The Cloud and Cybersecurity

What you need to know!

Mark Barton
President-Wild Prairie Computers

www.wildprairiecomputers.com

Today We're Going To Cover:

- A number of **serious and growing threats** to you that can no longer be ignored or passed off as "That won't happen to me..."
- Why firewalls and antivirus software **aren't enough anymore to protect yourself**, and what you need to have in place to protect yourself from the storm of trouble brewing.
- How mobile phones and cloud applications are **seriously jeopardizing** your security and data protection – and what you need to do to protect yourself.
- How to be proactive and some free or low-cost tools to use.

Ultimately We're Going To Cover...

How To **Avoid Being A Sitting Duck** To Cybercriminals and a Growing Number Of IT-Related Threats And

Protect Everything You've *Worked So Hard To Achieve*

Why I'm Talking To You About This Today

100% of the clients we've taken on as new clients in the past year were **SHOCKED** when we showed them they:

- **Were infected with malware and viruses**, even though they had antivirus installed and a firewall.
- **Did NOT** have all their data backed up.

And ALL firmly believed "That can *never* happen to *me*!"

The Biggest Danger Is Your Complacency

"Success breeds complacency. Complacency breeds failure. Only the paranoid survive."

– Andrew Grove, former CEO of Intel

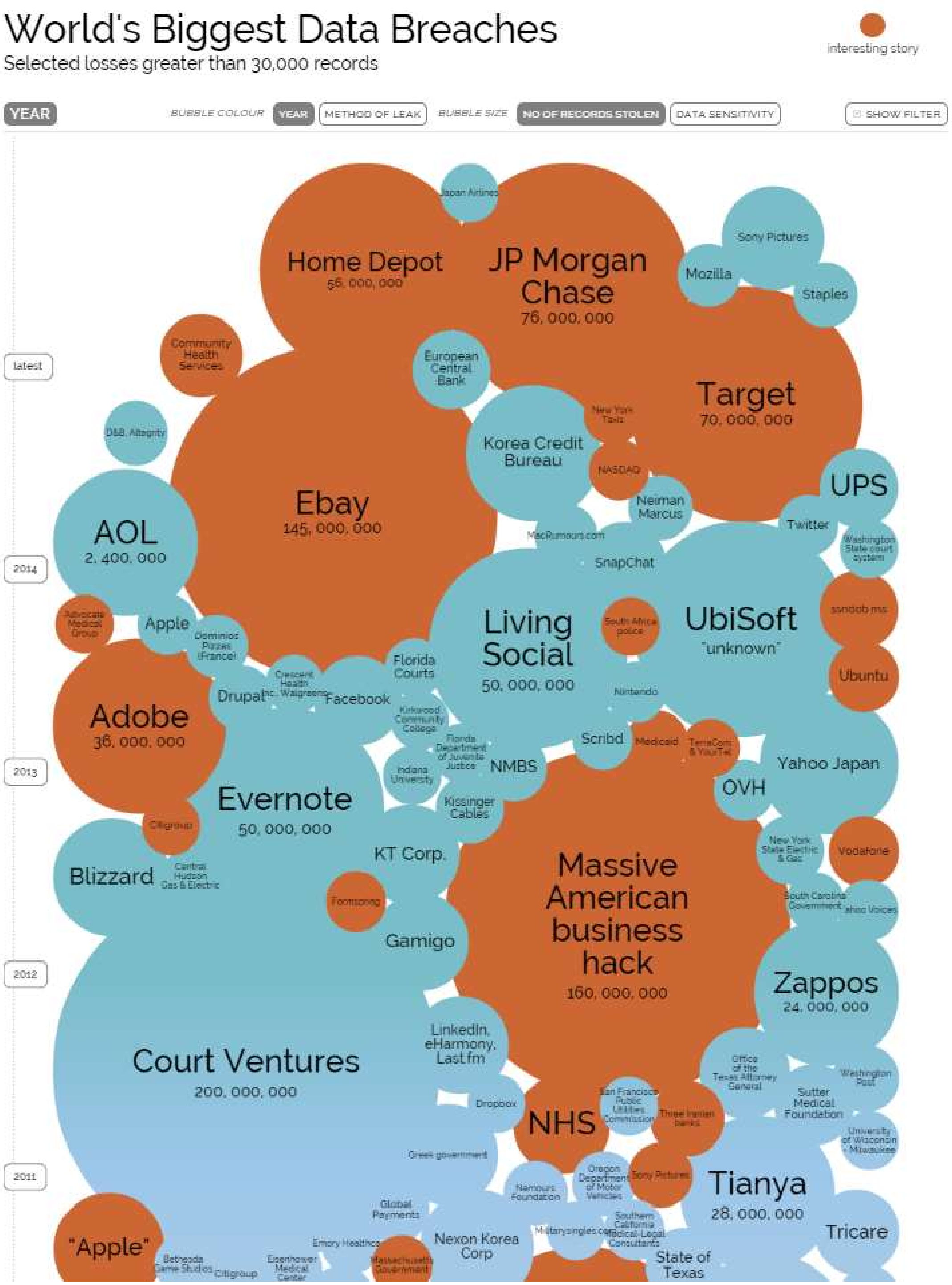
The Biggest Danger Is Your Complacency

Please **DO NOT underestimate** the importance of addressing and protecting yourself from this threat.

A Quick Overview Of The Sophistication And Proliferation Of The

Cybercrime Business

The Evolution Of Crime



World's Biggest Data Breaches

Selected losses greater than 30,000 records

80 Million Households And 7 Million Small To Medium Businesses HACKED

The Criminal Digital Underground's Thriving Black Market

- Credit card details sell for: **$2-$90**
- iTunes accounts sell for about: **$8**
- Physical credit cards sell for: **$190**
- Card cloners can be bought for: **$200-$300**
- Fake ATMs can be bought for: **$35,000**
- **THIS IS A BUSINESS:** anyone can easily buy training, tools and services for committing fraud, hacking systems, buying stolen credit cards, setting up fake websites, etc.

$201

Additional Damages And Costs NOT INCLUDED In The Above Number:

- Reputational damage
- Loss of clients
- Class action lawsuits, individual lawsuits
- Legal fees to handle a breach
- Compliance lawsuits (fines for non-compliance)
- Replacement of data
- Downtime, loss of productivity
- Time required to re-enter data and get your internal systems back up and running again

"But We're Small… Nobody Would Bother To Hack Us, Right?"

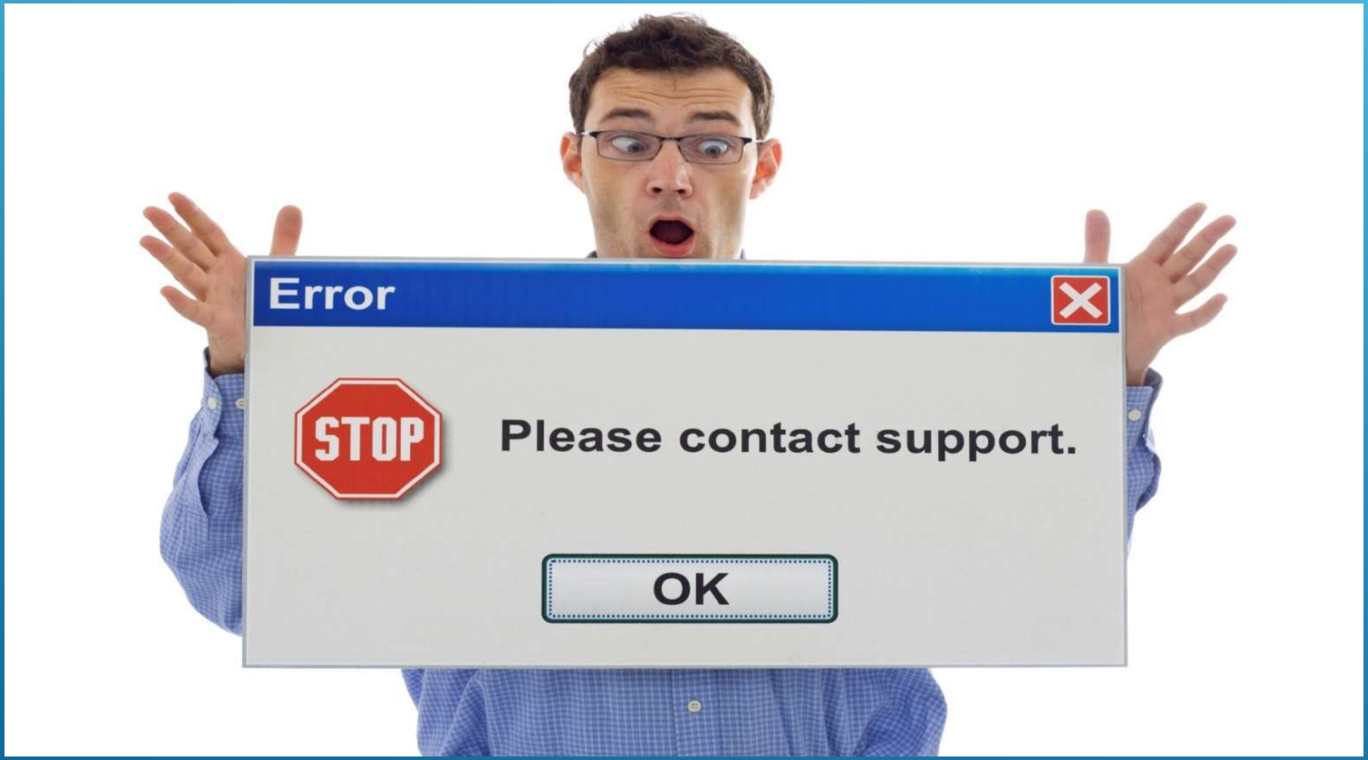
Wrong!

- **One in five** small businesses falls victim to cybercrime each year, and that number is GROWING.
  (Source: National Cyber Security Alliance)
- Small businesses **are low-hanging fruit** because they don't believe they are a target, and therefore have very loose or no security systems and protocols in place.
- **Half of all cyber-attacks** are aimed at SMBs.
  (Source: Forbes Article, "5 Ways Small Businesses Can Protect Against Cybercrime")

Why Don't You Hear More About It?

- It's extremely embarrassing to admit you've been hacked.
- Many people ***don't even know*** they've been hacked.
- ***Horrible PR; do you REALLY want your clients (or patients!) to know their information was accessed?***
- The legal ramifications (fines, lawsuits, legal fees) can be *significant*, so many incidents go unreported.

The 6 Biggest Threats
To you Right Now
And How To Stop Them



#1: Malware

82,000

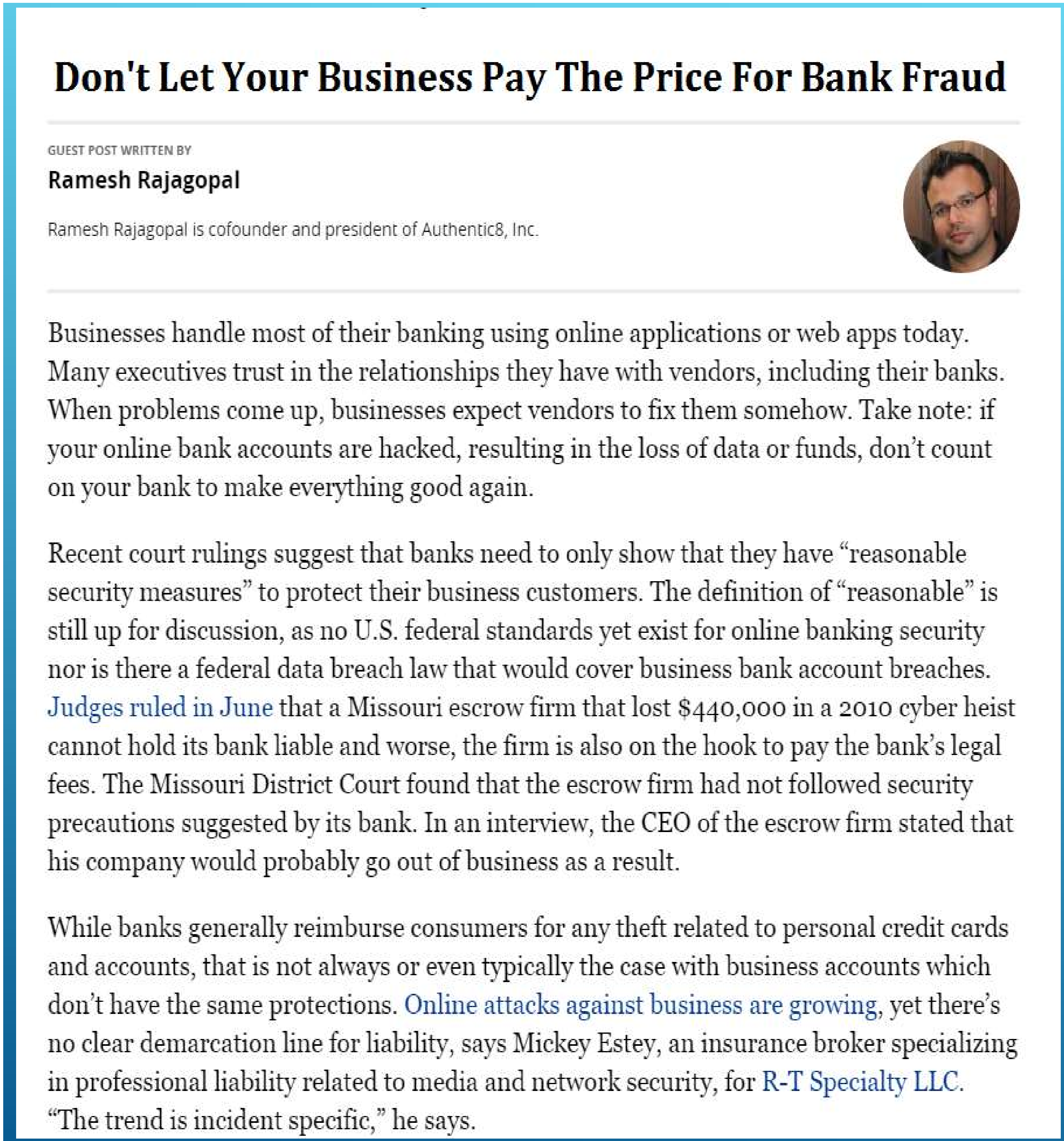
NEW Malware Threats Are Being Released *Per Day*

Source: PC World

#2: Bank Fraud

FDIC Does NOT Protect You From Bank Fraud, And The Bank Is NOT Responsible For Getting Your Money Back!!!

Banks Are Prevailing In Cybercrime Cases; PLUS You Might Have To Pay The Bank's Legal Fees If You Sue Them!



Don't Let Your Business Pay The Price For Bank Fraud

GUEST POST WRITTEN BY

Ramesh Rajagopal

Ramesh Rajagopal is cofounder and president of Authentic8, Inc.

Businesses handle most of their banking using online applications or web apps today. Many executives trust in the relationships they have with vendors, including their banks. When problems come up, businesses expect vendors to fix them somehow. Take note: if your online bank accounts are hacked, resulting in the loss of data or funds, don't count on your bank to make everything good again.

Recent court rulings suggest that banks need to only show that they have "reasonable security measures" to protect their business customers. The definition of "reasonable" is still up for discussion, as no U.S. federal standards yet exist for online banking security nor is there a federal data breach law that would cover business bank account breaches. Judges ruled in June that a Missouri escrow firm that lost $440,000 in a 2010 cyber heist cannot hold its bank liable and worse, the firm is also on the hook to pay the bank's legal fees. The Missouri District Court found that the escrow firm had not followed security precautions suggested by its bank. In an interview, the CEO of the escrow firm stated that his company would probably go out of business as a result.

While banks generally reimburse consumers for any theft related to personal credit cards and accounts, that is not always or even typically the case with business accounts which don't have the same protections. Online attacks against business are growing, yet there's no clear demarcation line for liability, says Mickey Estey, an insurance broker specializing in professional liability related to media and network security, for R-T Specialty LLC. "The trend is incident specific," he says.

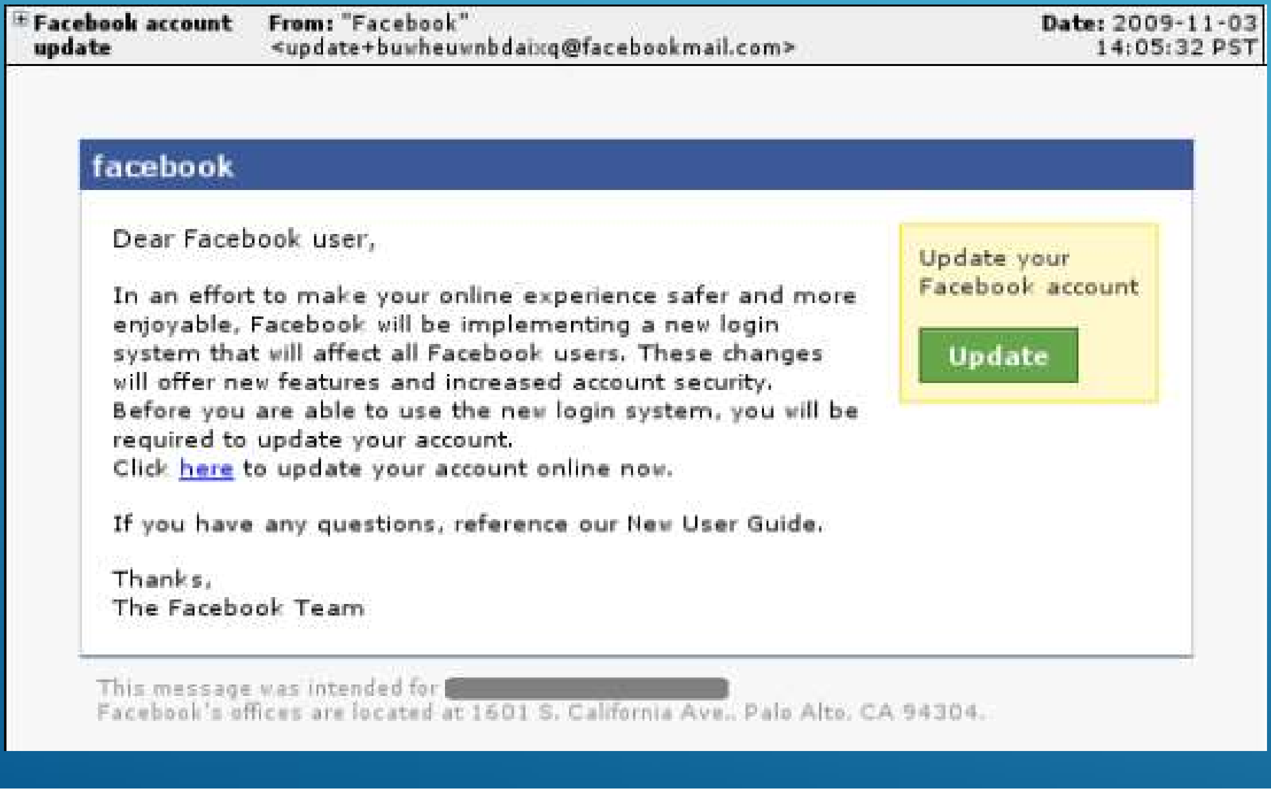
Tips For Protecting Yourself:

- Cancel your debit cards; they are the #1 way bank accounts get compromised.
- Have a dedicated PC for online banking and DON'T use that PC for accessing any other websites, e-mail access or social media sites, or for downloading files and applications.
- Sign up for e-mail alerts from your bank whenever a withdrawal over $100 happens.
- Require YOUR signature for any wire transfers.
- Have your money spread out in multiple accounts to minimize the risk.
- Carry CRIME insurance.

#3: Social Media

Threat #1: Security

600,000 Facebook Accounts Are Hacked Every Single DAY.



Facebook account update **From:** "Facebook" <update+buwheuwnbdaixq@facebookmail.com> **Date:** 2009-11-03 14:05:32 PST

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. Click here to update your account online now.

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

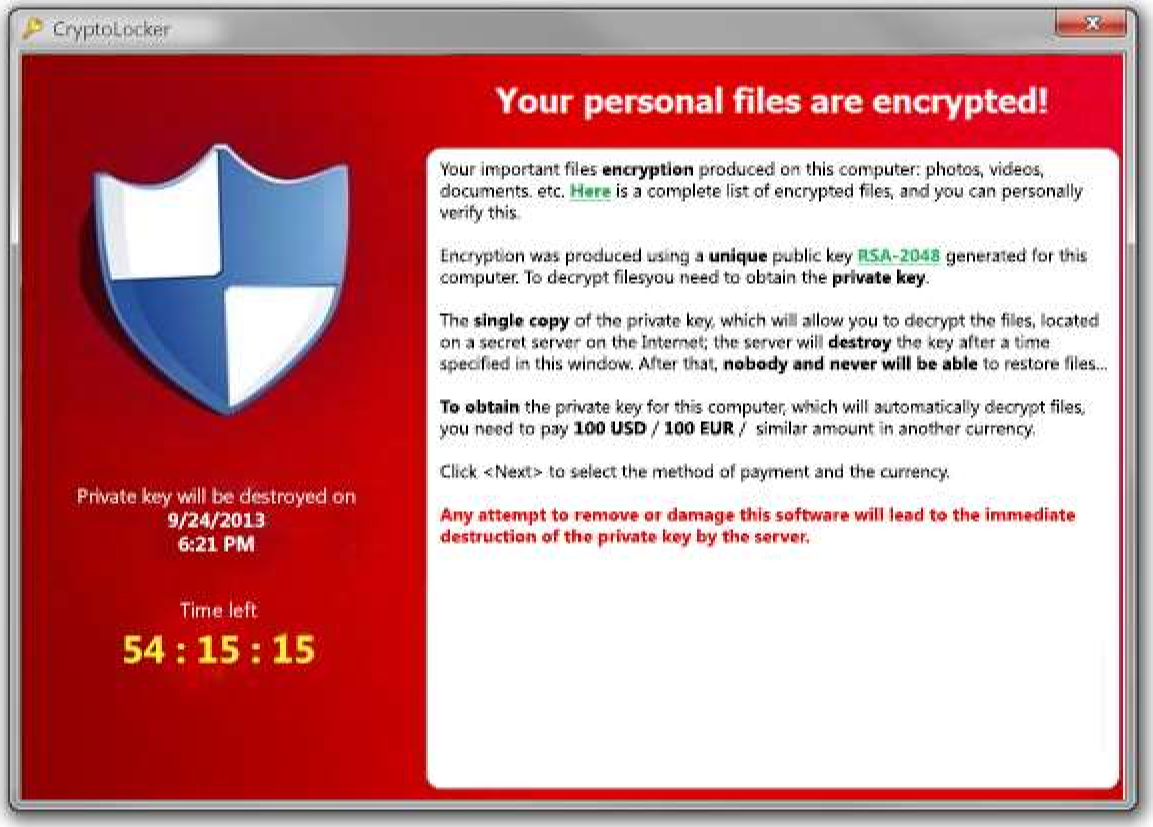
Update your Facebook account

This message was intended for [redacted]
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

#4: Ransomware

A writer once asked a literary agent, **“What kind of writing pays the most?”** Her answer was simple: **“Ransom notes.”**

That’s sort of what’s happening in the cybercrime world — sensitive data in the wrong hands is used to extort money.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

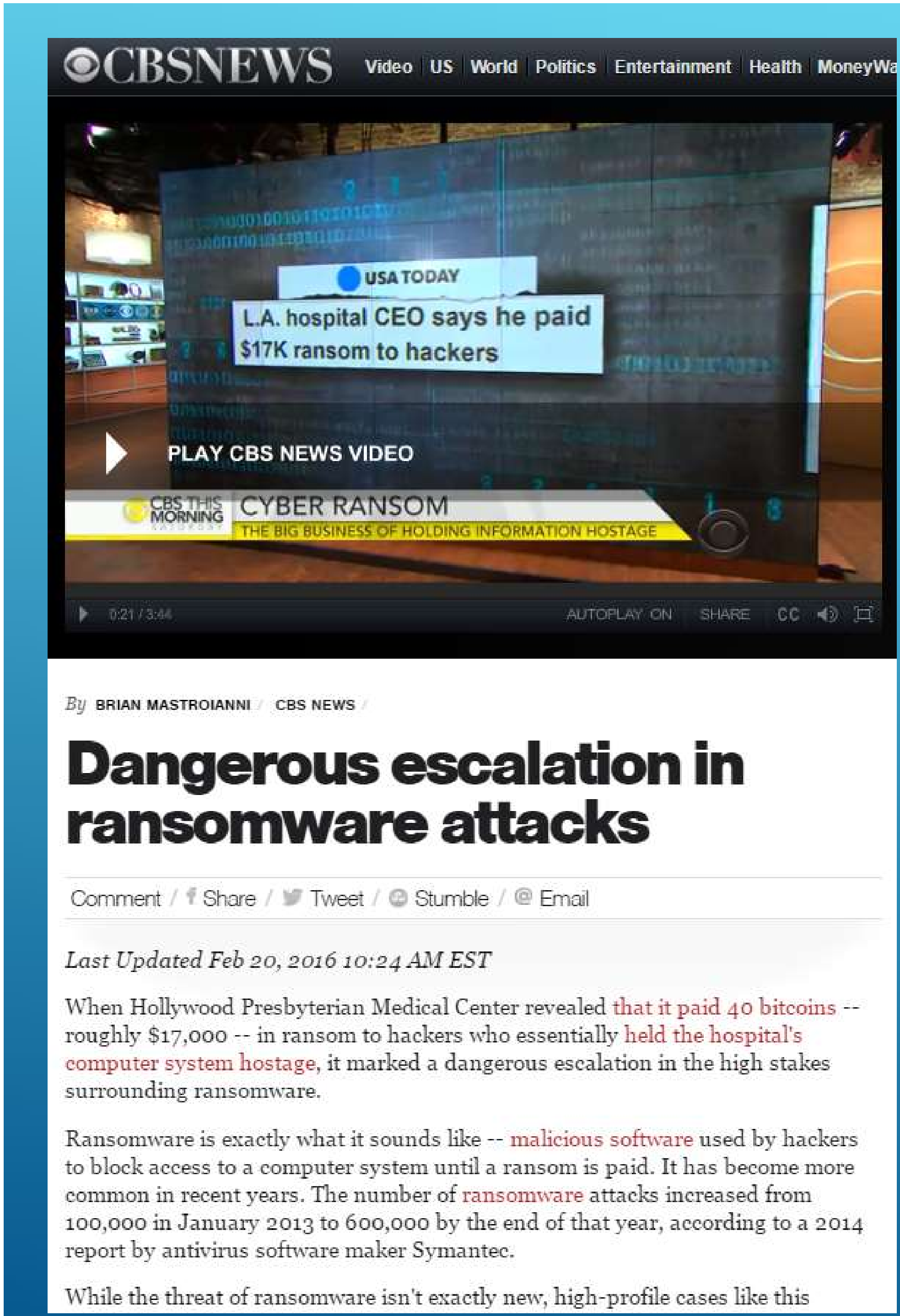
Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Ransomware Is Proliferating


CBSNEWS
Video | US | World | Politics | Entertainment | Health | MoneyWa
USA TODAY
L.A. hospital CEO says he paid $17K ransom to hackers
PLAY CBS NEWS VIDEO
CBS THIS MORNING SATURDAY
CYBER RANSOM
THE BIG BUSINESS OF HOLDING INFORMATION HOSTAGE
0:21 / 3:44
AUTOPLAY ON
SHARE
CC
Comment / Share / Tweet / Stumble / Email

By BRIAN MASTROIANNI / CBS NEWS /

Dangerous escalation in ransomware attacks

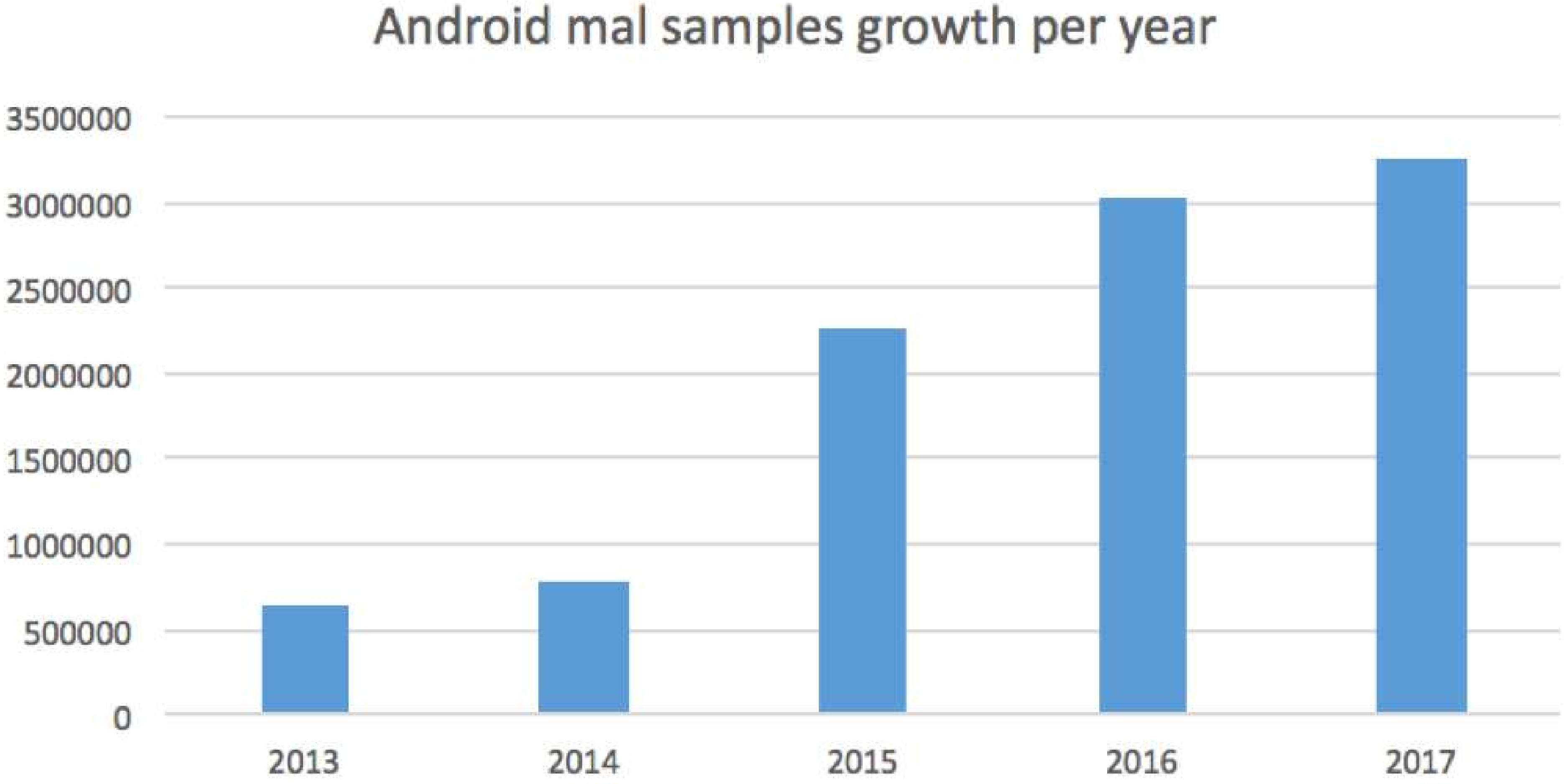
Last Updated Feb 20, 2016 10:24 AM EST

When Hollywood Presbyterian Medical Center revealed that it paid 40 bitcoins -- roughly $17,000 -- in ransom to hackers who essentially held the hospital's computer system hostage, it marked a dangerous escalation in the high stakes surrounding ransomware.

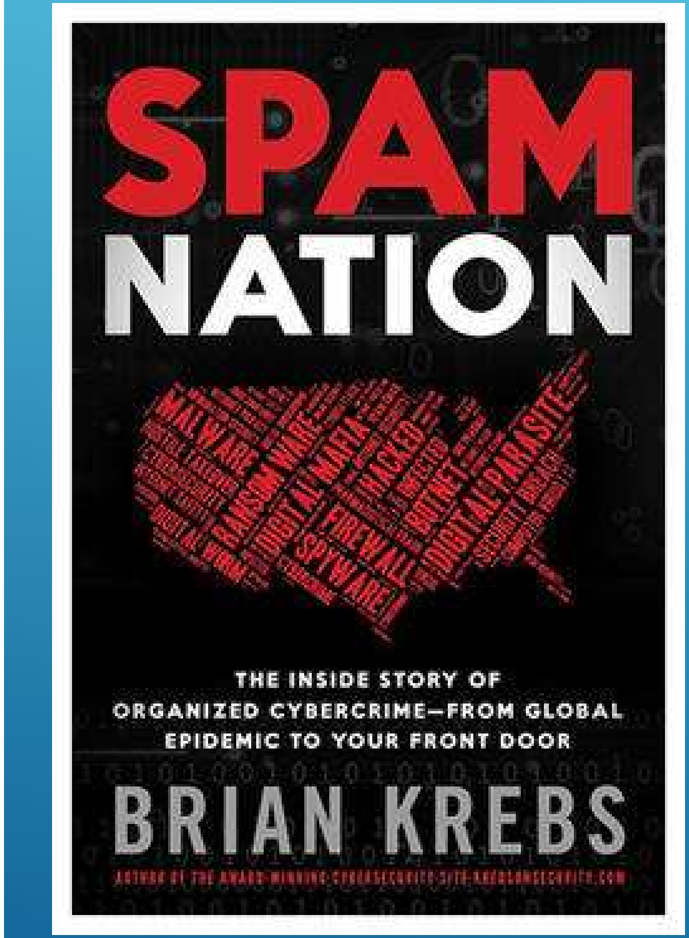
Ransomware is exactly what it sounds like -- malicious software used by hackers to block access to a computer system until a ransom is paid. It has become more common in recent years. The number of ransomware attacks increased from 100,000 in January 2013 to 600,000 by the end of that year, according to a 2014 report by antivirus software maker Symantec.

While the threat of ransomware isn't exactly new, high-profile cases like this

#5: Unsecured, Unmonitored Mobile Devices



#6: Spam!

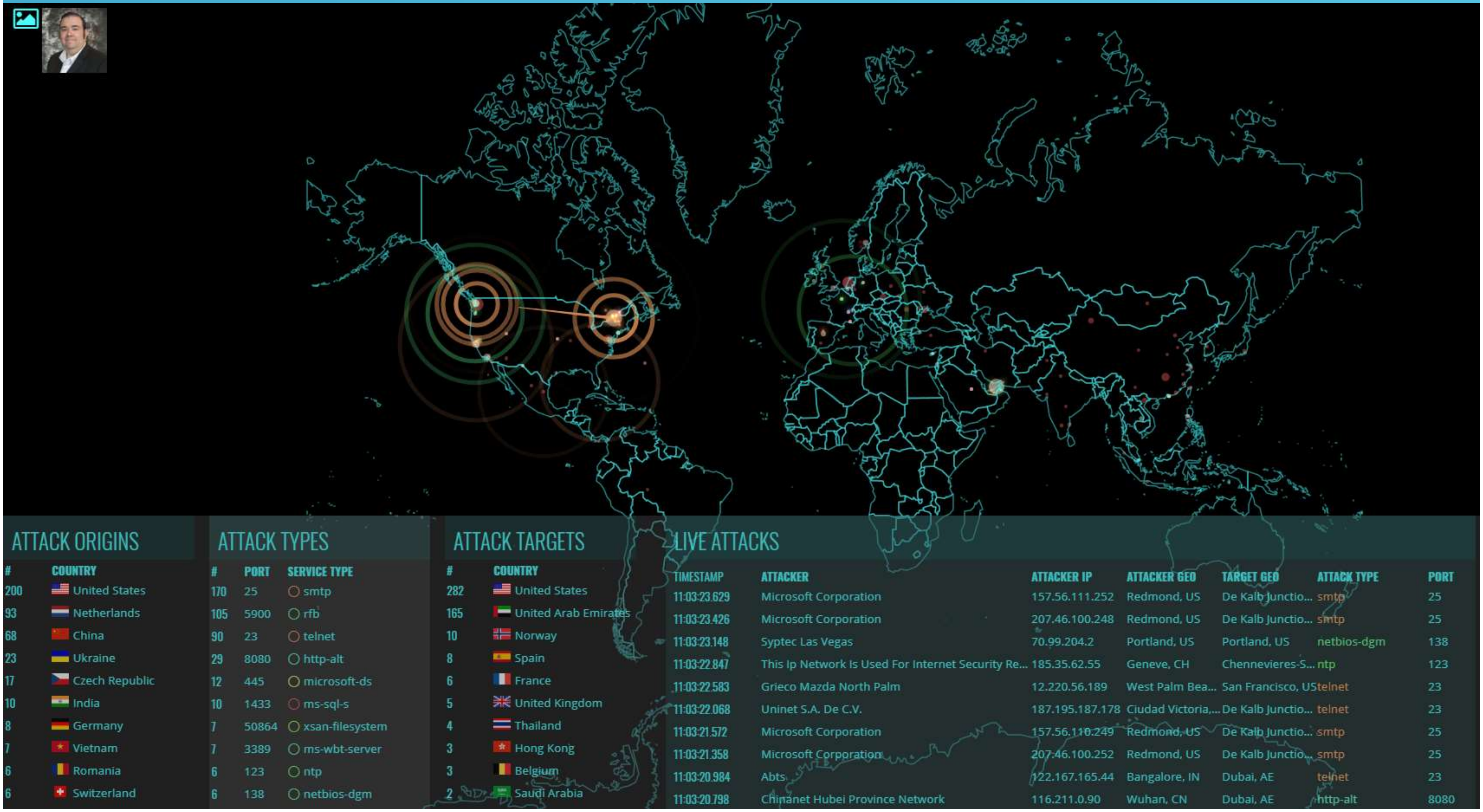

SPAM
NATION
THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS
AUTHOR OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM

"Spam remains the single biggest driver of big breaches today. If we look at some of the biggest data breaches in recent memory – JPMorgan, Target, RSA Security come to mind – they all began with poisoned e-mail."
– Brian Krebs, Spam Nation

https://krebsonsecurity.com/

SO HOW DO YOU PROTECT YOURSELF FROM THIS?

Active attacks at 11:05 am on 11/7/17



ATTACK ORIGINS

#	COUNTRY
200	United States
93	Netherlands
68	China
23	Ukraine
17	Czech Republic
10	India
8	Germany
7	Vietnam
6	Romania
6	Switzerland

ATTACK TYPES

#	PORT	SERVICE TYPE
170	25	○ smtp
105	5900	○ rfb
90	23	○ telnet
29	8080	○ http-alt
12	445	○ microsoft-ds
10	1433	○ ms-sql-s
7	50864	○ xsan-filesystem
7	3389	○ ms-wbt-server
6	123	○ ntp
6	138	○ netbios-dgm

ATTACK TARGETS

#	COUNTRY
282	United States
165	United Arab Emirates
10	Norway
8	Spain
6	France
5	United Kingdom
4	Thailand
3	Hong Kong
3	Belgium
2	Saudi Arabia

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
11:03:23.629	Microsoft Corporation	157.56.111.252	Redmond, US	De Kalb Junctio...	smtp	25
11:03:23.426	Microsoft Corporation	207.46.100.248	Redmond, US	De Kalb Junctio...	smtp	25
11:03:23.148	Syptec Las Vegas	70.99.204.2	Portland, US	Portland, US	netbios-dgm	138
11:03:22.847	This Ip Network Is Used For Internet Security Re...	185.35.62.55	Geneve, CH	Chennevieres-S...	ntp	123
11:03:22.583	Grieco Mazda North Palm	12.220.56.189	West Palm Bea...	San Francisco, US	telnet	23
11:03:22.068	Uninet S.A. De C.V.	187.195.187.178	Ciudad Victoria,...	De Kalb Junctio...	telnet	23
11:03:21.572	Microsoft Corporation	157.56.110.249	Redmond, US	De Kalb Junctio...	smtp	25
11:03:21.358	Microsoft Corporation	207.46.100.252	Redmond, US	De Kalb Junctio...	smtp	25
11:03:20.984	Abts	122.167.165.44	Bangalore, IN	Dubai, AE	telnet	23
11:03:20.798	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080

How To Protect Yourself:

- **Having a firewall and antivirus is NOT sufficient protection anymore**; today's sophisticated threats require a layered approach.
- **Get EDUCATED** on how to spot a phishing e-mail, what websites to avoid, what files you should never download, how to appropriately use e-mail, so you aren't inadvertently opening the door to cybercriminals. In some circumstances, **you might want to lock down and limit certain activities on your network** to prevent yourself from doing these things by mistake or something else doing them for you.
- You need to install and maintain a professional-grade backup **IMPORTANT:** If you're using 3rd-party cloud-based applications, it's CRITICAL to get your data backed up on-site or to a completely different place.
- You should have **ongoing monitoring and maintenance of computers and network** (firewall, software patches, backups, etc.).

Free or cheap tools:

Password Management:
Lastpass, Dashlane, Keepass

Antivirus and Anti-malware:
Webroot and Malwarebytes

DNS Filter:
OpenDNS personal

Firewall Scanner:
Shields Up by Gibson Research

Id Theft Protection:
LifeLock or ID Agent

Use 2FA with any service that offers it:
Yubico