

Paranoia 101

BhutanNOG / Thimphu

2017.06.05

101?

101 is the beginner's course

So this is a beginner's course
in System Administrator and
Network Operator Paranoia

Your Computer Infected



It Used to be 'Kiddies'

Now it is Almost All
for Financial Gain

You Are Pwned



How?

Software

If the automobile had followed the same development cycle as the computer, a Rolls-Royce would today cost \$100, get a million miles per gallon, and explode once a year, killing everyone inside.

-- Robert X. Cringely

[there are hardware
vulnerabilities too.
but not for this talk]

Where Viruses Hide

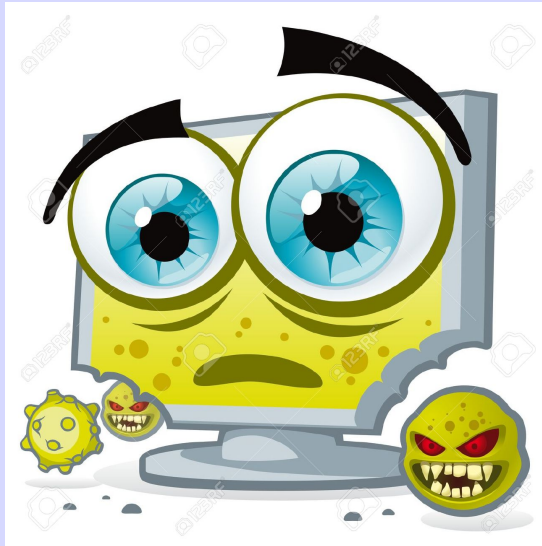
- Boot Sector - Reinstall every boot
- Applications
- Excel/Word Macros
- Libraries
- DLLs
- Compilers, etc
- Anti-Virus Software!!!

But It's Not Just
Your Computer

The Virus Wants to
Infect Your Network
Neighbors, LAN & WAN

What It Will Do

Send Spam
RansomWare



Infect Others
DDoS BOT

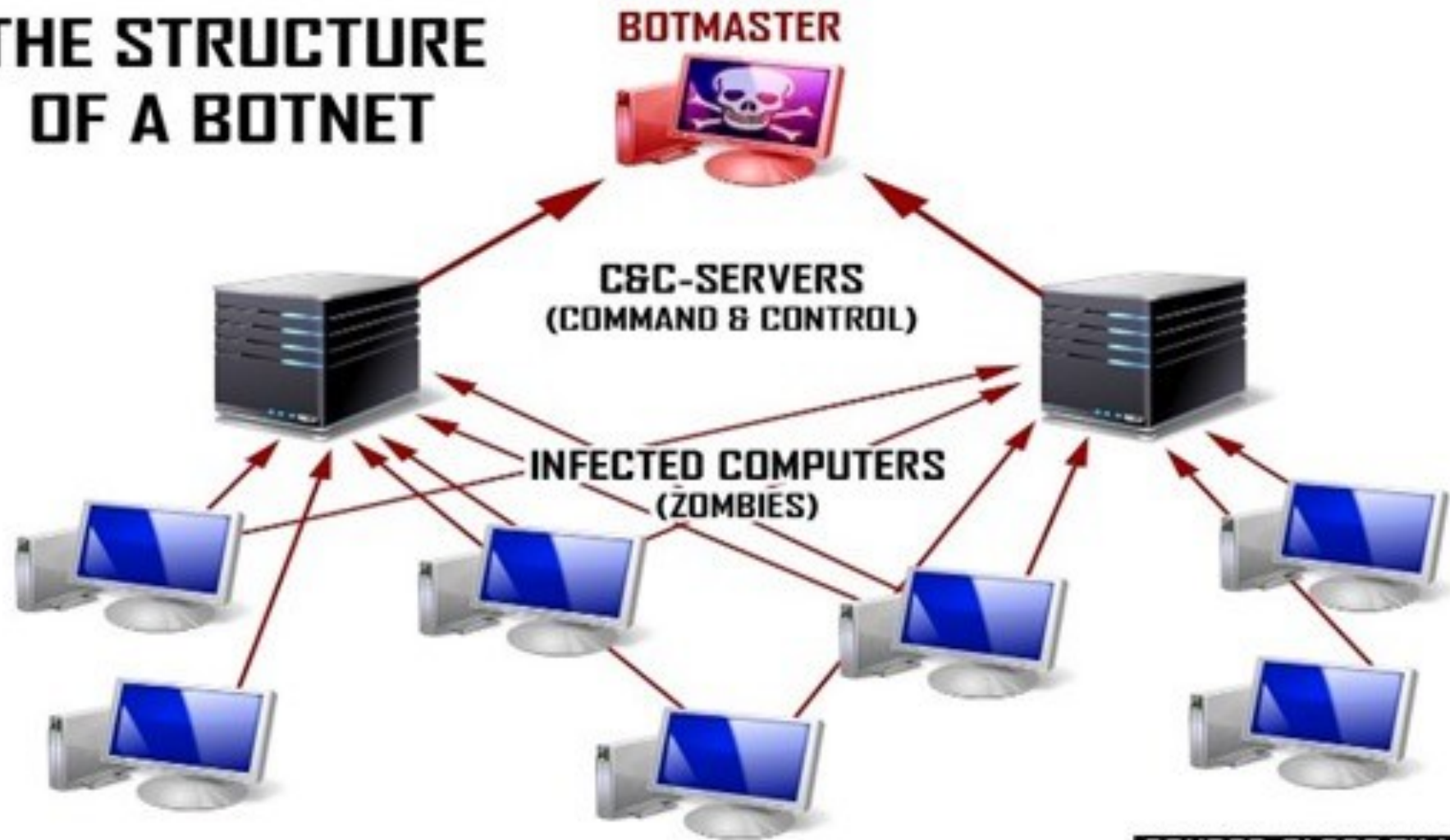
And Become Part of a
Massive BOT Army

Infect Others?

**Yes, it will look on the LAN
and the WAN for other
systems with the same
vulnerability and infect them.**

BOTnets

THE STRUCTURE OF A BOTNET



SOURCE: BLOGG.TKJ.SE

BOTnets

- Send SPAM, for which the BotMaster is paid
- Spread RansomWare
- DDoS Attacks for Hire
- Probe for Weakness in Banks, Gov, ...
- Look for Vulnerable Routers
- And, of course, Infect more Machines

RansomWare



RansomeWare



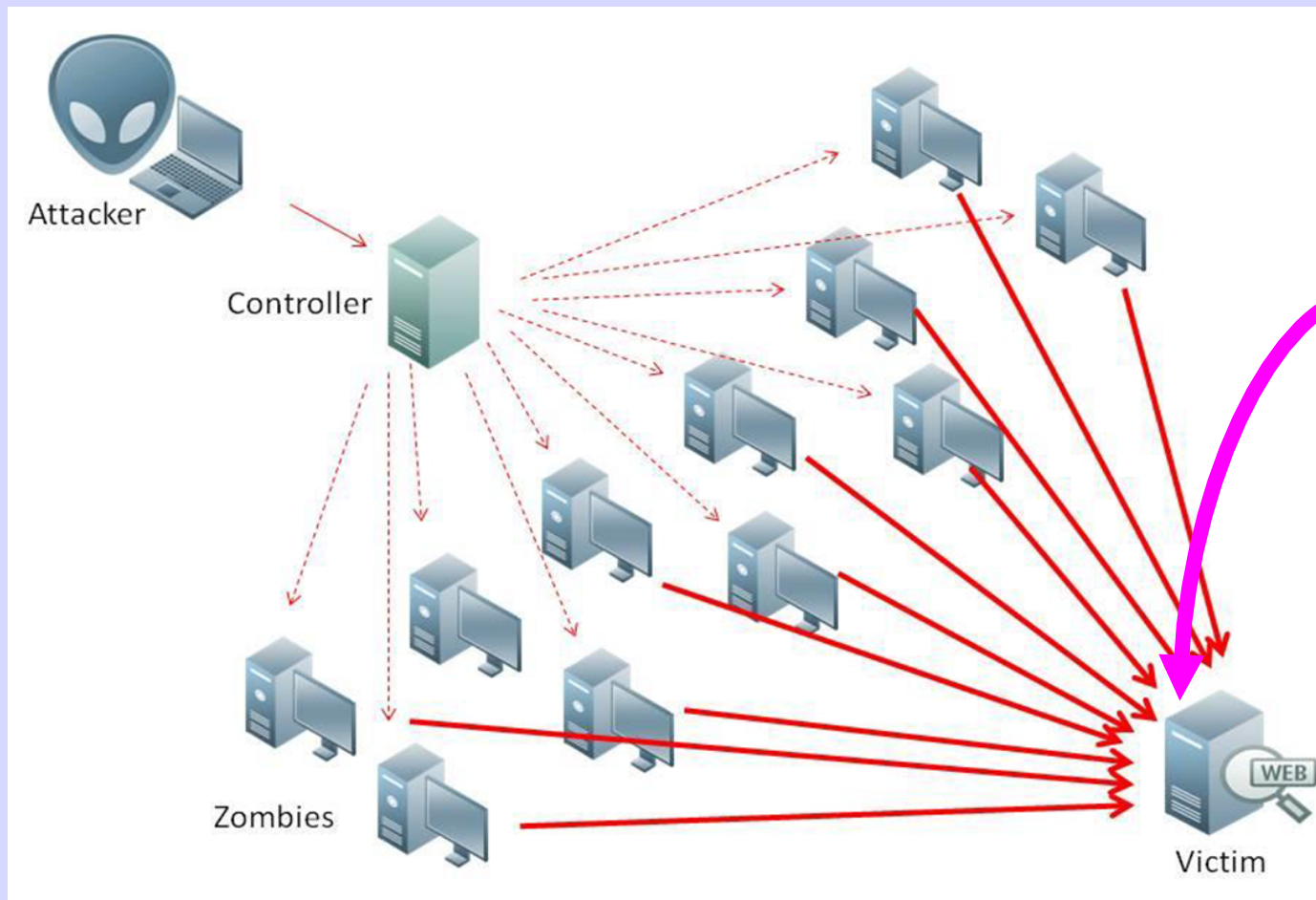
WannCryApril 2017



Infected hundreds of thousands of machines!

DDoS

Distributed Denial of Service



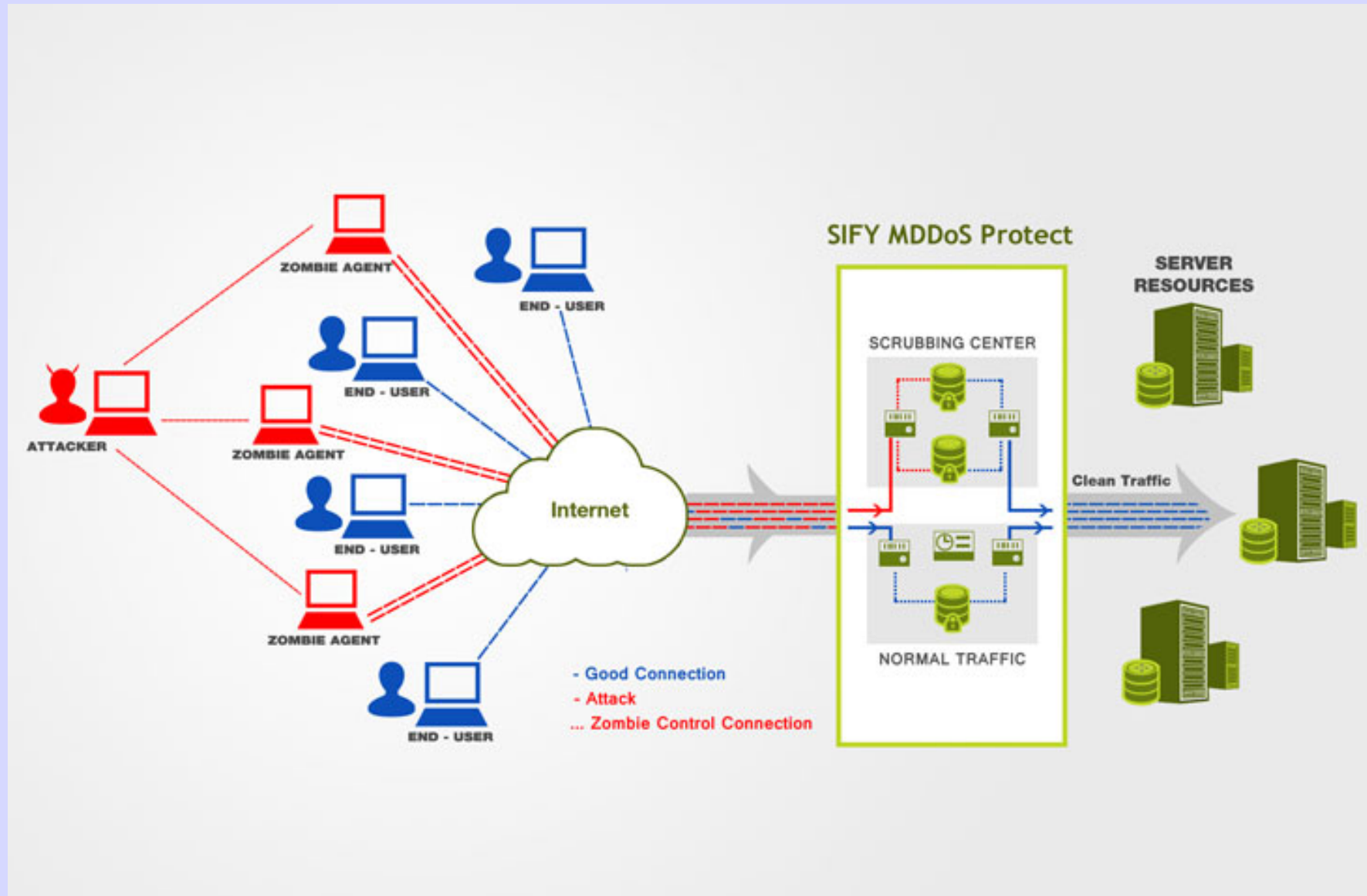
DDoS Extortion

We Control a Gigantic BOTnet

Unless You Send \$50,000 in BitCoin

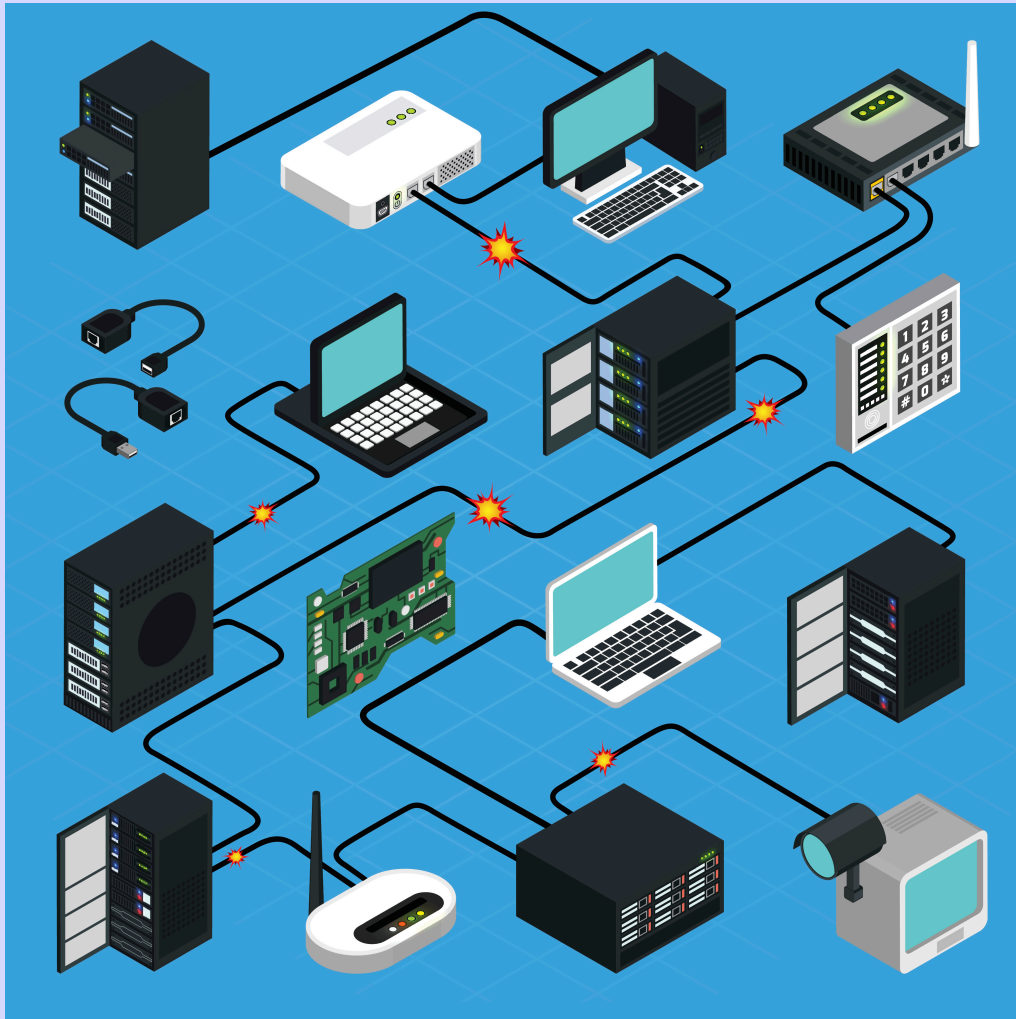
We Will Send you 50GB/sec for a Week

DDoS Mitigation



The "S" in "IOT" Stands for Security

Mirai BOTnet



All the IOT Devices used the same cheap and vulnerable custom Linux

Allowed telnet and simple password

CCTV, Modems, ... on the Internet

Attack scans for them and infects them. The infection spreads.

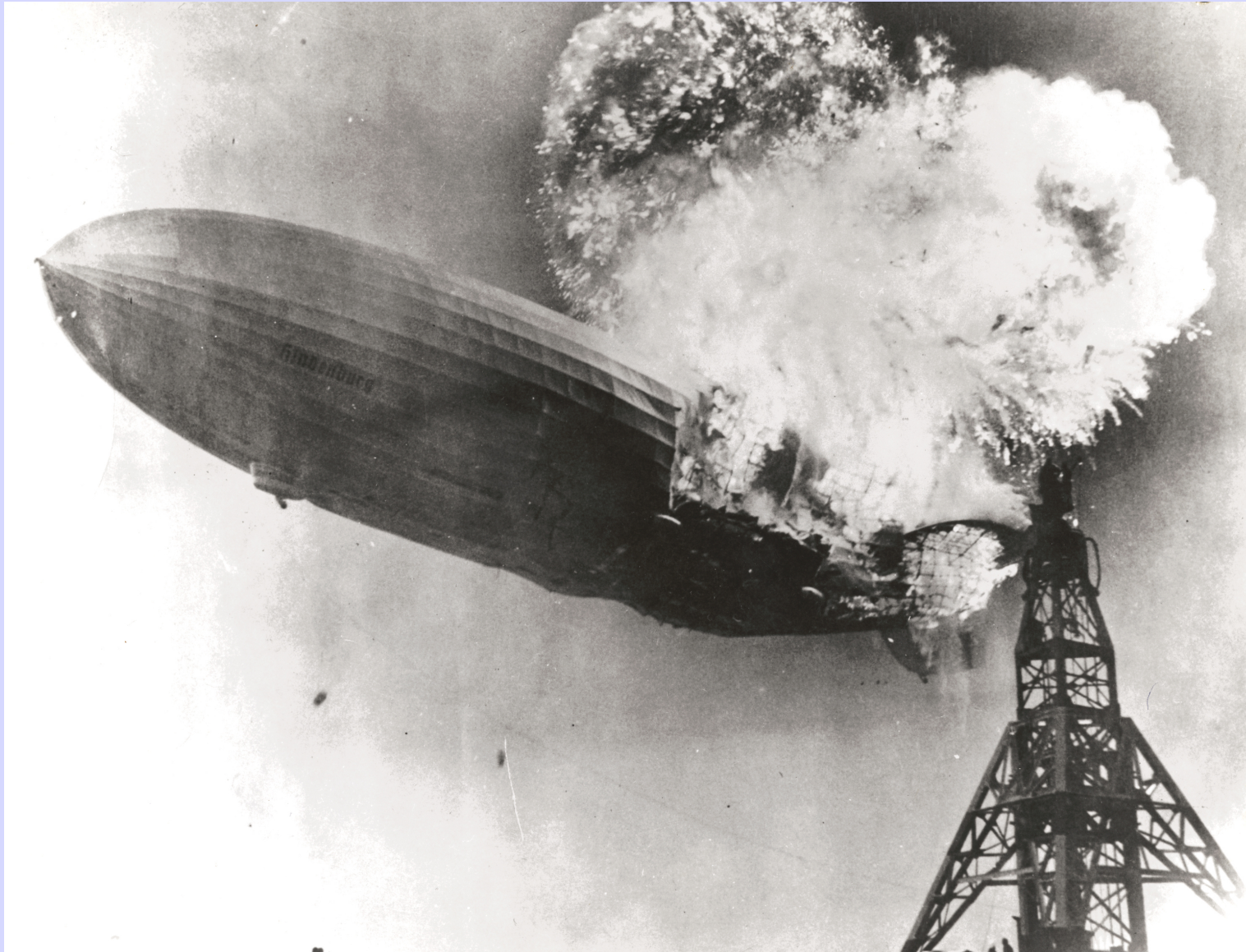
The infected IOT devices joined a very large BOTnet, >500,00 devices

And an 800GB/sec DDoS resulted

Hydrogen Fuel Cell



Hydrogen Filled Vehicle



Mirai – Amazingly Stupid

- Millions of tiny devices (cctv & routers)
- On the open internet
- Bought the same cheap Mirai Linux
- Allow telnet & ssh
- Trivial passwords
- Can not be upgraded in the field
- Scans for other vulnerable hosts and infects them too

This is Just the Start
of the
Internet of Things

Financial Targets



Willie Sutton

American Bank Robber 1920s-1950s

When asked why he robbed banks, said

"Because that's where the money is."

How to Get Into a Bank?

Phishing

Phishing

From: POLUX CO.,LTD. <zqiu@aanddtech.cn>
Subject: new order Hanyoung
Date: May 30, 2017 at 12:23
To: zone@pct.com.gr <zqiu@aanddtech.cn>

Blocked 1 external reference. The message is marked as Junk.
Loading external references can reveal information to the sender.

Good day,

In the attachment you find an inquire offer, please revert with price, availability and payment terms.

Best Regards,
Moonnie Oh

POLUX CO.,LTD.
Moonnie Oh / Assistant Manager
Tel. 82-32-209-8686 Fax. 82-32-343-2789
cid:image001.jpg@01D29F4D.6E6078C0

Open File and you're Infected!

IMG_30_Hanyoung Quote list doc.7z application/octet-stream 295.3 KiB Quick Look Save

SpearPhishing

Confirm account ownership x Google Account Recovery x

← → ↻ <https://mail.google.com/mail/?shva=1#inbox/1424046d9e362b7d>

Google

Click here to enable desktop notifications for Gmail. [Learn more](#) [Hide](#)

Gmail ▾

COMPOSE

Inbox (3)
Starred
Important
Chats
Sent Mail
Drafts
All Mail
Spam

gever1
technion i

Lumosity.com - Get smarter, think faster - Train your brain with Lumosity, the personal trainer designed

Confirm account ownership Inbox x

 **Google ArAutoBot** <accgmaiiautobot@gmail.com> 6:38 AM (24 minutes ago) ☆ 

to me ▾

Hello Hatechnion,

It's been a while since you last changed your password.

Please confirm account ownership by clicking on this link:

<https://www.google.com/ConfirmAccount?Email=hatechnion@gmail.com>

Thanks,
The Google Team.

Whaling



Going After the Biggest Fish



1

Cyber thieves use social media sites, such as LinkedIn, for gathering details to impersonate high-level executives and find lower-level employees to target.

2



Crooks register a domain name that appears similar to the actual company domain. For example, any-cornpany.com (note the r & n used in place of the m in company) is used to spoof the legitimate domain, any-company.com.

3



Recipient receives an email featuring relevant details about the impersonated executive and likely mentions a specific business initiative.

4



The target thinks the email is authentic and engages with the attackers. The hook is set.

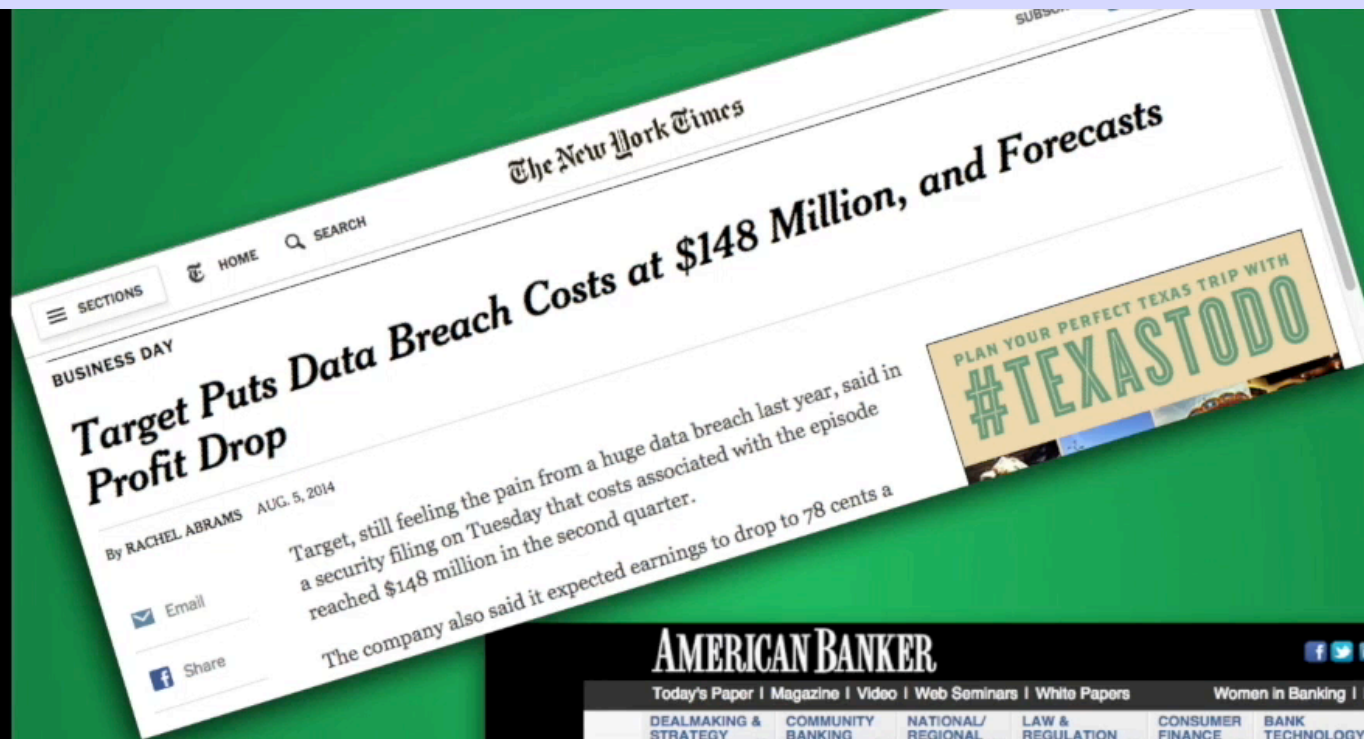
5



Cyber thieves request a wire transfer or for the recipient to send personal, employee or tax data.

Firewall?





Firewall?

We call that the
“hard crunchy outside”
and the
“soft gooey inside.”

Firewalls are 'Stateful'
they remember sessions

DDoS Overflows the
State Tables!
Dead Firewall!

StuxNet

- US & Israel wanted to damage Iran nuclear development capacity
- Worm on USB drive distributed where Iranian engineers would find it
- A quiet infection; waited until it could see centrifuges with SCADA on net
- Infected centrifuges and destabilized
- Destroyed 1,000; set Iran back years

But there is
Hope!

Canaries

- Mining for coal underground was dangerous, especially methane leaks
- Methane is odorless and hard to detect
- But a little bird, a canary, is very sensitive to methane
- They die at the slightest bit of it
- So they were taken down into the mines as a detection method

A Real Canary



Now Imagine a
Canary for your LAN

It Warns of Invasion!



Also Called 'HoneyPot'

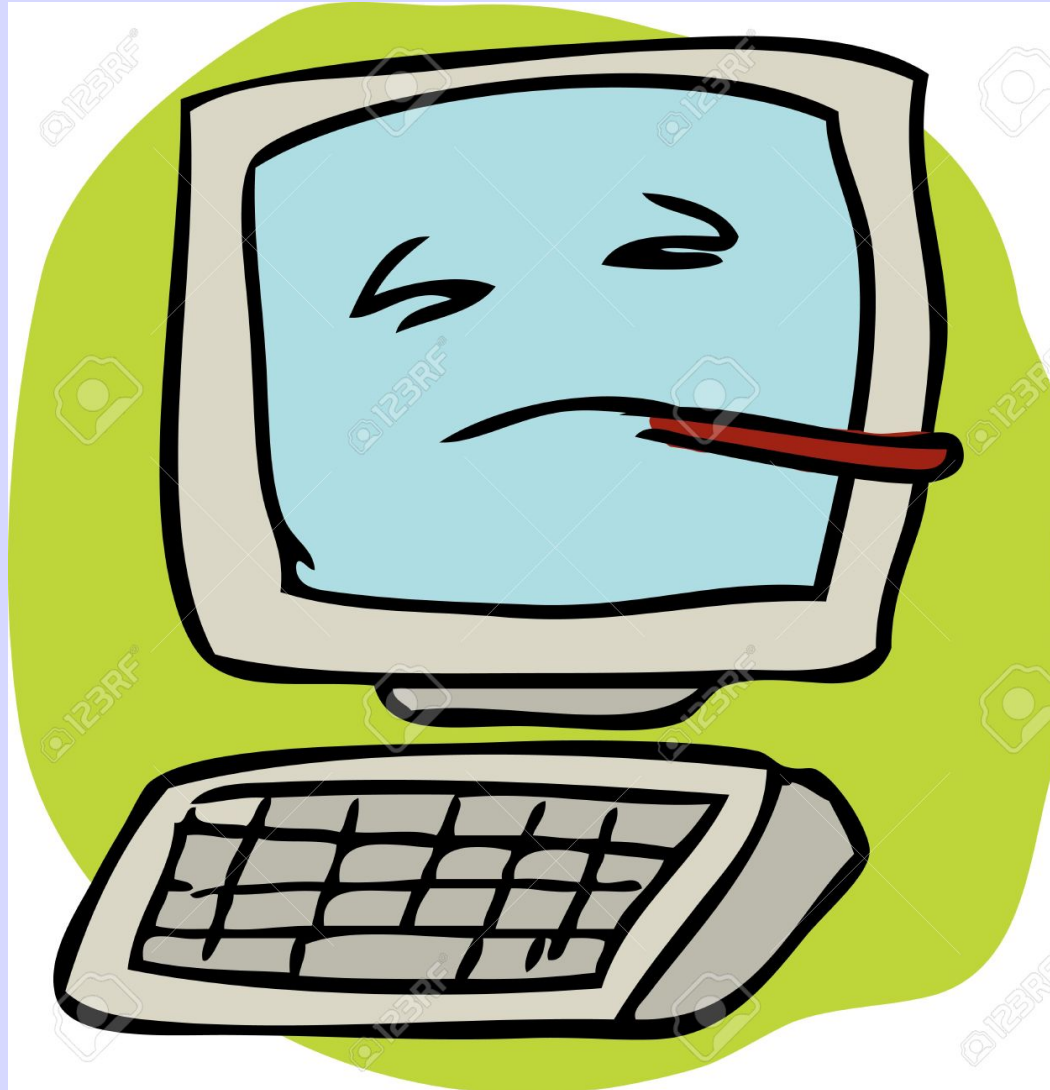


Free Open Source Telemetry Tools

- Monitor NetFlow, IPFIX, DNS, ... for Anomalies
- Intrusion Detection Systems: Bro and Snort; but complex, not plug and play
- Use macro-analytical telemetry first and then focus on packet capture

But Your Personal First Line of Defense

Your Computer's Health



And Eternal Vigilance

