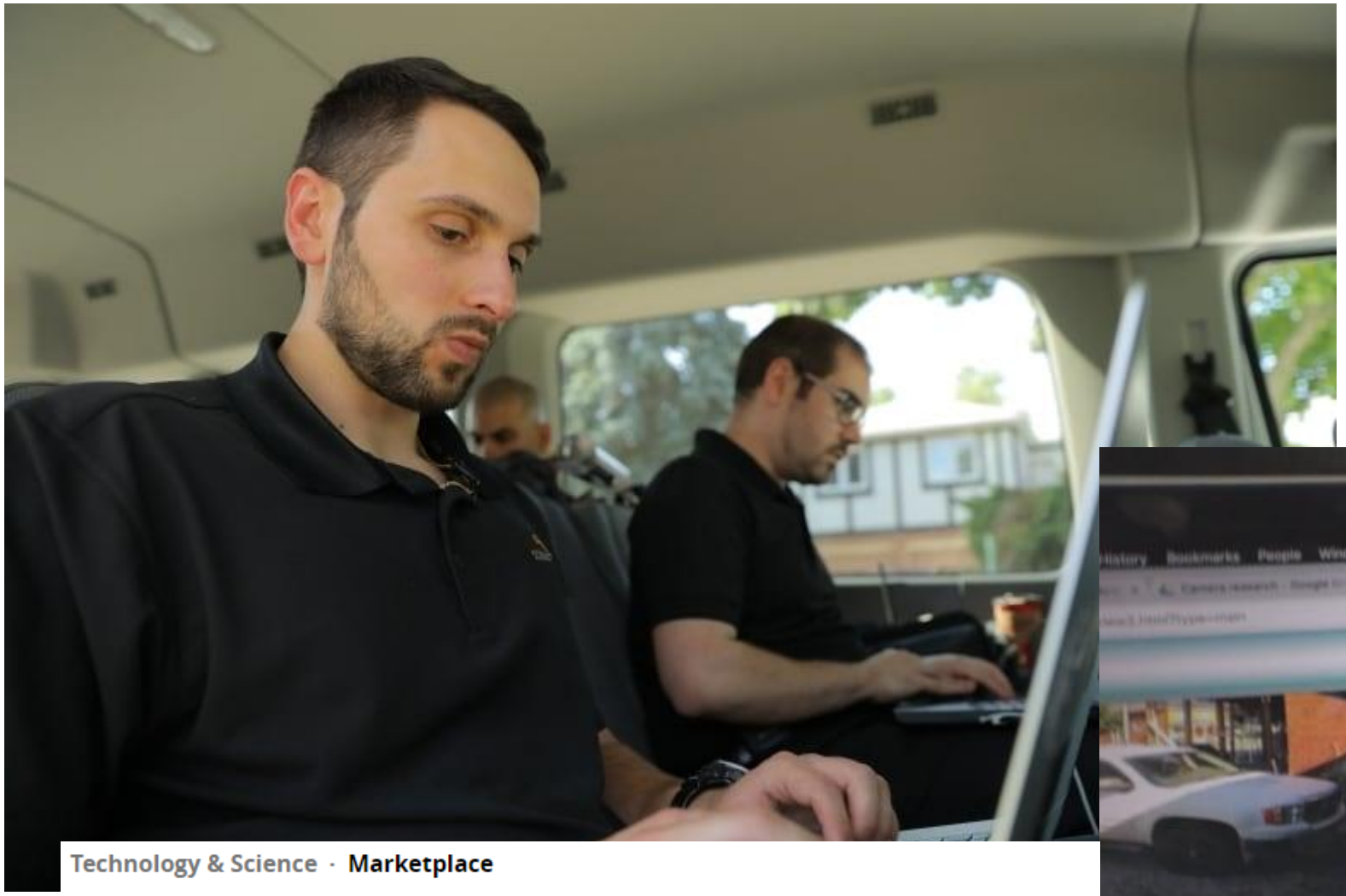
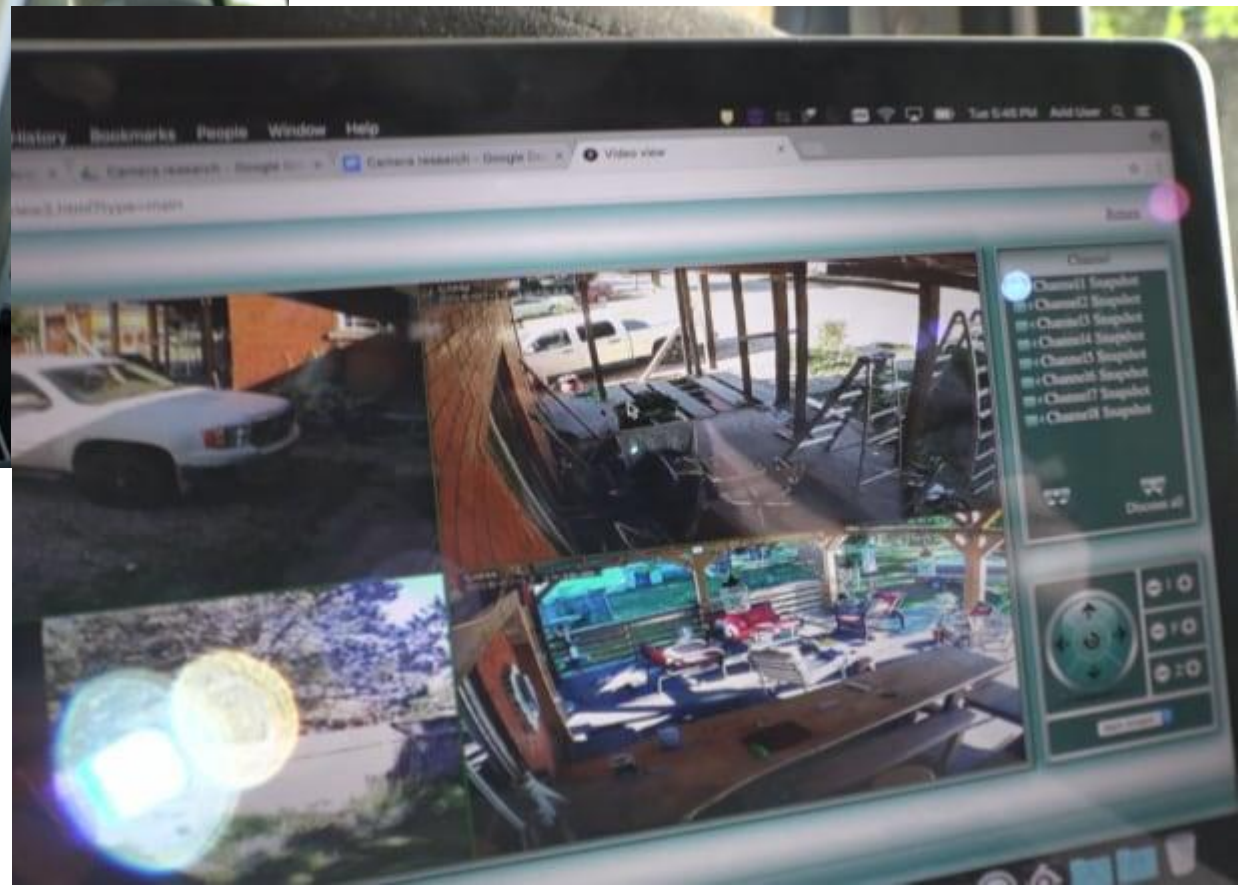

CYBER SECURITY



marketplace

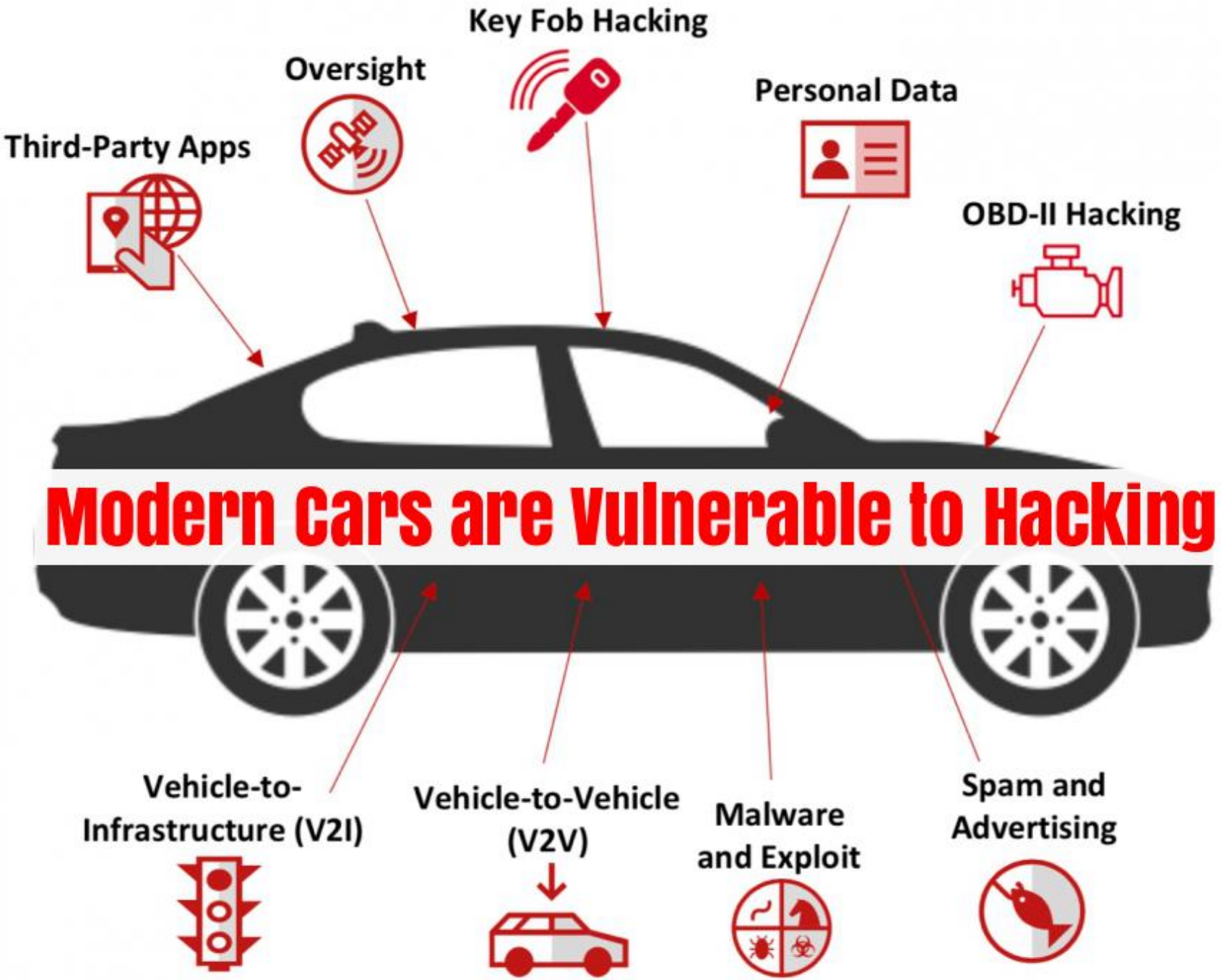


Technology & Science · **Marketplace**

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

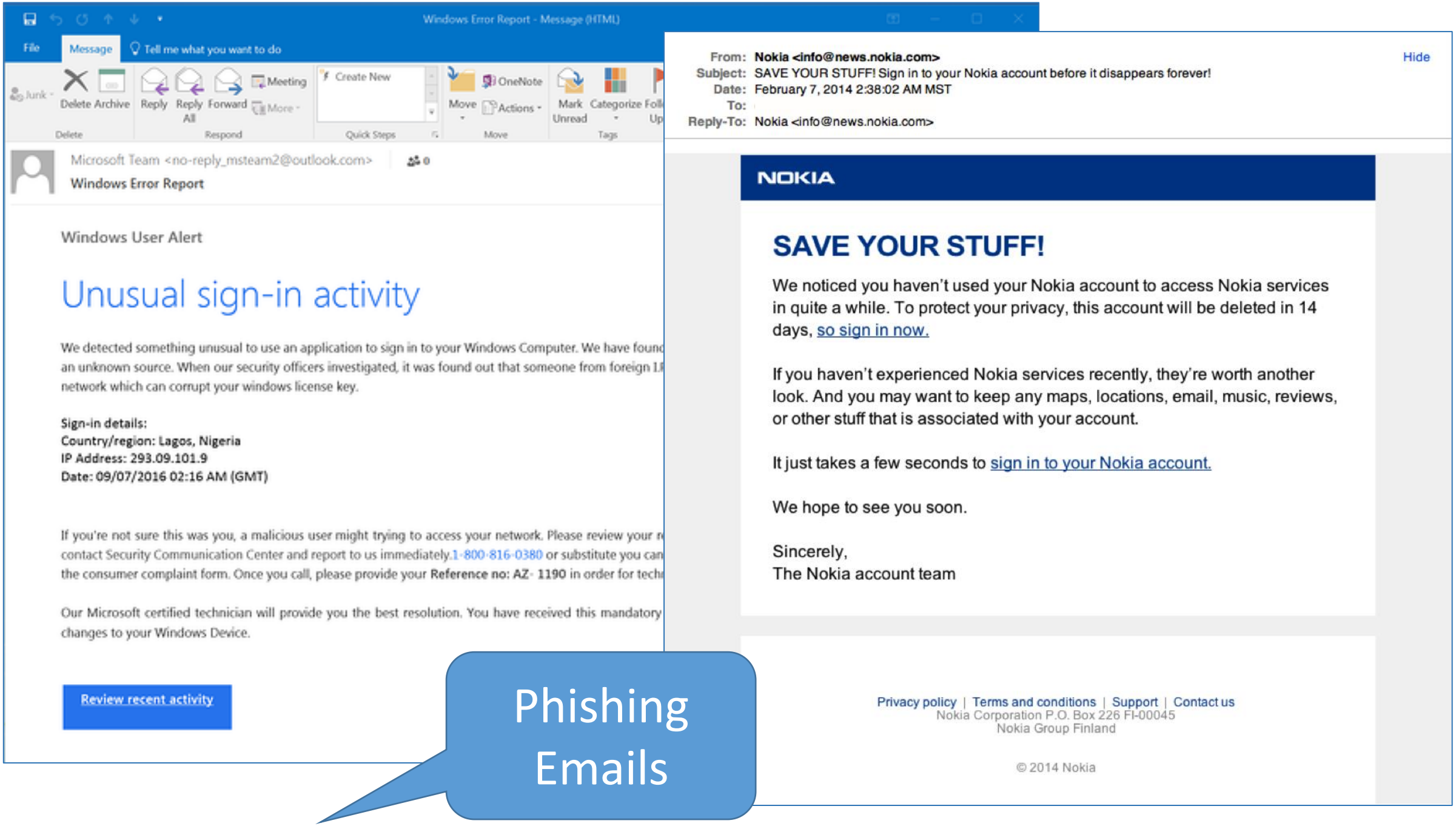


In 2012, researchers showed that it was possible to hack a car.

They used the radio to take control of the speed of the car.



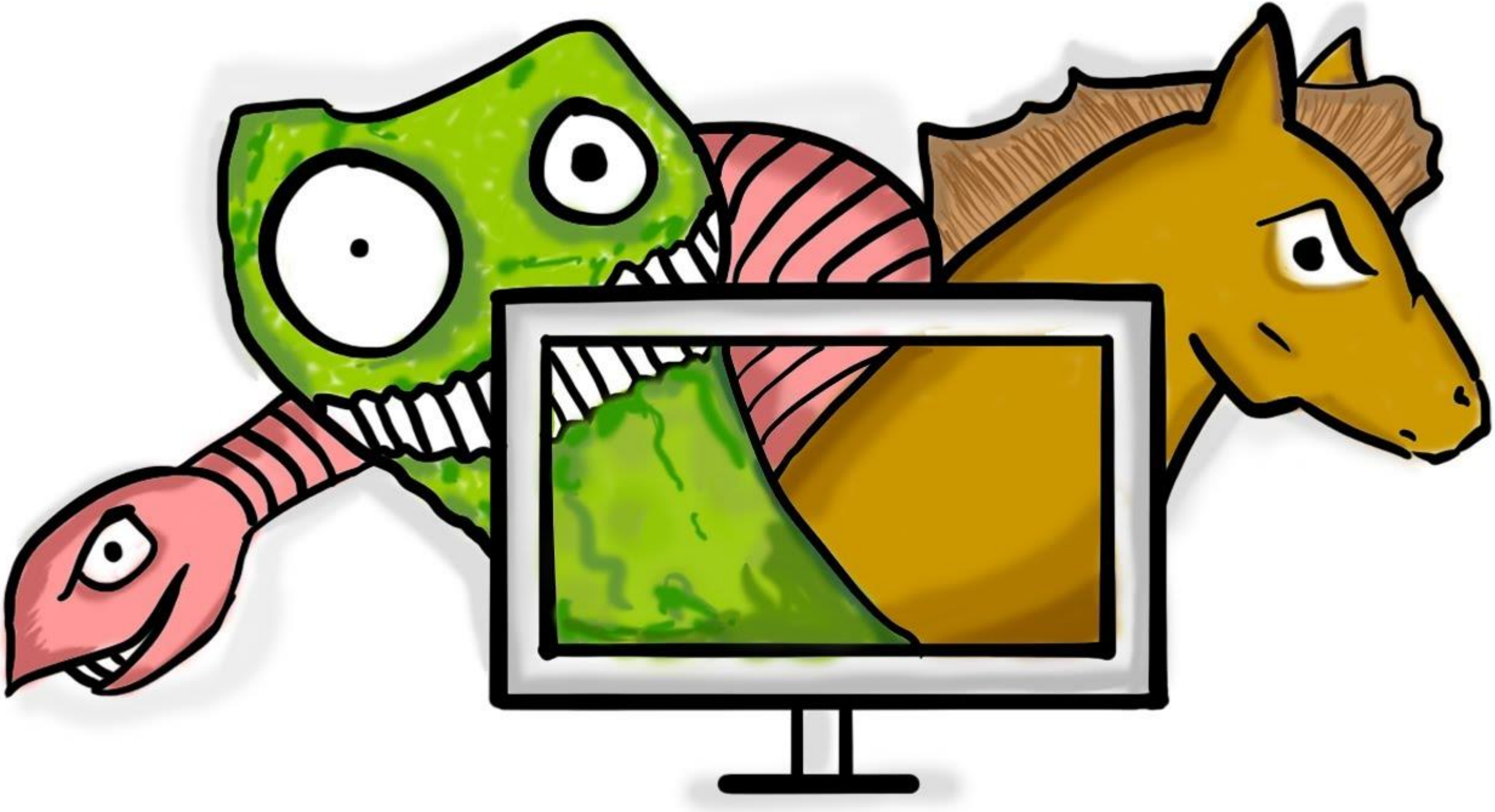
Researchers have also hacked Alexa. They were able to purchase things on the user's credit cards.


Windows Error Report - Message (HTML)
File
Message
Tell me what you want to do
Delete Archive
Reply
Reply All
Forward
Meeting
More
Create New
Move
OneNote
Actions
Mark Unread
Categorize
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 1
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 n
contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can
the consumer complaint form. Once you call, please provide your Reference no: AZ- 1190 in order for techi
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>
Subject: SAVE YOUR STUFF! Sign in to your Nokia account before it disappears forever!
Date: February 7, 2014 2:38:02 AM MST
To:
Reply-To: Nokia <info@news.nokia.com>
Hide
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 C

Name	Definition	Example
Hacking	Unauthorized access to a computer system	
	A form of _____ that can harm a computer system	_____ virus • 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 • 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

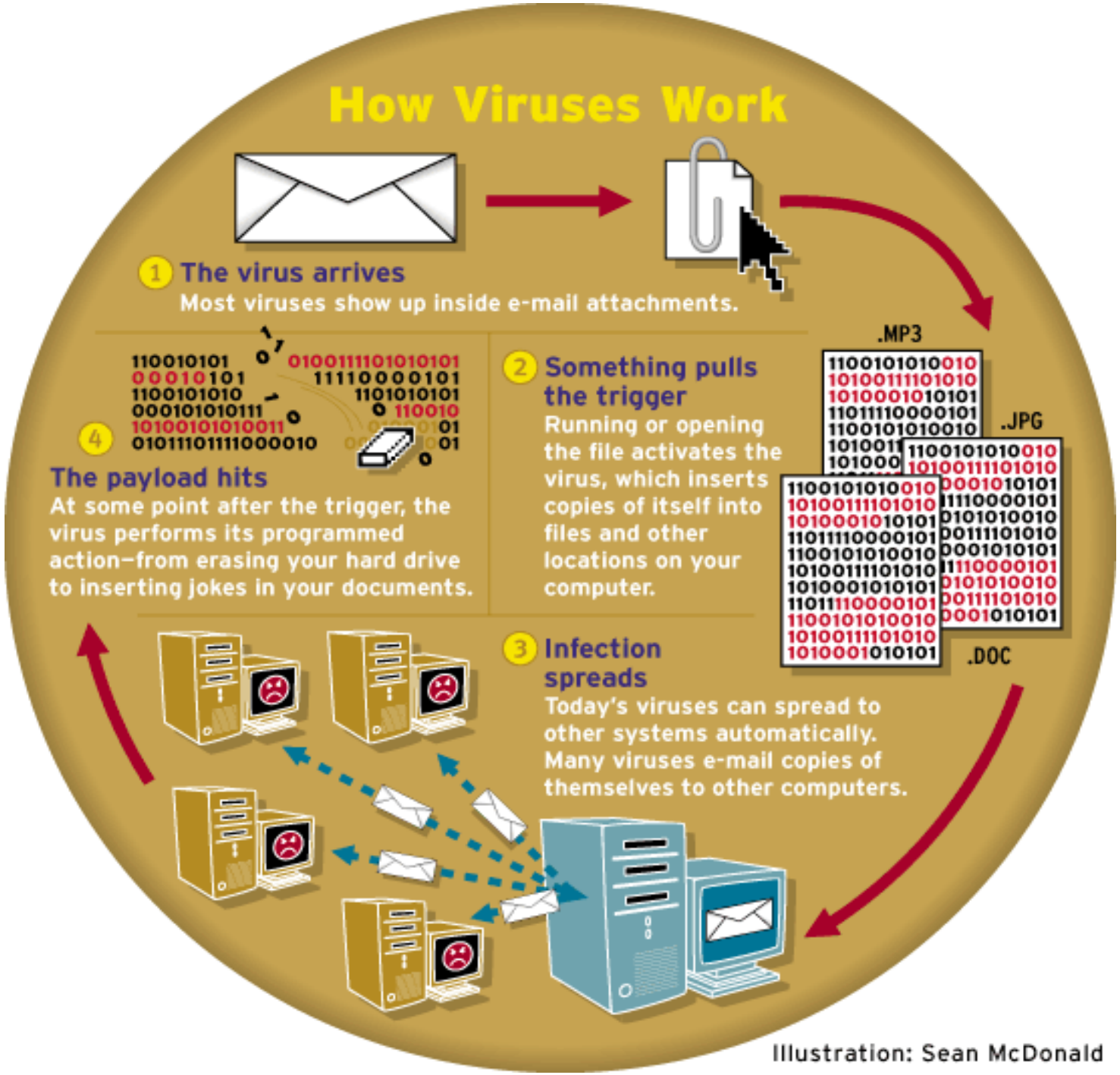


Illustration: Sean McDonald

Blaster Virus
August 2003







Disrupts Train Signals

Air Plane Booking systems are down.



Aug 14 Blackout



"All the News That's Fit to Print"

The New York Times

Late Edition

New York: Today, mostly sunny and hot. High 91. Tonight, clear and warm. Low 75. Tomorrow, partly sunny, humid, a late storm. High 87. Yesterday, high 88, low 75. Details, Page B11.

VOL. CLII . . . . No. 52,576 +

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

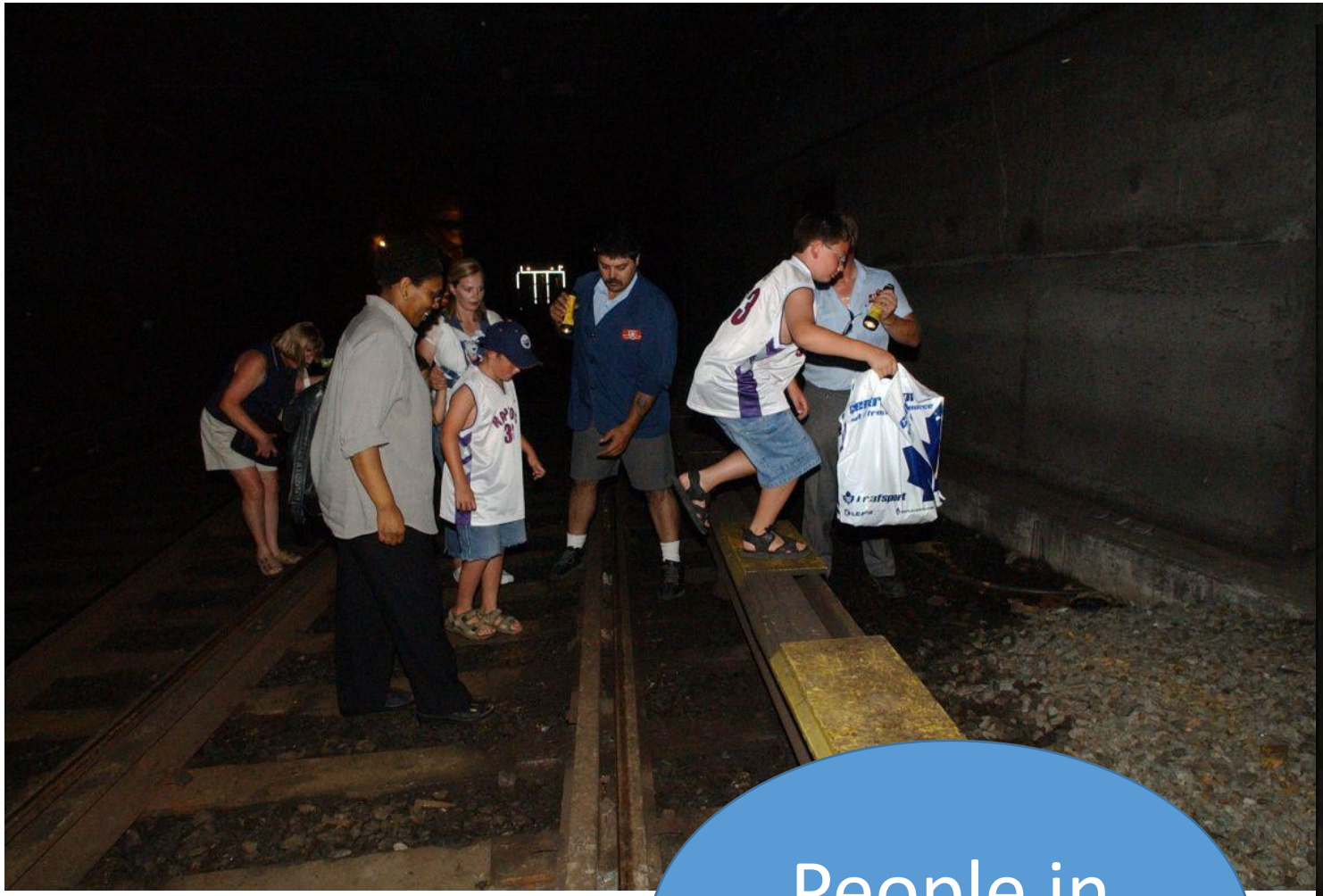
A surge of electricity to western New York and Canada touched off a series of power failures and forced blackouts yesterday that left parts of at least eight states in the Northeast and the Midwest without electricity. The widespread failures provoked the evacuation of office buildings, stranded thousands 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 4 p.m., the grid that distributes electricity to the eastern United States became overloaded. That tripped circuit breakers and other protective devices at gen-

11 deaths

Cost $6 billion


LIVE
CHOPPER 2
BREAKING NEWS
Major Blackout
NYC & NJ
LIVE
FROM
NEW YORK
CITY
WCBS
BREAKING NEWS
STATE OF EMERGENCY FOR
NEW YORK STATE
CNN
DOW
38.80



People in subways.




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

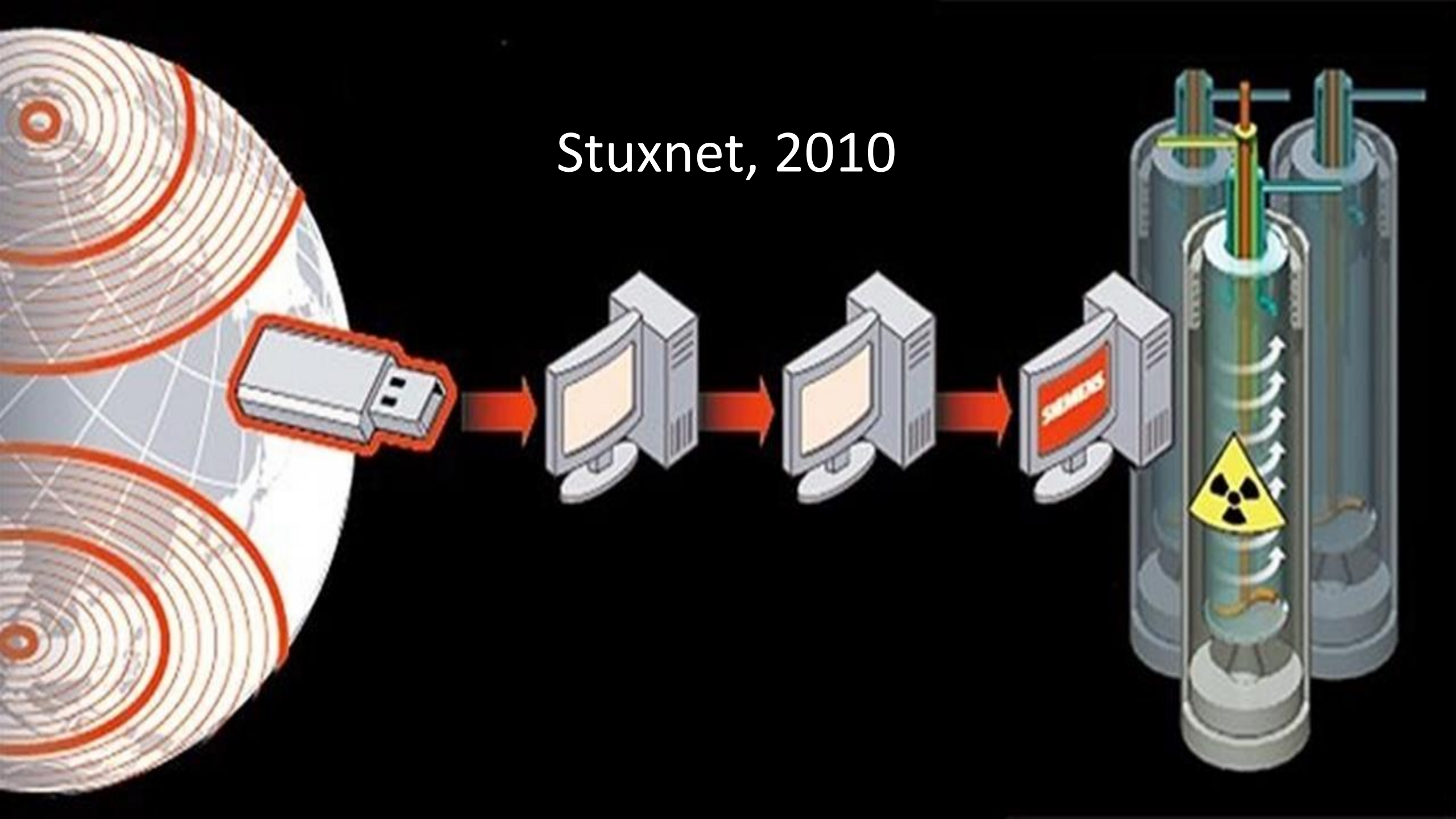
Security Problems

2.9 C

Name	Definition	Example
Hacking	Unauthorized access to a computer system	
Virus	A form of malware that can harm a computer system	Blaster virus • 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 • 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.


Centrifuges at Natanz (Iran) in 2008

Stuxnet, 2010




ZERODAY


W
E
R
S
STUXNET
D
DUQU
F
FLAME
G
GAUSS
Z
X
C
V
B

Security Problems

2.9 C

Name	Definition	Example
Hacking	Unauthorized access to a computer system	
Virus	A form of malware that can harm a computer system	Blaster virus • Caused the Northeastern blackout in August 2003 • Caused 11 deaths, $6 billion in damages
Worm	A form of a virus that can spread itself. It is another form of MALWARE.	Stuxnet worm • American + Israeli military hackers targeted Iran's nuclear reactors in 2010. • Zero-Day = used software bugs that had never been found before • Cyber war = a nation state attacking another's infrastructure using hacking or viruses.


Ghostnet

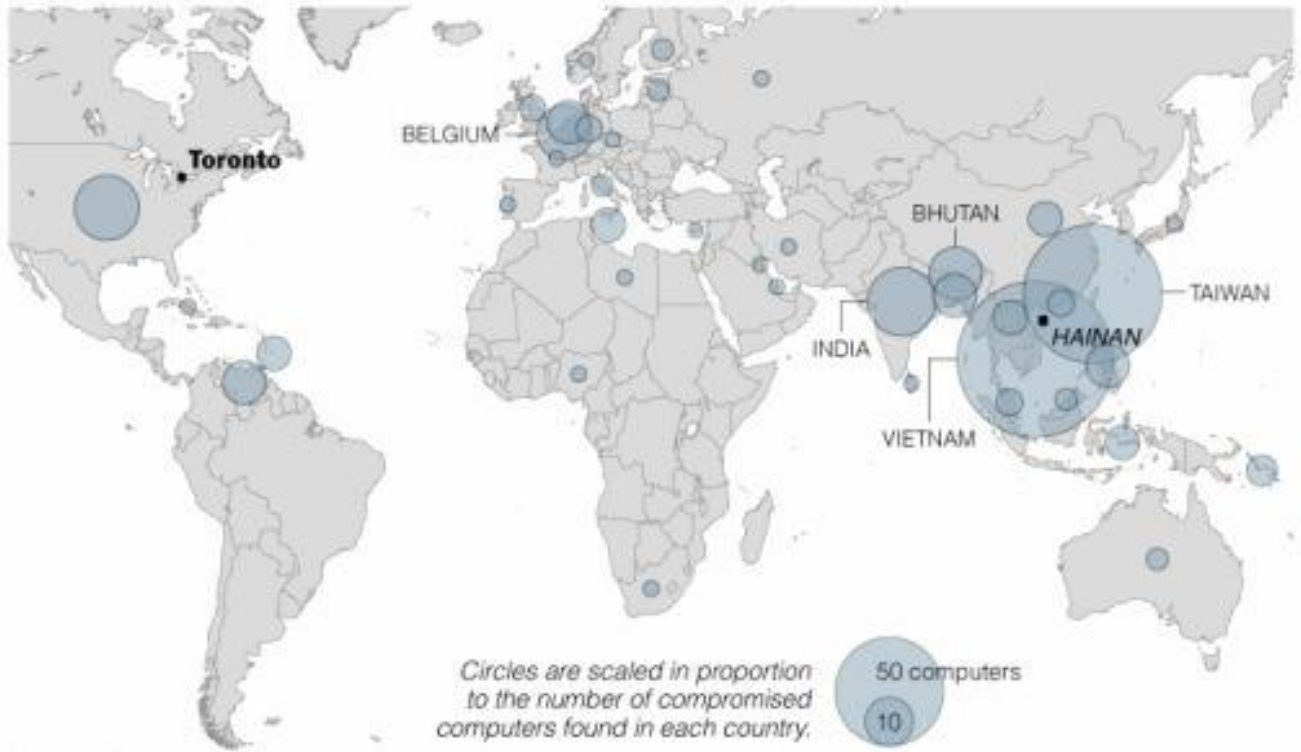


Using your webcam…
and microphone.

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.



Source: Information Warfare Monitor

THE NEW YORK TIMES

JR02-2009

Tracking *GhostNet*:

Investigating a *Cyber Espionage* Network

Information Warfare Monitor

March 29, 2009

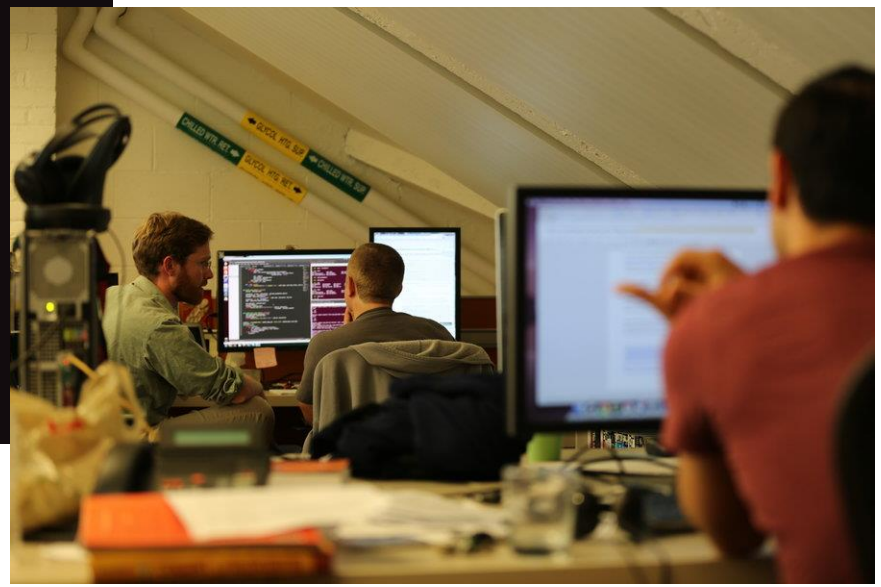
TheSecDevGroup

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

University of Toronto Munk Centre For International Studies At Trinity College

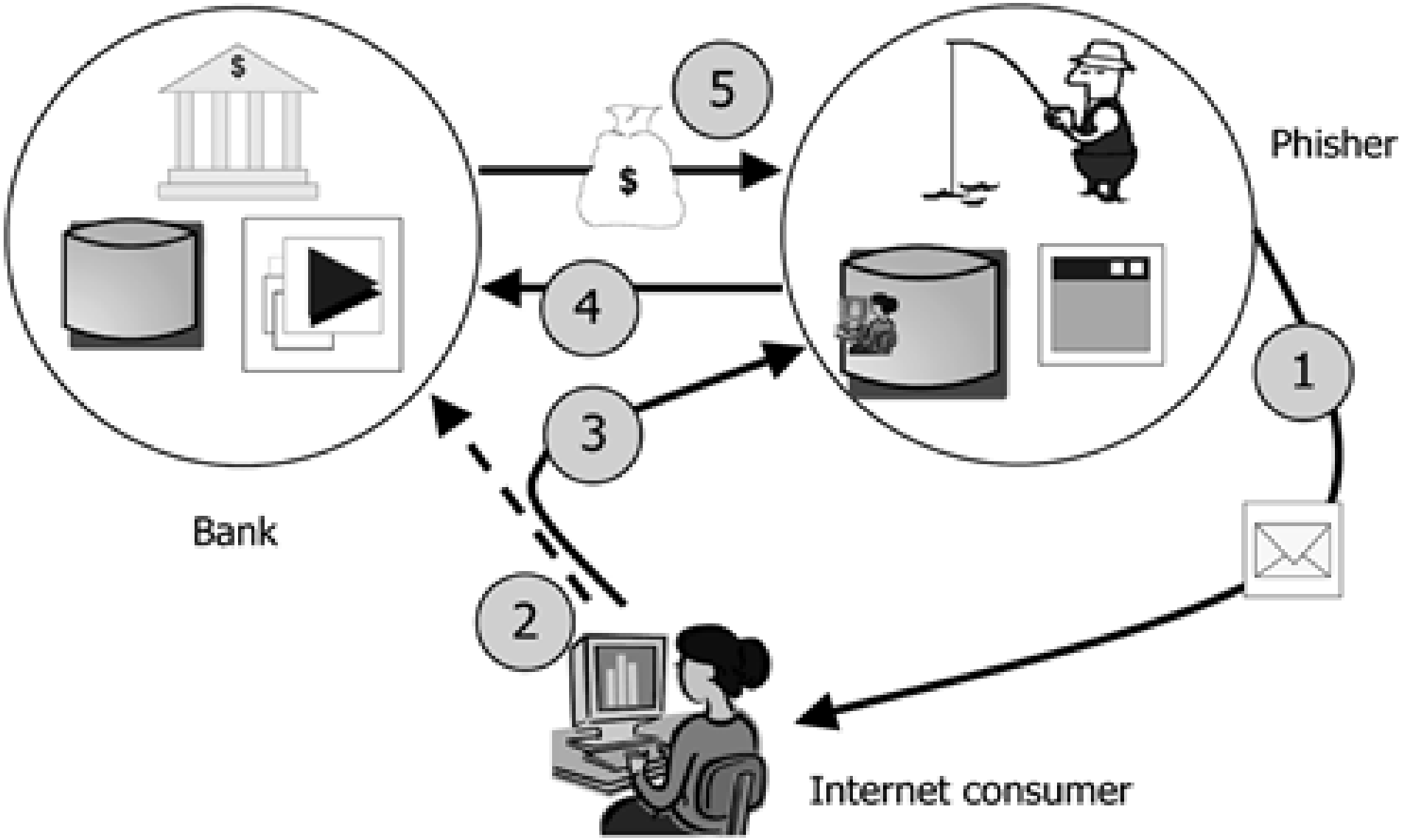
THE CITIZEN LAB







How a Trojan can be used in a Phishing Attack:



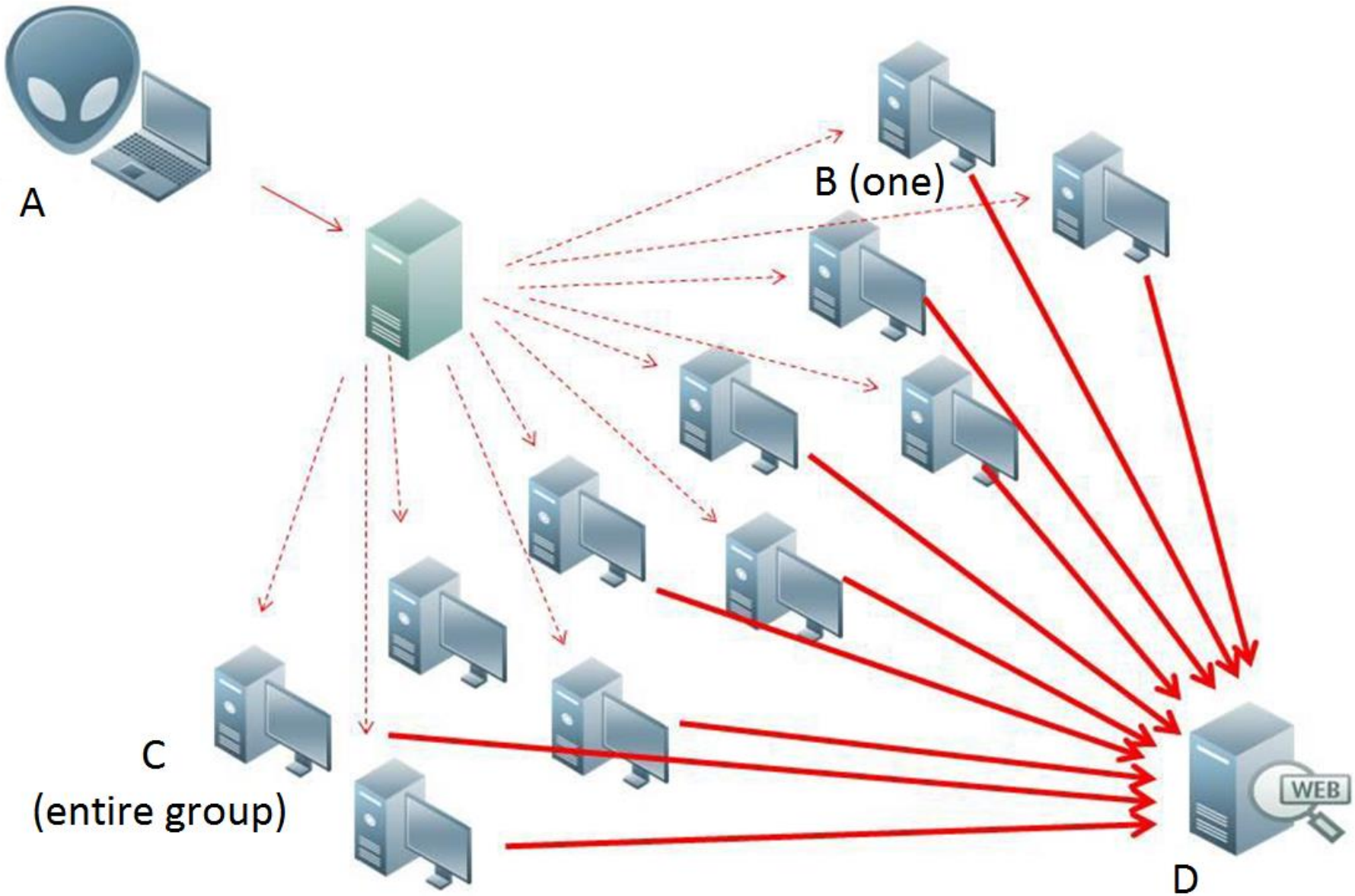
Security Problems

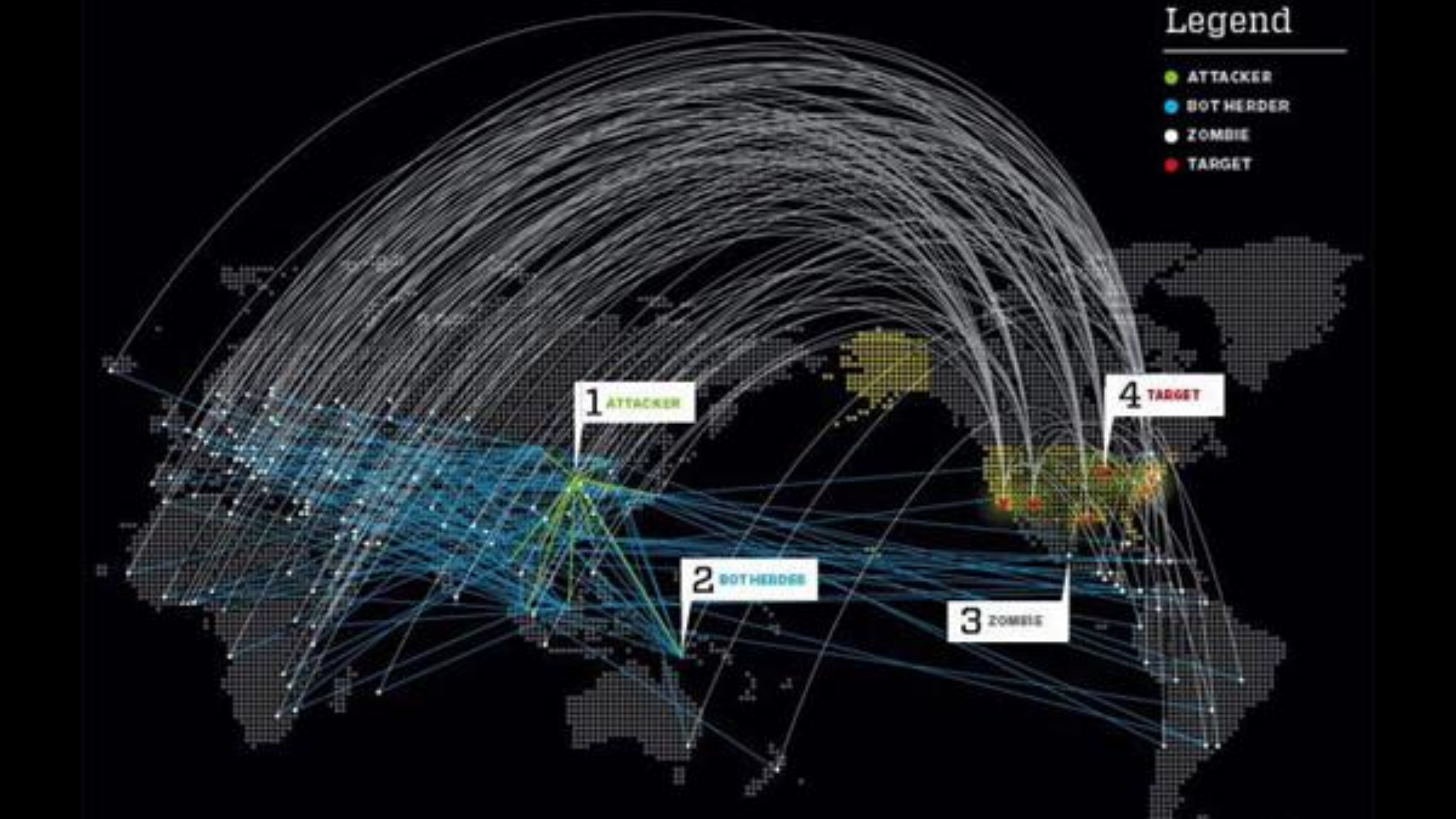
2.9 C

Further down the chart

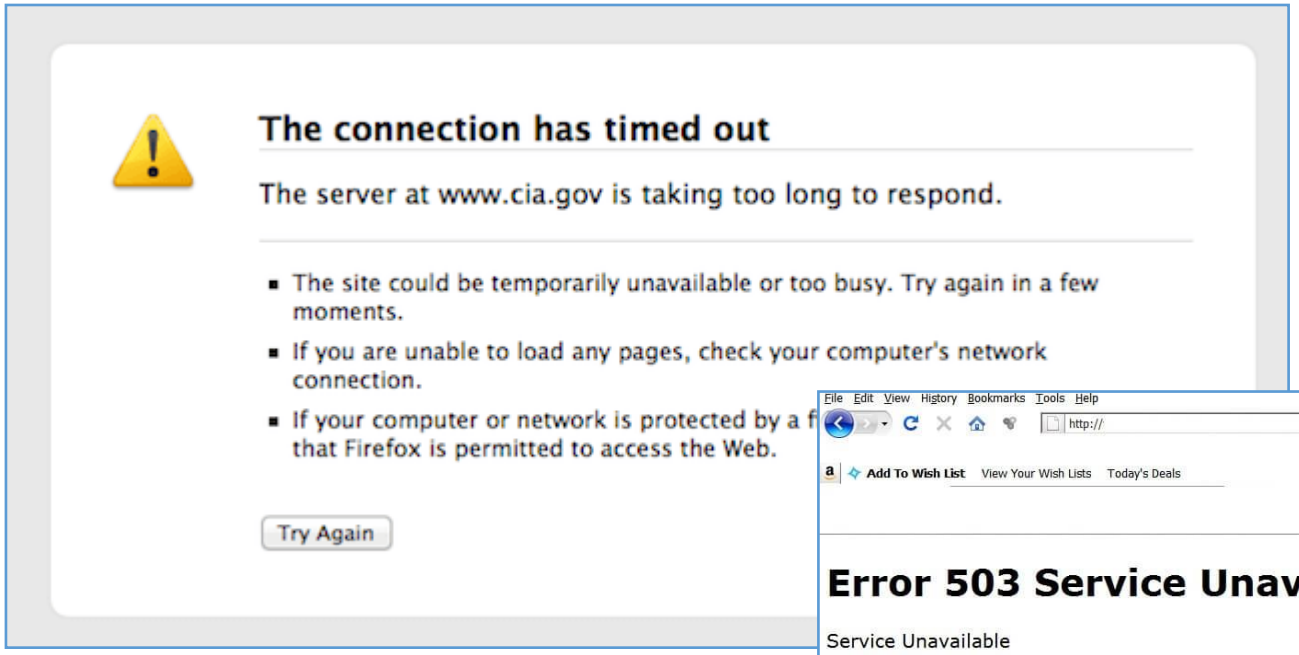
Trojan	A form of *malware* that grants a hacker complete access to your system.	*Ghostnet* • Found by Toronto's Citizen Lab in 2010. • Used by the Chinese government to listen in to government officials via webcam and microphones.
	• A hacker known as a _____, installs a Trojan on many computers. • These 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	_____ • 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.

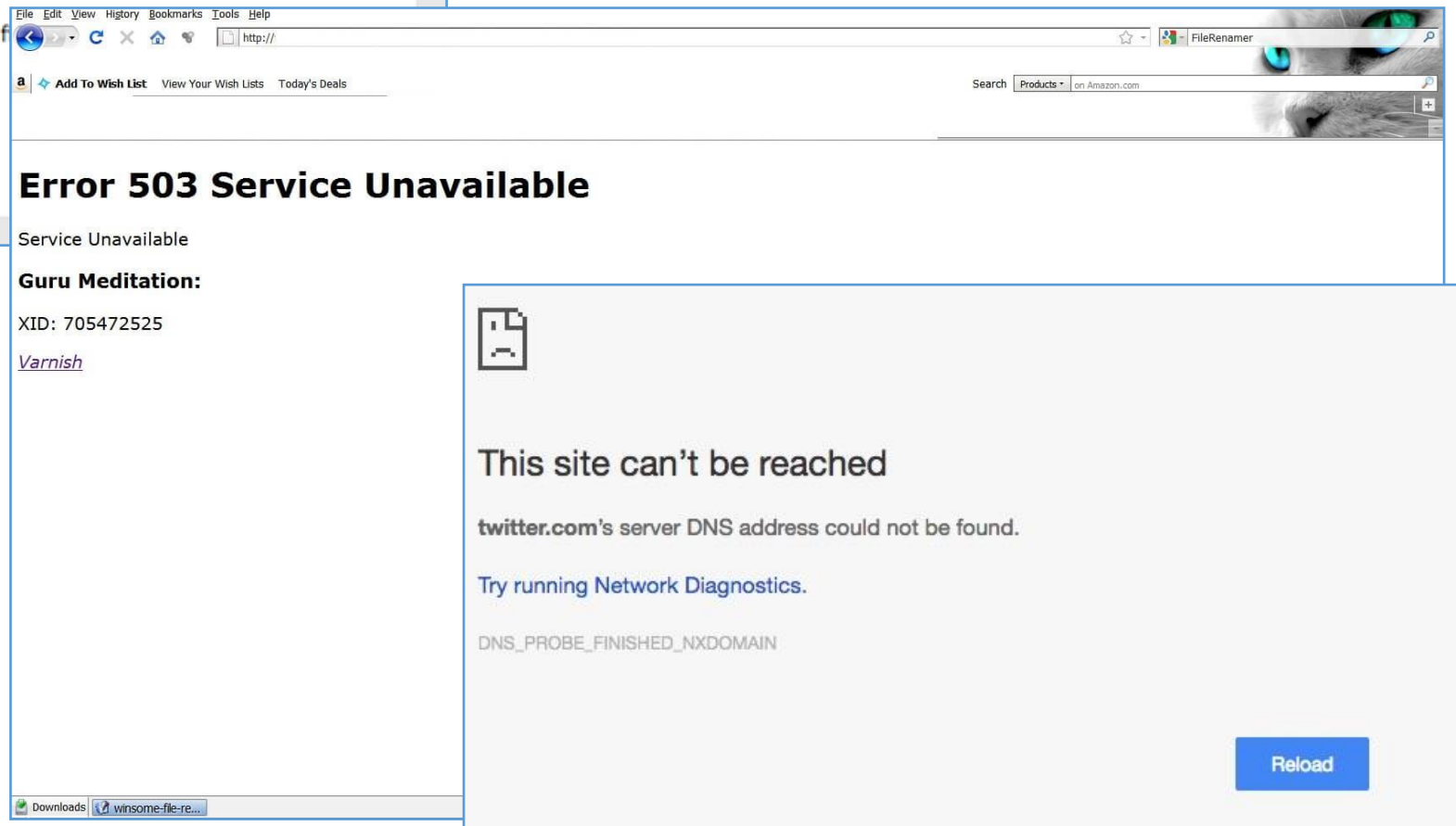

D-Dos

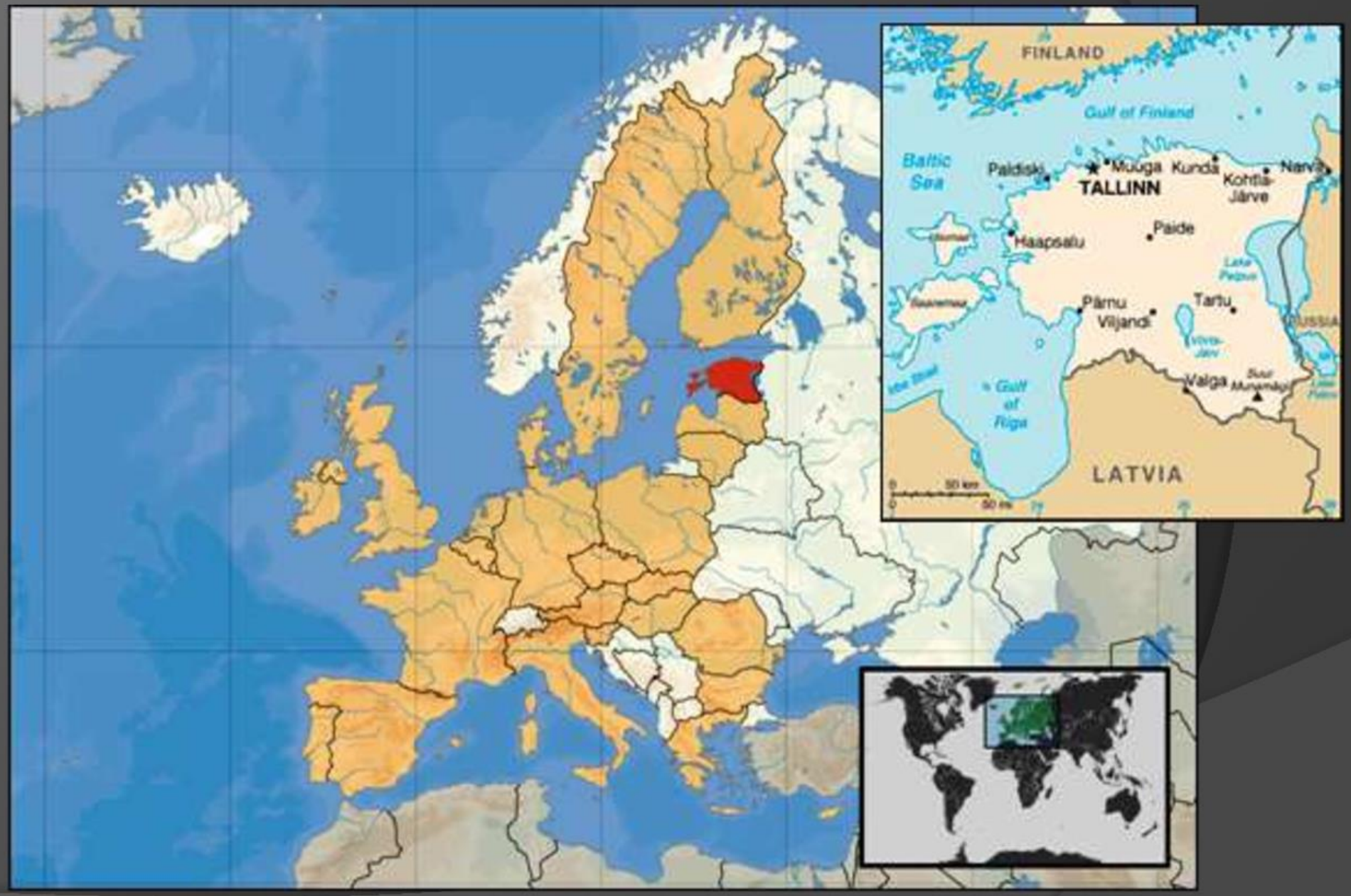

A
B (one)
C
(entire group)
WEB
D


Legend
ATTACKER
BOT HERDER
ZOMBIE
TARGET
1 ATTACKER
2 BOT HERDER
3 ZOMBIE
4 TARGET

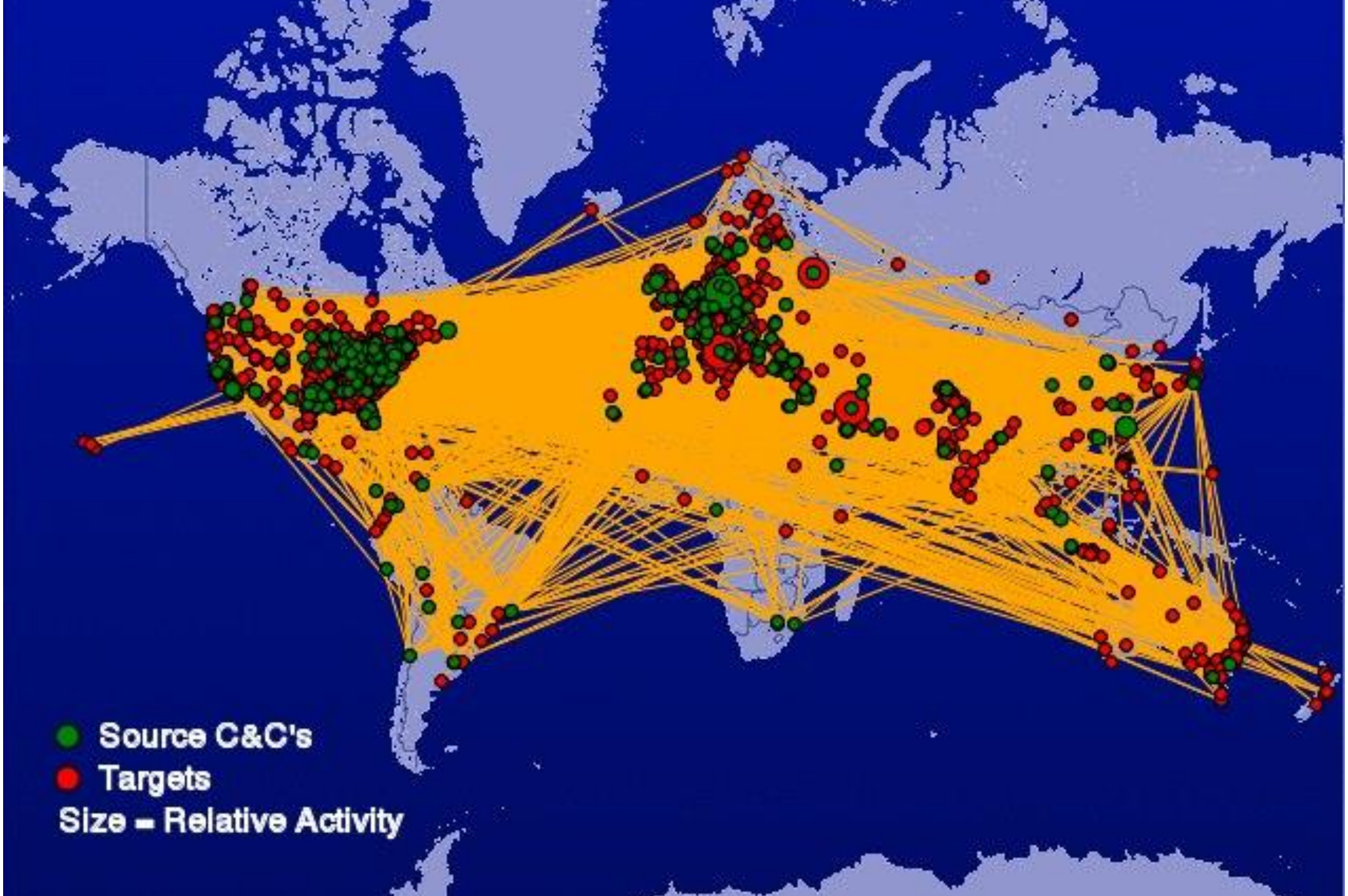
People trying to visit the site get this a time out message.






FINLAND
Gulf of Finland
Baltic Sea
Paldiski
Muuga
Kunda
Narva
TALLINN
Kohtla-Järve
Haapsalu
Paide
Pärnu
Viljandi
Tartu
RUSSIA
Valga
Gulf of Riga
LATVIA

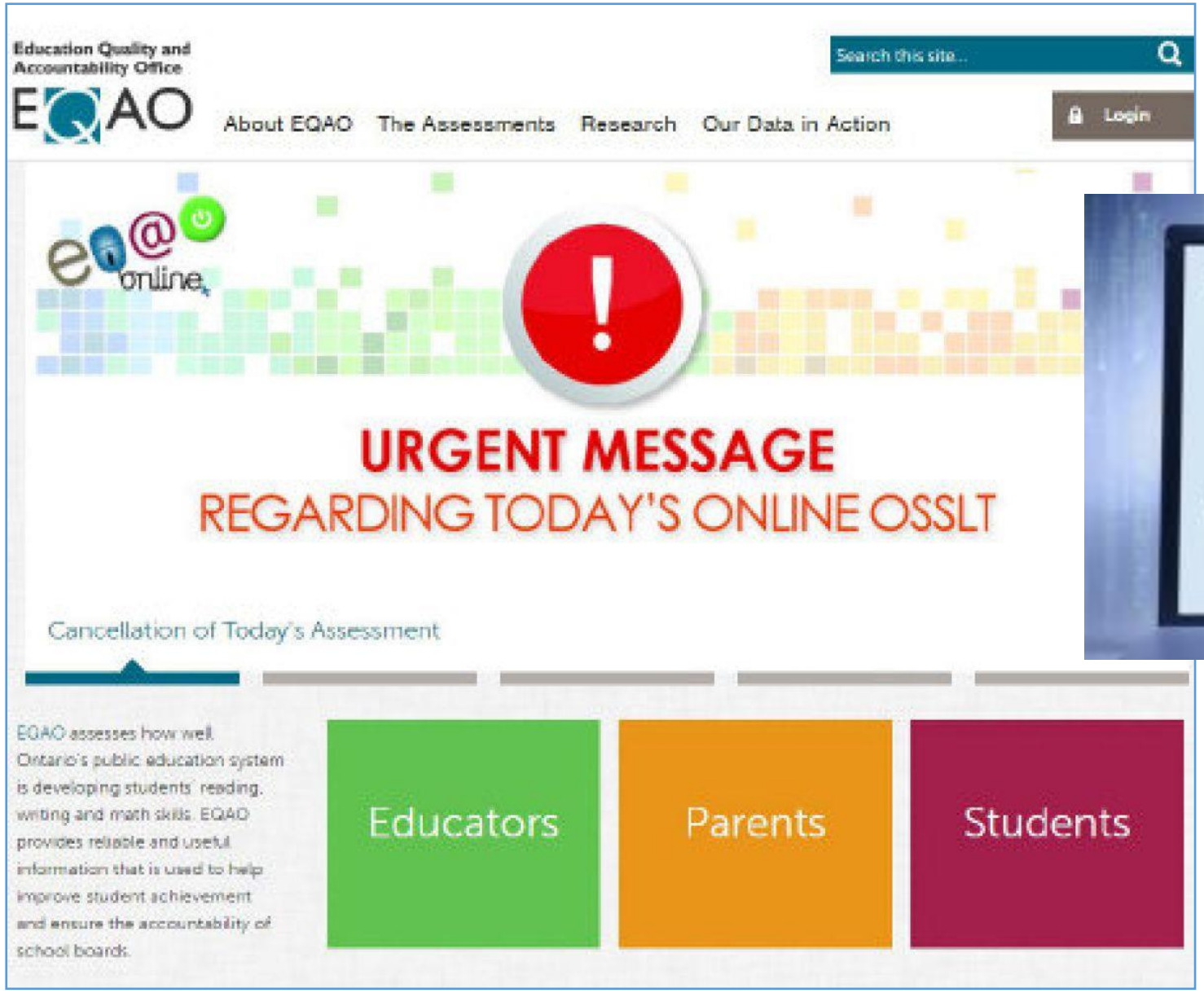

AP


Source C&C's
Targets
Size = Relative Activity



3 weeks

Couldn’t even access accounts outside the country.





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

Trojan	A form of *malware* that grants a hacker complete access to your system.	*Ghostnet* • Found by Toronto's Citizen Lab in 2010. • Used by the Chinese government to listen in to government officials via webcam and microphones
D-Dos attack Also called zombies.	• A hacker known as a *herder*, installs a Trojan on many computers. • These computers are known as *bots* and together they form a *botnet*. • The herder then uses all of the bots to overwhelm a website so no one can access it	*Estonia* • 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 *cyberwar* = a nation attacking another.

Ransomware: Don't get locked o

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

Canada

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




Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49
Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am





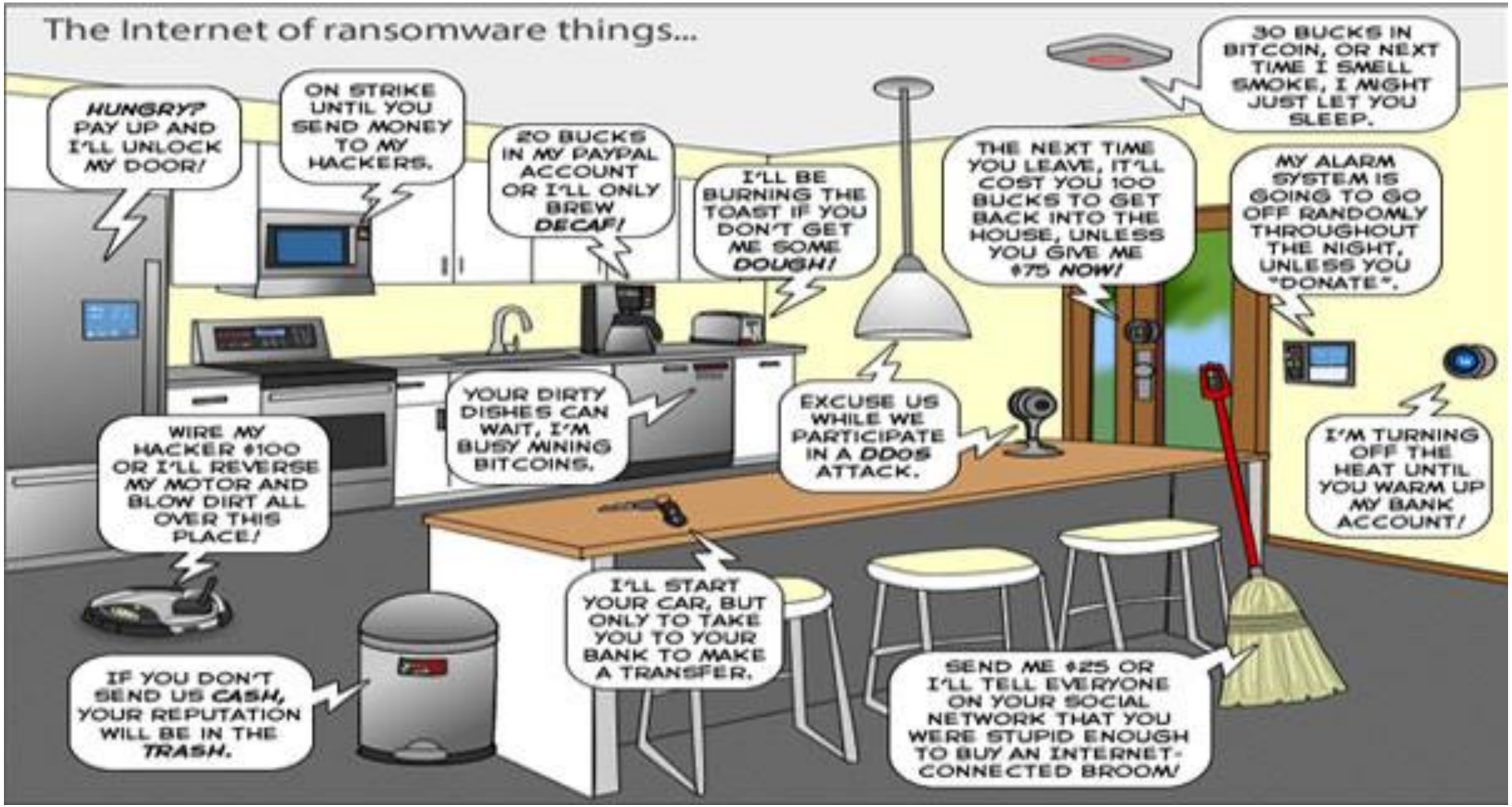
Smart thermostats have been hacked; the temperature was set to 90 degrees until the ransom was paid.

Security Problems

2.9 C

Further down the chart

Ransomware	• A hacker installs a virus on a computer that *encrypts* the files • To regain access to their files people must pay a *ransom* often using *Bitcoin*.	*Toronto Sick Kids* • In Dec 2022, Lockbit hackers encrypted lab and imaging results and the appointment system. • They later apologized and offered free decryption.


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!