

# Security Threats

And how to stop them.

Ransomware: Don't get locked out

Government of Canada Gouvernement du Canada

Canada.ca | Services | Departments| Français

# Canadian Centre for Cyber Security

## Canada

Search Canada.ca

Information & Guidance Services Cyber Incidents Education & Training Building the Community

Home → Ransomware: Don't get locked out

**ALERT**

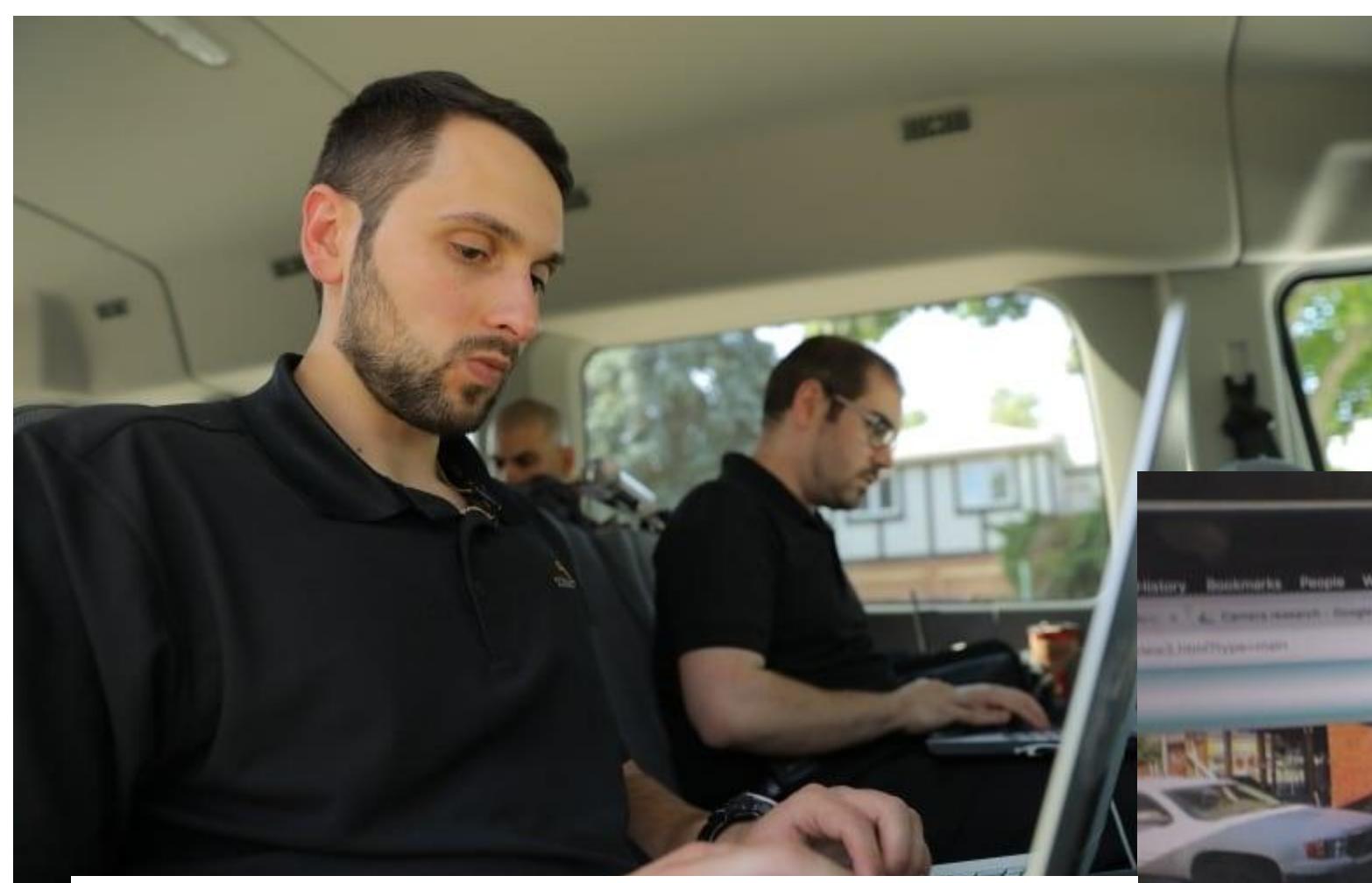
**Canadian organizations exploited via unpatched devices and inadequate authentication**

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





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



Windows Error Report - Message (HTML)

File Message Tell me what you want to do Hide

Junk Delete Archive Reply Reply All More Create New Meeting Move OneNote Actions Mark Categorize Folks Unread Up Delete Respond Quick Steps Move Tags

Microsoft Team <no-reply\_msteam2@outlook.com> Windows Error Report

Windows User Alert

## Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found an unknown source. When our security officers investigated, it was found out that someone from foreign IP network which can corrupt your windows license key.

Sign-in details:  
Country/region: Lagos, Nigeria  
IP Address: 293.09.101.9  
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your network contact Security Communication Center and report to us immediately. [1-800-816-0380](#) or substitute you can file the consumer complaint form. Once you call, please provide your Reference no: AZ- 1190 in order for technicians to resolve the issue.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory changes to your Windows Device.

[Review recent activity](#)

**From:** Nokia <[info@news.nokia.com](mailto:info@news.nokia.com)>  
**Subject:** SAVE YOUR STUFF! Sign in to your Nokia account before it disappears forever!  
**Date:** February 7, 2014 2:38:02 AM MST  
**To:** [info@news.nokia.com](mailto:info@news.nokia.com)  
**Reply-To:** Nokia <[info@news.nokia.com](mailto:info@news.nokia.com)>

**NOKIA**

## SAVE YOUR STUFF!

We noticed you haven't used your Nokia account to access Nokia services in quite a while. To protect your privacy, this account will be deleted in 14 days, [so sign in now](#).

If you haven't experienced Nokia services recently, they're worth another look. And you may want to keep any maps, locations, email, music, reviews, or other stuff that is associated with your account.

It just takes a few seconds to [sign in to your Nokia account](#).

We hope to see you soon.

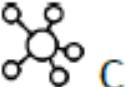
Sincerely,  
The Nokia account team

Privacy policy | Terms and conditions | Support | Contact us  
Nokia Corporation P.O. Box 226 FI-00045  
Nokia Group Finland

© 2014 Nokia

Phishing Emails

# Security Problems

2.9 

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



# How Viruses Work



## ① The virus arrives

**Most viruses show up inside e-mail attachments.**

110010101	0	0100111101010101
0 0 0 1 0 1 0 1		11110 0 0 0 1 0 1
1100101010	-	1101010101
000101010111	0	0 110010
10100101010011	0	0 0 0 0 1 0 1
0101110111000010		0 1

## 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.**

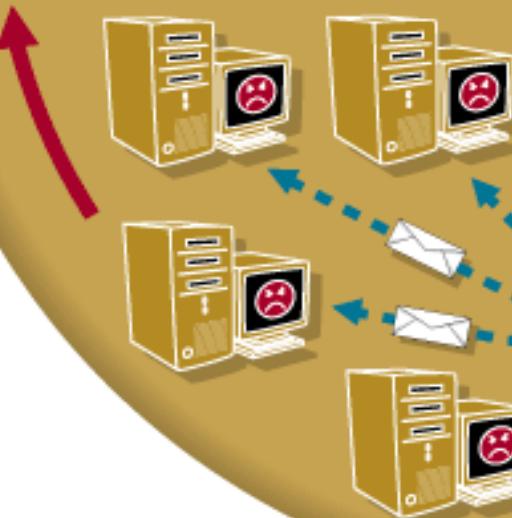
## ② Something pulls the trigger

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

.MP3

.JPG

100



### 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



"All the News  
That's Fit to Print"

Late Edition  
New York: Today, mostly sunny and hot. High 81. Tonight, clear and warm. Low 75. Tomorrow, partly sunny, humid, a late storm. High 81. Yesterday, high 80, low 75. Details, Page B1.

VOL. CLII . . . No. 52,576 + Copyright © 2003 The New York Times NEW YORK, FRIDAY, AUGUST 15, 2003 ONE DOLLAR

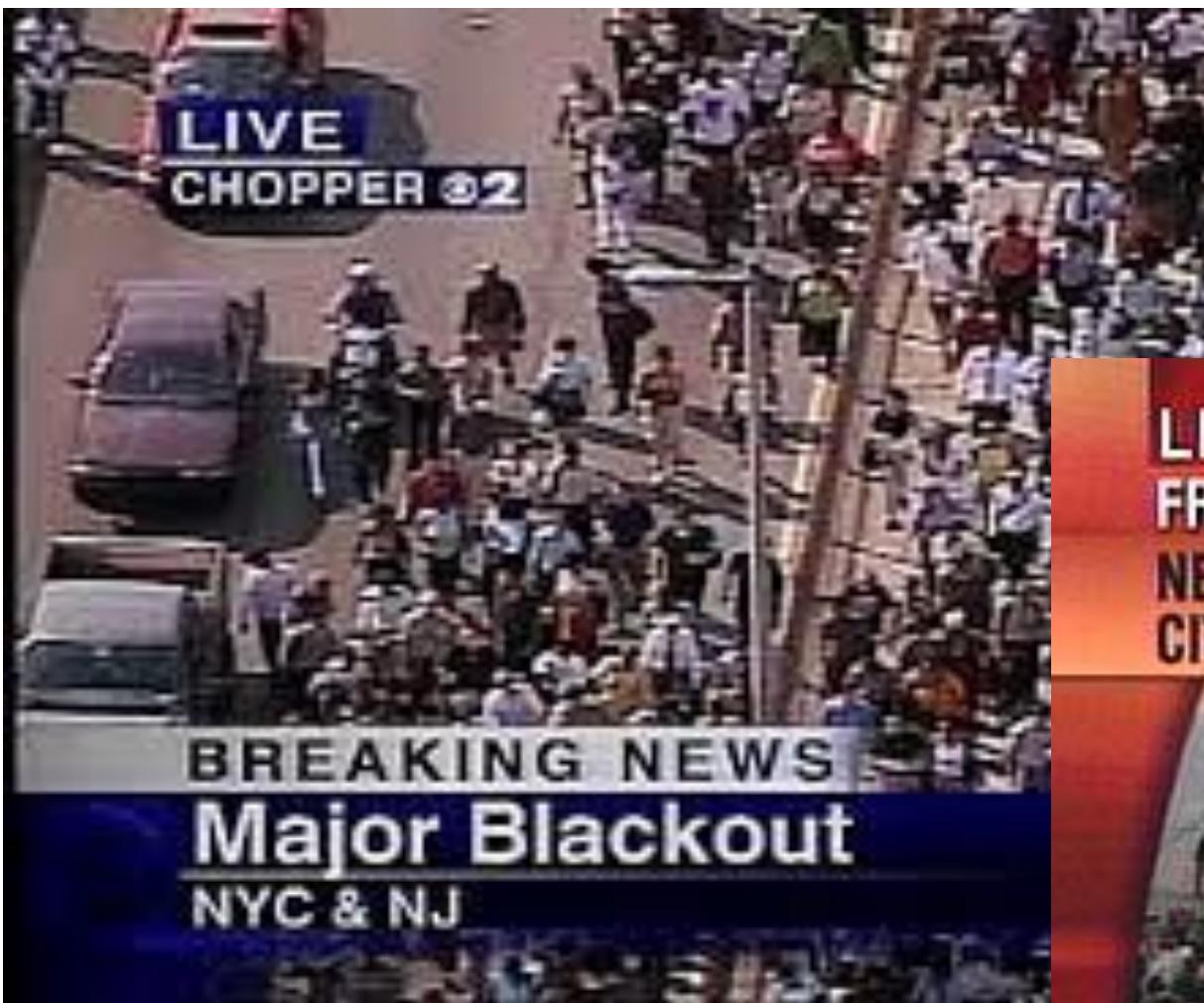
## POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN CANADA AND 8 STATES; MIDDAY SHUTDOWNS DISRUPT MILLIONS

OVERLOADED GRID  
Buildings Are Evacuated  
and Hospitals Fill —  
Bush Plans Review

JAMES BARRON  
A surge of electricity to western New York and Canada touched off a series of power failures and forced blackouts yesterday that left parts of the Northeast, the Great Lakes region and the Midwest without electricity. The widespread failures provided the evacuation of office buildings, stranding thousands of commuters and flooded some hospitals with people suffering in the stifling heat.  
In an instant that one utility official called "a blink-of-the-eye second" shortly after 1 p.m., the grid that supplies electricity to the eastern United States became overloaded. That tripped circuit breakers and other protective devices at gen-

11 deaths  
Cost \$6 billion

I SAT GeoStar 45  
23:15 EST 14 Aug. 2003





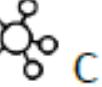
People in  
subways.





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

# Security Problems

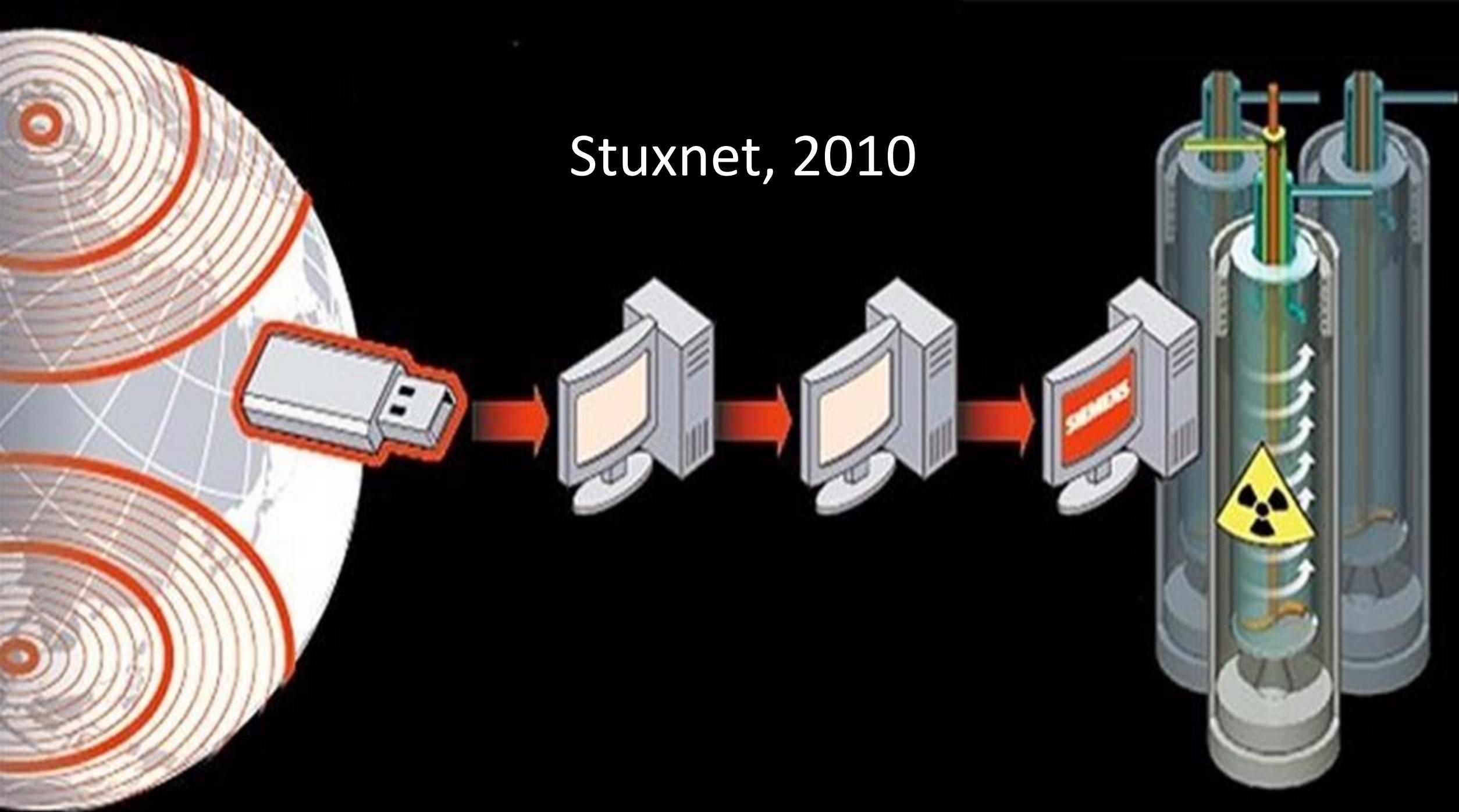
2.9 

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

# Centrifuges at Natanz (Iran) in 2008



# Stuxnet, 2010







Preliminary Purification

Initial Water Heating

View

Initial

Water

Heating

Preparation & Dosing

Final

Water

Temperature

Pressure

Flow

Level

Concentration

Quality

Time

Power

Cost

Efficiency

Capacity

Volume

Weight

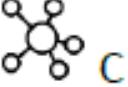
Size

Speed

Accuracy

Reliability

# Security Problems

2.9 

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



Ghostnet



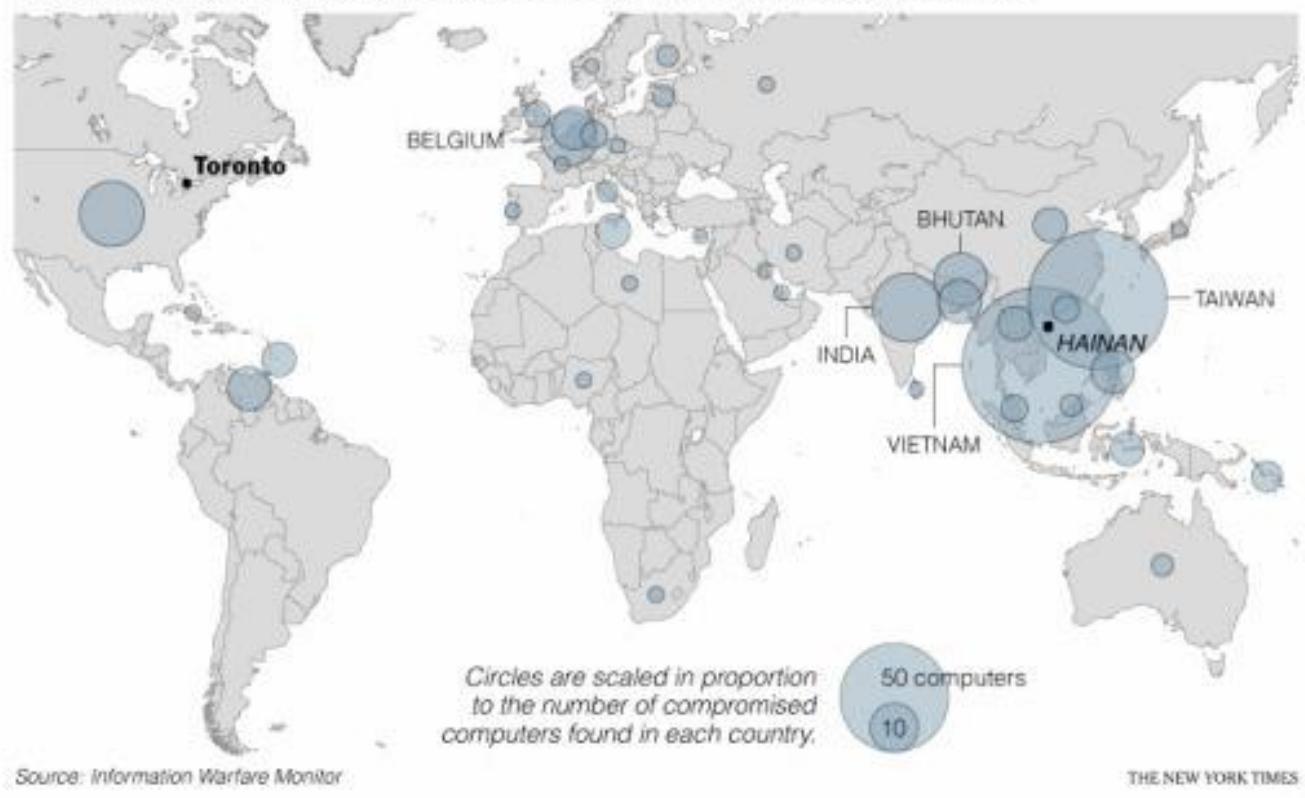
Using your webcam...  
and microphone.

The New York Times

March 28, 2009

## 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.



JR02-2009

## Tracking GhostNet:

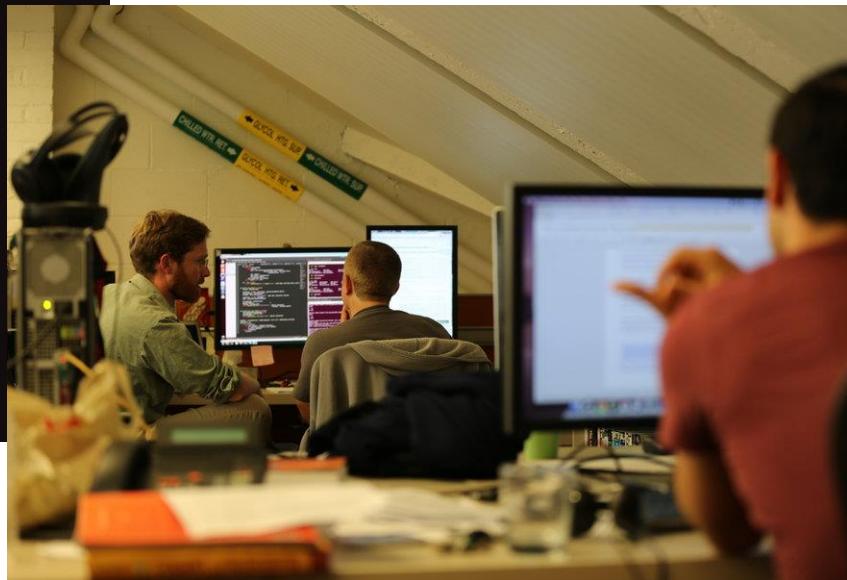
Investigating a *Cyber Espionage Network*

Information Warfare Monitor

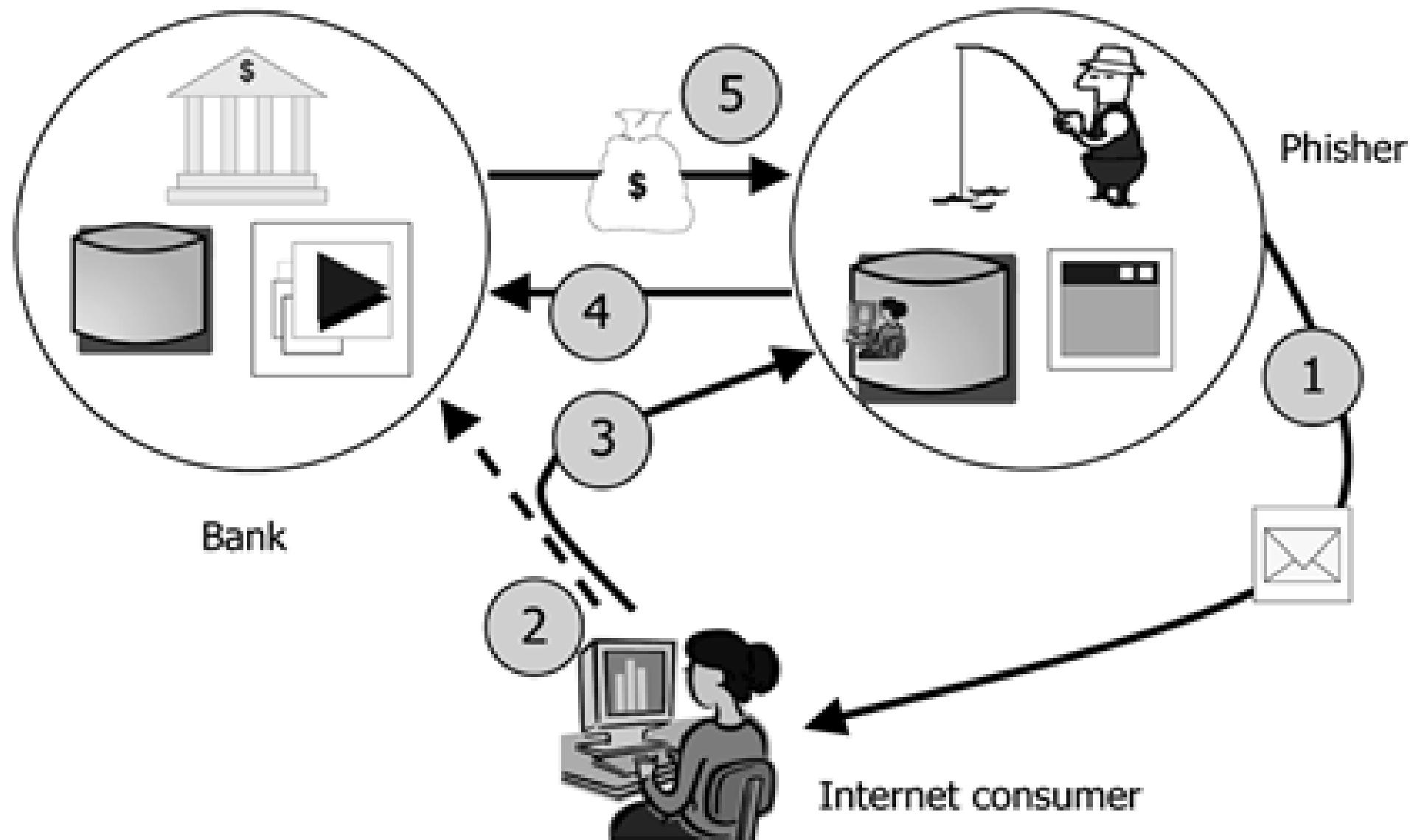
March 29, 2009



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



## How a Trojan can be used in a Phishing Attack:



# Security Problems

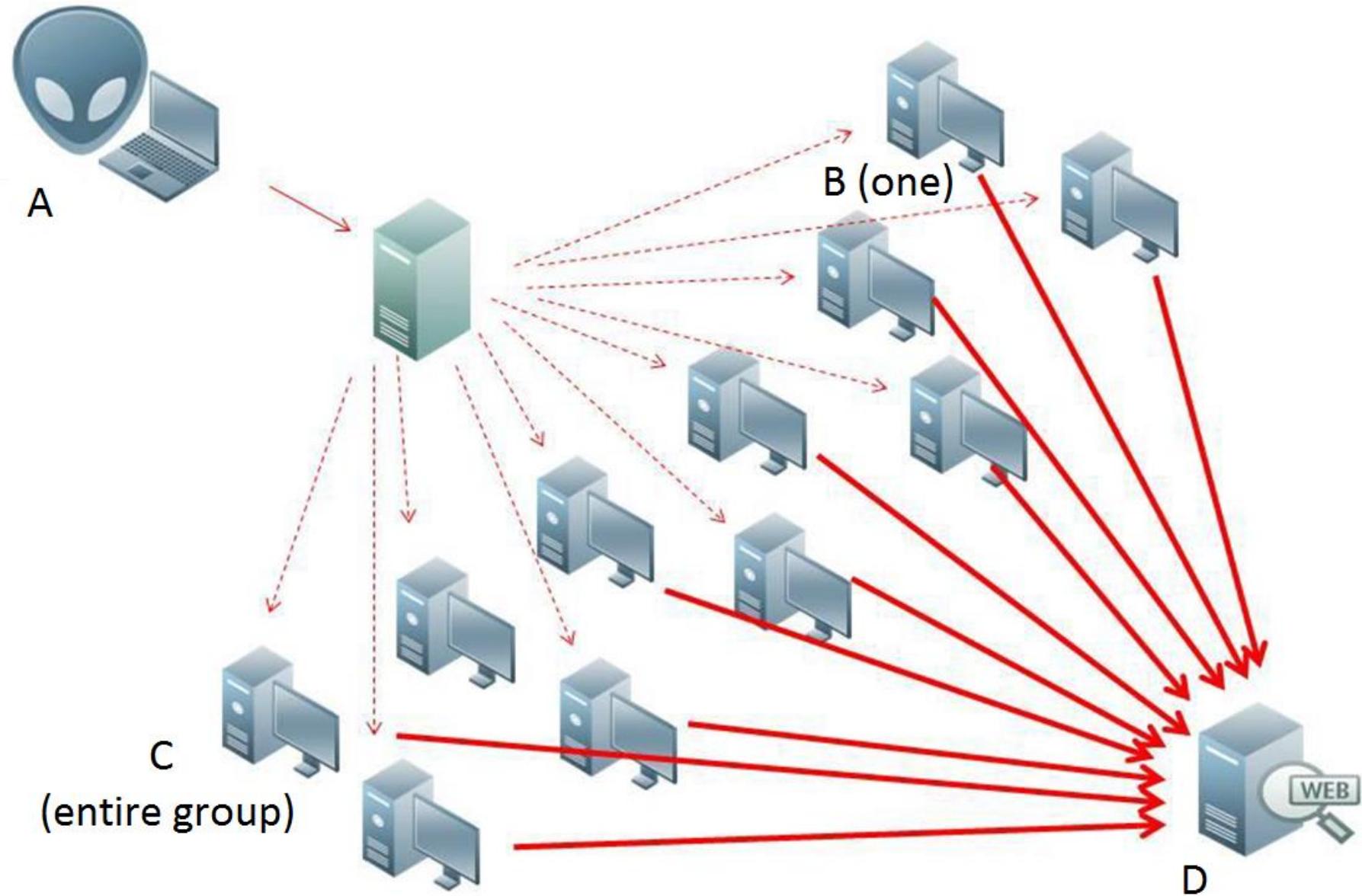
2.9 

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



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](#)



This site can't be reached

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

Try running Network Diagnostics.

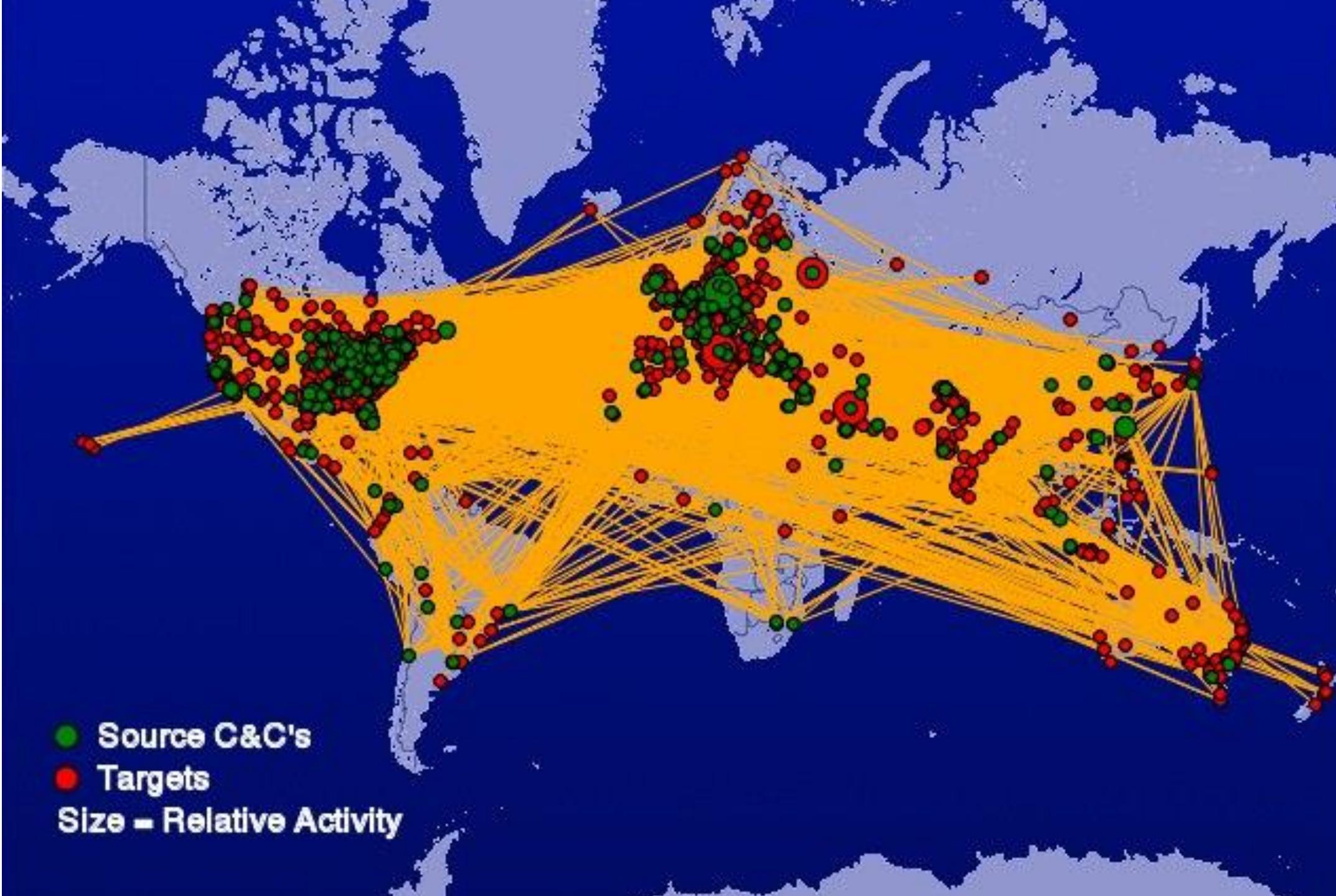
DNS\_PROBE\_FINISHED\_NXDOMAIN

Downloads winsome-file-re...

Reload









3 weeks  
Couldn't even  
access  
accounts  
outside the  
country.



## URGENT MESSAGE REGARDING TODAY'S ONLINE OSSLT

“...an intentional, malicious and sustained Distributed Denial of Service (DDoS) attack... initiated by an unknown entity or entities.”



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 

## *Further down the chart*

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

## **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.

## Section E Writing a News Report

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

## 1 Students Participate in Important Election



# 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.

### Section E Writing a News Report

page 7

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

#### ■ 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 .....,

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 ..... *residents* ..... of ..... *Tallinn, Estonia* .....,  
(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 ..... *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 ..... 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 ..... *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 .....  
(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 residents of Tallinn, Estonia,

were shocked to discover *that every network in their country wasn't working.*  
*(WHAT) What happened to them, generally?*

Further analysis by the NATO (WHO) *The expert group* showed that it was caused by Russian hackers (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).

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 *(CAUSE, WHY)*  
*(WHO) The expert group*

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

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..