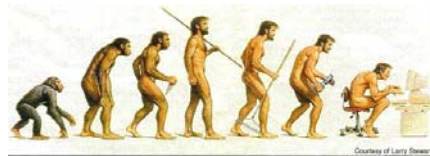


Technology Update

Jonathan Phillippe
David Babb, CPA

MAY 2016

Accounting Technology Evolution



Somewhere, something went terribly wrong

Accounting Technology, in the Beginning

ABACUS

- 2700-3200 BC
- Europe, Russia, China
- Hindu-Arabic Numeric System
- Still widely used



Accounting Technology, in the Beginning, Cont'd

PASCALINE

- Early 1600's
- First analog calculator with a "carry" function
- Rouen, France



Accounting Technology, in the Beginning, Cont'd

Difference Engine

- ▶ Charles Babbage
- ▶ 1800's
- ▶ Notable other inventions



Accounting Technology, in the Beginning, Cont'd

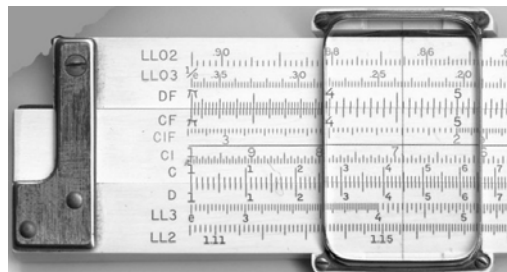
Cranking Calculators



Accounting Technology, 1950's and 1960's



Accounting Technology



Accounting Technology, 1970's and 1980's



Accounting Technology, 1970's and 1980's, Cont'd



Accounting Technology, 1970's and 1980's, Cont'd

	JANUARY	FEBRUARY	MARCH
SALES	200000	200000	212120
COST/SALE	100000	132100	136530
GR. PROFIT	110000	113200	115484
EXPENSES			
SALARIES	30000	30720	37454
RENT	200	200	200
UTIL	400	400	400
INSUR	600	600	600
PHONE	1200	1200	1200
OFFICE	1400	1400	1400
DEPRN	12000	12000	12000
TOTAL	36000	36720	37454
TOTAL EXPENSES	66000	66720	66720

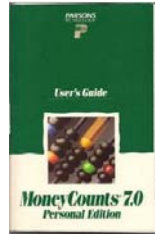
Figure 7.2 VisiCalc Spreadsheet

Accounting Technology, 1980's

	1982	1983	1984
Net sales	\$263,537	\$277,545	\$326,268
Total expenses	\$245,500	\$246,210	\$270,900

	1982	1983	1984
Sales			
Model TD520-V	\$20,635	\$20,393	\$71,000
Model RH619-P	\$45,645	\$39,256	\$58,500
Model FH521-A	\$35,900	\$30,922	\$30,500
Total sales	\$102,180	\$90,571	\$160,000

Accounting Technology, 1990's



Accounting Technology, 1990's



Accounting Technology, Today

- ▶ Software as a service (SaaS)
 - ▶ Software licensed on subscription basis
 - ▶ Monthly or annual fee versus upfront perpetual licensing fee
 - ▶ Centrally hosted (reduced IT support costs)
 - ▶ Accessible from any computer (or device) with internet
 - ▶ No application and server maintenance on - site
 - ▶ Downsides:
 - ▶ Timely payment woes, Trust, datacenter hacks
- ▶ Examples
 - ▶ Quickbooks Online
 - ▶ XERO
 - ▶ Freshbooks
 - ▶ Single-entry accounting?



Accounting Technology, Today

Single Entry Accounting:

- ▶ Used in the interest of simplicity, especially when accounting background is not present
- ▶ Emphasizes income statement accounting
- ▶ Not self balancing, errors are more likely



Accounting Technology, Today

Microsoft Office 365

- ▶ Office, in the cloud
- ▶ Subscription basis
- ▶ Home or business
- ▶ You always have the most up-to-date version
- ▶ Desktop installed version are also available for download
- ▶ reduces need for complex in-house hosting
- ▶ 1 user up to +50,000



Accounting Technology, Today

Excel 2016

- Features:
 - Quick Analysis Button
 - New Charts
 - Enhanced Database Features
 - New Templates
 - Equation Drawing
 - Touch / Mouse Mode
 - "Tell Me"



Accounting Technology, Today



Accounting Technology, Today

Skype for Business

LastPass

Accounting Technology, Today



Accounting Technology, Today

Accounting Technology, Today



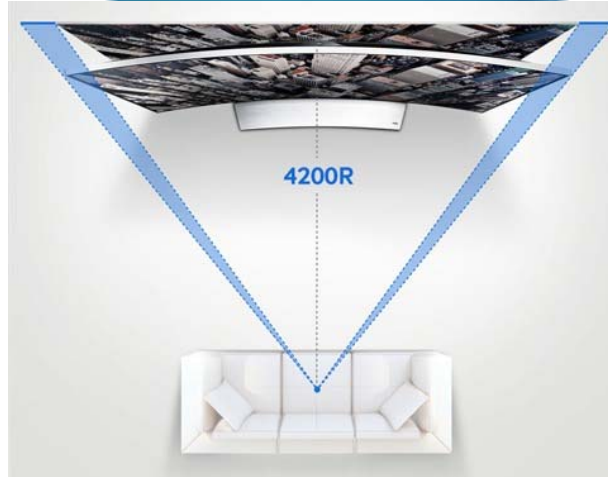
Accounting Technology, Today

Hardware

- ▶ Curved and large monitors
 - ▶ Perceived screen larger than reality
 - ▶ More immersive experience



Accounting Technology, Today



Accounting Technology, Today

Hardware, continued

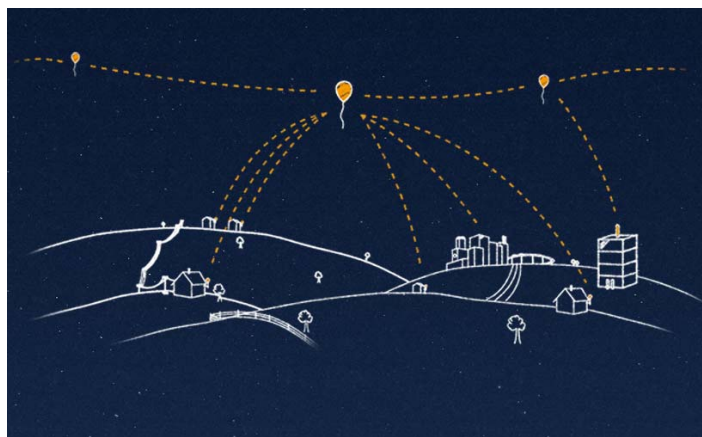
- ▶ Desktop virtualization (BYOC)
- ▶ microcomputers

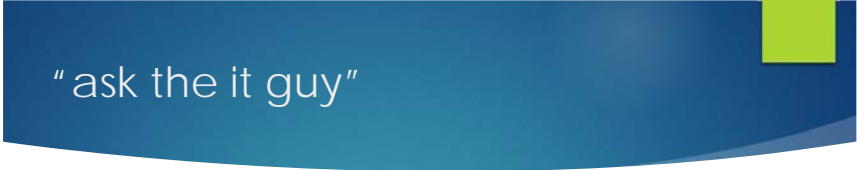


Other Cool Stuff!



Google X Project Loon





"ask the it guy"

Melissa Virus



Created in 1999 by David L. Smith

The Virus

The virus was a Microsoft Word macro. A macro is a series of commands or instructions that gets carried out automatically.

He claimed to have named the virus after an exotic dancer in Florida.

One of the first email-activated viruses

The Damage

Tens of thousands of people couldn't access their emails within six hours of the virus being posted.

Hundreds of websites were affected.

The Microsoft Corporation had to **disable all incoming and outgoing email**.

Caused **\$1.2 billion** in damages and losses.

- 1 **Shutting down** safeguards in those programs
- 2 **Lowering security** settings
- 3 **Disabling macro** security
- 4 The virus **spread itself** by sending an infected document via email

The email was designed to **trick people** into opening the file.

Computers which had Microsoft Outlook would **send** the infected document to the **top 50 contacts** in the user's address books.

If the day of the month matched the minute, the virus would insert a Bart Simpson quote into the document it sent: "Twenty-two points, plus triple-word score, plus fifty points for using all my letters. Game's over. I'm outta here!"

David L. Smith was:


- 

Fined **\$5,000**
- 

Sentenced to **20 months** in jail
- 

Forbidden from accessing computer networks without court authorization

ILOVEYOU Virus



Allegedly written by Onel de Guzman

The Virus

Typically spread through an infected email attachment.

Launched from the Philippines in 2000

The Damage

Roughly **one tenth** of all internet-connected computers in 2000 were infected with ILOVEYOU.

The virus caused an estimated **\$15 billion** in damages.

McAfee reported that a supermajority of their Fortune 100 clients were infected with the virus.

It caused **\$5.5 billion** in damages in the first week.

ILOVEYOU reached an estimated **45 million** people in one day.

The email's subject line would say that it was a love letter from a secret admirer.

The name of the original file was **"LOVE-LETTER-FOR-YOU.TXT.vbs"**.

.vbs is a Visual Basic Scripting file.

Due to formatting issues, some email clients omitted the ".vbs" in the file name. This caused users to think they were opening a plain text file.

The virus would:

- 1 **Overwrite** file types with copies of itself to let it **continue spreading** if the original version was removed from the computer.
- 2 **Reset** the infected computer's Internet Explorer home page.
- 3 **Send** the infected file to all of the user's contacts in Microsoft Outlook.
- 4 **Download and execute** a file that stole passwords and emailed them to the hacker's email address.

This erased a number of different files, including:

- MP3
- ZIP
- JIS
- HTA
- BPF
- COM
- EXE
- DOC
- PDF
- TXT

If the user entered a chat group with Internet Relay Chat, the virus would attempt to spread to all other users in the group.

Onel de Guzman was arrested on suspicion of creating the virus.

He and his co-conspirator were later released as the Philippines had no laws at the time against writing malware.

NIMDA VIRUS

Launched in September 2001, one week after 9/11

The Virus

The FBI had to refute rumors that the virus was connected to the terrorist attack.

In *Computerworld Magazine*, TrusteSec CTO Peter Tiggett reported that Nimda topped their list of viruses in just 22 minutes.

NIMDA = ADMIN

Nimda is "admin" spelled backwards.

The virus was the **fastest spreading piece of malware** at the time.

More than 2 million computers were infected in 24 hours.

While the virus could infect home PCs, its primary target were web servers.

The virus infected computers in a variety of ways:

- Email
- Local networks
- Drive-by downloads on websites
- Loopholes created by other worms
- Vulnerabilities in IS (Internet Information Server), Microsoft's web server

- Nimda allowed attackers to have the same access to an infected machine as the current user.
- If a user had admin-level privileges, so would the hacker.
- Nimda would install itself to the root of drives C, D, and E.
- It would also replicate itself in any folder where it found doc or .eml files.

The Damage

Caused **\$635 million** in losses.

A Florida Federal court had to operate using paper copies of all of their documents when their system was infected with a Nimda variant.

The virus spread so quickly that it significantly **slowed Internet browsing times** and crashed several networks.

CODE RED Virus

Code Red launched in July 2001

The Virus

A second version of the virus, Code Red II, acted similarly and was launched later in the year.

It infected Windows NT and 2000 machines by exploiting a buffer overflow vulnerability.

The Damage

Between **1 and 2 million computers** were infected overall.

CAIDA (the Center for Applied Internet Data Analysis) found that of those hosts infected by Code Red:

- 43.91% were from the US
- 10.57% were from Korea

In less than a day, the virus infected more than **359,000 computer systems**.

Caused over **\$2 billion** in losses.

- Works by sending the computer instructions after a long string of nonsense.
- Once the buffer has been filled with the nonsense information, the computer begins overwriting memory.

The memory is overwritten with the instructions for the virus.

- This meant that the user only had to be connected to the Internet to be infected.
- Infected Windows NT machines would crash more often than normal.
- Infected Windows 2000 machines would suffer a system-level compromise.
- This means that the computer could be controlled by the hacker.

The virus would behave differently depending on a few factors:

The date:

- 1st-19th:** Target random IP addresses and spread itself.
- 20th-28th:** Launch a DDoS (distributed denial-of-service) attack on the White House's IP address.
- 28th and after:** Go into "sleep" mode.

Page language: English-language web pages would be defaced with the words "Hacked by Chinese!"

Microsoft released a patch to fix the vulnerability exploited by the virus several months after the attack.

SQL SLAMMER/SAPPHIRE VIRUS

Launched in 2003

The Virus

Spread through a buffer overflow vulnerability in Microsoft's SQL Server database management service

Randomly selected IP addresses to infect

196.0.231.15

Servers infected with SQL Slammer would spawn millions of copies to infect other servers

Within 3 minutes of attacking its first victim, the number of servers infected by Slammer doubled every 8.5 seconds

The Damage

- Caused \$750 million in damages
- Crashed Bank of America's ATM service
- A number of other banks were affected by the virus
- Caused outages to Seattle's 911 service
- Infected Continental Airlines online ticketing systems and electronic kiosks, rendering them inoperable
- Alfred Hugler, from Symantec Security Response, reported that SQL Slammer caused network issues over the entire Internet.

South Korea lost almost all Internet access

At the time 70% were connected to the web

US Government websites affected included:

- Department of Agriculture
- Department of Commerce
- Defense Department

Several newspapers had publishing problems, including:

- The Atlanta Journal Constitution
- The Associated Press
- The Philadelphia Inquirer

SASSER VIRUS

Launched in 2004

Created by **Sven Jaschan**, a 17-year-old from Germany

The Virus

Sasser worked by exploiting a vulnerability in a Windows system called LSASS (Local Security Authority Subsystem Service)

The virus scanned IP addresses until it found one that was vulnerable

Then it downloaded itself into the Windows directory

The next time the computer was booted up, it would be infected

Unlike other viruses, users didn't have to open any email attachments in order to be infected by Sasser; they only needed to be online

Sasser also affected the operating system

This made shutting down infected computers without pulling the plug difficult

The Damage

- Infected all 19 of the British Coast-guard's control rooms
- Delayed British Airways flights
- Staff had to use paper maps and pens
- Caused \$500 million in damages
- Sasser brought down a third of Taiwan's post offices

Sven Jaschan was sentenced to:

- 1 year, 9 month probation
- 30 hours of community service
- He was tried as a junior

The virus affected Windows 2000 and XP

MYDOOM VIRUS

Launched in 2004

The Virus

Originally began spreading through KaZaA, a file-sharing application, but then spread to emails.

In both cases, users had to open a file in order to become infected.

At its peak, MyDoom infected one in 12 emails as it tried to spread itself.

The Damage

Caused \$38 billion in damages

McAfee reported that MyDoom:

- Slowed down Internet access worldwide by 10 percent
- Reduced access to some websites by as much as 50 percent

- Computers infected with MyDoom would launch a DDoS on www.sco.com (a Linux software company).
The virus would also open ports on victims' computers so that hackers would have backdoor access to their systems.
- A second attack later that year affected search engines.
MyDoom-infected computers would send search requests to search engines in an attempt to find email addresses. Some search engines received so many requests that they crashed.
- MyDoom was capable of spoofing its infection emails, making it more difficult to track.
"Spoofing" involves forging the "From" address in an email.
Infected between 600,000 and 700,000 computers.

CONFICKER Virus

Launched in 2008

The Virus

Took advantage of an exploit in Windows 2000, XP, and 2003 servers that could cause them to install an unauthenticated file.

It could even affect servers with firewalls, as long as they had print and file sharing enabled.

The Damage

Caused \$9.1 billion in damages

French fighter planes were grounded when they couldn't download their flight plans.

In England, military systems were infected, including:

- More than two dozen British Royal Air Force bases
- 75% of the Royal Navy fleet

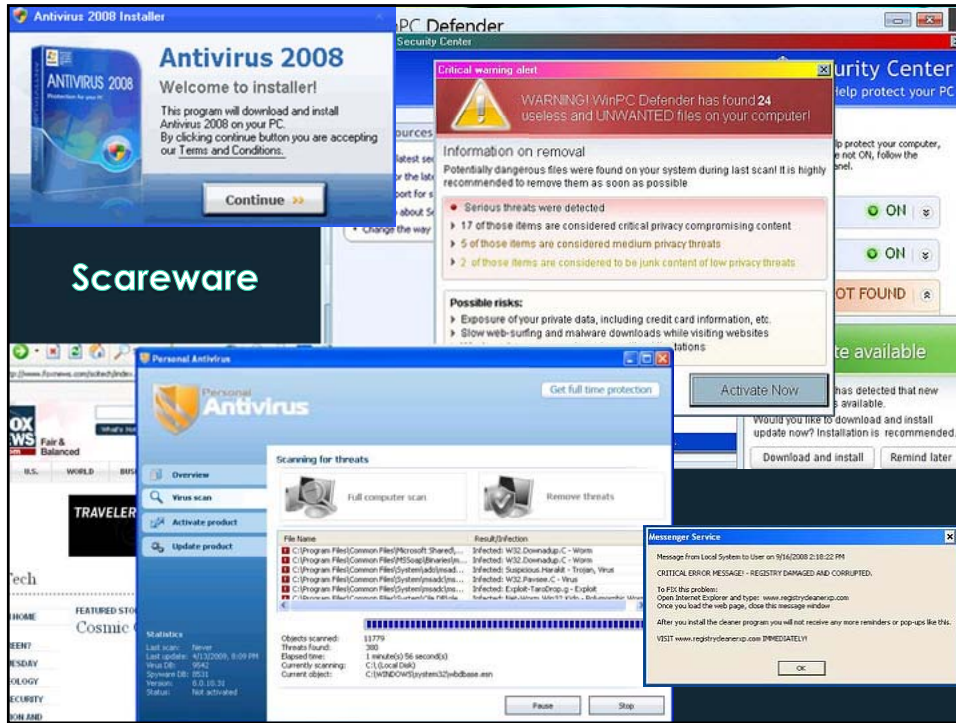
The Manchester City Council IT system went down, rendering the city unable to process fines.

Computers and medical devices at hospitals in the US and the UK were infected.

- Infected millions of computers. Spread by infected USB drives and over networks. Later variants were capable of:
 - Creating backdoors in firewalls
 - Disabling anti-malware programs

Conficker was supposed to do something on April 1, 2009, but nothing happened. Experts were worried computers infected with Conficker would possibly:

- Become a botnet
- Create a criminal version of a search engine, copying private information from infected systems and then selling that information
- Launch a massive DDoS attack



IMPACT OF ZEROACCESS BOTNET

ZEROACCESS BOTNET

One of the largest P2P botnets ever known
X 1.9 million

ZeroAccess carries out two revenue generation activities

BITCOIN MINING

CLICK FRAUD

*Botnet generates...

1.9Mx

Earns US\$ 2,165/day

Click fraud generates
488 TB network traffic/day
Per annum earnings:
Tens of millions US\$!!!

Uses **3,458 MWh/day** = **Power for > 111,000 homes/day**

Cost of electricity > US\$ 560,887/day

Sources: <http://www.symantec.com/about/press/2011/05/11/zeroaccess-botnet>, <http://www.symantec.com/about/press/2011/05/11/zeroaccess-botnet>, <http://www.symantec.com/about/press/2011/05/11/zeroaccess-botnet>, <http://www.symantec.com/about/press/2011/05/11/zeroaccess-botnet>

@thesymantec | www.symantec.com

WHAT IS MALVERTISING?

MALICIOUS ADVERTISING ("MALVERTISING") IS A TYPE OF ONLINE ATTACK WHEREIN MALICIOUS CODE HIDDEN WITHIN AN ONLINE AD INFECTS YOUR COMPUTER WITH MALWARE.

How Malvertising Works

You visit a website. It doesn't matter if the site is sketchy or legitimate -- the threat lies within the ads on the site.

Advertisements can come in a variety of shapes and sizes, though usually appear as banners or pop-ups.

Malvertising utilizes numerous tactics, such as using an iFrame, an invisible box that can secretly navigate to additional web pages.

THE IFRAME REDIRECTS TO AN "EXPLOIT LANDING PAGE."

THE LANDING PAGE IS WHERE MALICIOUS CODE ATTACKS YOUR SYSTEM.

THE ATTACK CODE EXPLOITS YOUR SYSTEM AND INSTALLS MALICIOUS SOFTWARE.

MALICIOUS BIDDING

CYBER CRIMINALS ARE ABLE TO UTILIZE MALVERTISING BY SUBMITTING BOOBY-TRAPPED ADVERTISEMENTS TO AD NETWORKS FOR A REAL-TIME BIDDING PROCESS.

AFTER THE AD WINS THE BID, IT IS PROPAGATED IN REAL TIME THROUGH VARIOUS PUBLISHERS AND WILL ONLY TRIGGER ITS MALICIOUS PAYLOAD IF SPECIFIC CONDITIONS ARE MET.

HARD TO CATCH

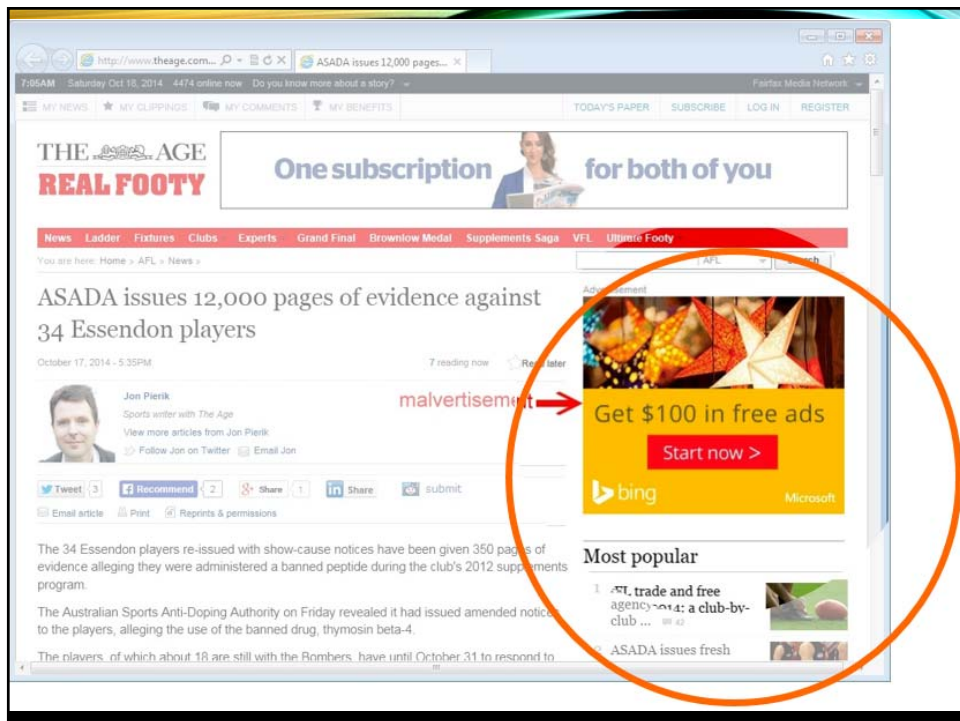

MALICIOUS ADS ROTATE IN WITH NORMAL ADS. THEREFORE, WHEN A USER VISITS AN INFECTED SITE, THEY MIGHT NOT BE ATTACKED.

BECAUSE DUPLICATING THE INFECTION IS DIFFICULT, THIS CAN MAKE IT VERY HARD FOR SECURITY RESEARCHERS TO STUDY A MALVERTISING ATTACK.

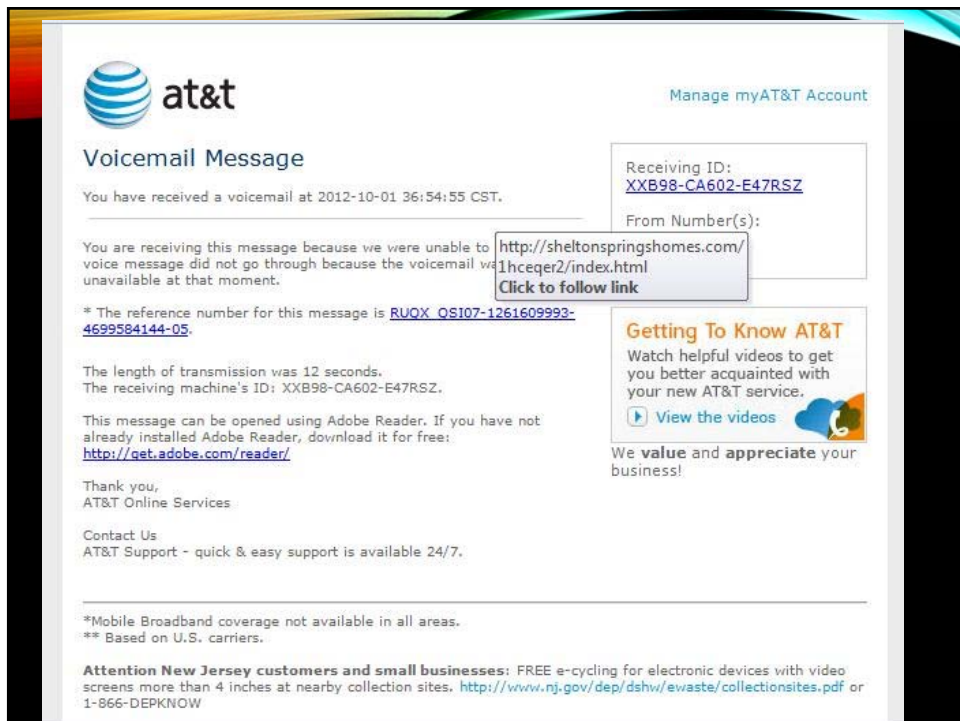
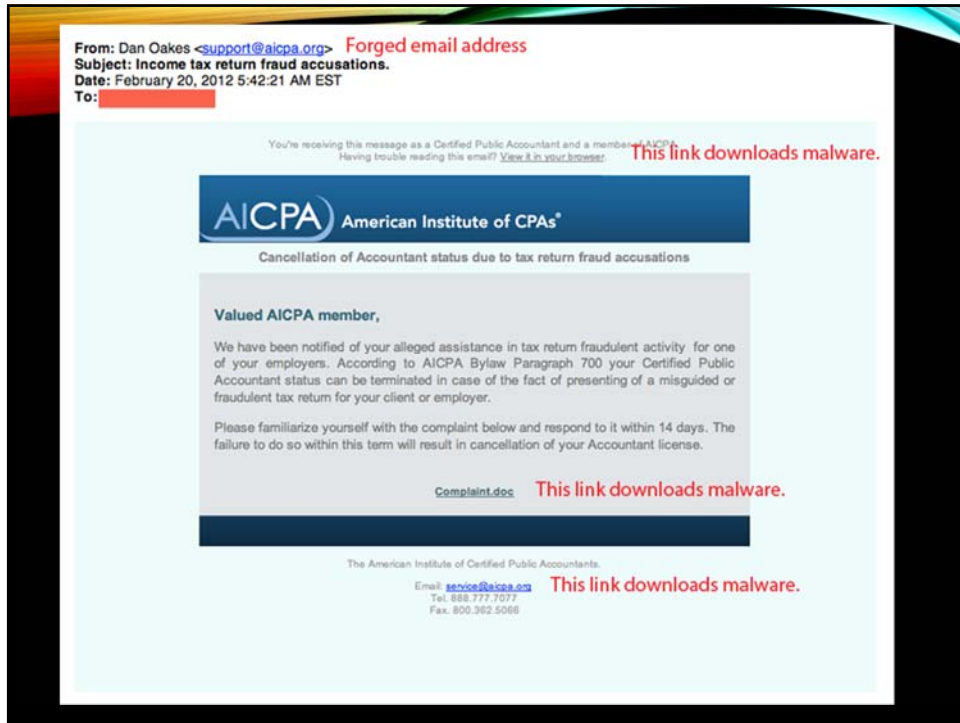
PROTECTION

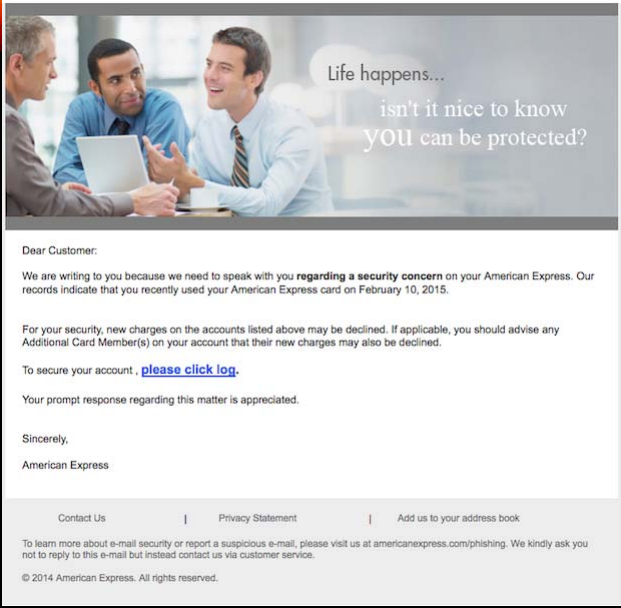
USING SOFTWARE LIKE POP-UP/AD BLOCKERS OFFERS SOME PROTECTION AGAINST MALVERTISING, BUT EMPLOYING ANTI-EXPLOIT SOFTWARE IN CONJUNCTION WITH AN ANTI-MALWARE IS YOUR BEST BET.

LEARN MORE AT WWW.MALWAREBYTES.ORG.



The screenshot shows a news article on 'THE AGE REAL FOOTY' website. The article title is 'ASADA issues 12,000 pages of evidence against 34 Essendon players'. A yellow advertisement for Bing is overlaid on the right side of the article, with the text 'Get \$100 in free ads' and a 'Start now >' button. A red arrow points to the word 'malvertisement' written in red on the page, which is positioned above the advertisement. The advertisement is circled in orange.





Life happens...
isn't it nice to know
YOU can be protected?

Dear Customer:

We are writing to you because we need to speak with you **regarding a security concern** on your American Express. Our records indicate that you recently used your American Express card on February 10, 2015.

For your security, new charges on the accounts listed above may be declined. If applicable, you should advise any Additional Card Member(s) on your account that their new charges may also be declined.

To secure your account, [please click log](#).

Your prompt response regarding this matter is appreciated.

Sincerely,
American Express

[Contact Us](#) | [Privacy Statement](#) | [Add us to your address book](#)

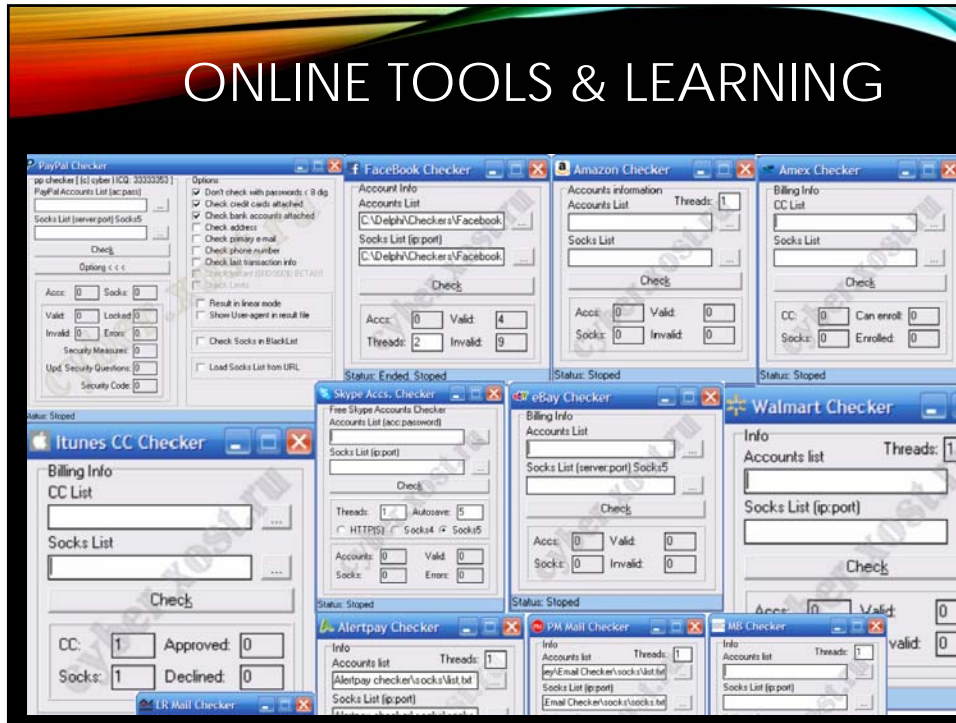
To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us via customer service.

© 2014 American Express. All rights reserved.

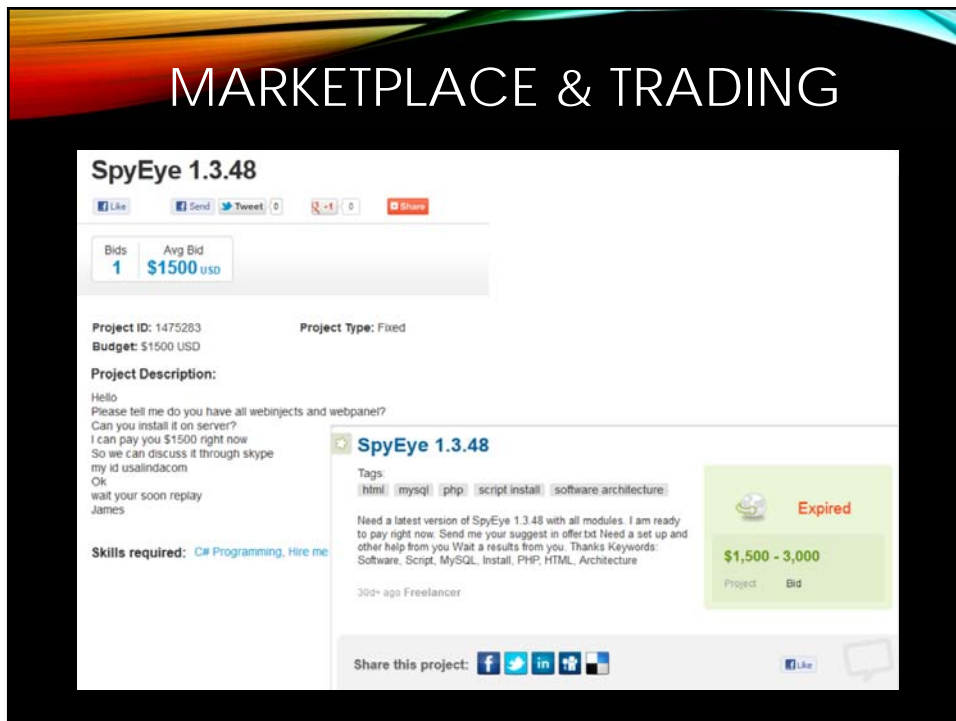
HACKING HAS EVOLVED

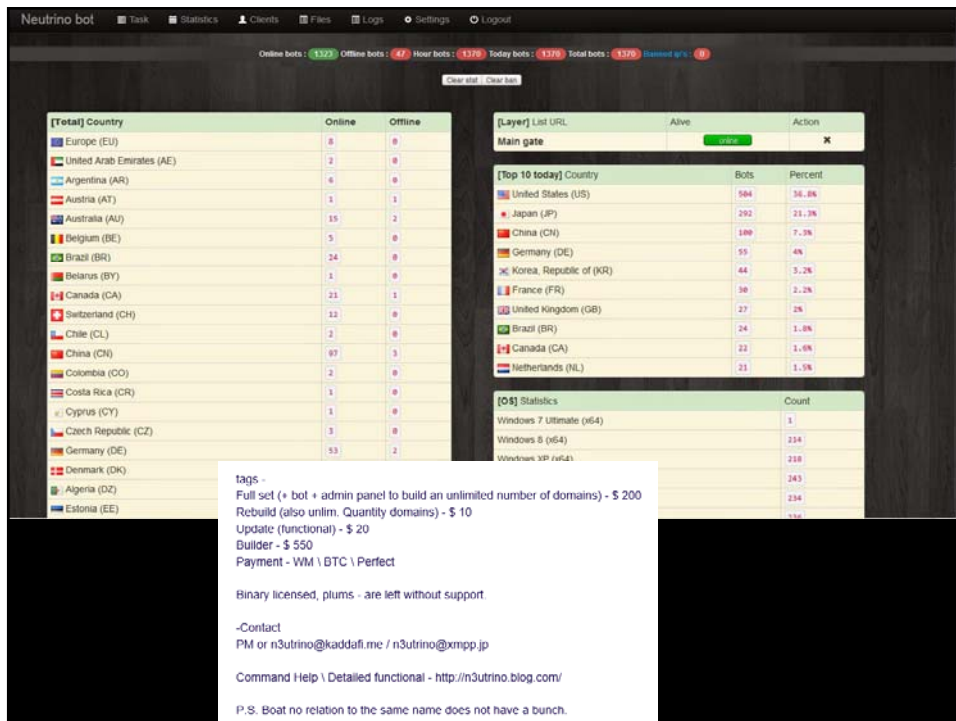
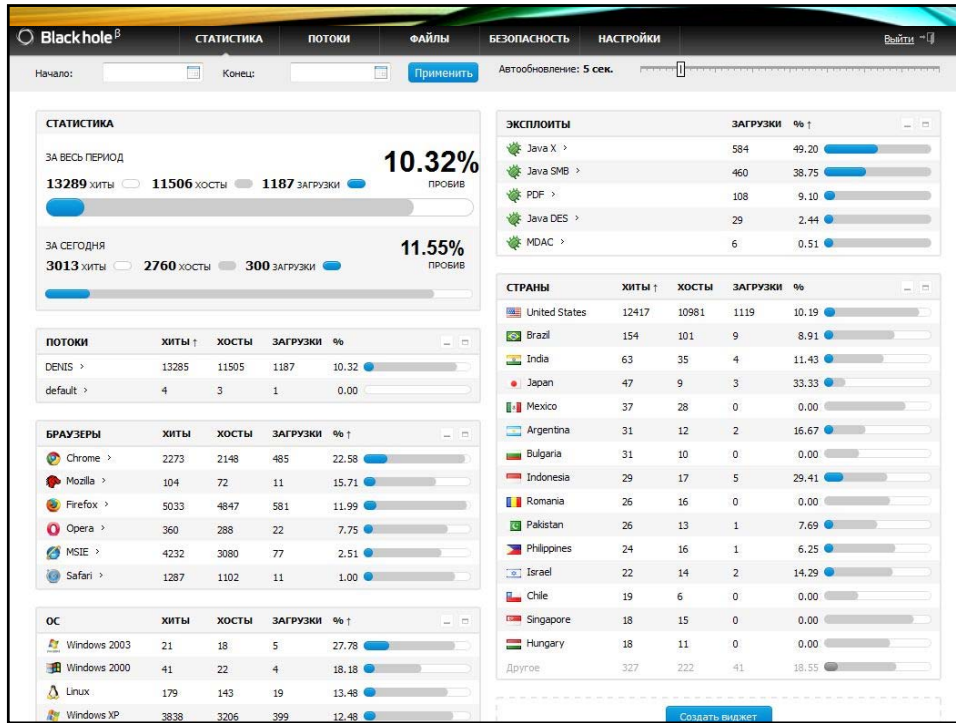
Old	New
• Centralized	• Distributed / Specialized
• Custom Built	• Purchase or rent
• Physical on Site Servers	• Online tools
• \$\$\$	• \$
• Target Large Business	• Small Business

ONLINE TOOLS & LEARNING



MARKETPLACE & TRADING





The screenshot shows a forum post on the Spambot.com website. The post is titled "Продам инсталлы MIX" (Selling MIX installs). The author is "Umbro" (Member), registered on 29.12.2007, with 216 messages. The post content is as follows:

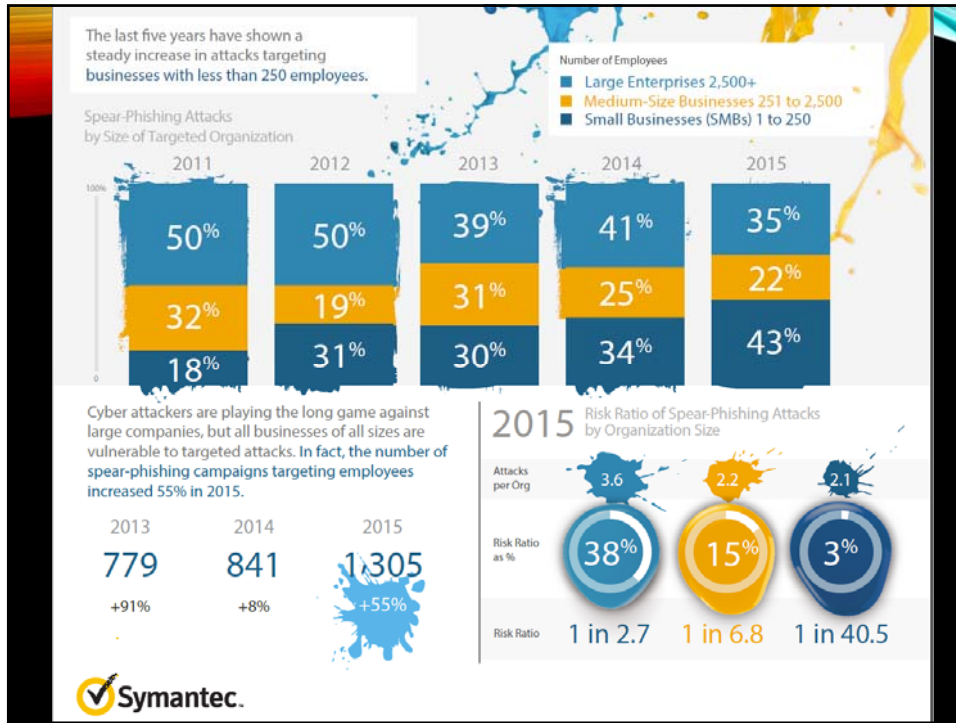
Приветствую всех!
Greetings to all!
 В связи с переполнением серверов ботов, продаю не нужные инсталлы.
Due to overstock I am selling unneeded installs.
 Цена: 50 евро за 1к
Price: \$60 WMZ for 1k
 Оплата: оплата вперед, без посредников.
Payment: in advance, with no escrow.
 География: вся земля, преимущественно без Азии.
Geography: A mix of countries, with virtually no Asia.
 Что грузится: грузится на бота только мой граббер и ВАШ спамбот (никого кроме спамботов не грузю принципиально)
Loads: Only my grabber and your spam bot is being loaded (nothing but spam bots allowed)
 Получение: сразу после оплаты. В течение 10 минут загрузится вся база ботов.
Delivery: You pay and I start running your exe in 10 minutes.
 Качество: исходя из того, что я написал выше, я не грузю ничего кроме своего граббера и вашего спамбота, загрузки не дохнут и я никого не выгружаю со времени, не грузю на 2 exe на 1 бота. Если качество и фидбэк откликнут, то брать можно и больше инсталлов.
Quality: As stated above, nothing else is loaded besides my grabber and your spambot, loads do not die, and I do not overutilize resources, or load 2 exe per bot. Inquire with others who have already purchased installs.
 Контакты: 312-456, когда случится, просьба сообщать ваш ник и что вы с форума по поводу инсталлов.
 Всем спасибо, приятного дня.

"TA530 customizes the e-mail to each target by specifying the target's name, job title, phone number, and company name in the email body, subject, and attachment names. On several occasions, we verified that these details are correct for the intended victim. While we do not know for sure the source of these details, they frequently appear on public websites, such as LinkedIn or the company's own website. The customization doesn't end with the lure; the malware used in the campaigns is also targeted by region and vertical.

"While these campaigns aren't approaching the size of, for example, Dridex and Locky blasts that go after very large numbers of random recipients, TA530 targets hundreds, thousands, or even tens of thousands of recipients in US, UK, and Australian organizations. These attacks are quite large relative to other selective or spear phishing campaigns.

"We observed TA530 at times targeting only a specific and narrow vertical, such as Retail and Hospitality. At other times, the campaigns appear more widespread. Overall, the volume of messages targeting each vertical is shown below."

Vertical	Relative Volume (approximate)
Financial Services	100
Retail	85
Manufacturing	75
Healthcare	65
Education	55
Business Services	45
Technology	40
Insurance	35
Energy/Utilities	30
Entertainment/Media	25
Pharmaceuticals	20
Construction	15
Legal	10
Telecommunications	10
Food & Beverage	10
Consulting	10
Hospitality/Leisure	10
Engineering	10
Real Estate	10
Transportation	10



CLASSIC DATA PROTECTION MODEL

ANTIVIRUS SOFTWARE

The New York Times had deployed Symantec anti-virus software to protect their systems, but Symantec's software was only able to successfully detect 1 of the 45 viruses which were installed on the New York Times computers (about a 2.2% success rate). When asked why their anti-virus software failed to protect the Times, **Symantec frankly stated:** "Anti-virus software alone is not enough." Instead they recommended a blended security approach using multiple types of protections.

<http://anti-virus-software-review.toptenreviews.com/history-of-the-computer-virus.html>

Antivirus Isn't Dead, It Just Can't Keep Up

submit Tweet Share 443 Like Share 96



Posted by Dr. Giovanni Vigna
5/23/14 10:00 AM



Much has been said in recent weeks about the state of antivirus technology. To add facts to the debate, Lastline Labs malware researchers studied hundreds of thousands of pieces of malware they detected for 365 days from May 2013 to May 2014, testing new malware against the 47 vendors featured in VirusTotal to determine which caught the malware samples, and how quickly.

The focus of this test is to determine how fast the anti-virus scanners catch up with new malware.

Note that the configuration of the various antivirus scanners used by VirusTotal is not necessarily optimal, and it is always possible that a better detection rate could be achieved by relying on external signals or using more "aggressive" configurations.

On any given day, according to Lastline Labs' analysis, much of the newly detected malware went undetected by as much as half of the antivirus vendors. Even after 2 months, one third of the antivirus scanners failed to detect many of the malware samples. By averaging the daily detection rates, we are able to plot the pace at which the antivirus scanners catch up with the malware. The least-detected malware - that is the malware in the 1-percentile "least likely to be detected" category - went undetected by the majority of antivirus scanners for months, and in some cases was never detected at all.

Even the best antivirus likely can't save your files from a ransomware infection

Den Turkal
Jan 24, 2016, 9:27 PM

Facebook LinkedIn Twitter Email Print

With new types of computer viruses being released every day, the internet can be a dangerous place, especially if you value the files on your computer.



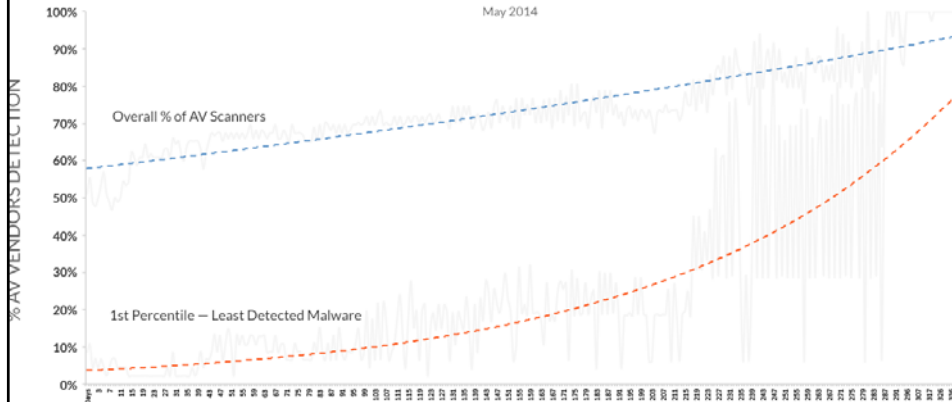
One of the most prevalent forms of malware out there right now is called ransomware, a virus that encrypts a user's files, leaving them scrambled unless the victim pays for the decryption key.

It's a criminal business model that has proven extremely profitable. Some of the largest actors may be making millions on the scam.

What makes the scam so effective is the fact that, without backups, paying is often a victim's only recourse. The problem has gotten so bad that FBI Assistant Special Agent Joseph Bonavolonta said at the 2015 Cyber Security Summit that FBI often advises victims to just pay the ransom. An FBI spokesperson has since walked back the comment, saying that the FBI doesn't make recommendations but rather presents the options - it's just that there aren't many options.

Probability of Malware Detection for Antivirus Solutions

May 2014



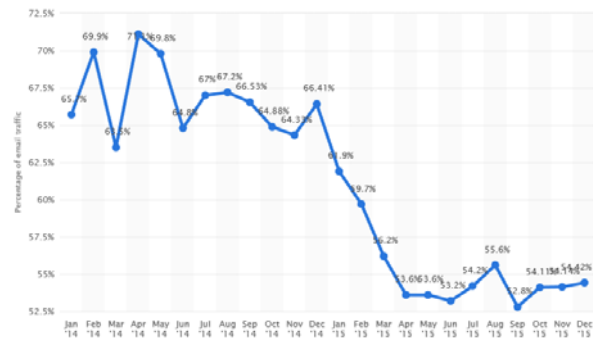
Data collected and research performed by Lastline Labs. For more information, please visit www.lastline.com/labs

SPAM FILTERING

- Google boasts it catches 99.9% of spam
- 2015 Spam at 12 year low
- We will always have spam

Global spam volume as percentage of total e-mail traffic from January 2014 to December 2015, by month

The statistics shows the share of global spam volume as percentage of total e-mail traffic as of December 2015, sorted by month. As of December 2014, spam messages accounted for 66.41 percent of e-mail traffic worldwide. This share decreased to 54.42 percent in the most recently reported period.



FIREWALLS / BLOCKING

- Not perfect
- Frequently misconfigured (human error)
- Mobile workers
- Not effective to stop CryptoWall/CryptoLocker

OS & SOFTWARE PATCHING

- Better than it has ever been / Still needs work
- Reactive
- The patch itself is a roadmap for a successful exploit
- Not effective to stop CryptoWall/CryptoLocker

ENCRYPTION

Encrypting data at rest is vital, but it's just not happening

Regulators and security strategists recommend encrypting data at rest, but few organisations do it, and most get it wrong. Good thing there are bigger problems to tackle first.



By Stigheimin | June 18, 2015 -- 01:47 GMT (09:47 PDT) | Topic: Storage, Fear, Loss, and Innovation

But according to IBRS security analyst James Turner, all of this is actually an argument against putting too much effort into encrypting the data.

"The question that needs to be asked about full-disc encryption is 'What is the attack that it's actually preventing?' If the computer is on and functioning, and someone's actually using it, then full-disc encryption really isn't protecting against anything. A hacker can just go through a web vulnerability or whatever, and get access to all the plaintext stuff," Turner told ZDNet.

Health Data Encryption Not Completely Effective, Study Finds

By Sara Heath on September 04, 2015

"CryptDB-based systems are often used by organizations because few changes are required to the legacy database infrastructure and they run on encrypted data in the 'same way as they would operate on plaintext data,' according to the paper," a [press release](#) states. These systems are also said to be faster than others.

To test CryptDB, researchers performed a series of four different kinds of cyberattacks on authentic patient information at over 200 large hospitals and 200 small hospitals. The researchers chose to test with data stored in EHRs because that is the data that is typically targeted by hackers and would yield the most accurate results.

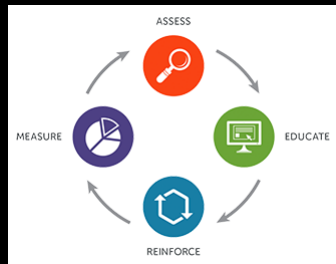
The study found that CryptDB is not always successful in protecting that information. In fact, the study's "cumulative attack" accessed disease severity, mortality risk, age, length of stay, admission month, and admission type for at least 80 percent of patients at 95 percent of the 200 large hospitals. The attack also accessed admission month, disease severity, and mortality risk for 100 percent of patients at nearly 100 percent of the 200 small hospitals.

BACKUPS

- Very important
- Always encrypt backup data
- An untested backup = no backup
- An undocumented = no backup
- Tape backups? (71% failure rate on restores)
- Online backups?
- Hard disk backups? (CryptoWall/CryptoLocker)
- 3-2-1 Rule

NEW EMERGING MODEL

STAFF RESPONSIBILITY & CONTINUOUS TRAINING



ASSUME YOU ARE COMPROMISED

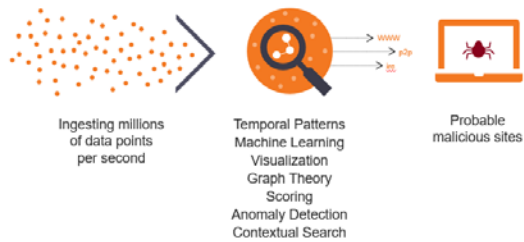
- System Monitoring
- Log changes
- Maintain incident response plans
- Regular computer reinstalls
- Develop baseline measurements and regularly check
- Intrusion testing
- Consult with legal & insurance

HOSTED SECURITY

OpenDNS

Our security intelligence

Leveraging the Internet to identify suspected threat origins



QUESTIONS?