ECG VOICE & VIDEO ENGINEERING

DEFENDING AGAINST MALWARE

THE WEBINAR WILL START A FEW MINUTES AFTER THE HOUR

ECG

www.ecg.co

PRESENTING ENGINEER

MARK R LINDSEY MS

SENIOR MEMBER OF TECHNICAL STAFF

SECURITY RESEARCHER SINCE 1993

www.ecg.co

AGENDA

ECG ENGINEERING: DEFENDING AGAINST MALWARE

- What is malware?
- Has malware affected core servers & telecom?
- Defenses against malware
- Actionable Lessons

www.ecg.co

WHAT IS MALWARE?

MALWARE: MALICIOUS SOFTWARE

- Malware originally the domain of PCs: Viruses
- First major network malware: *Internet Worm of 1988*
  - Exploited bugs exposed through Internet Mail (SMTP)
  - Launched a new process on each server and scanned for other servers

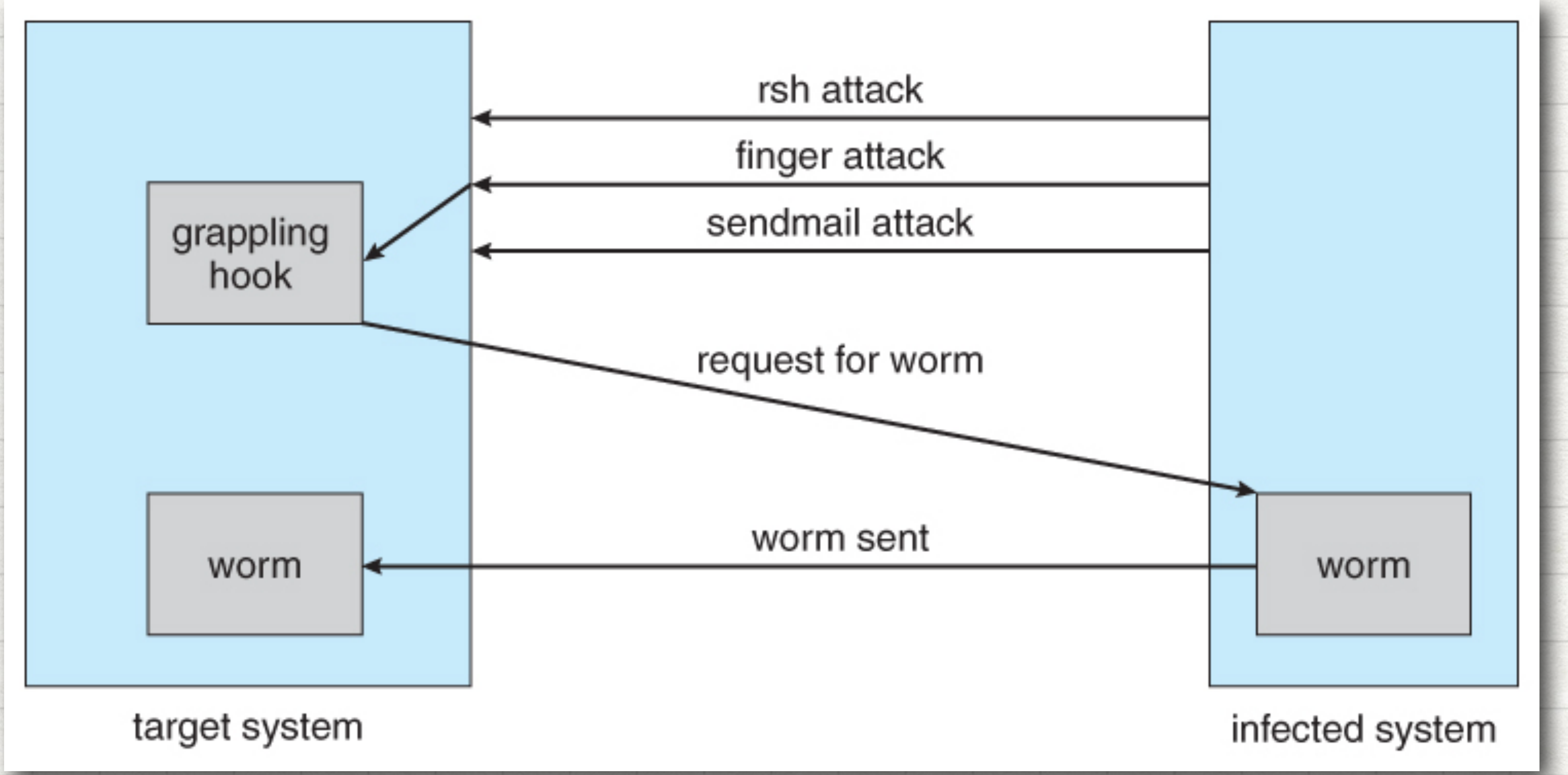
HOW DOES MALWARE SPREAD?

VULNERABILITIES

- Launches across network to exploit defects
- Firmware on USB Drives
- Code running inside PDFs
- Other Virtual Machines running on the same host
- "Trojan Horse" Modified Software

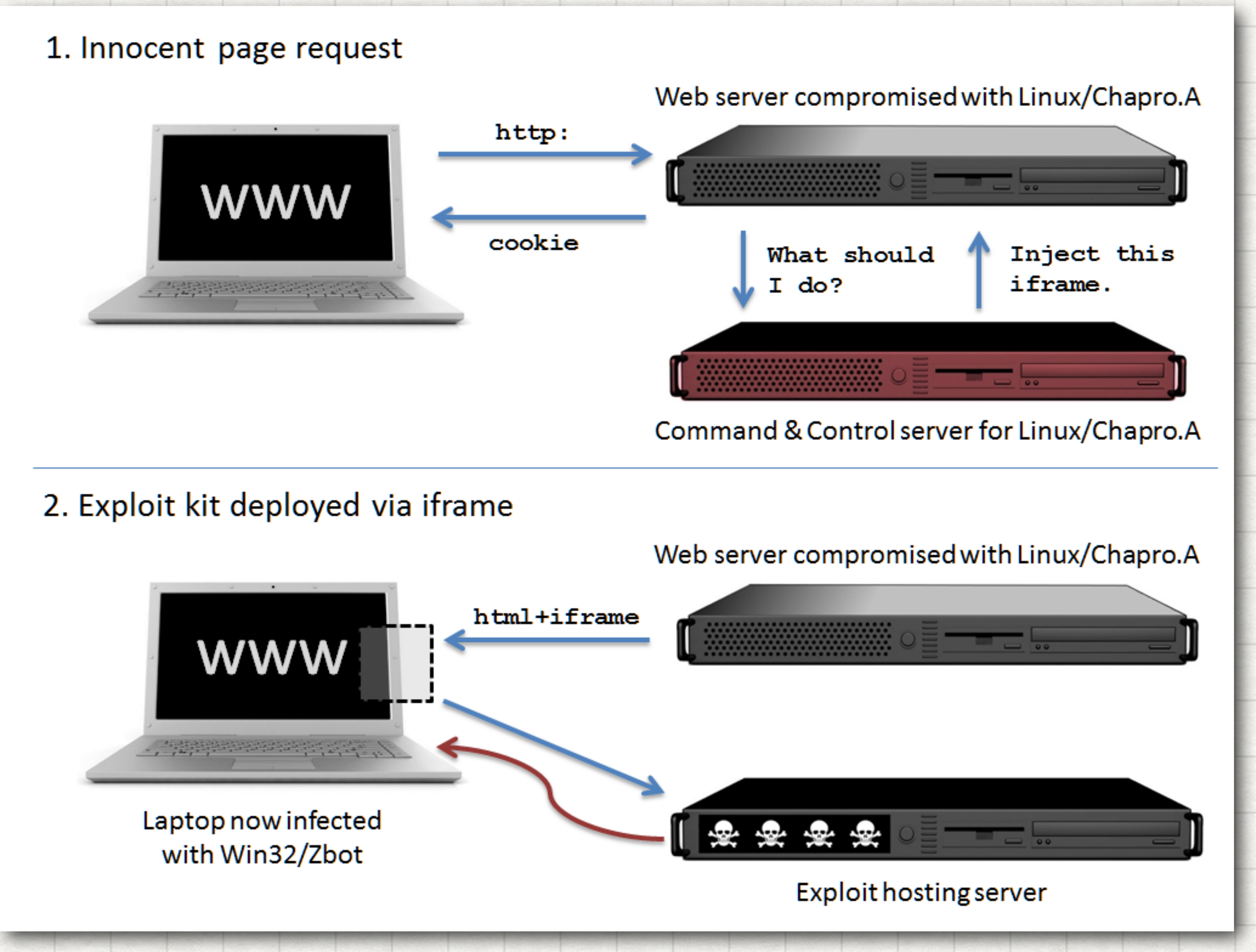
1988 MORRIS INTERNET WORM

DIAGRAM SOURCE: UNKNOWN



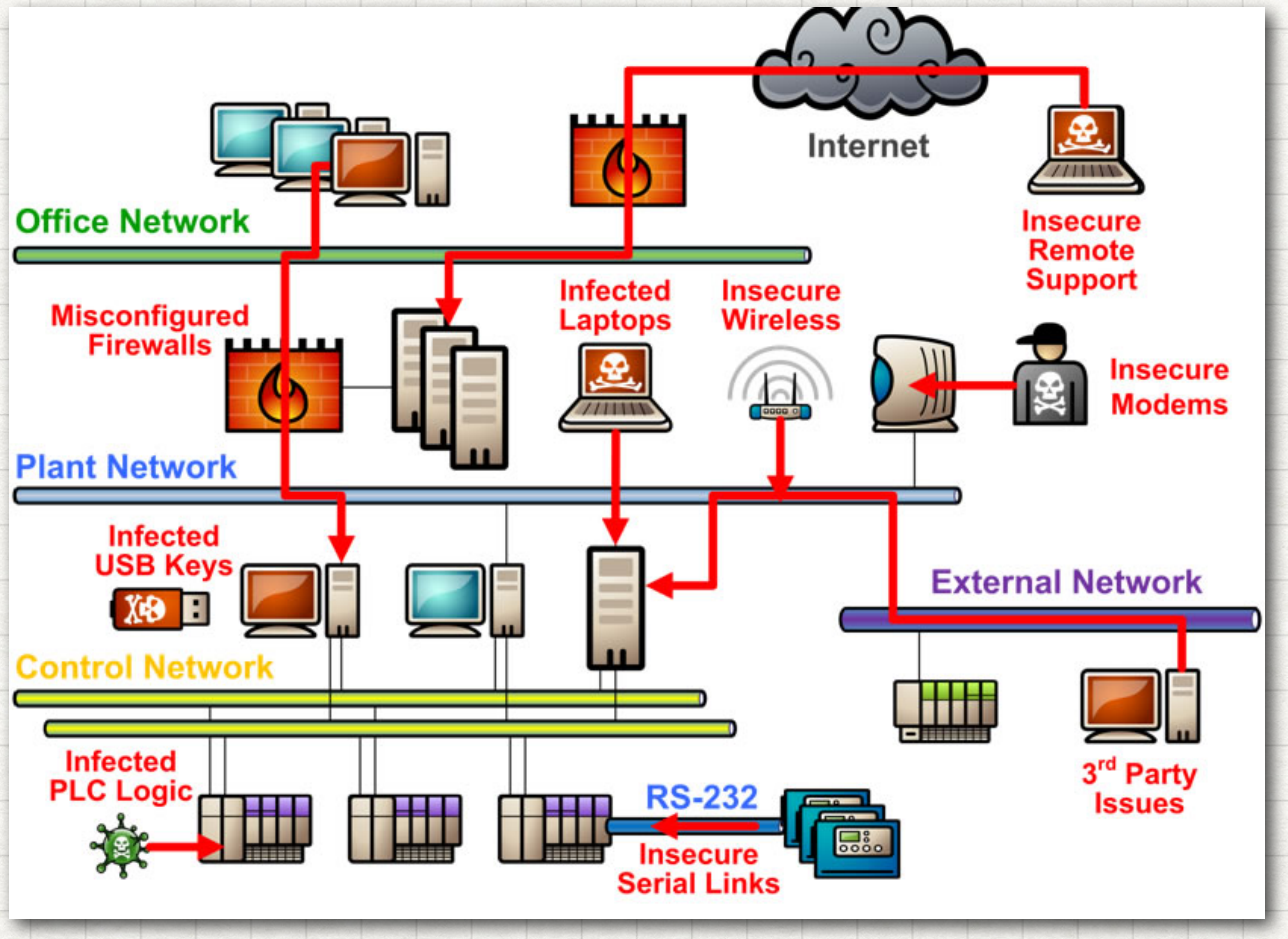
LINUX-MALWARE ASSIST

DIAGRAM: WELIVESECURITY


1. Innocent page request
Web server compromised with Linux/Chapro.A
www
http:
cookie
What should I do?
Inject this iframe.
Command & Control server for Linux/Chapro.A
2. Exploit kit deployed via iframe
Web server compromised with Linux/Chapro.A
www
html+iframe
Laptop now infected with Win32/Zbot
Exploit hosting server

STUXNET-LIKE INFRASTRUCTURE ATTACKS

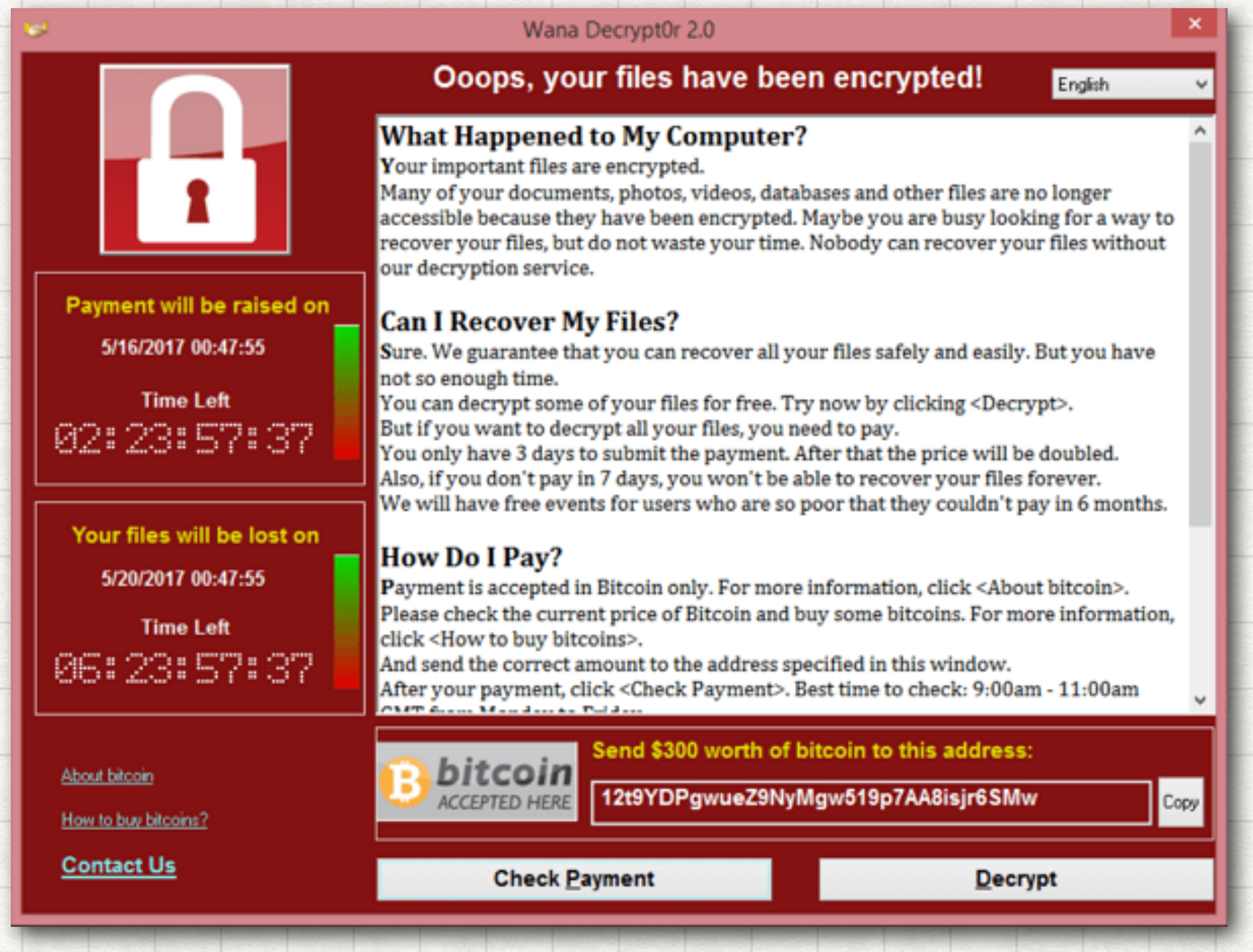
DIAGRAM: TOFINO SECURITY



HAS MALWARE AFFECTED CORE SERVERS & TELECOM?

WANNACRY - FEDEX AND UK NHS HIT

MAY 2017 - $130,634 EARNED



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

About bitcoin

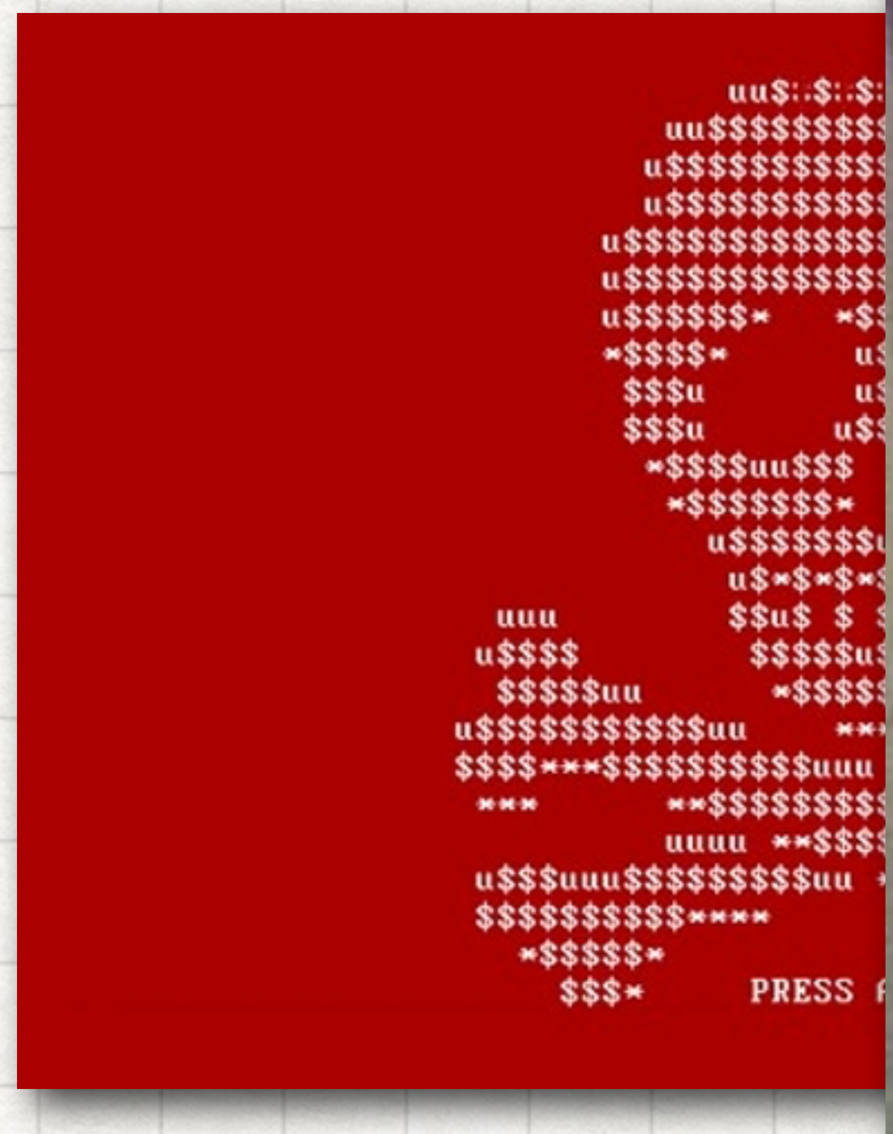
How to buy bitcoins?

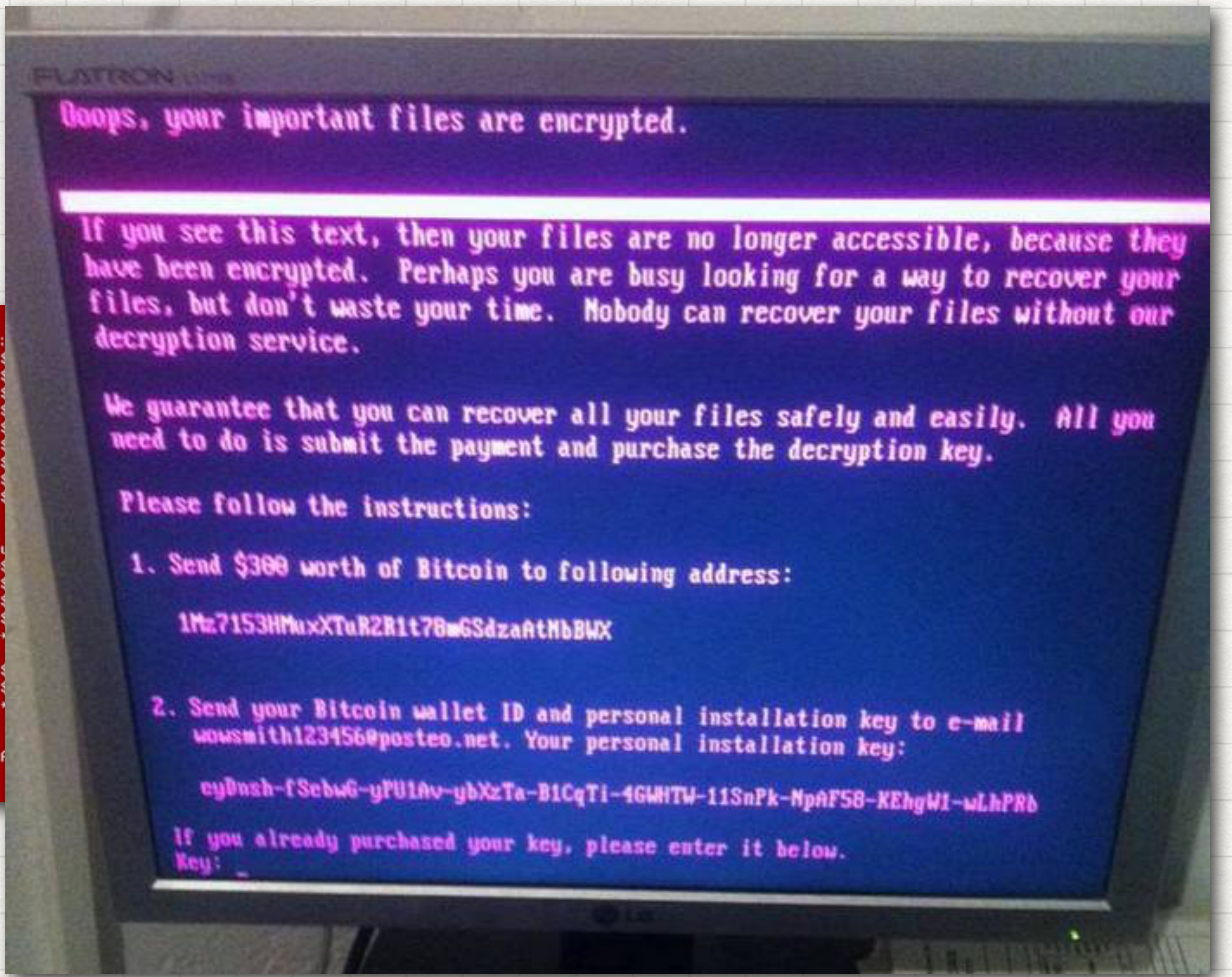
Contact Us

www.ecg.co

PETYA / NOTPETYA

ESTIMATED $121 BILLION IN DAMAGE





```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   cyDnsh-fSebwG-yPU1Av-ybXzTa-B1CqTi-4GWHTW-11SnPk-MpAF58-KEhgW1-wLhPRb

If you already purchased your key, please enter it below.
Key: _
```

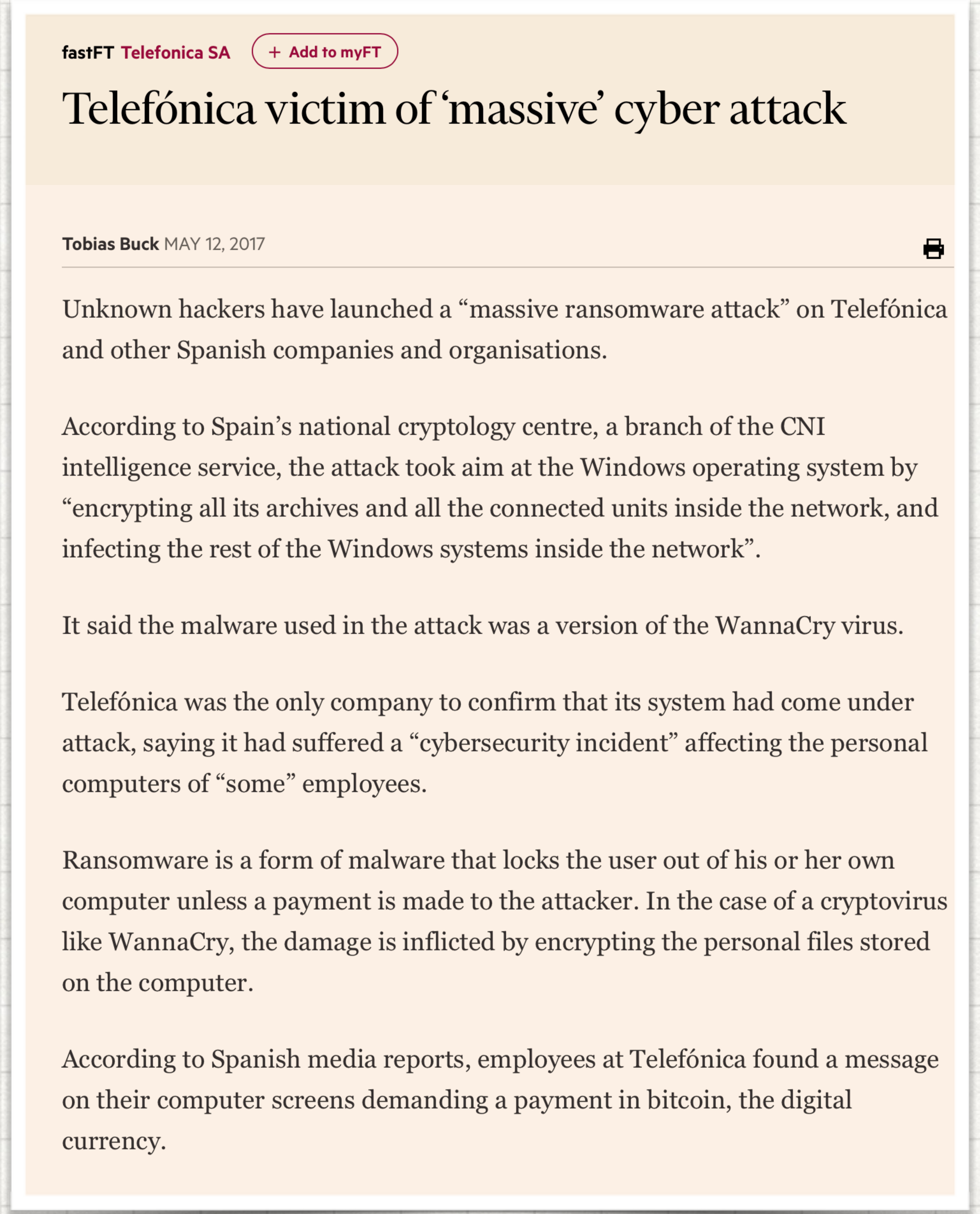
2017'S MALWARE IMPACT - $121B *SIMILAR TO HURRICANE KATRINA*

- Maersk shipping halted - ports closed
- Drugs manufacturing shutdown
- Telecommunications providers partly disabled
- Fedex package shipping affected
- UK National Health Service hampered

www.ecg.co

TELEFÓNICA

MASSIVE MALWARE ATTACK



fastFT Telefonica SA + Add to myFT

Telefónica victim of ‘massive’ cyber attack

Tobias Buck MAY 12, 2017

Unknown hackers have launched a “massive ransomware attack” on Telefónica and other Spanish companies and organisations.

According to Spain’s national cryptology centre, a branch of the CNI intelligence service, the attack took aim at the Windows operating system by “encrypting all its archives and all the connected units inside the network, and infecting the rest of the Windows systems inside the network”.

It said the malware used in the attack was a version of the WannaCry virus.

Telefónica was the only company to confirm that its system had come under attack, saying it had suffered a “cybersecurity incident” affecting the personal computers of “some” employees.

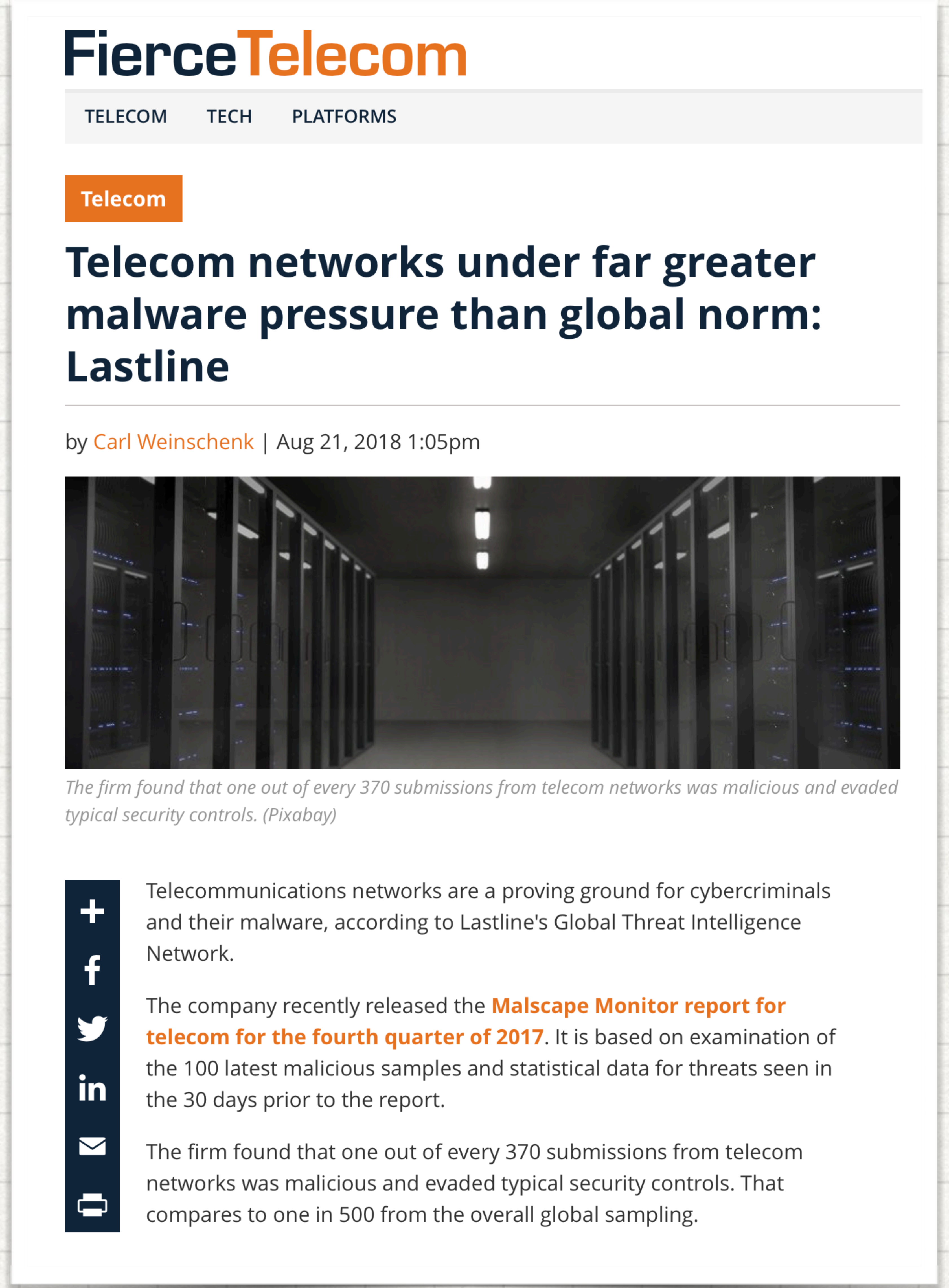
Ransomware is a form of malware that locks the user out of his or her own computer unless a payment is made to the attacker. In the case of a cryptovirus like WannaCry, the damage is inflicted by encrypting the personal files stored on the computer.

According to Spanish media reports, employees at Telefónica found a message on their computer screens demanding a payment in bitcoin, the digital currency.

www.ecg.co

TELECOM FIRMS TARGETED

ABOVE-AVERAGE MALWARE



FierceTelecom

TELECOM TECH PLATFORMS

Telecom

Telecom networks under far greater malware pressure than global norm: Lastline

by Carl Weinschenk | Aug 21, 2018 1:05pm

The firm found that one out of every 370 submissions from telecom networks was malicious and evaded typical security controls. (Pixabay)

Telecommunications networks are a proving ground for cybercriminals and their malware, according to Lastline's Global Threat Intelligence Network.

The company recently released the **Malscape Monitor report for telecom for the fourth quarter of 2017**. It is based on examination of the 100 latest malicious samples and statistical data for threats seen in the 30 days prior to the report.

The firm found that one out of every 370 submissions from telecom networks was malicious and evaded typical security controls. That compares to one in 500 from the overall global sampling.

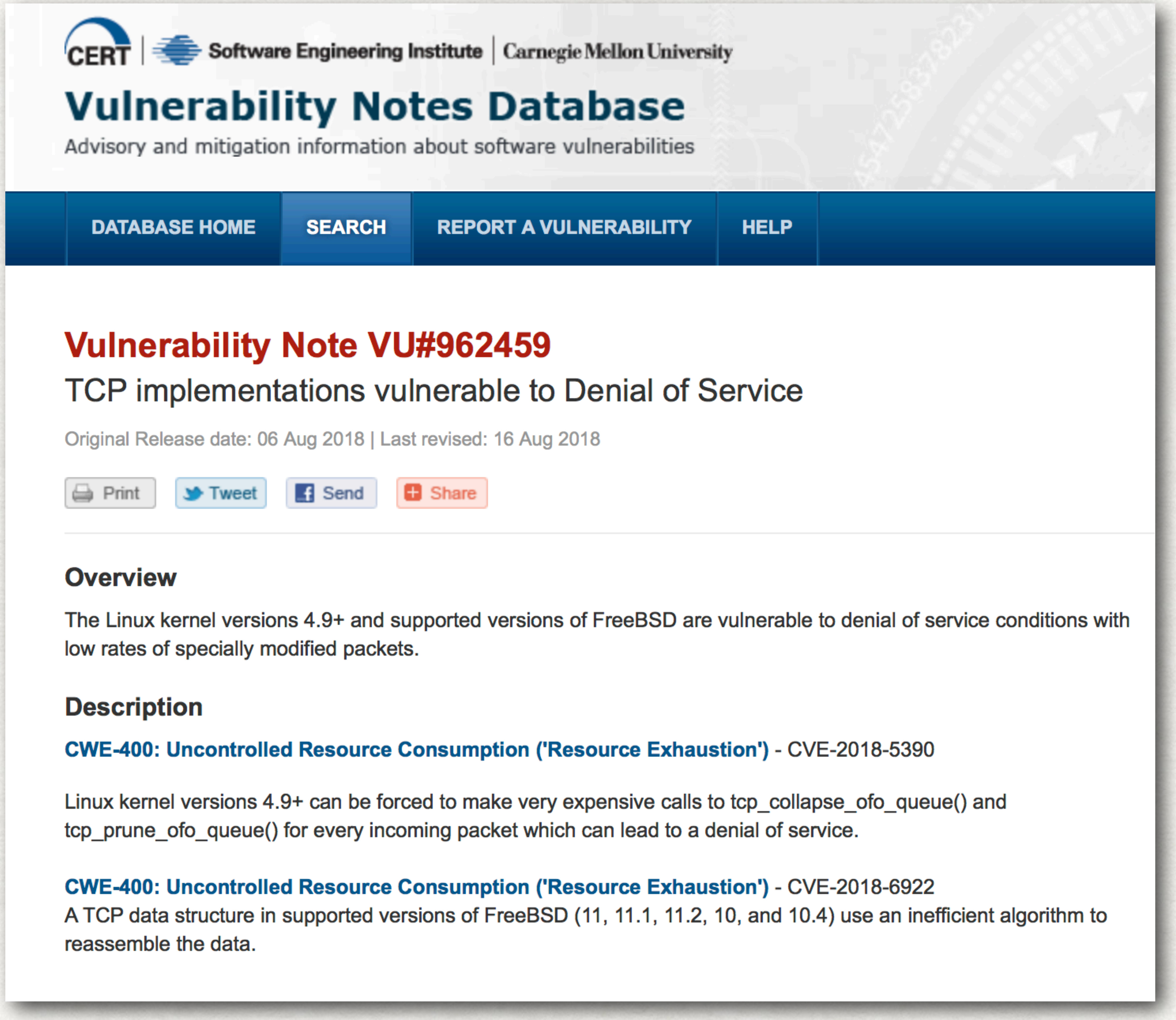
www.ecg.co

MALWARE - PATH TO DAMAGE

- Windows servers heavily damaged directly

- Linux servers also vulnerable when OS vulnerabilities unpatched

- New Linux kernel vulnerabilities revealed July 2018



CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

DATABASE HOME
SEARCH
REPORT A VULNERABILITY
HELP

Vulnerability Note VU#962459

TCP implementations vulnerable to Denial of Service

Original Release date: 06 Aug 2018 | Last revised: 16 Aug 2018

Overview

The Linux kernel versions 4.9+ and supported versions of FreeBSD are vulnerable to denial of service conditions with low rates of specially modified packets.

Description

CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion') - CVE-2018-5390

Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service.

CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion') - CVE-2018-6922

A TCP data structure in supported versions of FreeBSD (11, 11.1, 11.2, 10, and 10.4) use an inefficient algorithm to reassemble the data.

www.ecg.co

www.ecg.co

KEY DEFENSES AGAINST MALWARE

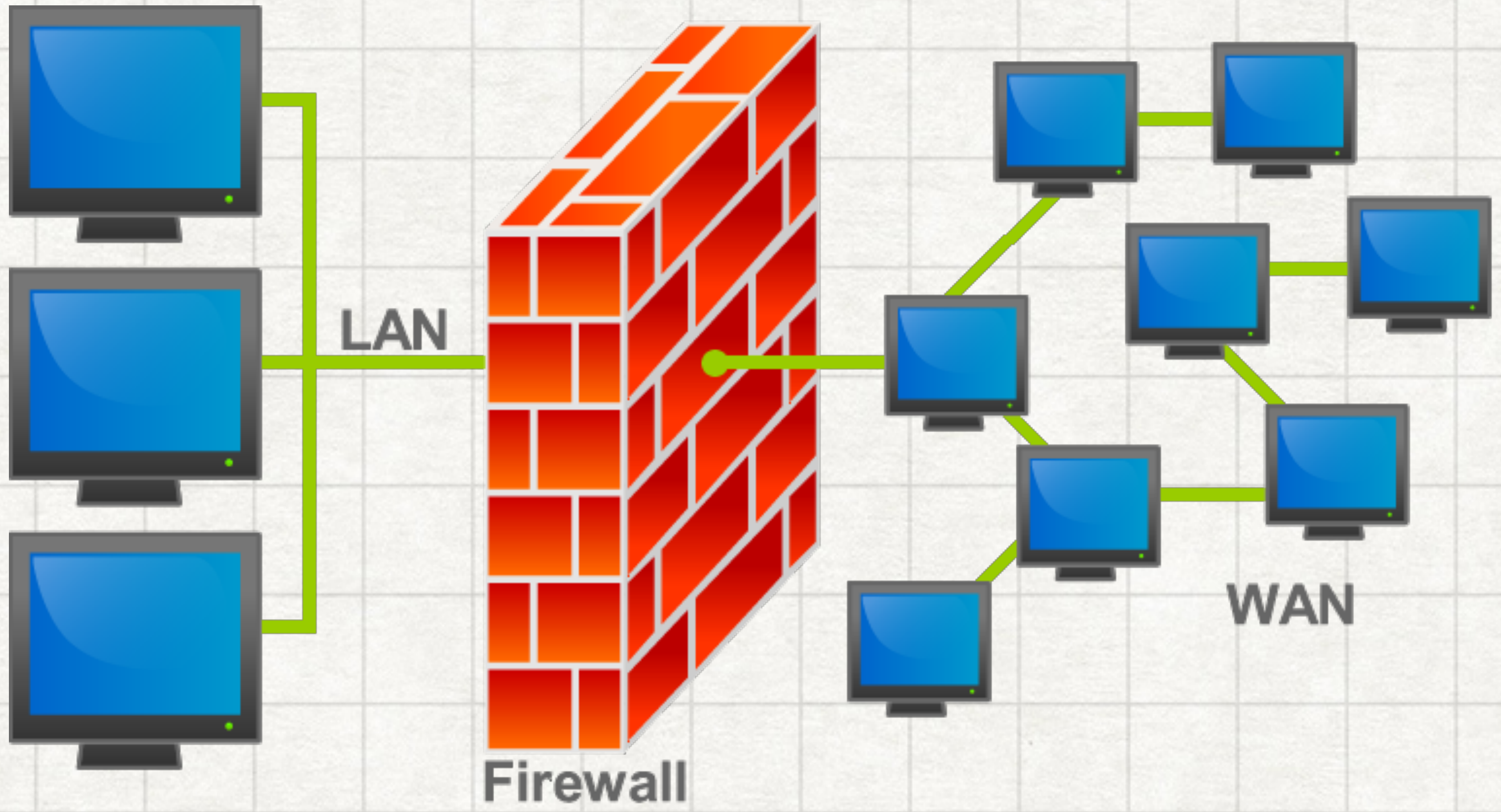
DEFENSE AREA A

CONSTANT OS UPDATES

www.ecg.co

DEFENSE AREA B

STRICT FIREWALL POLICY



www.ecg.co

1. PREPARE FOR UPDATES

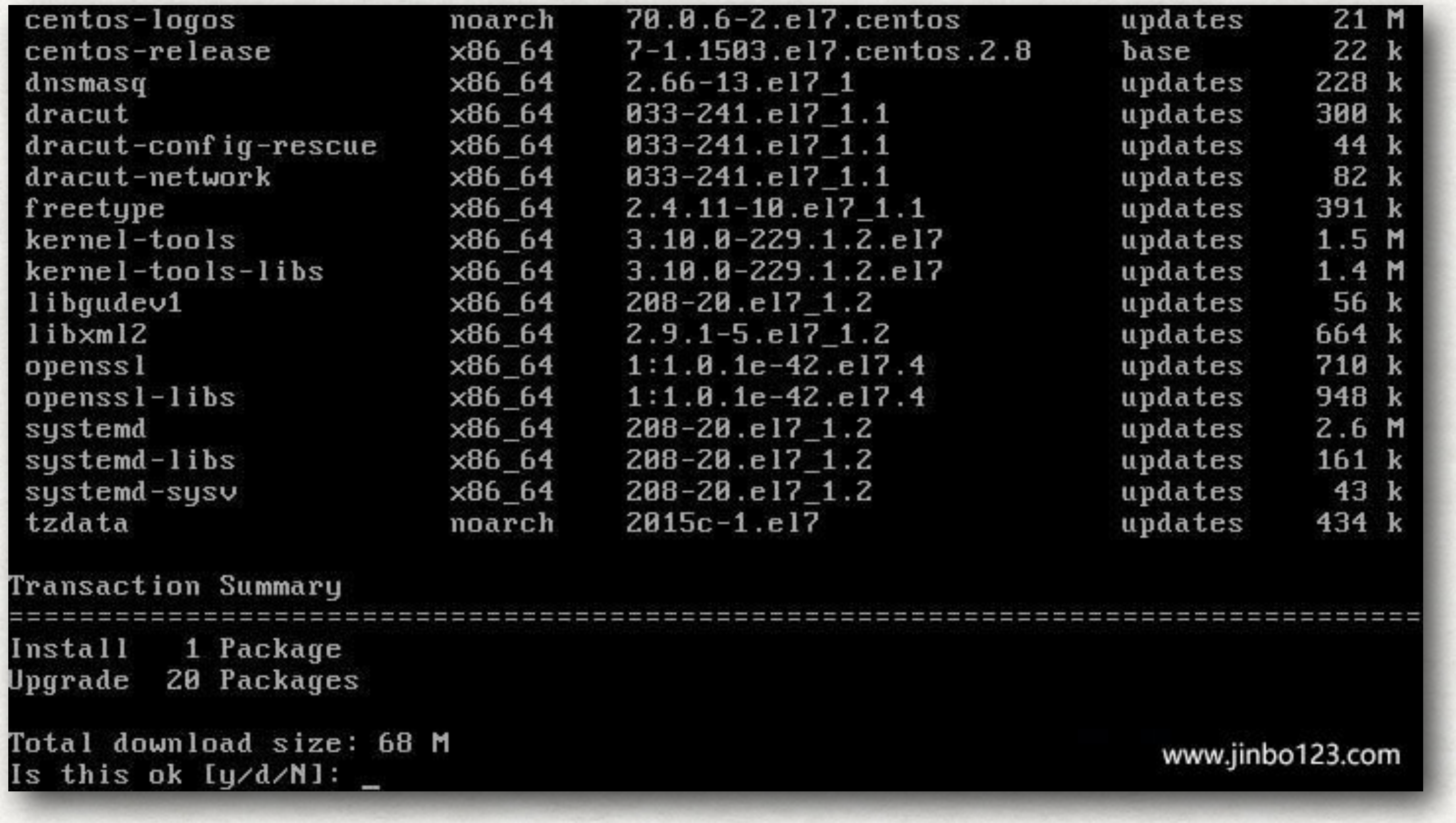
"MAKE THE RIGHT THING THE EASY THING"

- Many core servers are not updated
- OS Updates can be difficult to test and install: Licenses, Firewalls
- MUST-HAVE 1:
  Routine Monitoring for OS Updates and Continuous Access
- MUST-HAVE 2: ***Lab Network for Testing and Schedule***
- MUST-HAVE 3: ***Working Redundancy for OS Patches***

2. KEEP SYSTEMS PATCHED

NOTPETYA GAVE YOU 60 DAYS

- Update OS patches on all new installation
- MUST-HAVE 4: ***Schedule and Resources for Lab Patch Testing***
- MUST-HAVE 5: ***Phased Rollout Schedule for Production Patching***



```
 centos-logos            noarch    70.0.6-2.el7.centos            updates    21 M
 centos-release          x86_64    7-1.1503.el7.centos.2.8        base       22 k
 dnsmasq                 x86_64    2.66-13.el7_1                  updates   228 k
 dracut                  x86_64    033-241.el7_1.1                updates   300 k
 dracut-config-rescue    x86_64    033-241.el7_1.1                updates    44 k
 dracut-network          x86_64    033-241.el7_1.1                updates    82 k
 freetype                x86_64    2.4.11-10.el7_1.1              updates   391 k
 kernel-tools            x86_64    3.10.0-229.1.2.el7             updates   1.5 M
 kernel-tools-libs       x86_64    3.10.0-229.1.2.el7             updates   1.4 M
 libgudev1               x86_64    208-20.el7_1.2                 updates    56 k
 libxml2                 x86_64    2.9.1-5.el7_1.2                updates   664 k
 openssl                 x86_64    1:1.0.1e-42.el7.4              updates   710 k
 openssl-libs            x86_64    1:1.0.1e-42.el7.4              updates   948 k
 systemd                 x86_64    208-20.el7_1.2                 updates   2.6 M
 systemd-libs            x86_64    208-20.el7_1.2                 updates   161 k
 systemd-sysv            x86_64    208-20.el7_1.2                 updates    43 k
 tzdata                  noarch    2015c-1.el7                    updates   434 k

Transaction Summary
================================================================================
Install    1 Package
Upgrade   20 Packages

Total download size: 68 M
Is this ok [y/d/N]: _
```

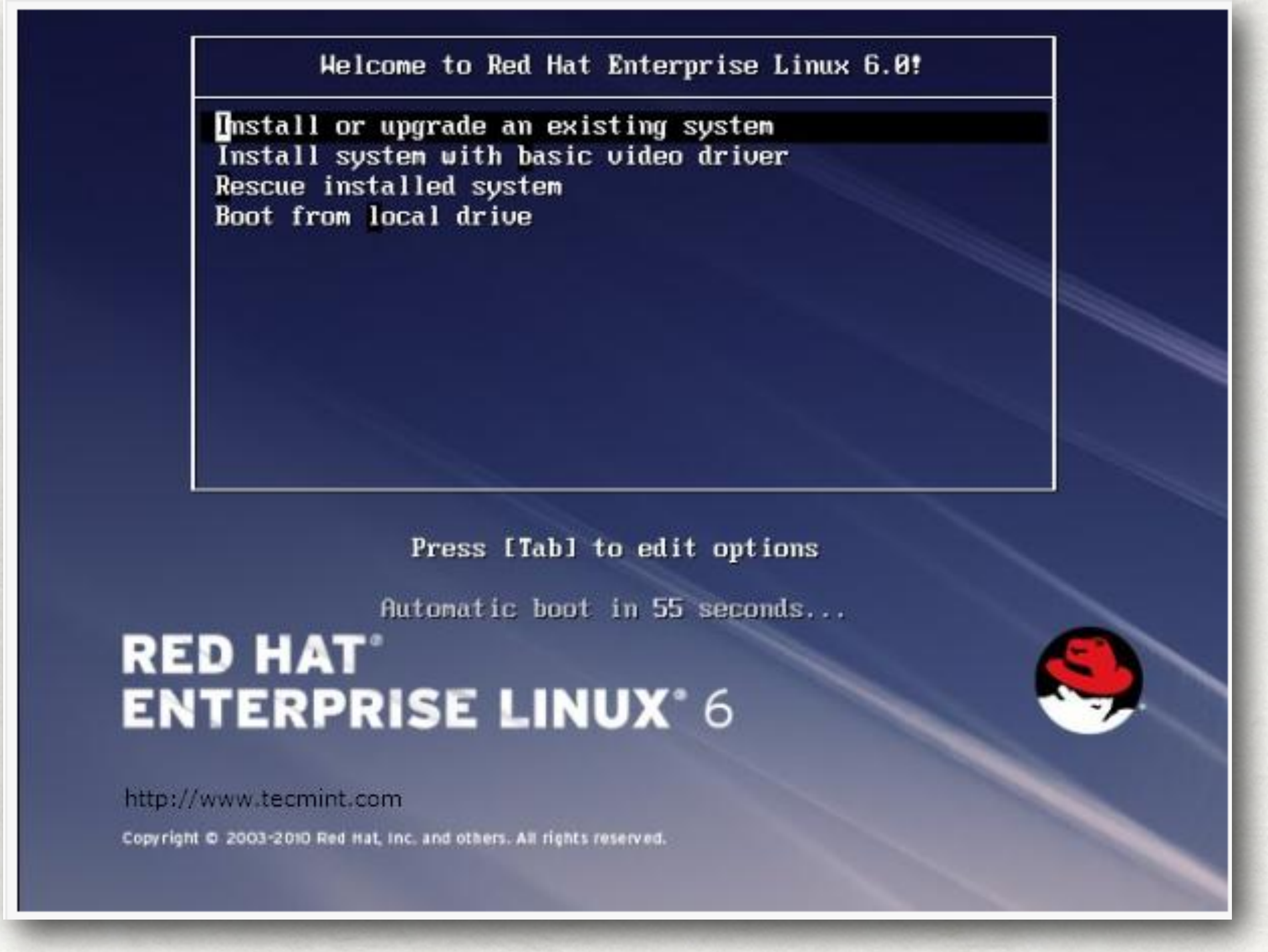
www.jinbo123.com

www.ecg.co

3. REPLACE INFECTED SERVERS

ONCE INFECTED, ALWAYS INFECTED

- It's infeasible to completely clean an exploited server
- Disable infected server completely and replace the server
- MUST-HAVE 6:
  Proven Backup Method to replace any server at any time.



```
Welcome to Red Hat Enterprise Linux 6.0!

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive

Press [Tab] to edit options

Automatic boot in 55 seconds...
```

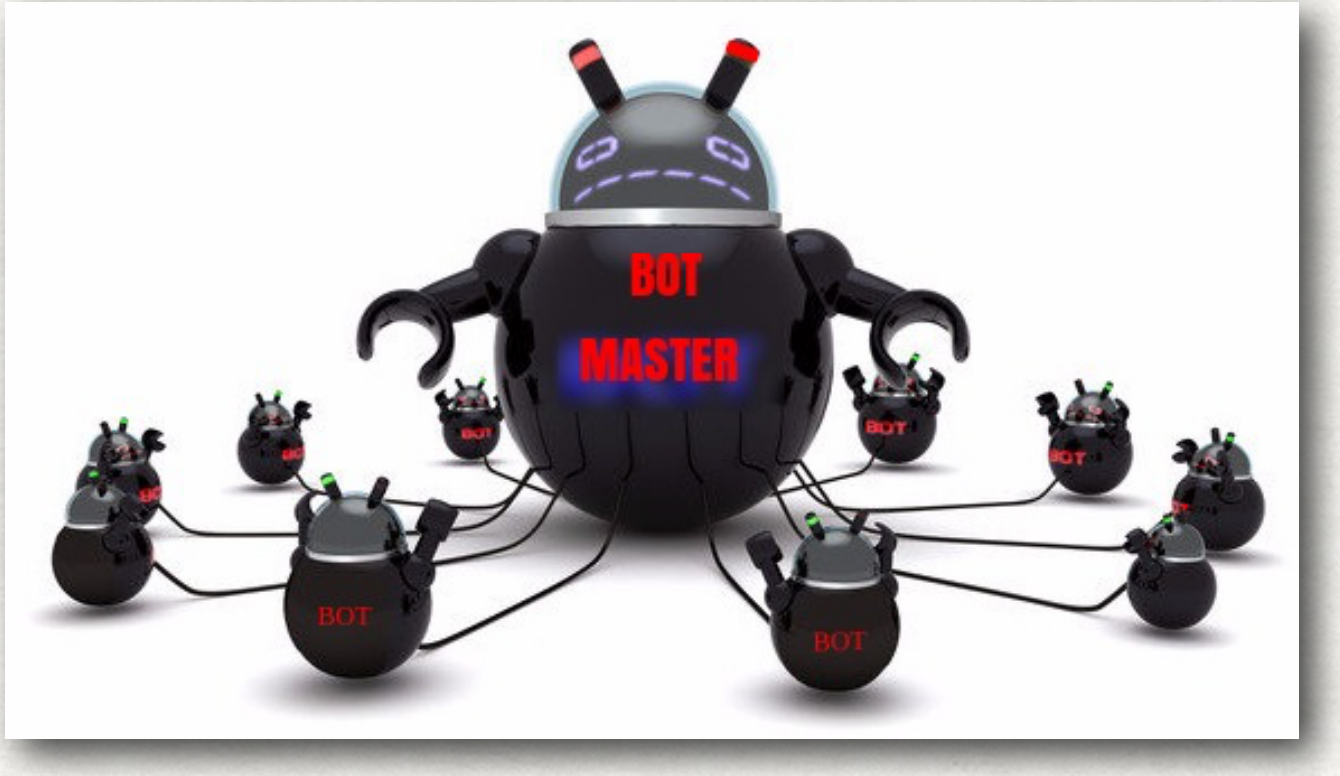
http://www.tecmint.com

Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

4. TIGHTLY RESTRICT FIREWALL RULES

LIMIT INBOUND FROM CORP, OUTBOUND TO INTERNET

- Exploits can cross from Windows, Mac, iPhone to Linux
- Command-and-control (C&C) systems usually connect outbound from infected systems to get instructions
- MUST-HAVE 7: ***Firewall must minimize access from Corporate and Management networks***
- MUST-HAVE 8: ***Block outbound Internet access from core servers***



www.ecg.co

5. ROUTINELY MONITOR FOR LINUX MALWARE

GOVERNMENTS WORKING ON LINUX MALWARE

- Regularly monitor for news of Linux malware
- Prepare to modify your security strategies to protect against it

I cannot defend American espionage using incredibly powerful tools if we cannot keep them secret.
General Michael Hayden, September 21, 2017
Photo: Gettys

www.ecg.co

ECG CAN HELP

CONTACT: INFO@ECG.CO / +1-229-244-2099

- *ECG maintains security in Service Provider, Corporate, Government, and Sensitive systems*
- Build Testing Labs
- Design, Audit, Test Firewalls
- Establish and Audit OS Update Practices
- Notify you when updates are required
- Test and rollout updates
- Replace exploited servers

www.ecg.co