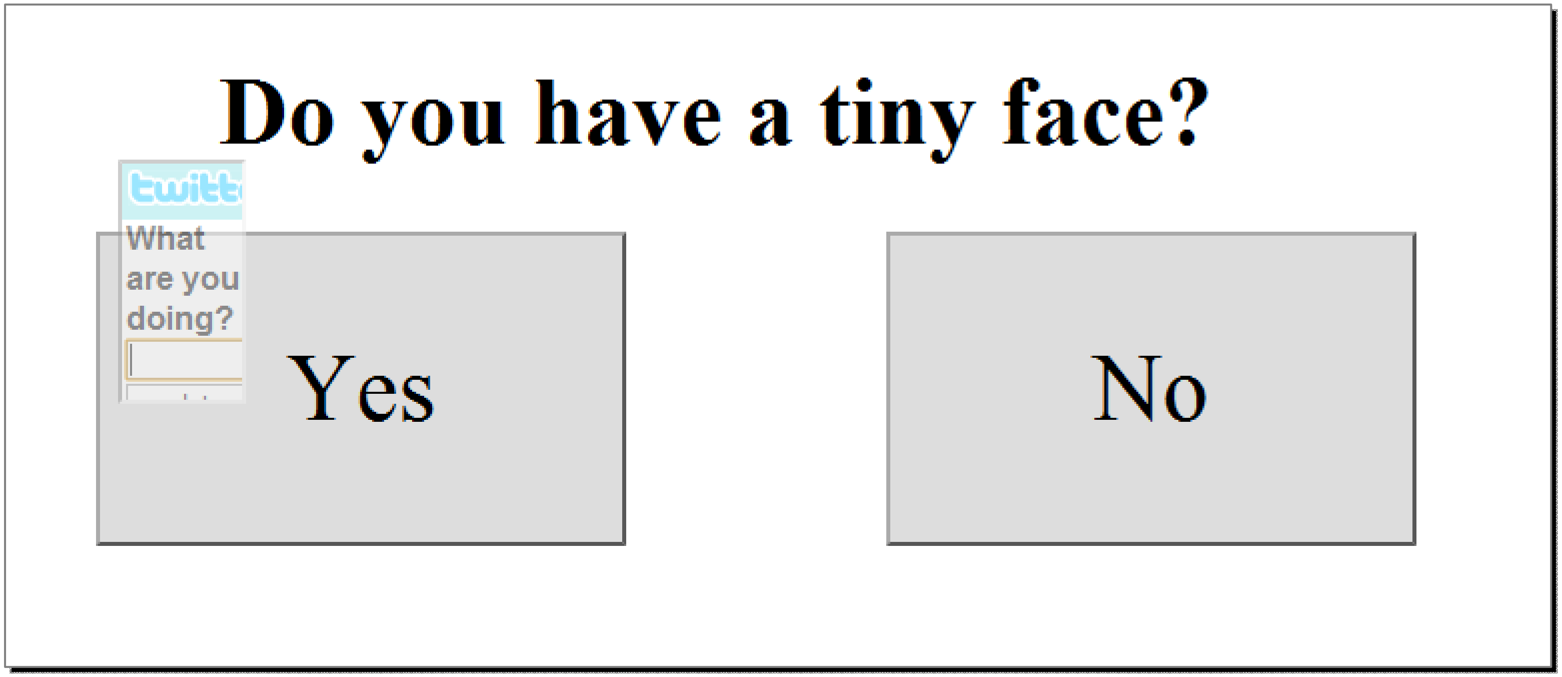
CSRF

- Crafted links submit GET requests to authenticated applications.

Clickjacking

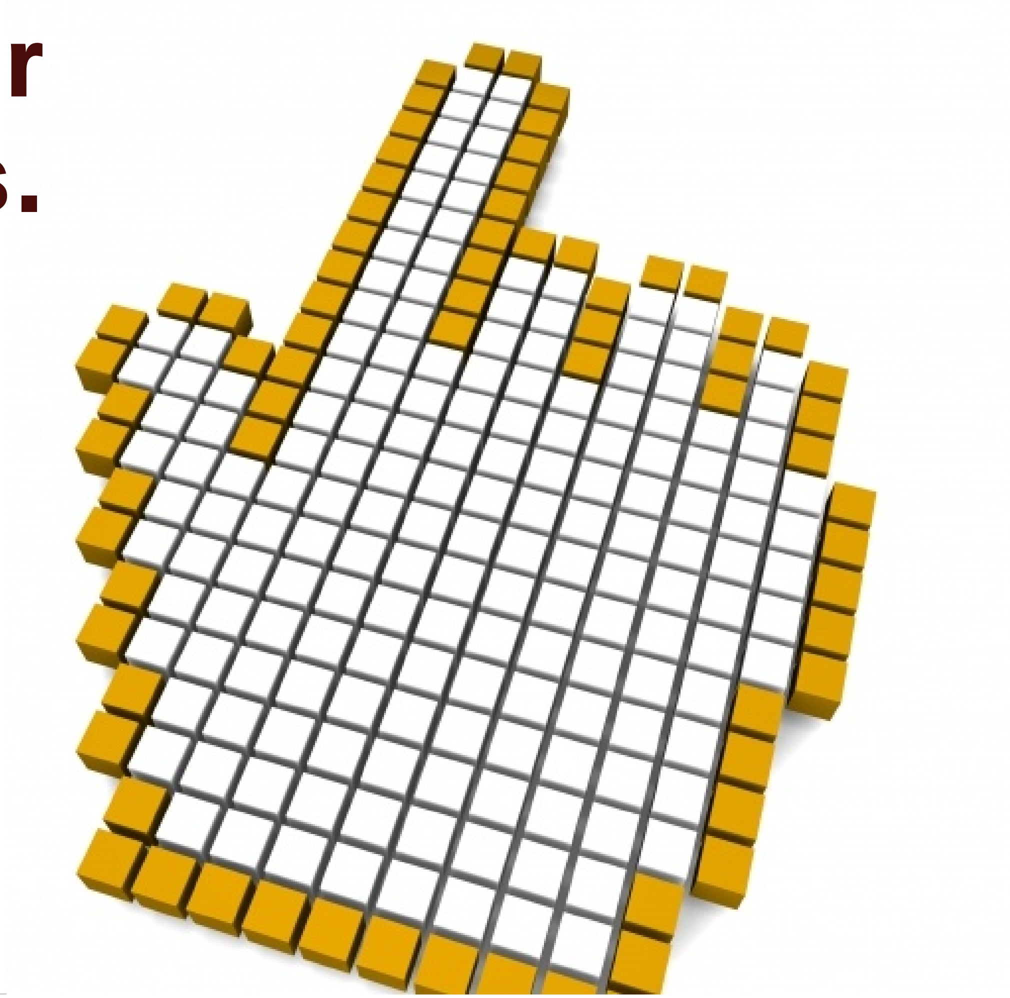
- The true destination of the click is the targeted link or button on the invisible frame.

Example: Proof-of-concept clickjacking for Twitter.

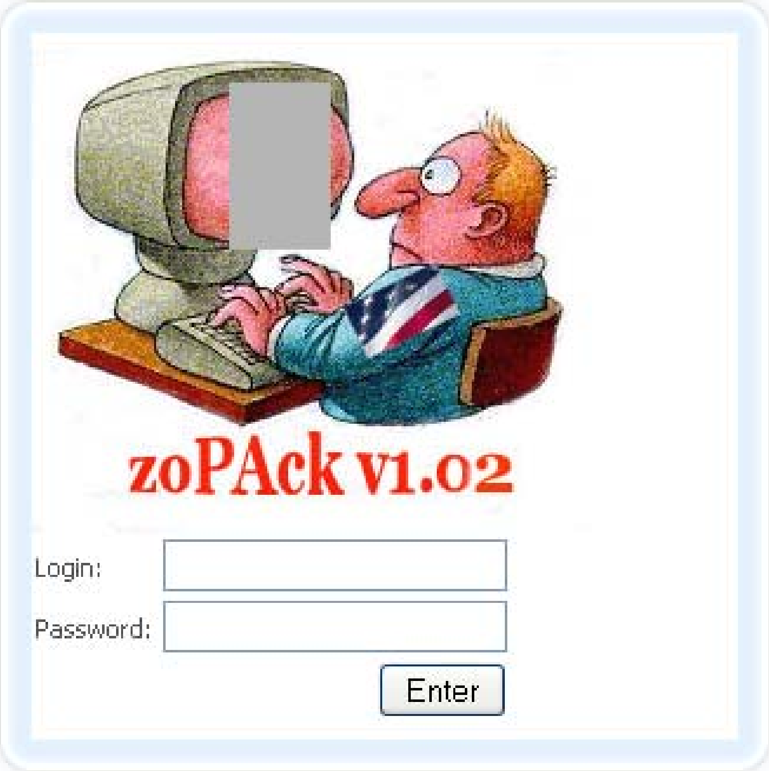


Do you have a tiny face?

Drive-by infections target browser vulnerabilities.



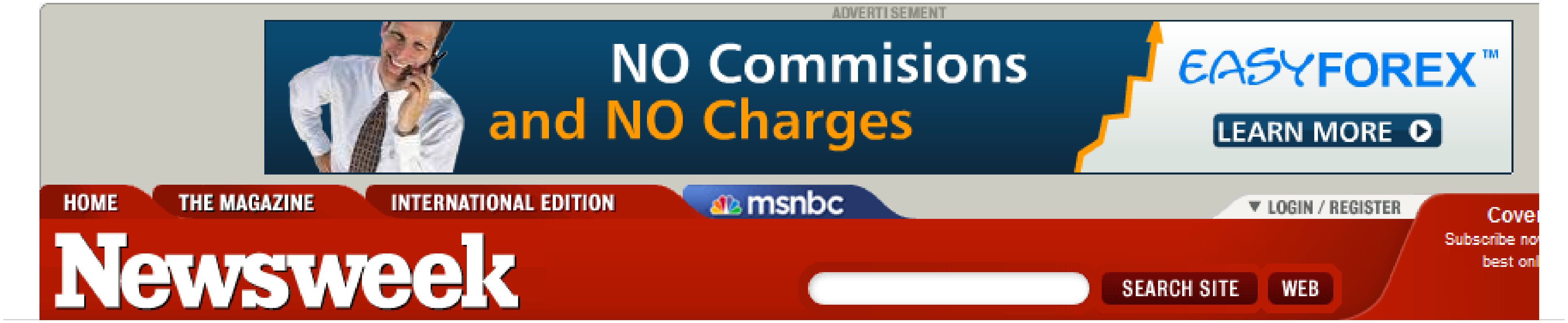
Exploit kits automate infection campaigns.



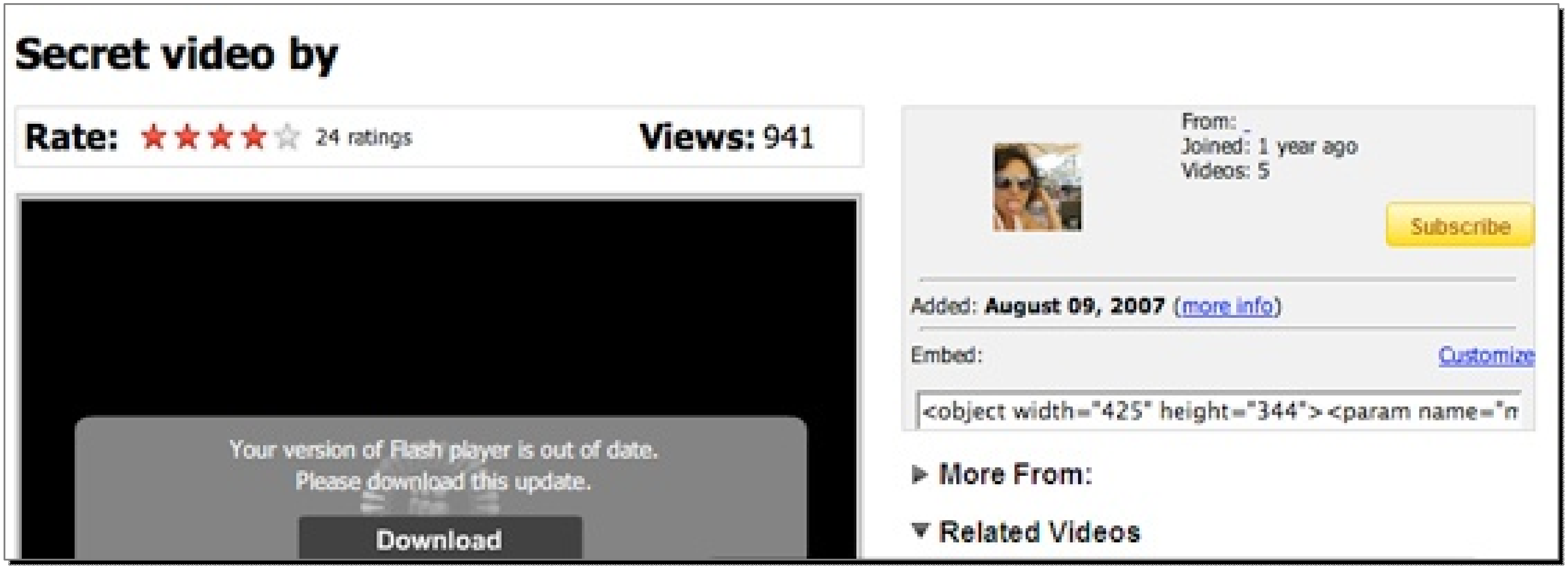
- ZoPack
- El-Fiesta
- IcePack
- Neosploit
- AdPack
- … and many others

Victims are targeted via malicious and obfuscated Flash ads.

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



Attackers are paying more attention to social networking sites.



Secret video by

Rate: ★★★★☆ 24 ratings

Views: 941

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

From: _
Joined: 1 year ago
Videos: 5

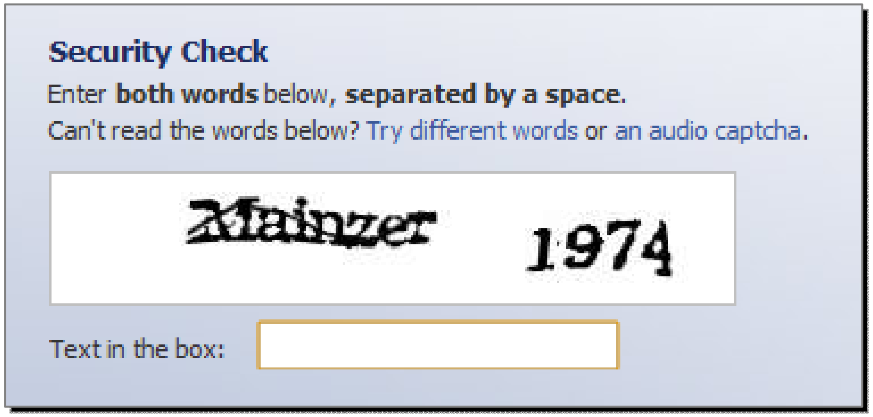
Added: August 09, 2007 (more info)

Embed:

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

“LOL. You’ve been catched on hidden cam, SearchFinancialSecurity.com INFORMATION SECURITY FINANCIAL INFORMATION SECURITY DECISIONS

Attackers solve CAPTCHAs to access websites automatically.



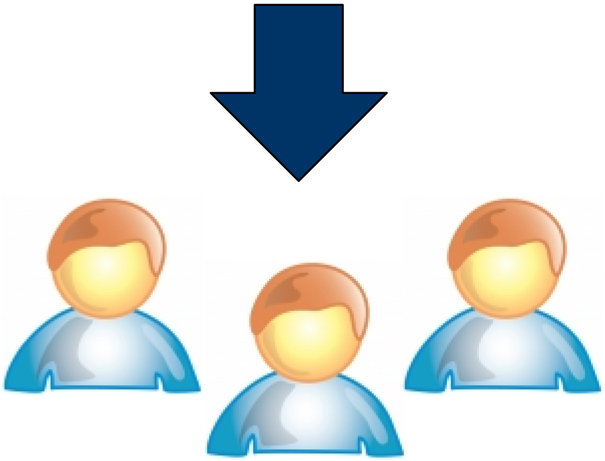
Security Check

Enter **both words** below, **separated by a space.**

Can't read the words below? Try different words or an audio captcha.

Mainzer 1974

Text in the box:



Human labor supplements botnet CAPTCHA efforts.

“Work for students. Looking for persons to recognize images. Get paid $4 for every 1,000 images recognized. From past experience, it takes about 1 hour to recognize 1,000 pictures, so you could earn $60-70 after a hard day’s work.”

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 accoun	900,000

UC Santa Barbara

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

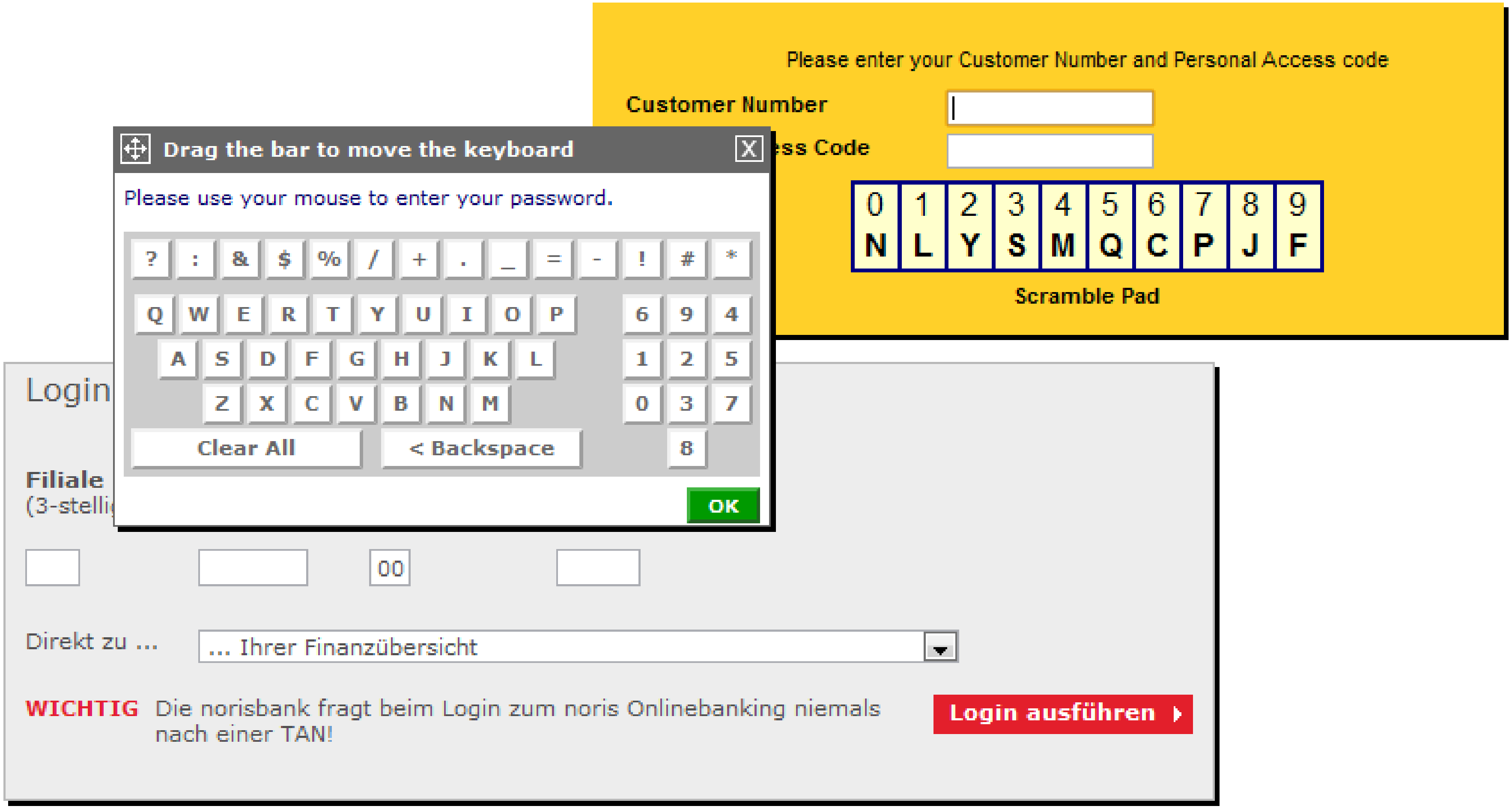
Logs keystrokes

Opens a backdoor

Removes other malware

Source: Michael Hale Ligh

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



Please enter your Customer Number and Personal Access code

Customer Number

ess Code

0	1	2	3	4	5	6	7	8	9
N	L	Y	S	M	Q	C	P	J	F

Scramble Pad

Drag the bar to move the keyboard

Please use your mouse to enter your password.

Login

Filiale
(3-stelli

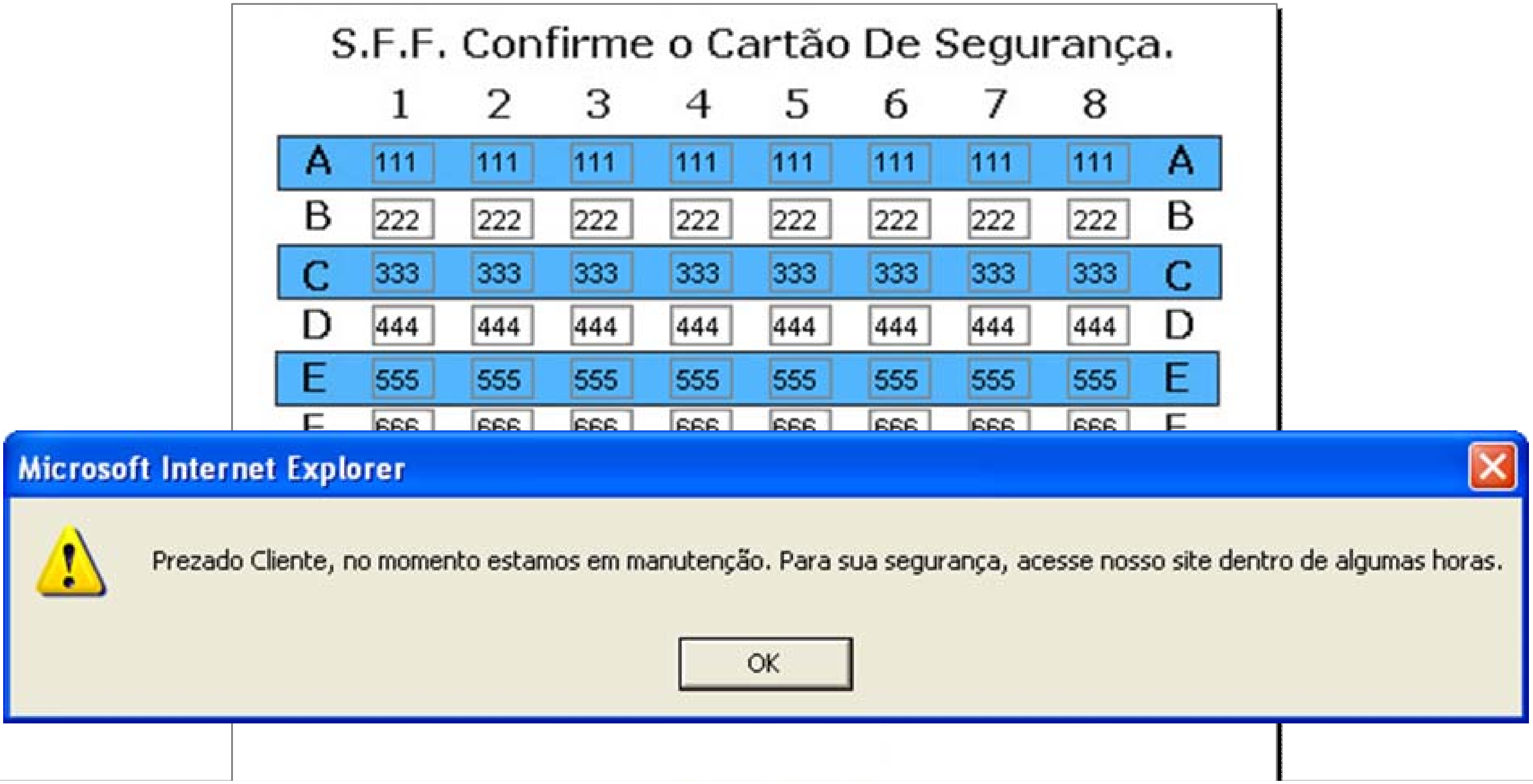
00

Direkt zu ...

... Ihrer Finanzübersicht

WICHTIG Die norisbank fragt beim Login zum noris Onlinebanking niemals nach einer TAN!

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

Microsoft Internet Explorer

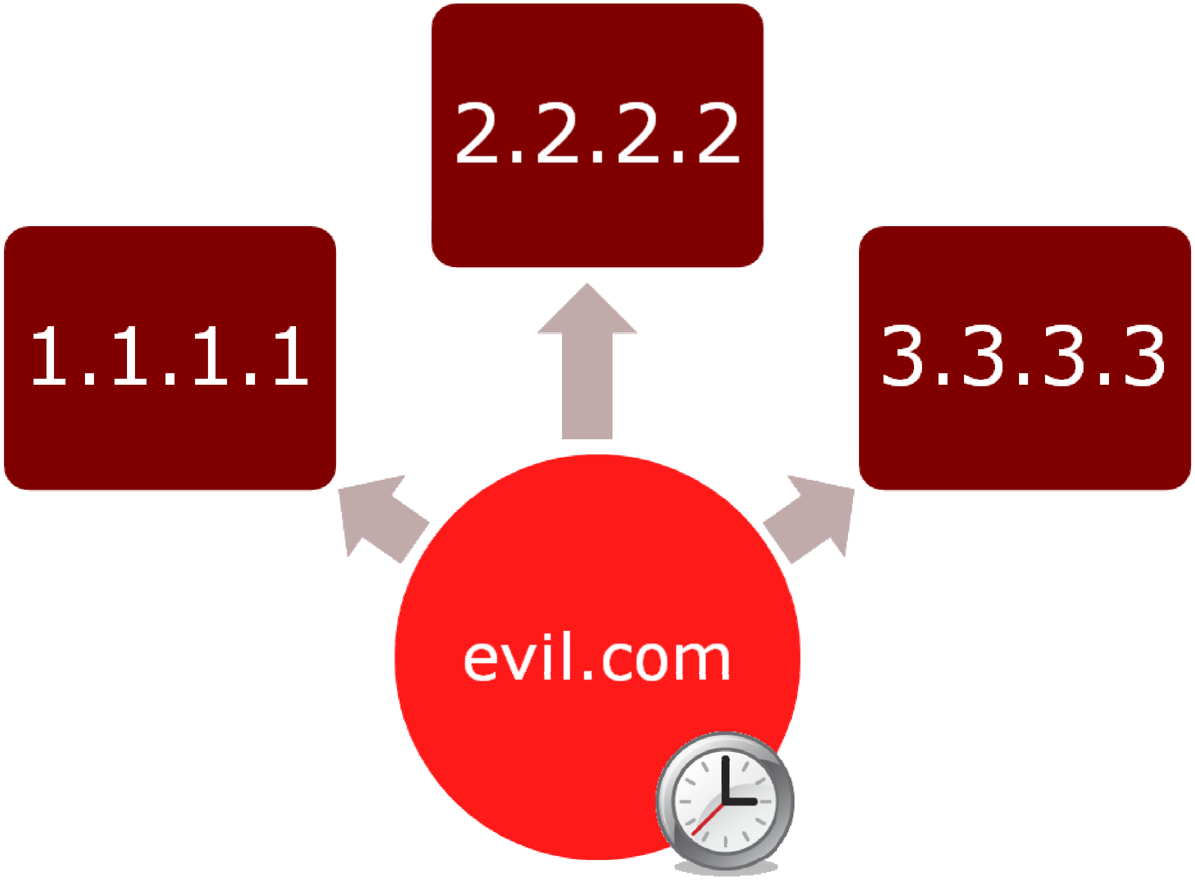
Prezado Cliente, no momento estamos em manutenção. Para sua segurança, acesse nosso site dentro de algumas horas.

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

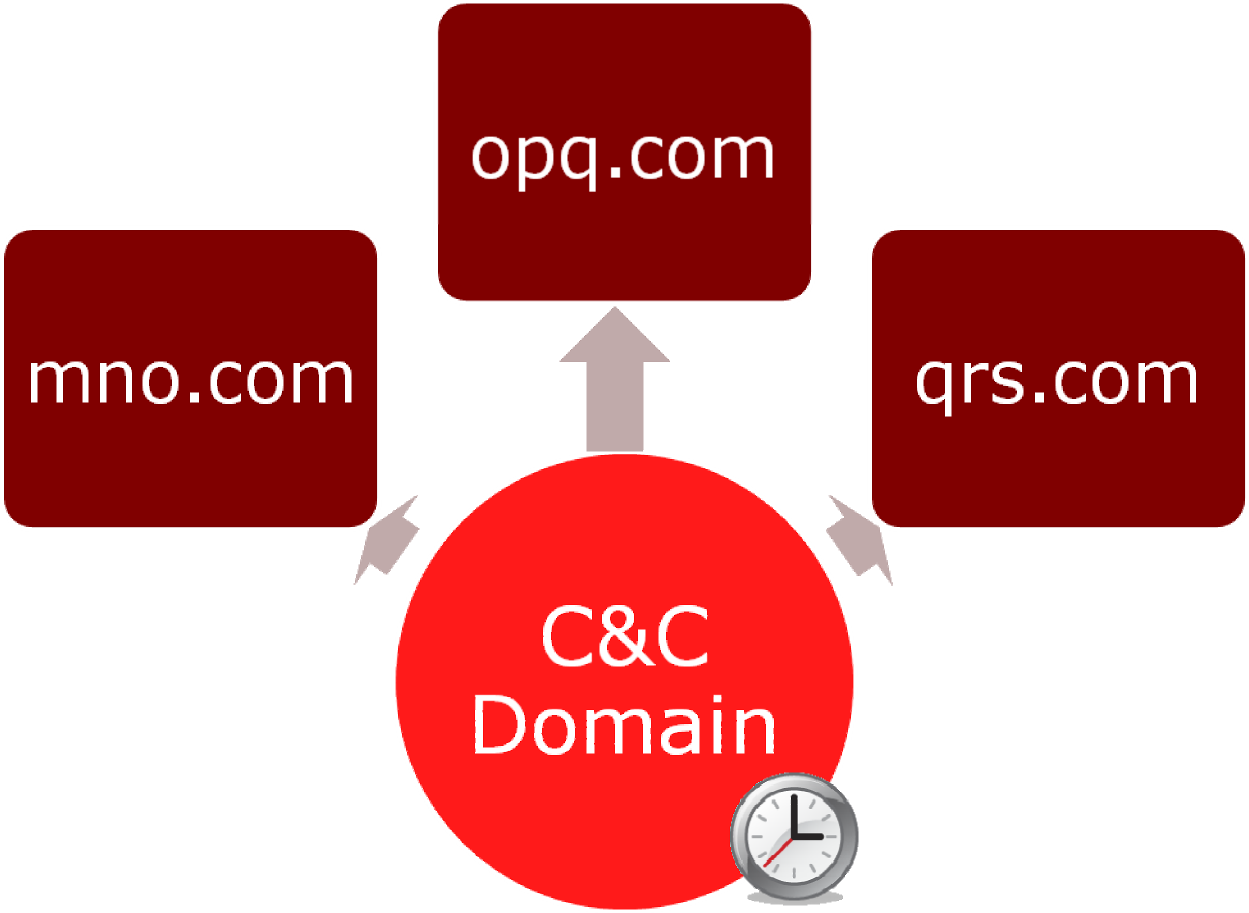
Cutwail	175,000
Rustock	130,000
Donbot	125,000

Source: SecureWorks

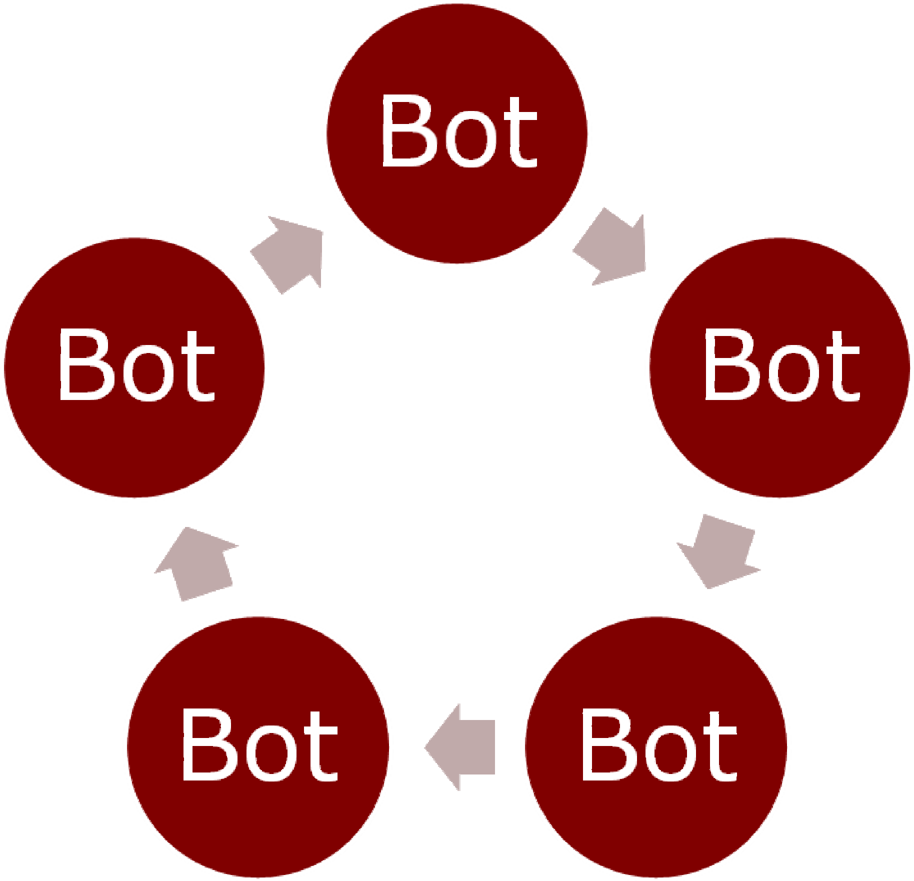
Fast flux DNS complicates tracking of botnets and malicious sites.



Bots may generate C&C domain names on the fly via an algorithm.



Some botnets use P2P, without a central node.



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

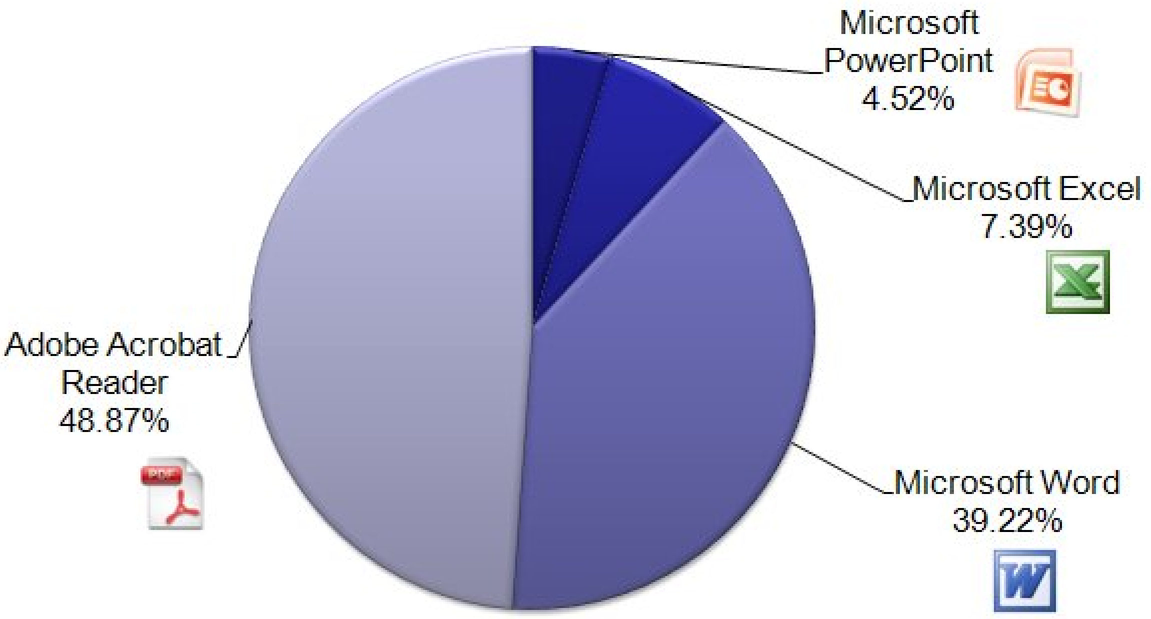
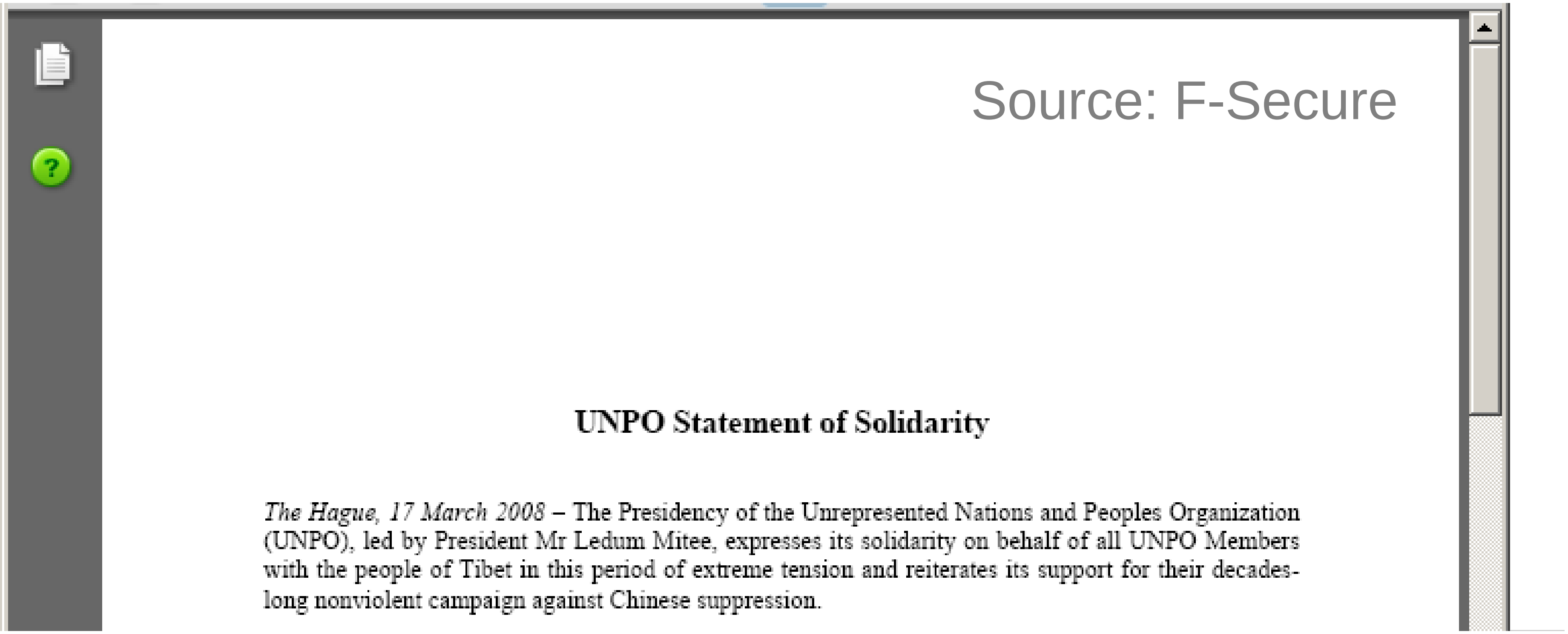


Image Source: F-Secure

Focused, polished attacks on pro-Tibet groups.

Documents attached to emails carried exploits.

Spoofed as if from a trusted source.



Source: F-Secure

UNPO Statement of Solidarity

The Hague, 17 March 2008 – The Presidency of the Unrepresented Nations and Peoples Organization (UNPO), led by President Mr Ledum Mitee, expresses its solidarity on behalf of all UNPO Members with the people of Tibet in this period of extreme tension and reiterates its support for their decades-long nonviolent campaign against Chinese suppression.

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.

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

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

Source: Symantec

Marketplace for stolen data and malware is very 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/week - $50/week for hosting
Mailers	$1-$10

Source: Symantec

One could get paid for installing spyware.

Country	Price ($US)
US	$50
UK	$60
Italy	$60
Spain	$25
Asia	$3

Source: MessageLabs

Prices per 1,000 downloads.

Spam fuels the Internet criminal economy.

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

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 you.

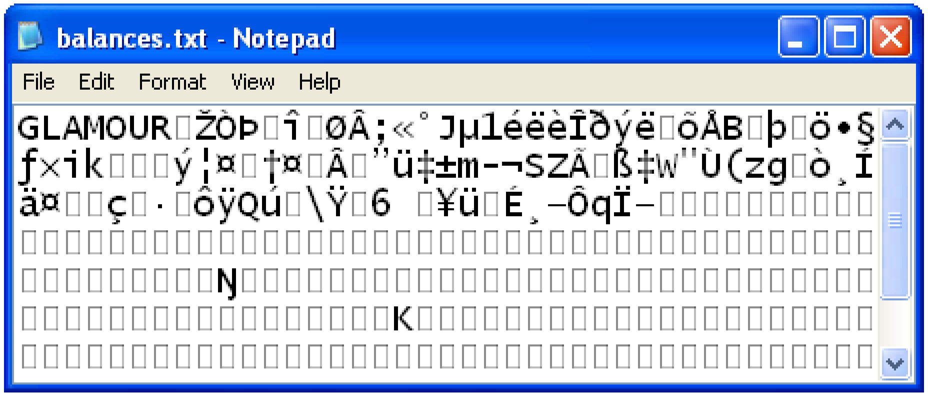
Pump-and-dump is profitable.

Ramanathan traded via compromised brokerage accounts.

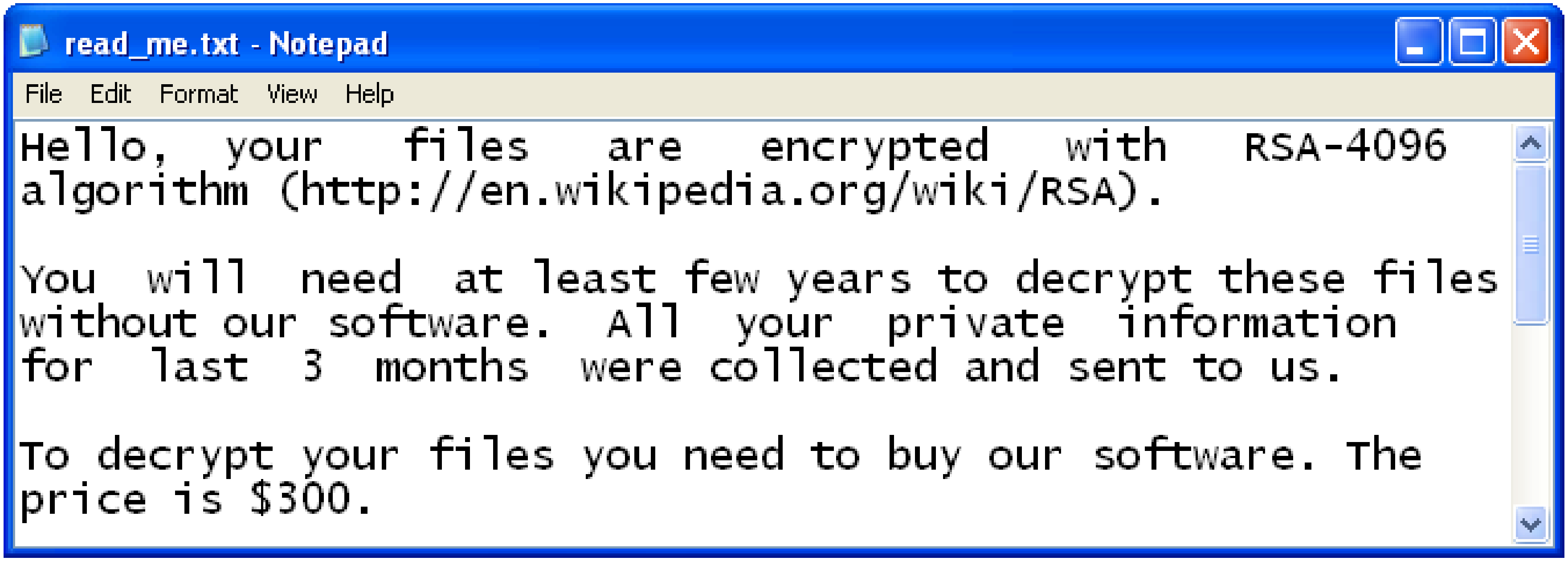
Extortion makes money and takes many forms.

Cañón del S.XVIII,cedido por
la Autoridad Portuaria de
Gijón, utilizado como bolardo
en el Dique de Sta.Catalina
desde 1864 hasta 1987

Gpcoder encrypted local files.



```
GLAMOUR□ŽÒÞ□î□ØÂ;«˚JµléëèÎðýë□õÅB□þ□ö•§
ƒ×ik□□□ý¦¤□†¤□Â□”ü‡±m-¬SZÃ□ß‡W"Ù(zg□ò¸Í
ä¤□□ç□·□ôÿQú□\Ÿ□6 □¥ü□É¸–ÔqÏ–□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□Ŋ□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□K□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

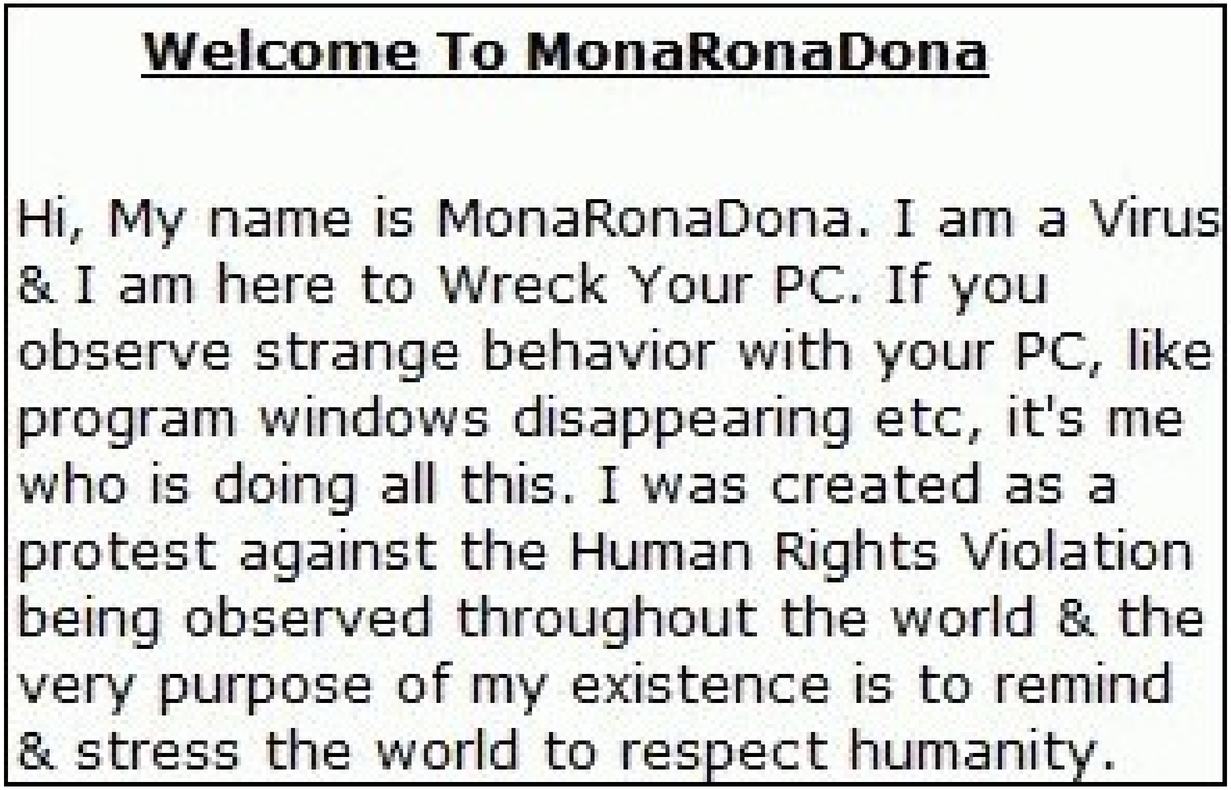


Hello, your files are encrypted with RSA-4096 algorithm (http://en.wikipedia.org/wiki/RSA).

You will need at least few years to decrypt these files without our software. All your private information for last 3 months were collected and sent to us.

To decrypt your files you need to buy our software. The price is $300.

MonaRonaDona wanted the victim to search for a removal tool.



Welcome To MonaRonaDona

Hi, My name is MonaRonaDona. I am a Virus & I am here to Wreck Your PC. If you observe strange behavior with your PC, like program windows disappearing etc, it's me who is doing all this. I was created as a protest against the Human Rights Violation being observed throughout the world & the very purpose of my existence is to remind & stress the world to respect humanity.

Image Source: Washington Post

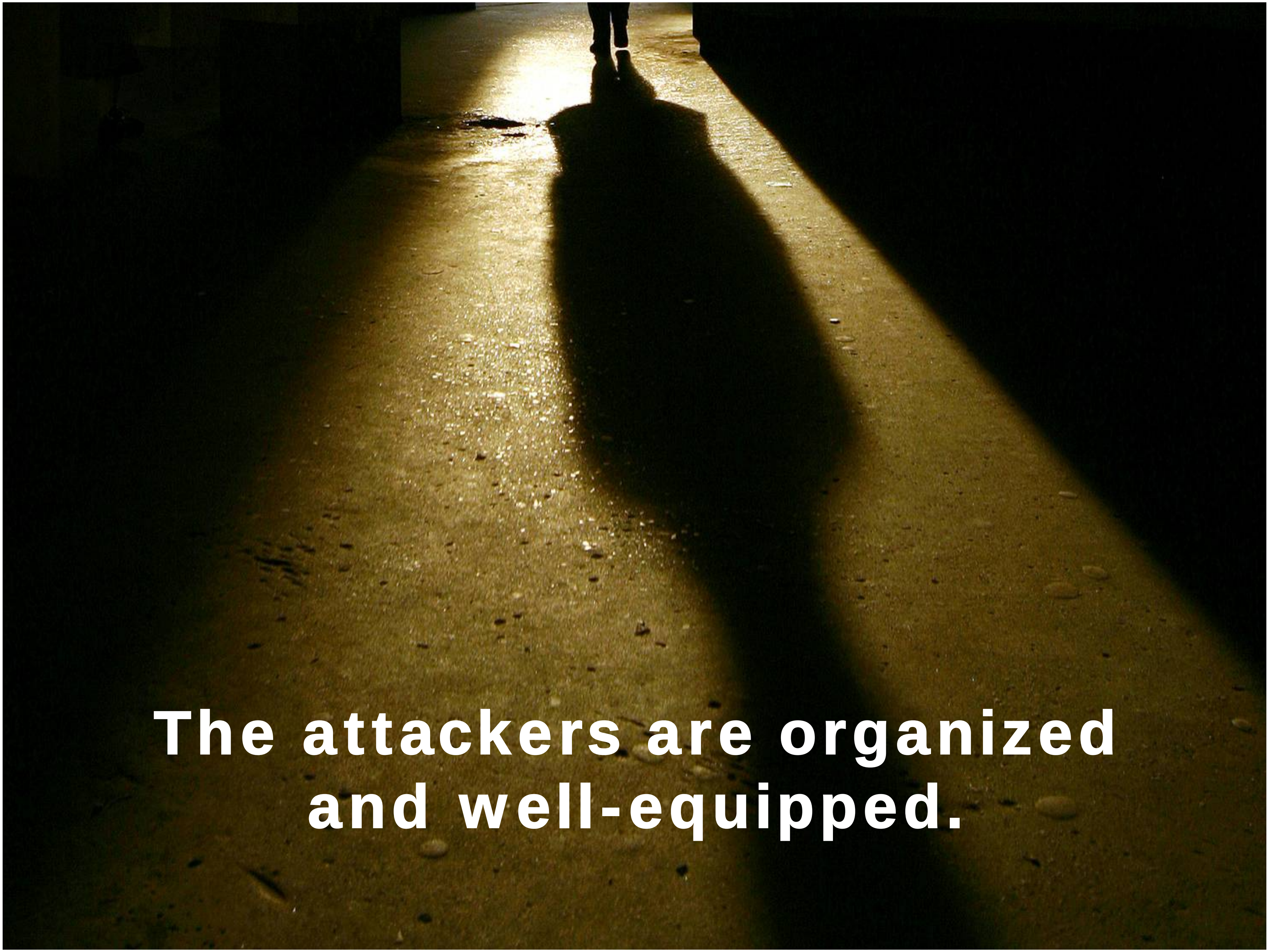
An extortionist demanded $10 mil for 8 mil patient records.

> “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).



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

Lenny Zeltser

www.zeltser.com
twitter.com/lennyzeltser
lenny.zeltser@savvis.net