

Security Threats

And how to stop them.

Ransomware: Don't get locked out

cyber.gc.ca/en/ransomware-dont-get-locked-out

Government of Canada

Gouvernement du Canada

Canada.ca | Services | Departments | Français

Canadian Centre for Cyber Security



Search Canada.ca

Search

Information & Guidance

Services

Cyber Incidents

Education & Training

Building the Community

Home

Ransomware: Don't get locked out

ALERT

Canadian organizations exploited via unpatched devices and inadequate authentication

The Cyber Centre has become aware of recent and continuing exploitation of network infrastructures in Canada. Read the alert and suggested mitigation

Read More

Ransomware: Don't get locked out



The logo for 'marketplace' features a yellow chevron pointing right, followed by the word 'marketplace' in a white, lowercase, sans-serif font on a solid red background.

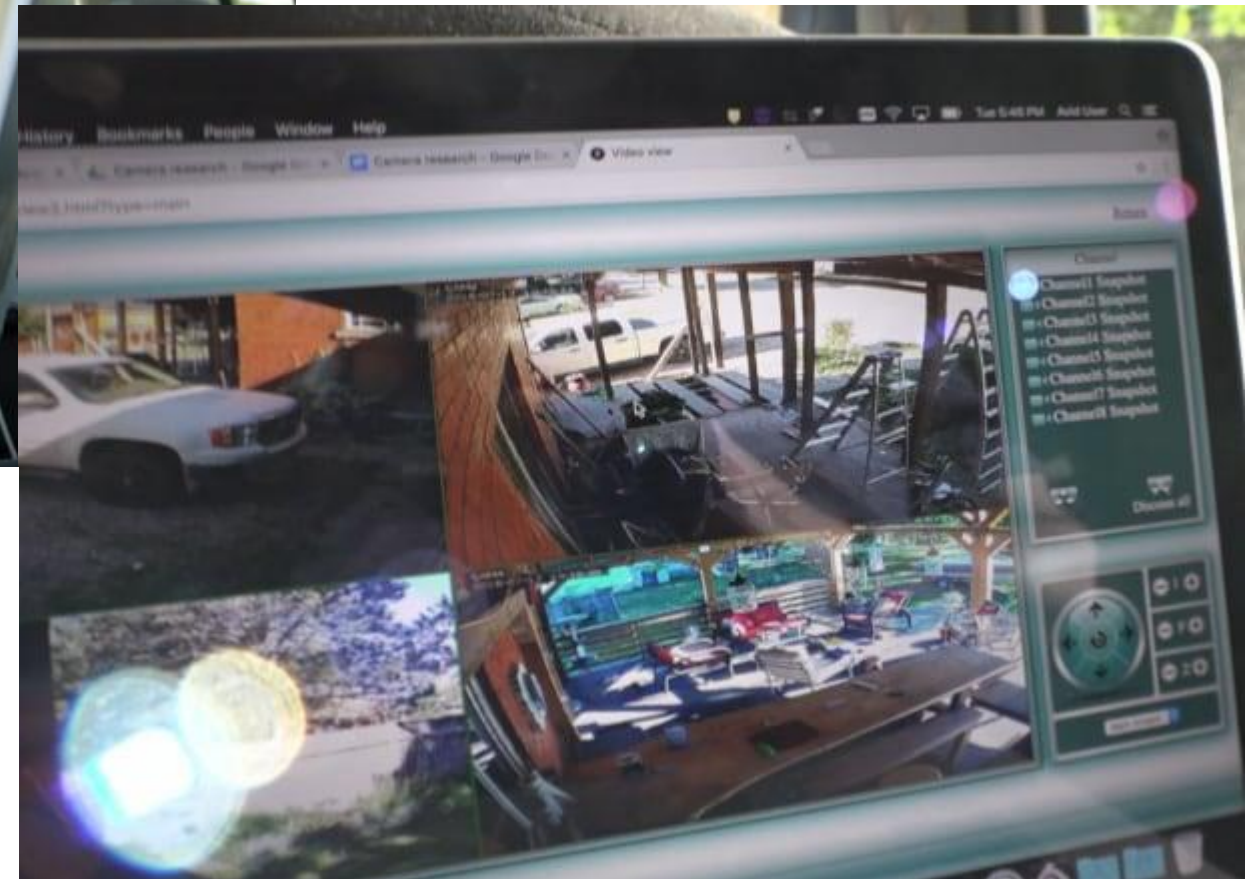
Technology & Science · Marketplace

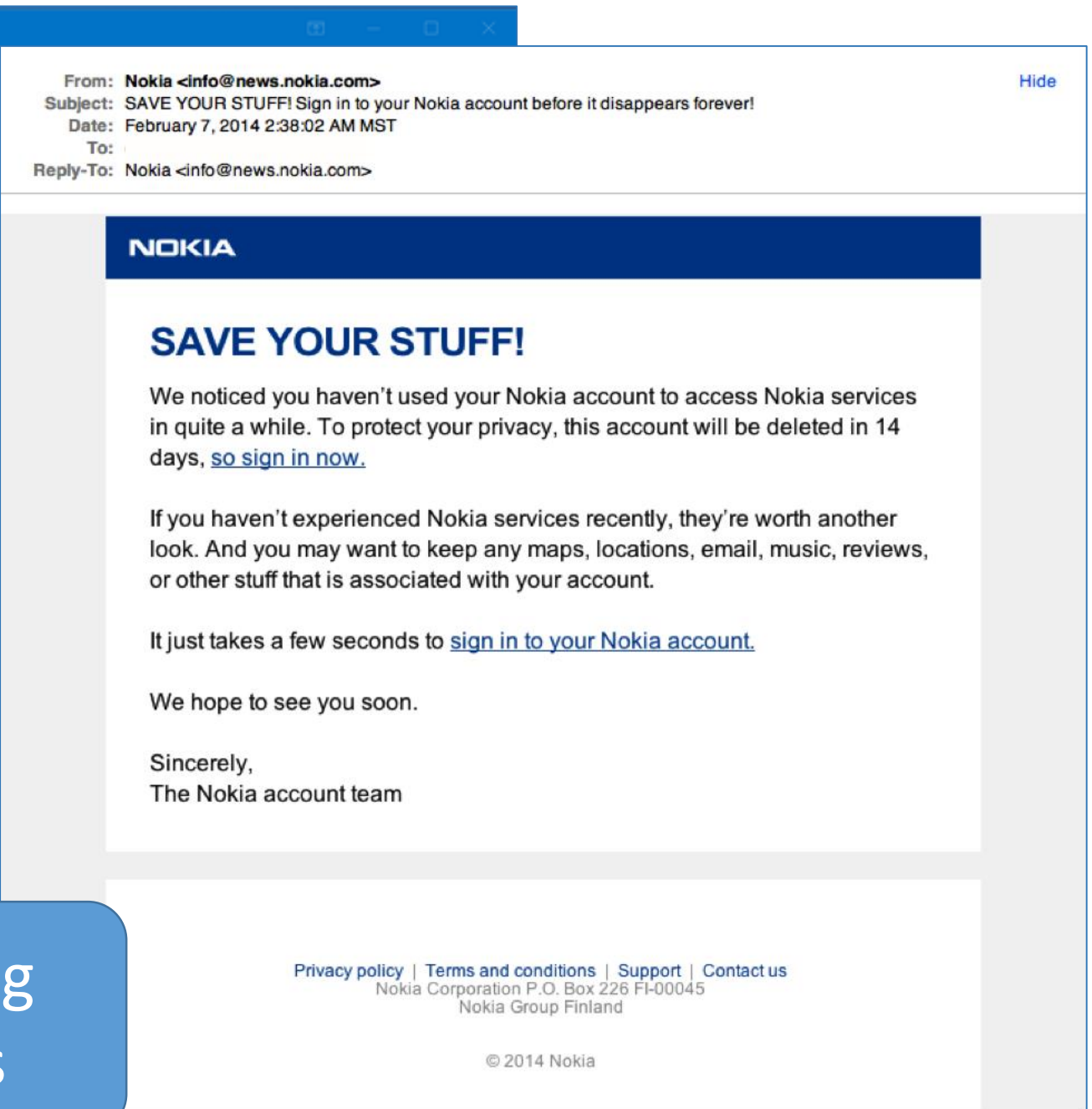
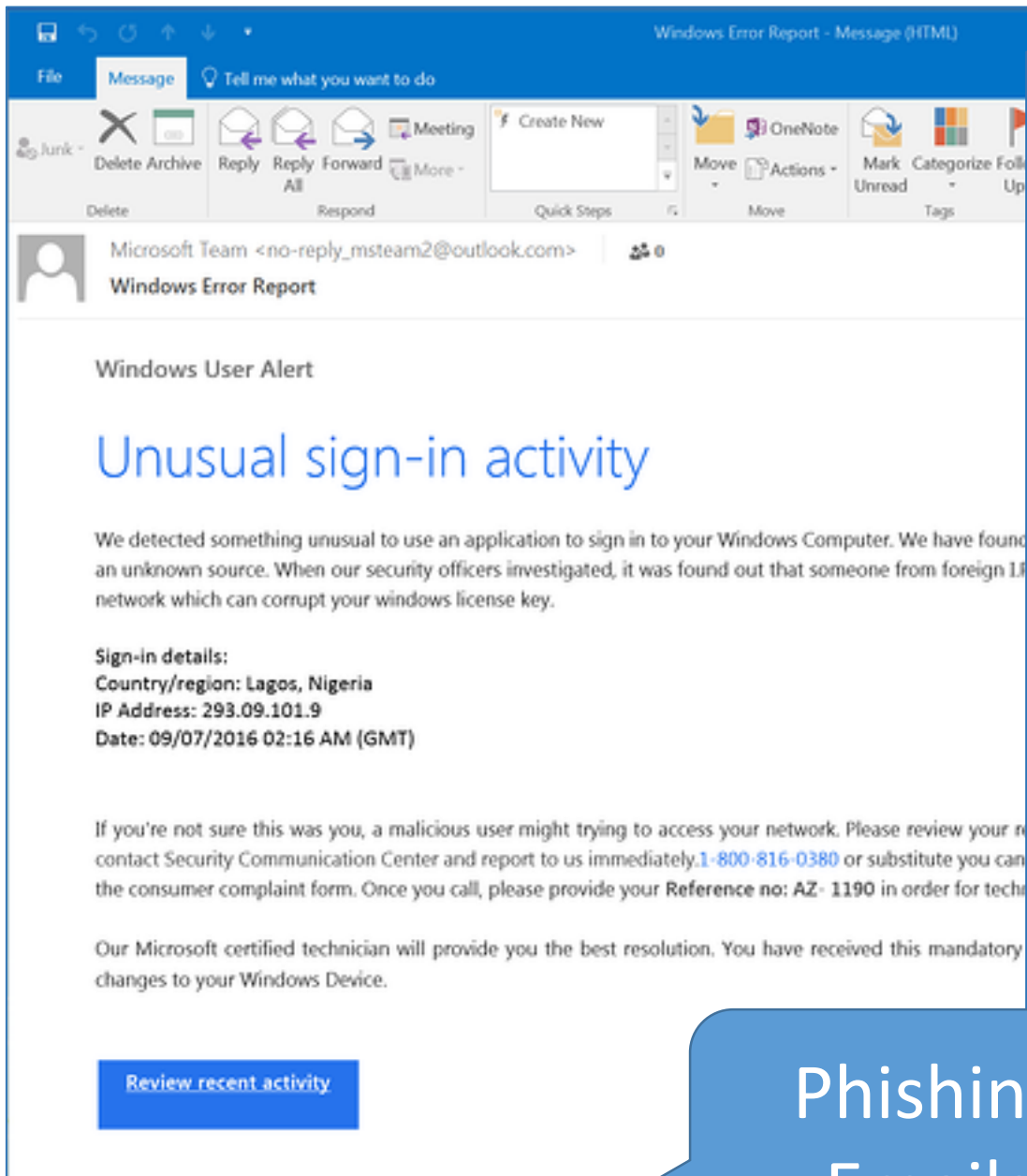
We hired ethical hackers to hack a family's smart home – here's how it turned out

Vulnerabilities revealed in smart home devices prompt 1 manufacturer to immediately beef up protections

[Luke Denne](#), [Greg Sadler](#), [Makda Ghebreslassie](#) · CBC News ·

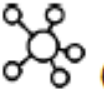
Posted: Sep 28, 2018 4:00 AM ET | Last Updated: September 30, 2018





Phishing
Emails

Security Problems

2.9  c

Name	Definition	Example
<i>Hacking</i>	Unauthorized access to a computer system	
	A form of _____ that can harm a computer system	_____ virus <ul style="list-style-type: none">• Caused the Northeastern blackout in August 2003• Caused 11 deaths, \$6 billion in damages
	A form of a virus that can spread itself. It is another form of MALWARE.	_____ worm <ul style="list-style-type: none">• American + Israeli military hackers targeted Iran's nuclear reactors in 2010.• _____ = used software bugs that had never been found before• _____ = a nation state attacking another's infrastructure using hacking or viruses.



How Viruses Work

1 The virus arrives

Most viruses show up inside e-mail attachments.



2 Something pulls the trigger

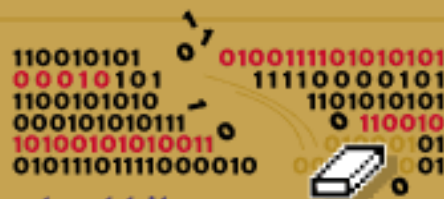
Running or opening the file activates the virus, which inserts copies of itself into files and other locations on your computer.



4

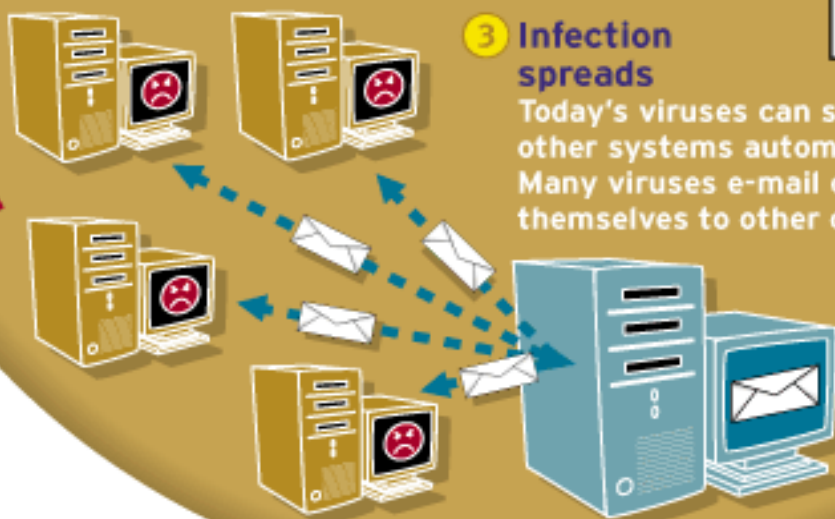
The payload hits

At some point after the trigger, the virus performs its programmed action—from erasing your hard drive to inserting jokes in your documents.



3 Infection spreads

Today's viruses can spread to other systems automatically. Many viruses e-mail copies of themselves to other computers.



Blaster Virus August 2003





Disrupts Train
Signals

Air Plane
Booking
systems are
down.

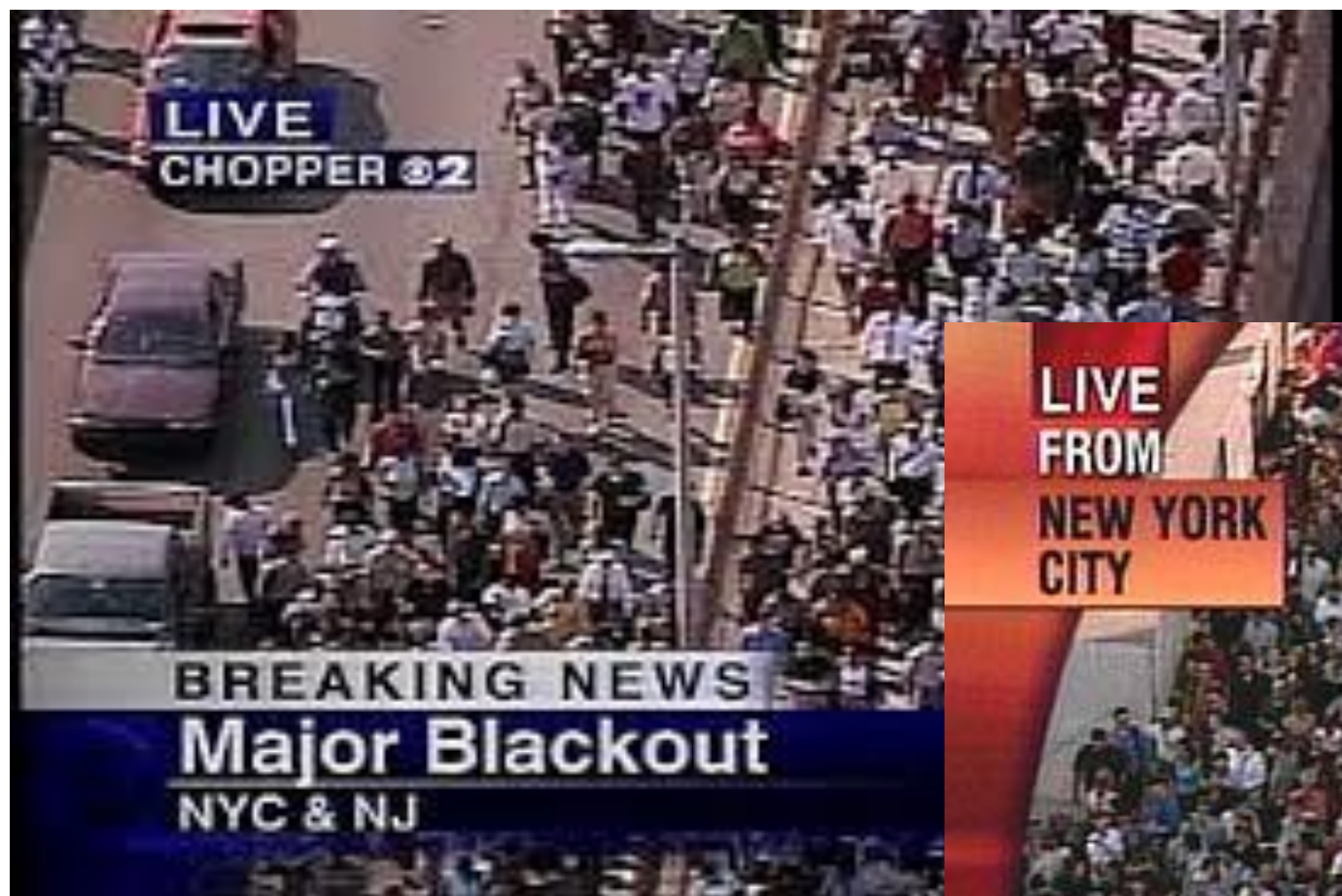
003/45/7844

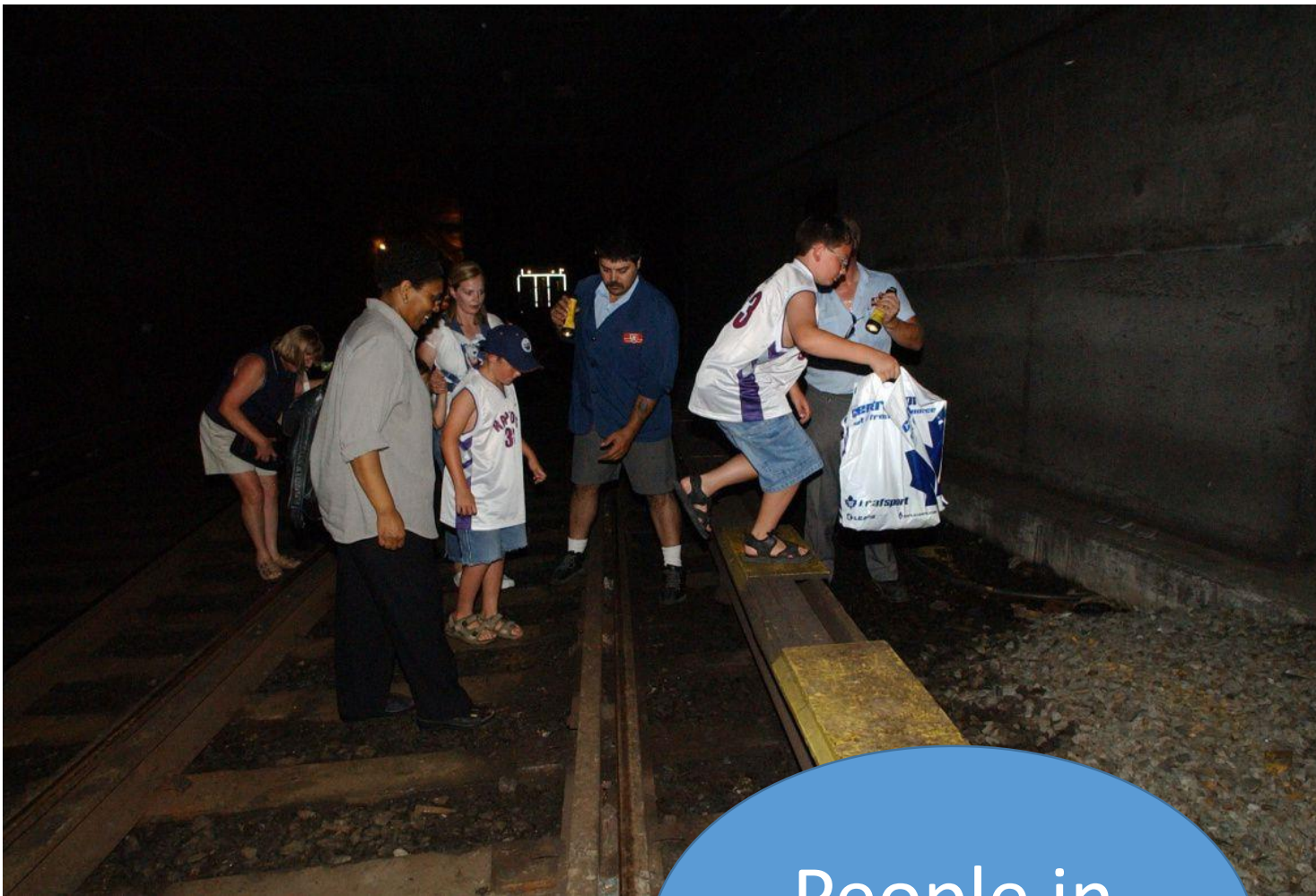
Aug 14 Blackout

ISAT GeoStar 45
23:15 EST 14 Aug. 2003



11 deaths
Cost \$6 billion





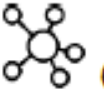
People in
subways.





Jeffrey Lee Parson,
18 years old.
Sentenced to 18
months in prison.

Security Problems

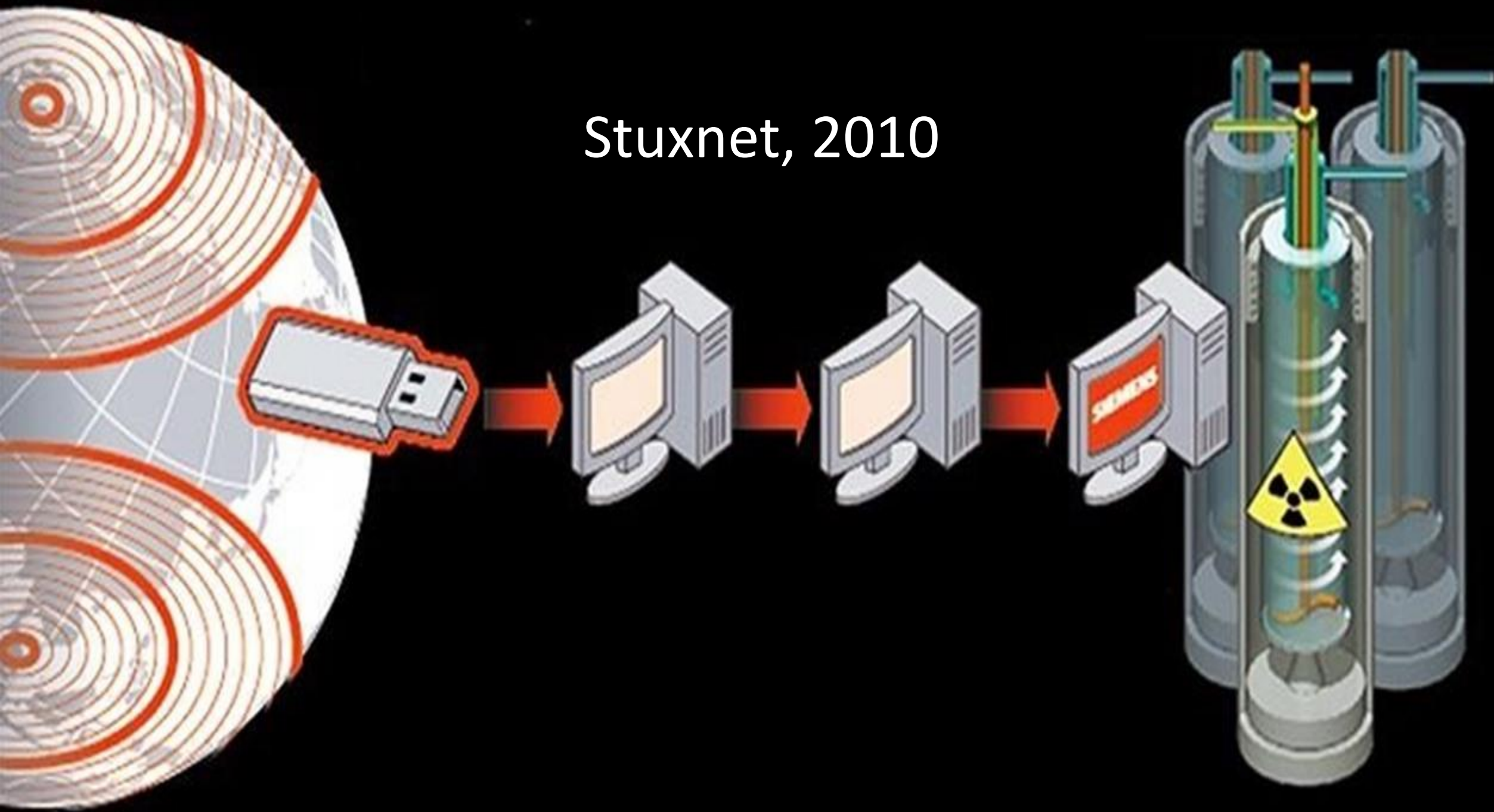
2.9  c

Name	Definition	Example
<i>Hacking</i>	Unauthorized access to a computer system	
<i>Virus</i>	A form of <u>malware</u> that can harm a computer system	<u>Blaster</u> virus <ul style="list-style-type: none">• Caused the Northeastern blackout in August 2003• Caused 11 deaths, \$6 billion in damages
	A form of a virus that can spread itself. It is another form of MALWARE.	<u> </u> worm <ul style="list-style-type: none">• American + Israeli military hackers targeted Iran's nuclear reactors in 2010.• <u> </u> = used software bugs that had never been found before• <u> </u> = a nation state attacking another's infrastructure using hacking or viruses.

Centrifuges at Natanz (Iran) in 2008



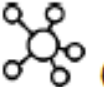
Stuxnet, 2010







Security Problems

2.9  c

Name	Definition	Example
<i>Hacking</i>	Unauthorized access to a computer system	
<i>Virus</i>	A form of <u>malware</u> that can harm a computer system	<u>Blaster</u> virus <ul style="list-style-type: none">• Caused the Northeastern blackout in August 2003• Caused 11 deaths, \$6 billion in damages
<i>Worm</i>	A form of a virus that can spread itself. It is another form of MALWARE.	<u>Stuxnet</u> worm <ul style="list-style-type: none">• American + Israeli military hackers targeted Iran's nuclear reactors in 2010.• <u>Zero-Day</u> = used software bugs that had never been found before• <u>Cyber war</u> = a nation state attacking another's infrastructure using hacking or viruses.



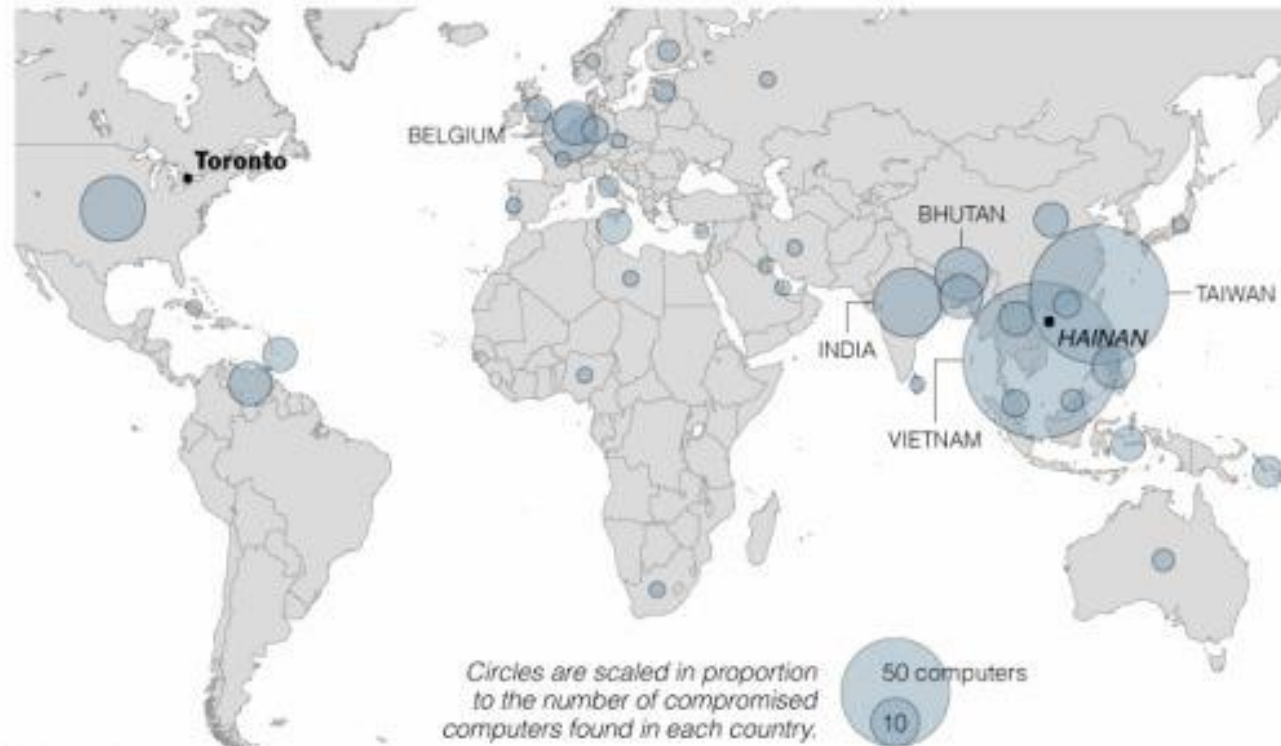
Ghostnet



Using your webcam...
and microphone.

The Vast Reach of 'GhostNet'

Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 347 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.



Source: Information Warfare Monitor

THE NEW YORK TIMES

JR02-2009

Tracking GhostNet:

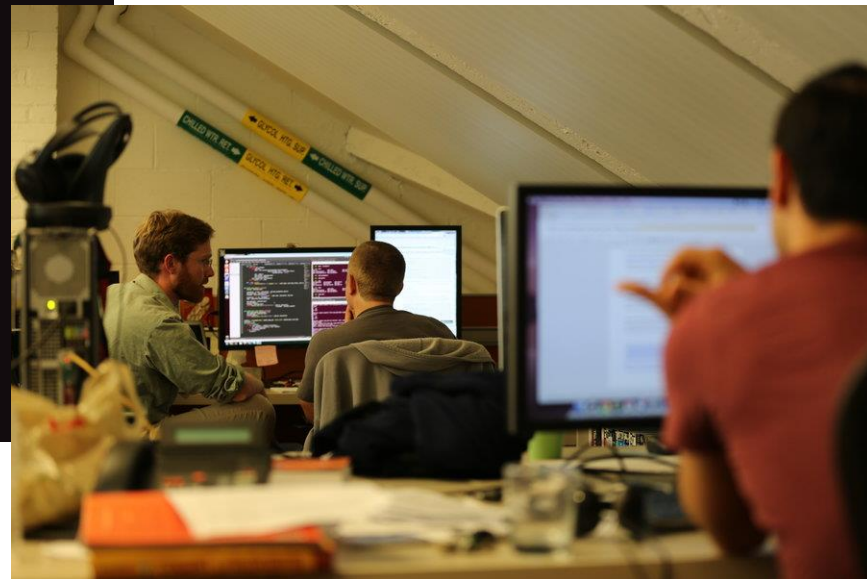
Investigating a Cyber Espionage Network

Information Warfare Monitor

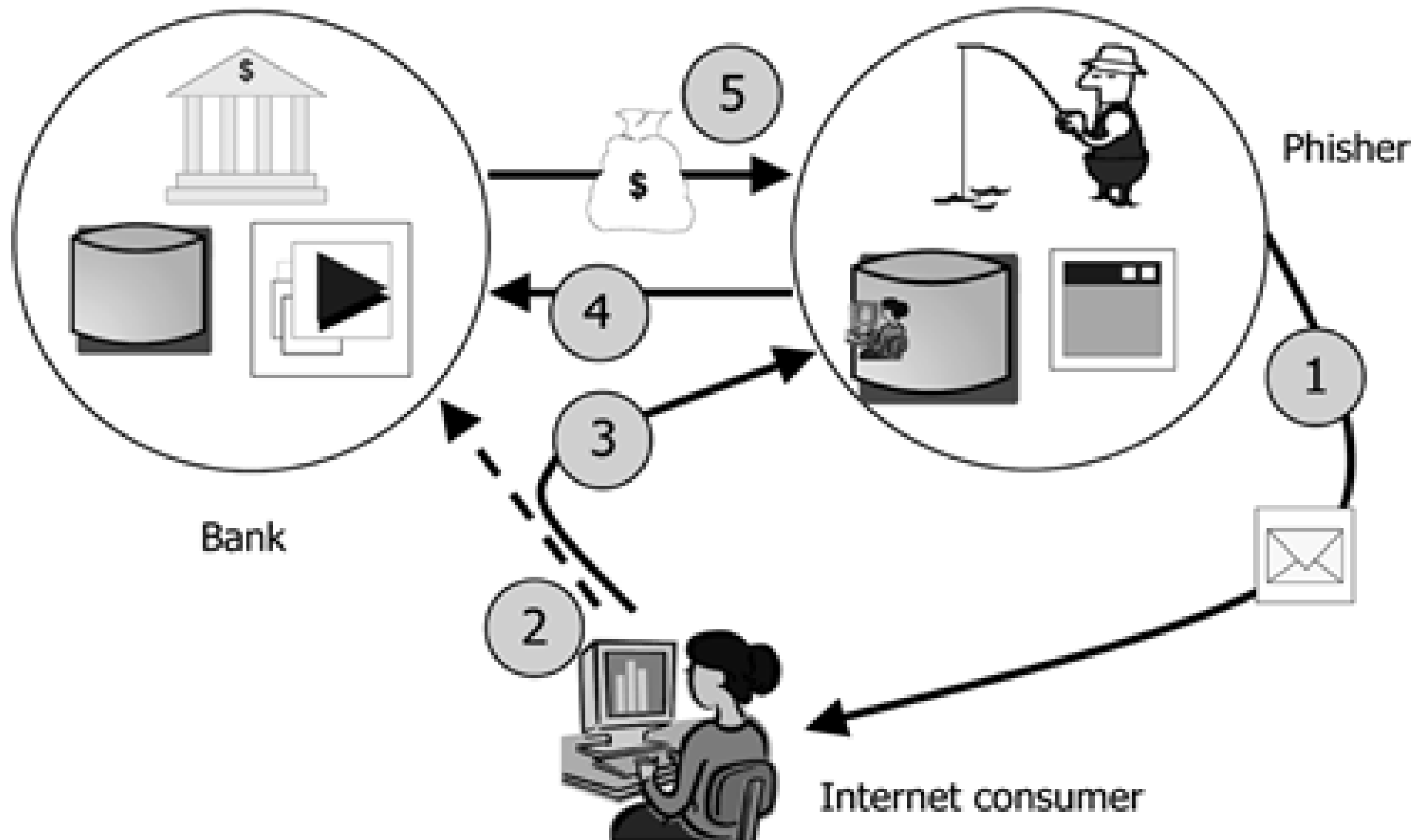
March 29, 2009



<http://www.infowar-monitor.net/ghostnet>
<http://www.tracking-ghost.net>



How a Trojan can be used in a Phishing Attack:



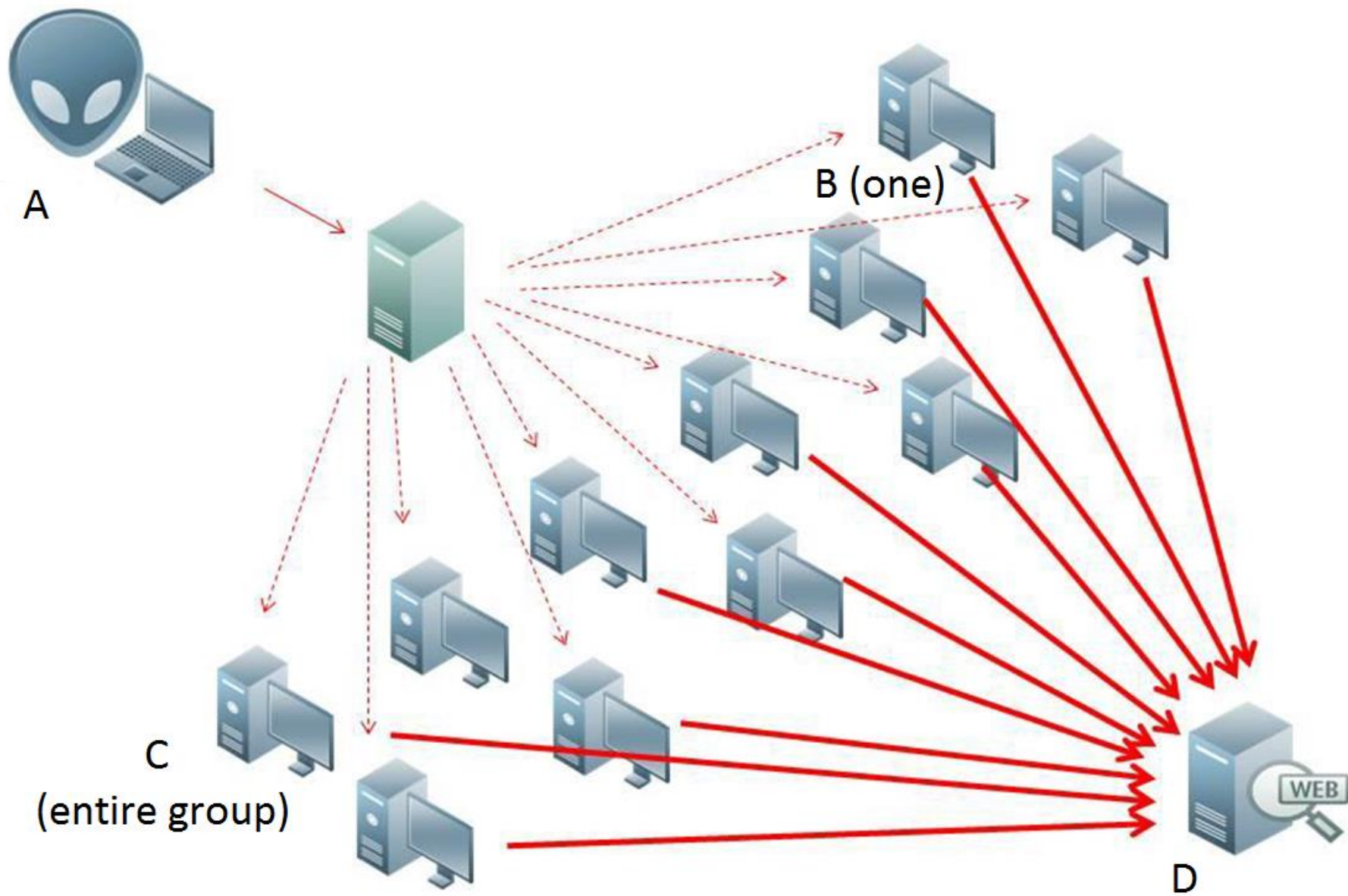
Further down the chart

2.9 C

<i>Trojan</i>	A form of <u>malware</u> that grants a hacker complete access to your system.	<u>Ghostnet</u> <ul style="list-style-type: none"> Found by Toronto's Citizen Lab in 2010. Used by the Chinese government to listen in to government officials via webcam and microphones.
	<ul style="list-style-type: none"> A hacker known as a _____, installs a Trojan on many computers. These computers are known as _____ and together they form a _____. The herder then uses all of the bots to overwhelm a website so no one can access it 	<u> </u> <ul style="list-style-type: none"> Russian hackers used a DDos attack to take down all Estonia networks for 3 weeks in 2007. No credit cards, debit cards, internet for that space of time. Another example of _____ = a nation attacking another.

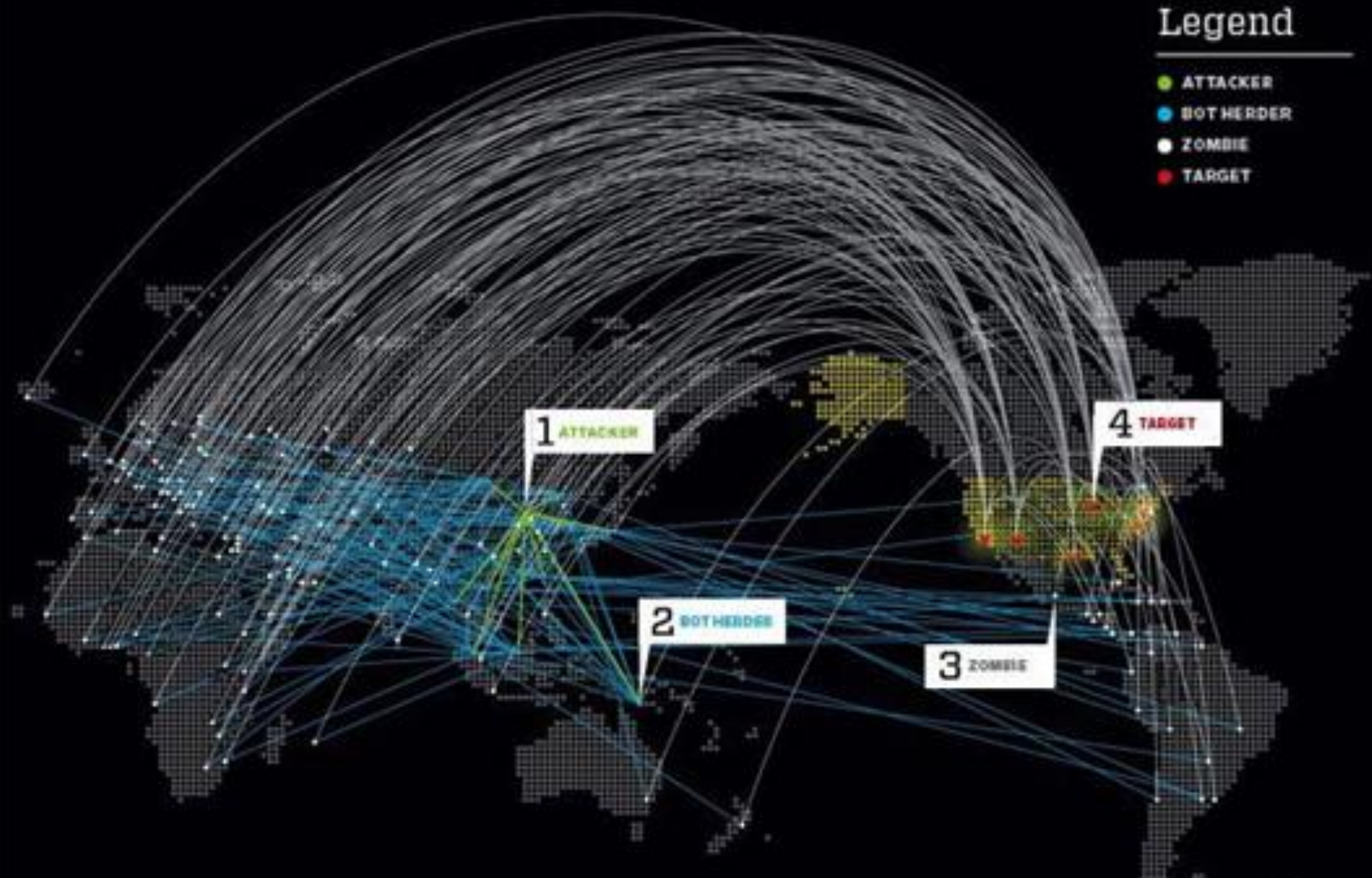
D-Dos





Legend

- ATTACKER
- BOT HERDER
- ZOMBIE
- TARGET





The connection has timed out

The server at www.cia.gov is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

People trying to visit the site get this a time out message.

File Edit View History Bookmarks Tools Help

http://

Add To Wish List View Your Wish Lists Today's Deals

Search Products on Amazon.com

Error 503 Service Unavailable


Service Unavailable

Guru Meditation:

XID: 705472525

[Varnish](#)

Downloads winsome-file-re...



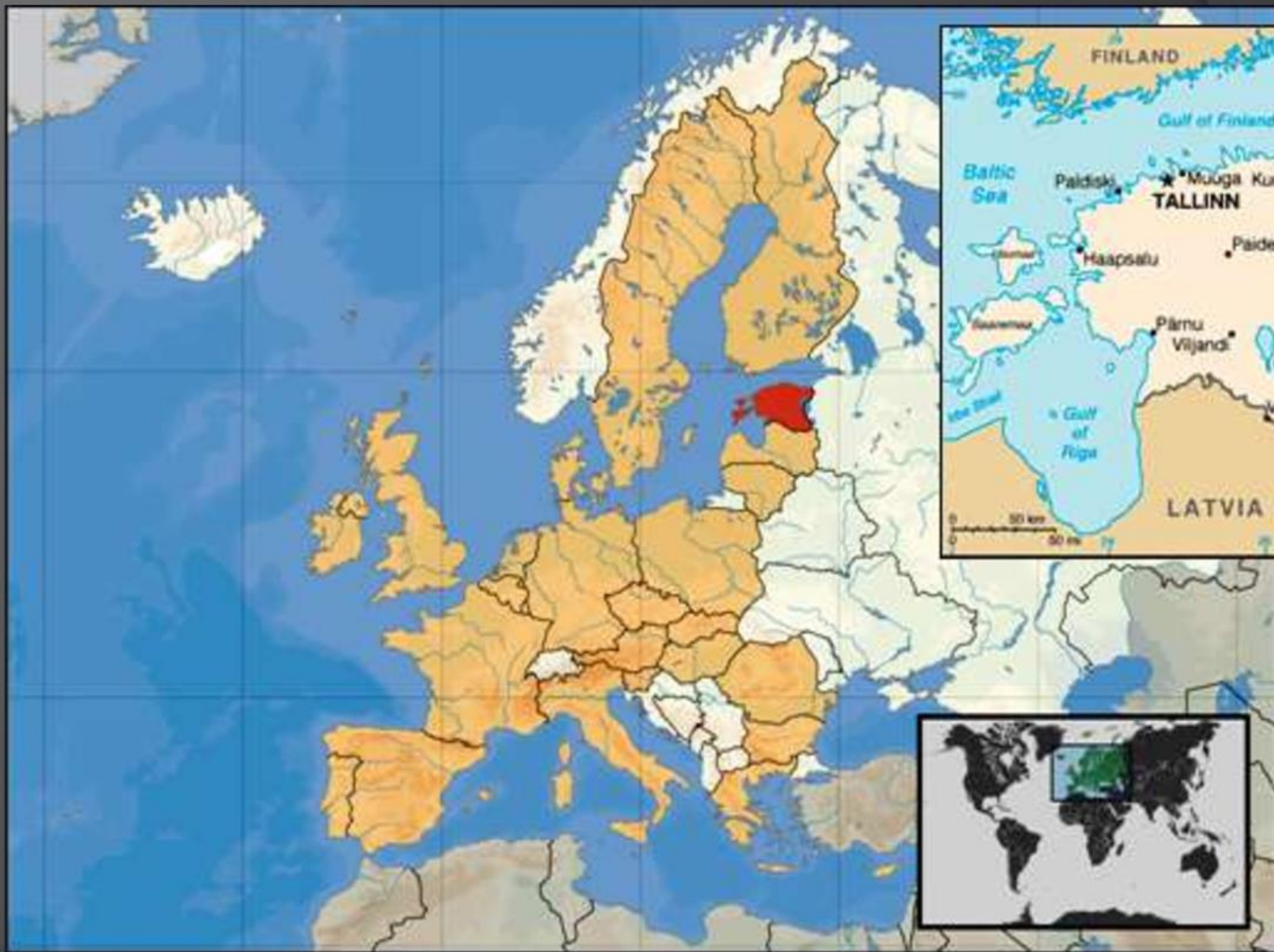
This site can't be reached

twitter.com's server DNS address could not be found.

Try running [Network Diagnostics](#).

DNS_PROBE_FINISHED_NXDOMAIN

Reload







● Source C&C's
● Targets
Size – Relative Activity



3 weeks

Couldn't even
access
accounts
outside the
country.

Education Quality and Accountability Office

EQAO

About EQAO The Assessments Research Our Data in Action

Search this site...

Login

e@online



URGENT MESSAGE
REGARDING TODAY'S ONLINE OSSLT

Cancellation of Today's Assessment

EQAO assesses how well Ontario's public education system is developing students' reading, writing and math skills. EQAO provides reliable and useful information that is used to help improve student achievement and ensure the accountability of school boards.

Educators


Parents

Students



October 20, 2016
Trial run of On-line Literacy Test – tens of thousands of students impacted.

Security Problems

2.9  c

Further down the chart

<i>Trojan</i>	A form of <u>malware</u> that grants a hacker complete access to your system.	<u>Ghostnet</u> <ul style="list-style-type: none">• Found by Toronto's Citizen Lab in 2010.• Used by the Chinese government to listen in to government officials via webcam and microphones
<i>D-Dos attack</i> <div>Also called zombies.</div>	<ul style="list-style-type: none">• A hacker known as a <u>herder</u>, installs a Trojan on many computers.• These computers are known as <u>bots</u> and together they form a <u>botnet</u>.• The herder then uses all of the bots to overwhelm a website so no one can access it	<u>Estonia</u> <ul style="list-style-type: none">• Russian hackers used a DDos attack to take down all Estonia networks for 3 weeks in 2007.• No credit cards, debit cards, internet for that space of time.• Another example of <u>cyberwar</u> = a nation attacking another.

Students Participate in Important Election



1 Task:

Write a **news report** based on the headline and picture above.

- You will have to make up the facts and information to answer some or all of the following questions: Who? What? Where? When? Why? How?
- You must relate your news report to **both** the headline **and** the picture.

Read the question in *Question Booklet 1* before providing your answer here.

■ Students Participate in Important Election

[illegible]

Students Participate in Important Election



1 Task:

Write a **news report** based on the headline and picture above.

- You will have to make up the facts and information to answer some or all of the following questions: Who? What? Where? When? Why? How?
- You must relate your news report to **both** the headline **and** the picture.

Read the question in *Question Booklet 1* before providing your answer here.

1 Students Participate in Important Election

Opening Paragraph



Paragraph with quotation #1
(name, position, quotation)

Paragraph with quotation #2
(name, position, quotation)

Conclusion. Final Thought.

Write the opening paragraph for a newspaper article about the Estonia cyber-attacks (April 27, 2007).

On , , the of ,
(WHEN) Specific Date Year (WHO) Group of people (WHERE) City

were shocked to discover
(WHAT) What happened to them, generally?

Further analysis by the showed that it was caused by
(WHO) The expert group (CAUSE, WHY)

.....

Write the opening paragraph for a newspaper article about the Estonia cyber-attacks (April 27, 2007).

On *April 27*, *2007*, the of,
(WHEN) Specific Date *Year* *(WHO) Group of people* *(WHERE) City*
were shocked to discover
(WHAT) What happened to them, generally?
Further analysis by the showed that it was caused by
(WHO) The expert group *(CAUSE, WHY)*

.....

Write the opening paragraph for a newspaper article about the Estonia cyber-attacks (April 27, 2007).

On
(WHEN) Specific Date *Year* *(WHO) Group of people* *(WHERE) City*
the of
were shocked to discover
(WHAT) What happened to them, generally?
Further analysis by the showed that it was caused by
(WHO) The expert group *(CAUSE, WHY)*

.....

Write the opening paragraph for a newspaper article about the Estonia cyber-attacks (April 27, 2007).

On
(WHEN) Specific Date *Year* *(WHO) Group of people* *(WHERE) City*
the of ,
were shocked to discover
(WHAT) What happened to them, generally?

Further analysis by the showed that it was caused by
(WHO) The expert group *(CAUSE, WHY)*

.....

Write the opening paragraph for a newspaper article about the Estonia cyber-attacks (April 27, 2007).

On
(WHEN) Specific Date
Year , the
(WHO) Group of people of
(WHERE) City,

were shocked to discover
(WHAT) What happened to them, generally?
.....

Further analysis by the
(WHO) The expert group showed that it was caused by
(CAUSE, WHY)

.....

Write the opening paragraph for a newspaper article about the Estonia cyber-attacks (April 27, 2007).

On *April 27* , *2007* , the *residents* of *Tallinn, Estonia* ,
(WHEN) Specific Date Year (WHO) Group of people (WHERE) City ,
were shocked to discover *that every network in their country wasn't working.*
(WHAT) What happened to them, generally?

Further analysis by the *NATO* showed that it was caused by *Russian hackers*
(WHO) The expert group (CAUSE, WHY)
..... *in response to the removal of a statue honouring Russian soldiers.*

Write the opening paragraph for a newspaper article about the EQAO D-Dos (October 20, 2016).

On , , the of ,
(WHEN) Specific Date Year (WHO) Group of people (WHERE) City

were shocked to discover
(WHAT) What happened to them, generally?

Further analysis by the showed that it was caused by
(WHO) The expert group (CAUSE, WHY)

.....

Write the opening paragraph for a newspaper article about the EQAO D-Dos (October 20, 2016).

On *October 20*, *2016*, the of,
(WHEN) Specific Date *Year* *(WHO) Group of people* *(WHERE) City*,
were shocked to discover
..... *(WHAT) What happened to them, generally?*

Further analysis by the showed that it was caused by
..... *(WHO) The expert group* *(CAUSE, WHY)*

.....

Write the opening paragraph for a newspaper article about the EQAO D-Dos (October 20, 2016).

On *October 20*, *2016*, the *Gr 10 students* of *Brampton Centennial*,
(WHEN) Specific Date Year (WHO) Group of people (WHERE) City

were shocked to discover
(WHAT) What happened to them, generally?

Further analysis by the showed that it was caused by
(WHO) The expert group (CAUSE, WHY)

.....

Write the opening paragraph for a newspaper article about the EQAO D-Dos (October 20, 2016).

On *October 20*, *2016*, the *Gr 10 students* of *Brampton Centennial*,
(WHEN) Specific Date Year (WHO) Group of people (WHERE) City

were shocked to discover *their EQAO literacy test screens were completely frozen.*
(WHAT) What happened to them, generally?

Further analysis by the showed that it was caused by
(WHO) The expert group (CAUSE, WHY)

.....

Write the opening paragraph for a newspaper article about the EQAO D-Dos (October 20, 2016).

On *October 20*, *2016*, the *Gr 10 students* of *Brampton Centennial*,
(WHEN) Specific Date Year (WHO) Group of people (WHERE) City

were shocked to discover *their EQAO literacy test screens were completely frozen.*
(WHAT) What happened to them, generally?

Further analysis by the *OPP* showed that it was caused by
(WHO) The expert group (CAUSE, WHY)

.....

Write the opening paragraph for a newspaper article about the EQAO D-Dos (October 20, 2016).

On October 20, 2016, the Gr 10 students of Brampton Centennial,
(WHEN) Specific Date Year (WHO) Group of people (WHERE) City

were shocked to discover . . . *their EQAO literacy test screens were completely frozen.*
(WHAT) What happened to them, generally?

Further analysis by the *OPP* showed that it was caused by *a hacker*
(WHO) The expert group (CAUSE, WHY)

who unleashed a D-Dos attack to stop the on-line literacy test..