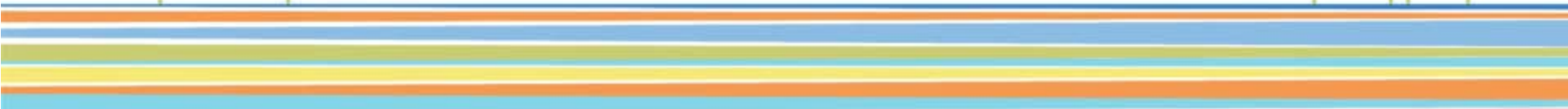


How attackers use social engineering to bypass your defenses.

Lenny Zeltser

Senior Faculty Member, SANS Institute
Product Management Director, NCR Corporation



Social engineers influence victims to perform actions desired by the attacker.

As the result:

Outsider == Insider

What social engineering tactics are being used?

Let's look at examples, so we can learn from them.

Alternative Channels

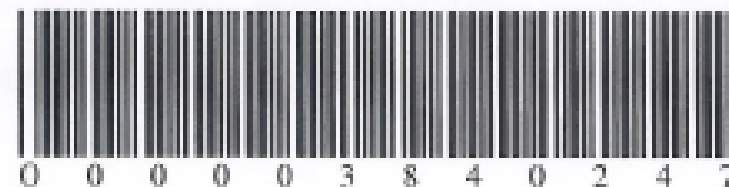
Notices in the “physical” world invited victims to visit a fraudulent website.

PARKING VIOLATION

This vehicle is in violation of
standard parking regulations.

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

**Registration of the International Trademark
RENEW**



A 2010/3840247/317423



CANADA

Registration Number:

3,840,247

Publication Date:

2010/08/31

International Class(es):

9

By Cheque

Beneficiary: WDTP s.r.o.

Address: P.O.BOX 652, CZ-66152 Brno, Czech Republic

By Credit Card

Visit URL: <http://app.wipd.biz/pay/1000317423>

4164

va, Slovak Republic

Wire transfer, cheque or credit card. Don't forget to quote the order number: 1000317423

Phishing scam directed the target to a phone number.

“Your card has been suspended because we believe it was accessed by a third party. Please press 1 now to be transferred to our security department.”

Customers of Liberty Bank of Boulder Creek, CA

Source: BankInfoSecurity <http://j.mp/3Gj0AA>

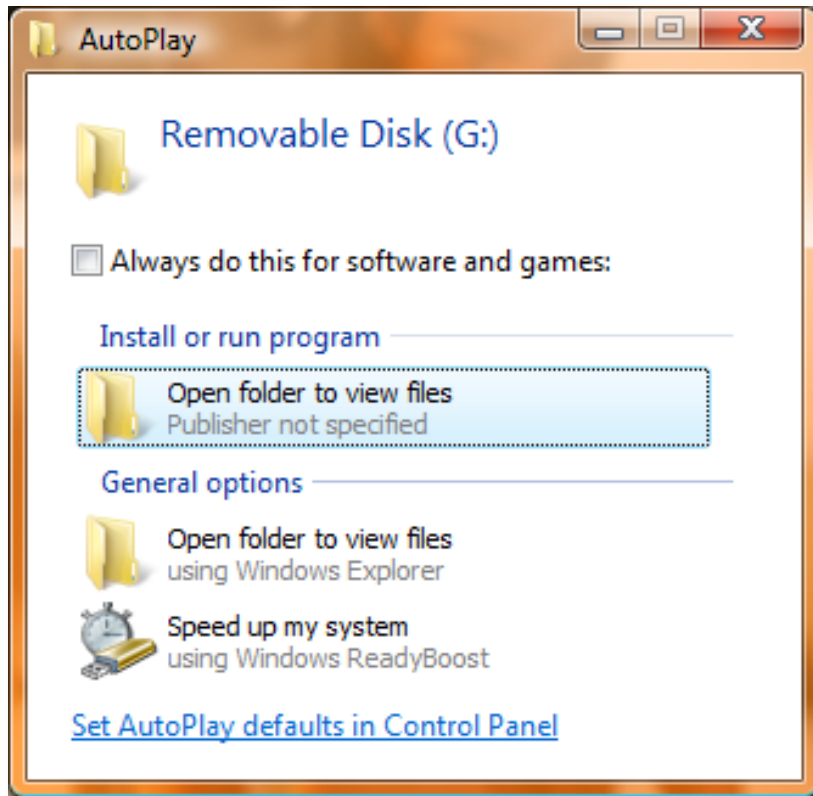
USB keys were used as an infection vector.

Action=Open folder to view files

Icon=%systemroot%\system32\shell32.dll,4

ShellExecute=. \RECYCLER\S-5-3-42-28199...

(Conficker)



“Real world” procedures were used to place malicious ads on Gawker sites.

A similar scam targeted the New York Times and other media sites.



Yes,
two 5
al
Crash



Feds Recall Lexus,
Toyota Floor Mats
Due To Potential
For Fiery Death



The Full List Of
Every Cash For
Clunkers Trade-In



The ads served PDF exploits to visitors.

History
2014
2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
2003
2002
2001
2000
1999
1998
1997
1996
1995
1994
1993
1992
1991
1990
1989
1988
1987
1986
1985
1984
1983
1982
1981
1980
1979
1978
1977
1976
1975
1974
1973
1972
1971
1970
1969
1968
1967
1966
1965
1964
1963
1962
1961
1960
1959
1958
1957
1956
1955
1954
1953
1952
1951
1950
1949
1948
1947
1946
1945
1944
1943
1942
1941
1940
1939
1938
1937
1936
1935
1934
1933
1932
1931
1930
1929
1928
1927
1926
1925
1924
1923
1922
1921
1920
1919
1918
1917
1916
1915
1914
1913
1912
1911
1910
1909
1908
1907
1906
1905
1904
1903
1902
1901
1900

History Login



For Tokyo, Subaru revealed the WRX STI Carbon. It takes the Subaru WRX STI, replaces the regular roof with carbon fiber, adds suede seats to enhance "driving excitement" and the JDM-spec automatic transmission. More »

Comment on [Subaru's 2011 WRX STI Carbon](#) (10 comments) | [Subaru's 2011 WRX STI Carbon](#) is the article... | [Full list of comments...](#) | [Other threads](#)

Image Source: Business Insider
<http://j.mp/lwnntL>

Chrysler brand will handle Fiat 500 in U.S. [Car Tech: an Automotive Blog from CNET]

Navigation and social media icons including arrows, a search icon, and social media icons for Facebook, Twitter, and YouTube.

“We want to run a performance campaign for Suzuki across your network. Our budget to start is \$25k+. Campaign should be live by the end of the month.”

Scammers called home users to help disinfect their PCs.

They pretended to find malware and clean it up; requested payment and other details.

“i got a call off a onlinepcdoctors.com and they said my pc was running slower because of malcious [sic] files. i let them take remote access of my computer...”



PC SUPPORT @ YOUR FINGERTIPS

GET AN OPPORTUNITY TO LEARN THE BEST TECH TRICKS

FIX YOUR PC IN MINUTES

WITH OUR EXPERTS YOU CAN GET:

FOCUSSED: WITH FULL FOCUS AND ATTENTION TO YOUR PC

FRIENDLY: C

FUN: HA

FAST: PRO

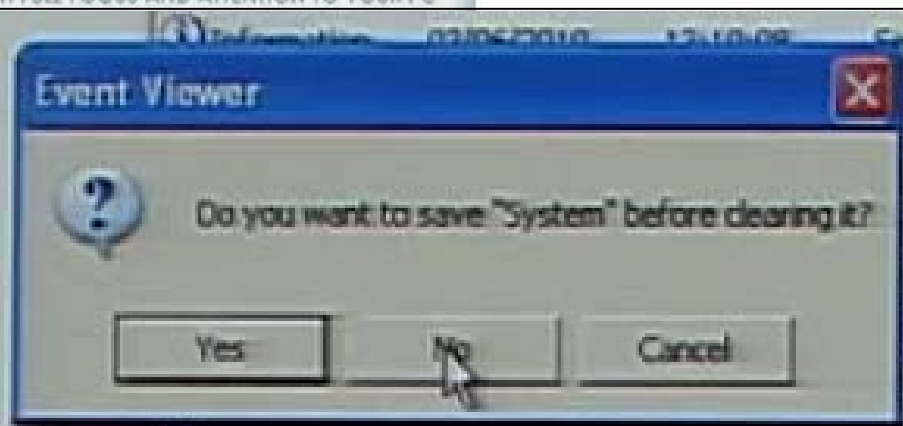
Welcome to **Online PC**

Let Us Call You

Name

Email

Phone



Event Viewer

Do you want to save "System" before clearing it?

Yes [] Cancel []

Information	03/06/2010	11:46:53	Service Control Manager	No
Information	03/06/2010	11:46:36	Service Control Manager	No
Information	03/06/2010	11:46:36	Service Control Manager	No
Information	03/06/2010	11:44:33	Service Control Manager	No
Information	03/06/2010	11:44:33	Service Control Manager	No
Information	03/06/2010	11:42:16	Service Control Manager	No
Information	03/06/2010	11:42:16	Service Control Manager	No

Zeus on a Windows PC asked victims to install a security program on their Android phones.

Due to the becoming more frequent internet fraud cases with text messages it is strongly recommended to the customers owning mobile phones with Android OS to install a special application which will help to protect you from fraud.

For the software installation open the internet browser on the mobile and enter the following address:

[http://\[REDACTED\].com/tr.apk](http://[REDACTED].com/tr.apk)

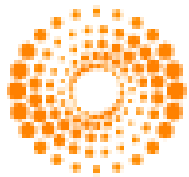
When the installation is completed you'll see a new program called "Trusteer Rapport" Application folder on your mobile. You need to start the program then enter the activation code indicated there into the field below and press "Activate".

Activation code:

Activate

Personally-Relevant Messaging

Malware spread by localizing its message (Waledac).



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

See <http://j.mp/IG10kH>

Geolocation was similarly used in a work-from-home scam.

Kelly Richards of **Clifton, New Jersey** is a regular mom who lost her job last year, after an unsucce

Kelly Richards of **Portland, Oregon** is a regular mom who lost her job last year, after an unsucce

Kelly Richards of **Roubaix, Nord-Pas-de-Calais** is a regular mom who lost her job last year, after an unsuccessful job hunt she

Malware spoofed email from
trusted senders.

“Unfortunately we were not able to deliver the postal package ...

Please print out the invoice copy attached and collect the package at our department.

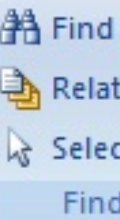
United Parcel Service of America.”

Malicious messages matched the content the victim was used to receiving.

The attachments targeted client-side vulnerabilities.

Message

Add-Ins



From: Alexis Moore [alexis.mo88@gmail.com]
To:
Cc:
Subject: Meeting agenda

Message | Agenda.PDF (947 KB)

Hi everyone!

I hope everyone has been as busy as I have reviewing our set of reference documents! With the meeting approaching, we can maximize our productivity with everyone familiar with the various projects & active work effort.

here is an agenda outline for the upcoming meeting. I look forward to seeing everyone there, and hope your meeting is uneventful.

-Alexis

Hey, **Neil**, it's Michelle here, it has been a long time huh ? how're you doing ?
? Is everything ok there ? Hey, can you believe it! I got married to Brian ! Yes
answer. You have changed your number, haven't you? Just give me your curre
this mail. It's really a pity that we did not see you in our wedding. I wanted to
I'm sending you a **few pics taken in our wedding.**

<http://www.weddingphotos4u.net/Photos/Michelle/>

Let's keep in touch then.

Love,

Michelle & Brian

Attackers provided customer service to appear legitimate.



Image Source: Symantec
<http://j.mp/HJOwGU>

LiveSupport » Live Chat

Tom Smith

but the SEP antivirus software after a scan shows nothing

Mary Ann Kovalsky

More likely your other anti-virus is outdated or simply incapable of detecting that particular virus/malware item. We have anti-virus solutions got blocked or modified by dangerous viruses and malware, resulting in them reporting no threats. We can help with our software activation, so that you could take full advantage of its virus and malware removal capabilities,

Tom Smith

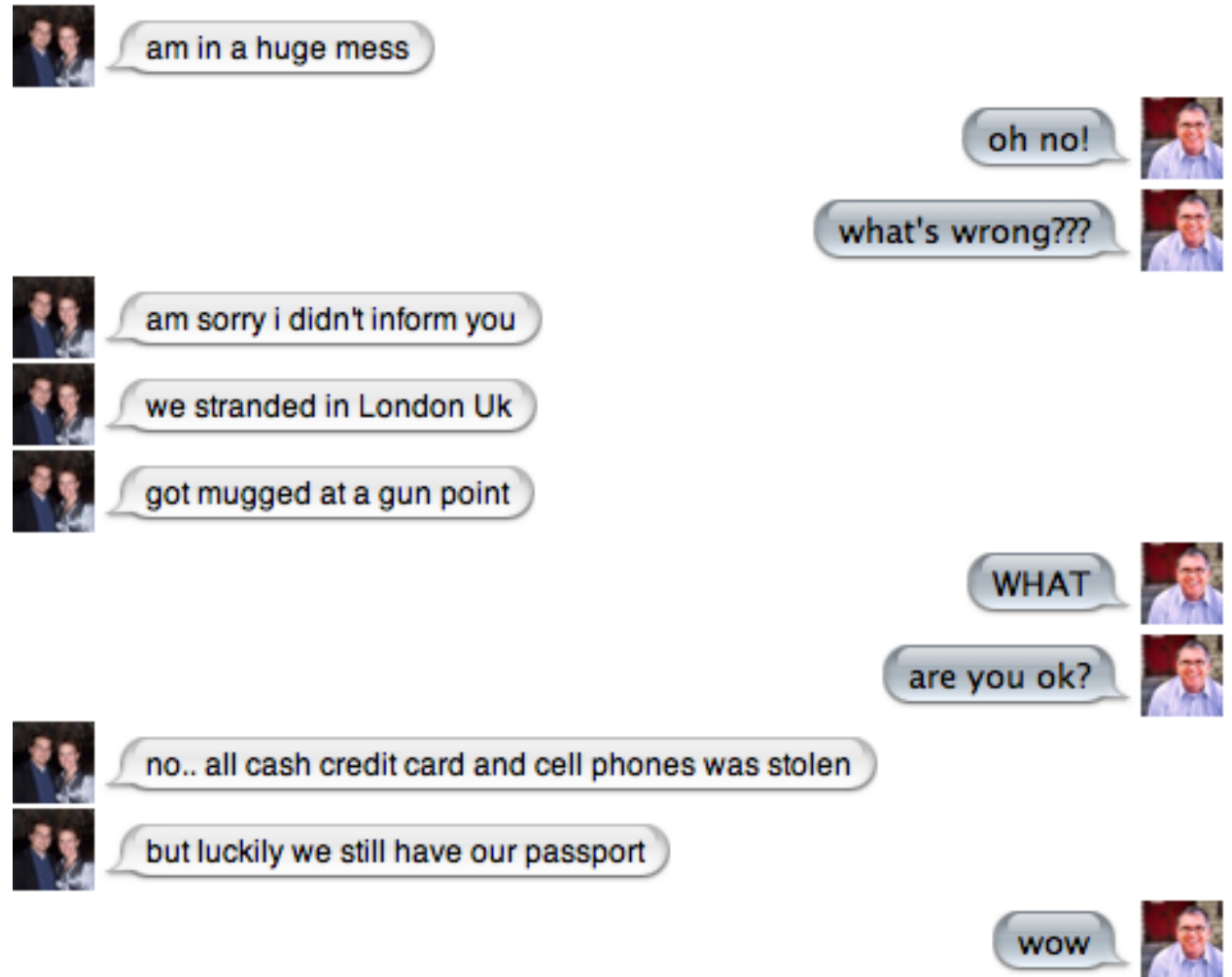
Can I get more information on the viruses on my system from somewhere?

Mary Ann Kovalsky

You can follow the paths stated in the warning messages of our soft and see that infected files really exist on your PC


Tom Smith

Fraudsters used Facebook chat for the “stuck in London” scam.



Profile Spy claimed to track who viewed victims' Facebook profiles.



Sevi  **Friday afternoons:** Find Out Who Has Been Viewing Your Facebook Profile With Profile Spy!!! >>>> <http://fbspys.info/>



Find Out Who Has Been Viewing Your Facebook Profile With Profile Spy!!! >>>> <http://fbspys.info/>

fbspys.info

Find Out Who Has Been Viewing Your Facebook Profile With Profile Spy!!!
>>>> <http://fbspys.info/>



The screenshot shows a web browser window with the address bar displaying <http://profilespsyer.com/>. The browser's address bar includes navigation icons (back, forward, home, refresh, close) and a search engine icon (Google). Below the address bar, there are navigation buttons for 'Favorites' and 'Follow steps to Activate Profile Spy!'. The main content area shows the Facebook interface with the 'facebook' logo, a search bar, and a 'News Feed' section. A 'Profile Spyer' advertisement is visible at the bottom of the page, featuring the Facebook logo and the text 'Profile Spyer'. The browser's status bar at the bottom shows 'facebook Profile Spyer'.

Social Compliance

Malware spoofed product review sites to legitimize a fake anti-virus 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 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

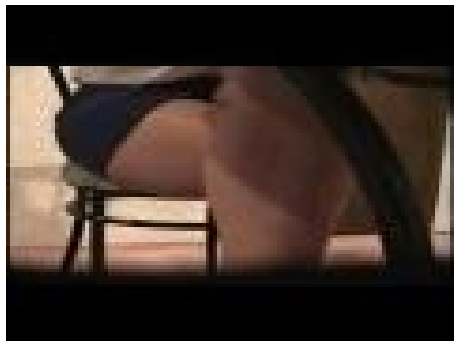
Social networks have been used to spread malware (Koobface).

My home video :)

<http://tinyurl.com/l4bslp>



Abel Saavedra Amazing Video <http://snimka31082009.com/youtube>
seefilm



snimka31082009.com

Source: snimka31082009.com

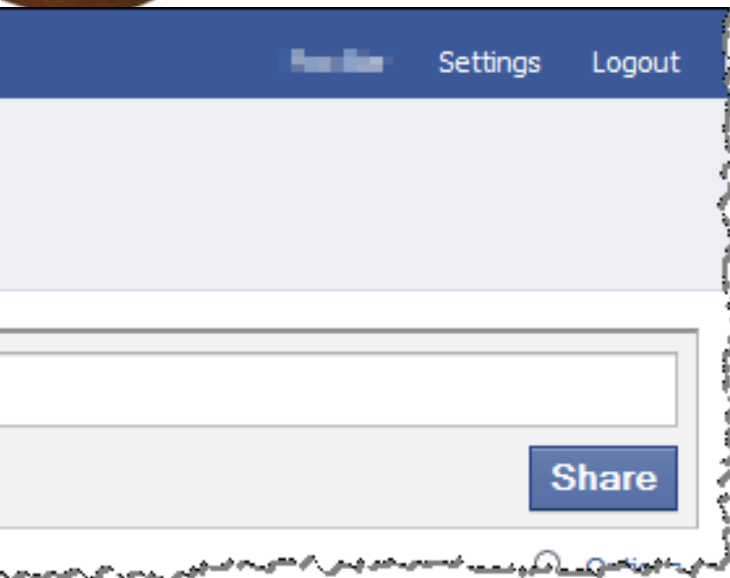


Yesterday at 7:09am

Source: Nick FitzGerald
<http://j.mp/HEsg4l>



Want 2 C Something Hot?

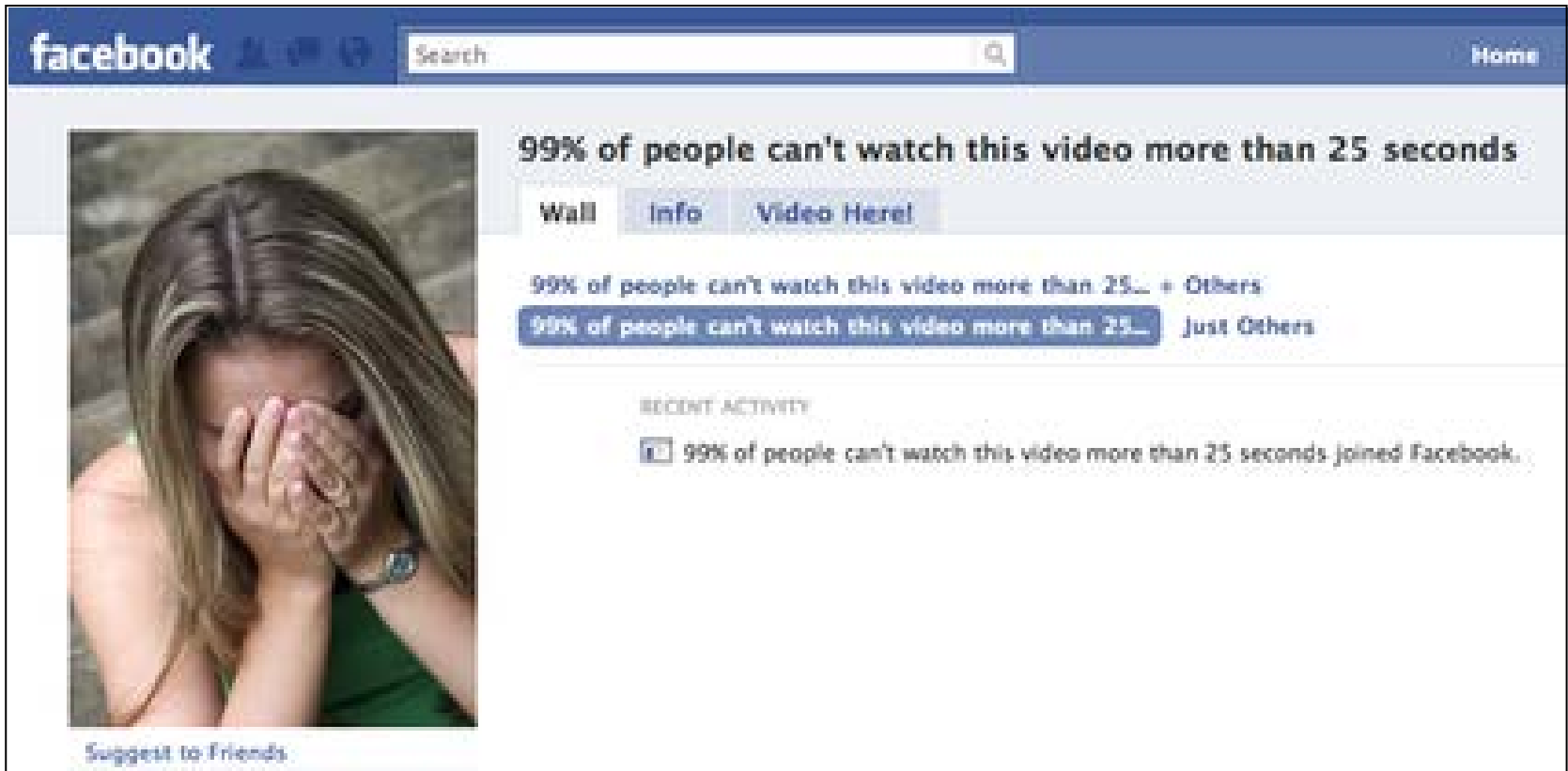


on, baby!

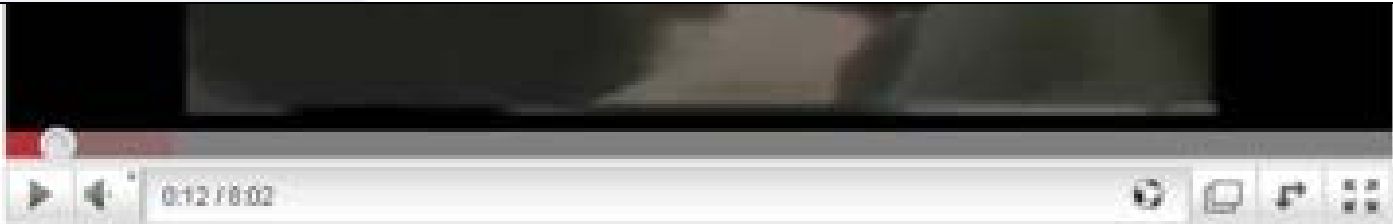
Malware dared victims to click the link to get them hooked.

Then asked to copy and paste JavaScript to spread on Facebook.

Source: AVG <http://j.mp/pQDv9G>



The screenshot shows a Facebook interface. At the top, the word "facebook" is on the left, a search bar is in the center, and "Home" is on the right. Below the navigation bar, there is a video player. The video thumbnail shows a woman with long brown hair covering her face with her hands, appearing to be crying. To the right of the video, the title "99% of people can't watch this video more than 25 seconds" is displayed. Below the title are three tabs: "Wall", "Info", and "Video Here!". Underneath the tabs, there is a social sharing section with two buttons: "99% of people can't watch this video more than 25..." and "+ Others". Below this is a "RECENT ACTIVITY" section with a single entry: "99% of people can't watch this video more than 25 seconds joined Facebook." At the bottom left of the video player, there is a "Suggest to Friends" link.



Copy the code below, paste it into your browser's address bar and press enter to load this video..Plz wait 7-8 secs for processing!!!

Malware manipulated download counters to appear popular (Nugache).

Most popular downloads For last week

	Downloads
1. AVG Anti-Virus Free Edition	1,947,847
 Protect your computer from viruses and malicious programs.	
2. Avira AntiVir Personal - Free Antivirus	1,143,291
3. Avast Free Antivirus	1,051,029
4. Advanced SystemCare Free	715,108
5. Malwarebytes Anti-Malware	695,084
6. YouTube Downloader	596,517
7. WinRAR (32-bit)	382,111
8. LimeWire	351,987
9. Orbit Downloader	340,659

This is a sample screenshot. It's not representative of the sites actually manipulated by Nugache.

Newest

Popular

Freeware

1

Outlook Express

This e-mail client integrates fully with your OS. It rivals many commercial products and...
Freeware

2

VideoSpirit Pro

VideoSpirit Pro is the most easily used Video Converter/Editor tools.
Shareware

3

WinISO

This tool lets you open an image file, display the file tree and run files from within the...
Shareware

4

IrfanView

This free image viewer and converter supports an extensive list of formats.
Freeware

5

FL Studio

This program lets you create your own songs and audio loops.
Demo

Money-mule recruiting sites looked like sites of many other legitimate companies.



24 Hour
Express Service



❖ ABOUT US

❖ CONTACT US

❖ SERVICES

❖ JOBS FOR YOU

Lets Work Together
To Achieve **Success!**



Latest News

— November 25, 2009

Job Opening!

Find details by visiting the "Jobs For You" section of our website. [read more](#)

— February 20, 2009

Our IT experts are working at creation of increasingly convenient methods of money processing and provide every our manager with support and advice.

Welcome



Welcome To Our Company

24 Hour Express Service company the competence of leading consultants, specialists and analysts in the sphere of investment and strategic consulting. Project groups and a high-qualified manager are assigned to each project. This method guarantees individual approach to every client, adequate understanding of his problems and in the meantime allows solving a complete range of objectives settled. Competence in business specificity of every client ensures a high level of service granted.

A scam emphasized the popularity of the “work from home” kit.

See <http://j.mp/HGVHU9>



Reliance on Security Mechanisms

Similar to the fake counterfeit
money-testing pen con.

“Security update” messages in several forms convinced users to download and install software.



Flash Player upgrade required

You must download and install the latest version of the Adobe Flash Player to view this content.

[Download Flash](#)

Welcome to Video

Your life in motion.

Share your personal videos.

Upload and tag videos of you and your friends on Facebook. [Upload a new video](#)

Record and send video messages.

Use your webcam to record yourself in a video message. [Record a video message](#)

Fake anti-virus tools confused the user about the need for security.

Windows Internet Explorer



NOTICE: If your computer is infected, you could suffer data loss, erratic PC behavior, PC freezes and crashes. Detect and remove viruses before they activate themselves on your PC to prevent all these problems.

Do you want to install AntiSpywareMaster to scan your PC for malware now? (Recommended)

OK

Cancel



There were errors during security settings restore!


System has detected spyware infection! It is recommended to use antispyware tool to prevent data loss and privacy information exposure

Click OK to download antispyware tool

OK



Security

- Allow active content from CDs to run on my computer*
- Allow active content to run in files on My Computer*
- Allow software to run or install even if the signature is invalid
- Check for publisher's certificate revocation
- Check for server certificate revocation*
- Check for signatures on downloaded programs
- Do not save encrypted pages to disk
- Empty Temporary Internet Files folder when browser is closed
- Enable Integrated Windows Authentication*
- Enable native XMLHTTP support
-  Phishing Filter
 - Disable Phishing Filter
 - Turn off automatic website checking
 - Turn on automatic website checking
- SSL 2.0

Victims sometimes even got to choose their preferred rogue anti-virus product.

Antivirus	Scan result	Bases update	Removal tool
 NOD32 Anti Virus System	Nothing	1 hours ago	<input type="button" value="Free Install"/>
 Red Cross	Unknown Trojan	6 hours ago	<input type="button" value="Free Install"/>
 IKARUS security software	Nothing	6 hours ago	<input type="button" value="Free Install"/>
 VirusBuster	Nothing	24 hours ago	<input type="button" value="Free Install"/>
 Dr.Web	Nothing	2 hours ago	<input type="button" value="Free Install"/>
 avast!	Nothing	24 hours ago	<input type="button" value="Free Install"/>
 Peak Protection	Trojan Horse	24 hours ago	<input type="button" value="Free Install"/>
 McAfee	Nothing	1 hours ago	<input type="button" value="Free Install"/>
 bitdefender	Nothing	3 hours ago	<input type="button" value="Free Install"/>
 SOPHOS	Nothing	3 hours ago	<input type="button" value="Free Install"/>
 eTRUST	Nothing	Last bases	<input type="button" value="Free Install"/>
 AVG	Nothing	24 hours ago	<input type="button" value="Free Install"/>
 Clam AV	Nothing	11 hours ago	<input type="button" value="Free Install"/>

Antivirus	Scan result
 A-SQUARED	Nothing
 TREND MICRO	Nothing
 Major Defense Kit	RootKit
 F-Secure	Nothing
 Windows Live	Nothing
 AntiVir	Nothing
 ewido	Nothing
 Panda	Nothing
 Vexira	Nothing
 NORMAN	Nothing
 Solo	Nothing
 ArcaVir	Nothing
 Webroot	Nothing

Source: Sunbelt Software <http://j.mp/IG29Jh>

Malicious files were hosted behind a CAPTCHA screen.

See <http://j.mp/HGWfJF>



Downloading: 1271323402.exe | 0.1 MB

Please wait 54 seconds or [click here](#) to get a high speed

hotfile

[News](#) [Upload](#) [Premium](#) [Affiliate](#) [FAQ](#) [Contacts](#)



Downloading: 1271323402.exe | 0.1 MB

Or 

Type the two words:



[Download the file](#)

Scammers associated their
“products” with trusted brands.



Google Approved Pharmacy Directory

Web Pages

Viewing in Google PageRank order

[Generic Kamagra 10 capsules x 100mg = \\$68.84. Bonus pills. Mastercard and Visa](#)

Kamagra (Generic) 30 capsules x 100mg = \$195.98 No prescription required, Confidentiality, Guaranteed Fast Worldwide Delivery, 24/7 customer service.

<http://www.bestdrugsite.com>

[Buy brand Kamagra online](#)

Get quality medication online. Brand Kamagra delivered to your door for 2 USD per pill.

<http://www.viagramedic.com/?product=kamagra>

[Certified Canadian Pharmacy - kamagra](#)

Our products it's Hight Quality Medications! No prescription needed. We

Attackers signed malware with certificates.

Some certs were stolen with malware. Some were obtained through identity theft.

See <http://j.mp/9HbPLC>



Malicious websites presented a security warning to the users, asking to download an update.


Reported Attack Page! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://update.mozilla.org/

Most Visited

Reported Attack Page!



Reported Attack Page!

This web page has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Download Updates!](#)

The page at http://update.mozilla.org says:

This web page has been blocked based on your security preferences. Click 'OK' to download and install Firefox secure updates.

OK Cancel

See <http://j.mp/ITLj9g>

So What?

Social engineering works.

It seems to tap into psychological factors that are part of the human nature.

Discuss recent social engineering approaches with employees, partners and customers.

Alternative Channels

Personally-Relevant Messaging

Social Compliance

Reliance on Security Mechanisms

Assume some social engineering
will work anyway.

Focus on... internal segmentation,
least privilege, need-to-know and
monitoring.



Lenny Zeltser

blog.zeltser.com

twitter.com/lennyzeltser

About The Author:

Lenny Zeltser is a seasoned IT professional with a strong background in information security and business management. As a director at NCR Corporation, he focuses on safeguarding IT environments of small and midsize businesses worldwide. Before NCR, he led an enterprise security consulting team at a major IT hosting provider. Lenny's most recent work has focused on malware defenses and cloud-based services. He teaches how to analyze and combat malware at the SANS Institute, where he is a senior faculty member. He also participates as a member of the board of directors at the SANS Technology Institute and volunteers as an incident handler at the Internet Storm Center.

Lenny frequently speaks on security and related business topics at conferences and industry events, writes articles, and has co-authored books on forensics, network security, and malicious software. He is one of the few individuals in the world who have earned the highly-regarded GIAC Security Expert (GSE) designation. Lenny has an MBA degree from MIT Sloan and a computer science degree from the University of Pennsylvania.