

Internet Security Threat Report

ISTR

Ajay K. Sood
VP, Symantec Canada

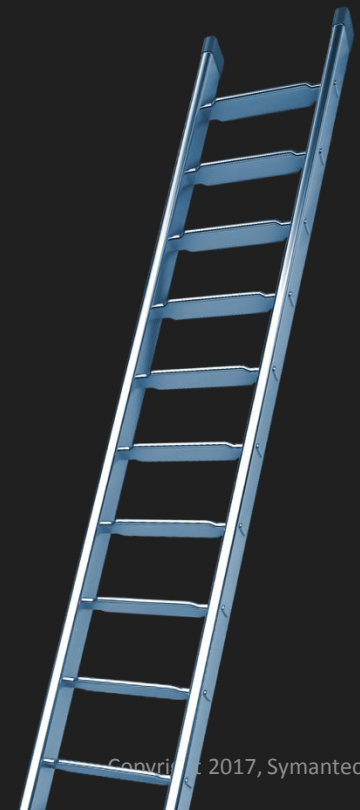


Volume

22



Is This Ladder a Threat?



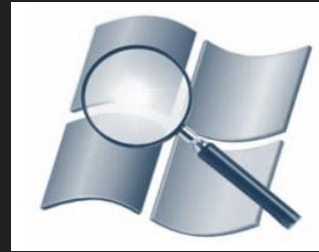
Is This Ladder a Threat?



Living off the Land

Attackers are using what's available to attack us

- These tools are ubiquitous
- These tools are easy to use for malicious purposes
- These tools don't arouse suspicion, and can be difficult to determine intent.





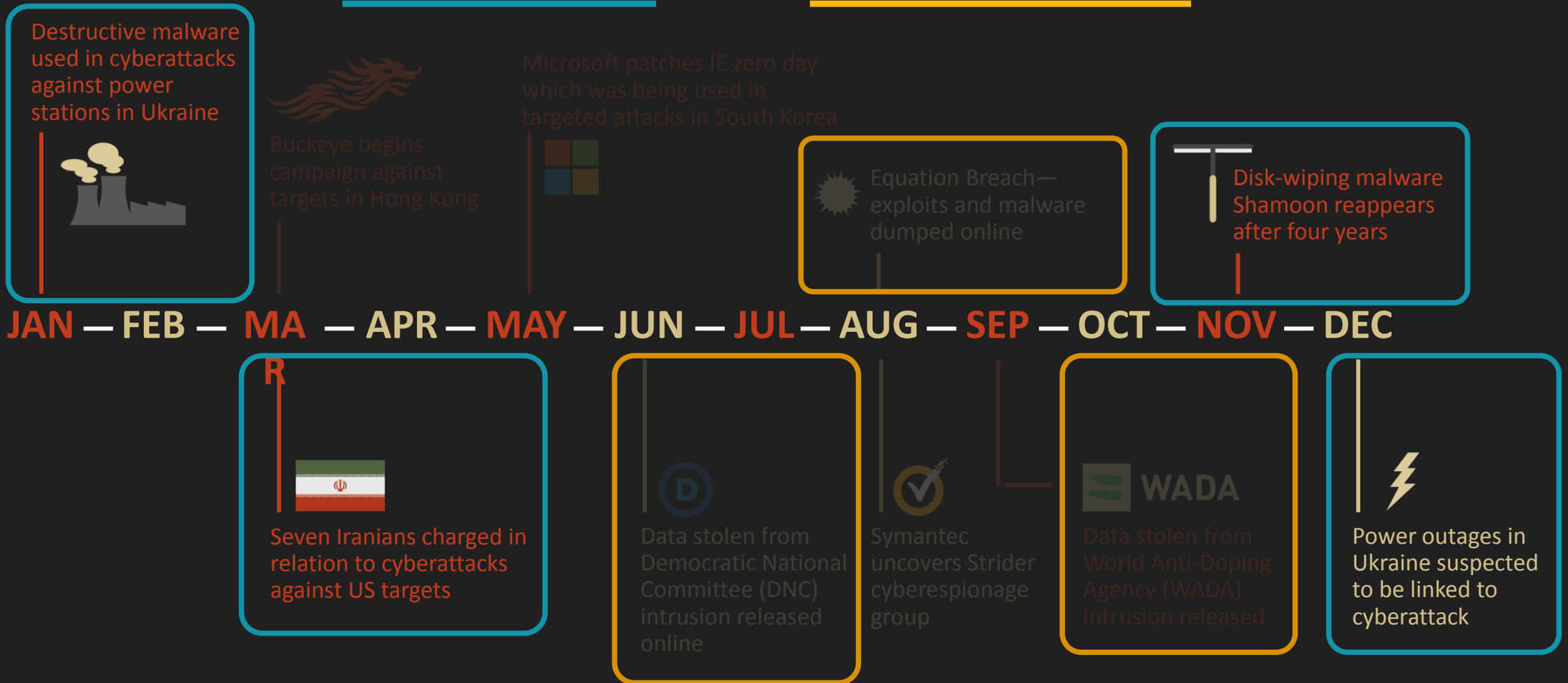
Targeted Attacks

Targeted Attacks Shift from Economic Espionage to Politically Motivated Sabotage and Subversion

Timeline of notable targeted attack incidents during 2016

SABOTAGE

SUBVERSION

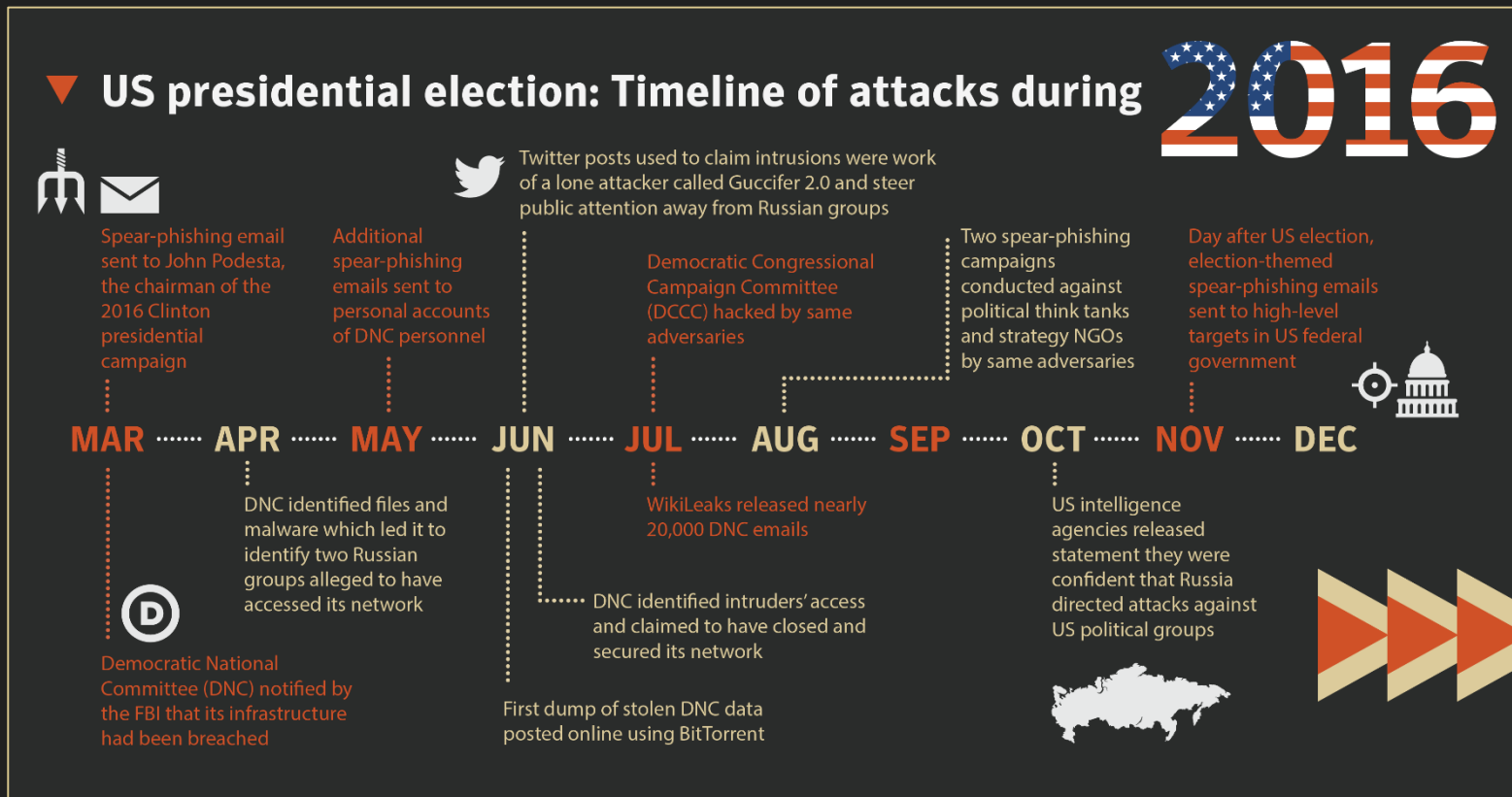


Resurgence of sabotage

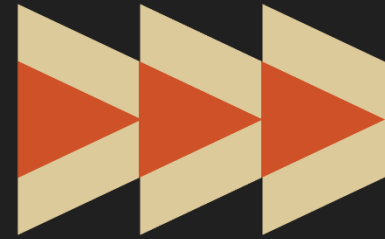
Sabotage campaigns represent another form of politicized and disruptive attack



Subversion



- Carried out by known Russian groups, active for almost a decade
- Subversive activities represent shift away from previous low-profile espionage
- US intelligence community has stated that campaigns were an attempt to influence elections
- **Reflects a broader shift towards highly-publicized, overt campaigns**



Cyber Bank Heists

North Korea Had \$1 Billion in Their Sights, Got Away With \$94 Million

Bank in Bangladesh compromised

- Credentials stolen
- Wire transfers requested
- \$81M to Philippines
- ~~\$20M to Sri Lanka~~
- \$15M of \$81M recovered from casino in Philippines



Trojan.Banswift



- Uses custom malware designed to manipulate SWIFT system
- Attackers demonstrated in-depth knowledge of SWIFT
- Doctored confirmation messages to cover tracks
- Started on long weekend to limit change of discovery
- Symantec linked these tools to the Lazarus gang
 - The FBI linked Lazarus to Sony attacks in 2014
 - Used in attacks against US and South Korea since 2009

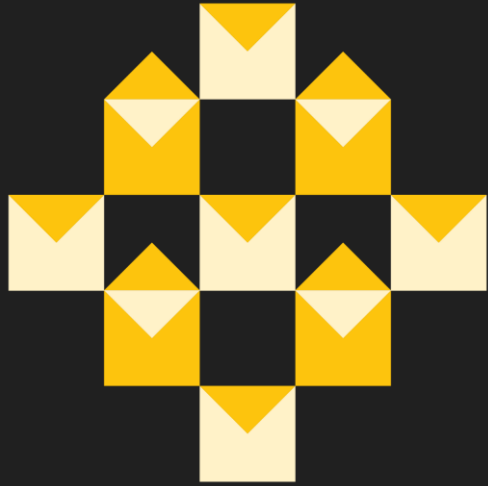
Trojan.Banswift

A world map with a dark grey background. Countries affected by Trojan.Banswift attacks are highlighted in a bright orange color. The highlighted areas include North America (USA, Canada), Mexico, South America (Brazil, Chile, Argentina), Europe (UK, Ireland, Spain, Turkey, Germany, France, Italy, Greece, Poland, Czech Republic, Slovakia, Austria, Hungary, Switzerland, Netherlands, Belgium, Luxembourg, Denmark, Norway, Sweden, Finland, Iceland, Portugal, Russia), Africa (Tunisia, Morocco, Egypt, Algeria, Libya, Mauritania, Mali, Niger, Chad, Sudan, Ethiopia, Kenya, Uganda, Rwanda, Burundi, Tanzania, Mozambique, Zimbabwe, Botswana, Namibia, South Africa, Lesotho, Swaziland), Asia (Vietnam, Philippines, Indonesia, Malaysia, Singapore, Thailand, Cambodia, Laos, Myanmar, Vietnam, Laos, Cambodia, Myanmar, Thailand, Malaysia, Singapore, Philippines, Vietnam), and Oceania (Australia, New Zealand).

Attacks not limited to 1 bank

- Vietnam 2015
- Ecuador 2015
- Philippines 2016
- Poland 2016

Plus 104 banks in 30 other countries



Email Attacks

Email Becomes the Weapon of Choice for 2016



Number of Powerball Lottery tickets with a \$7 payoff: **317**
1 out of

Emails with attached malware or links to malware: **131**
1 out of

Malicious Emails Hit the Highest Rate in Five Years



1 out of

244



1 out of

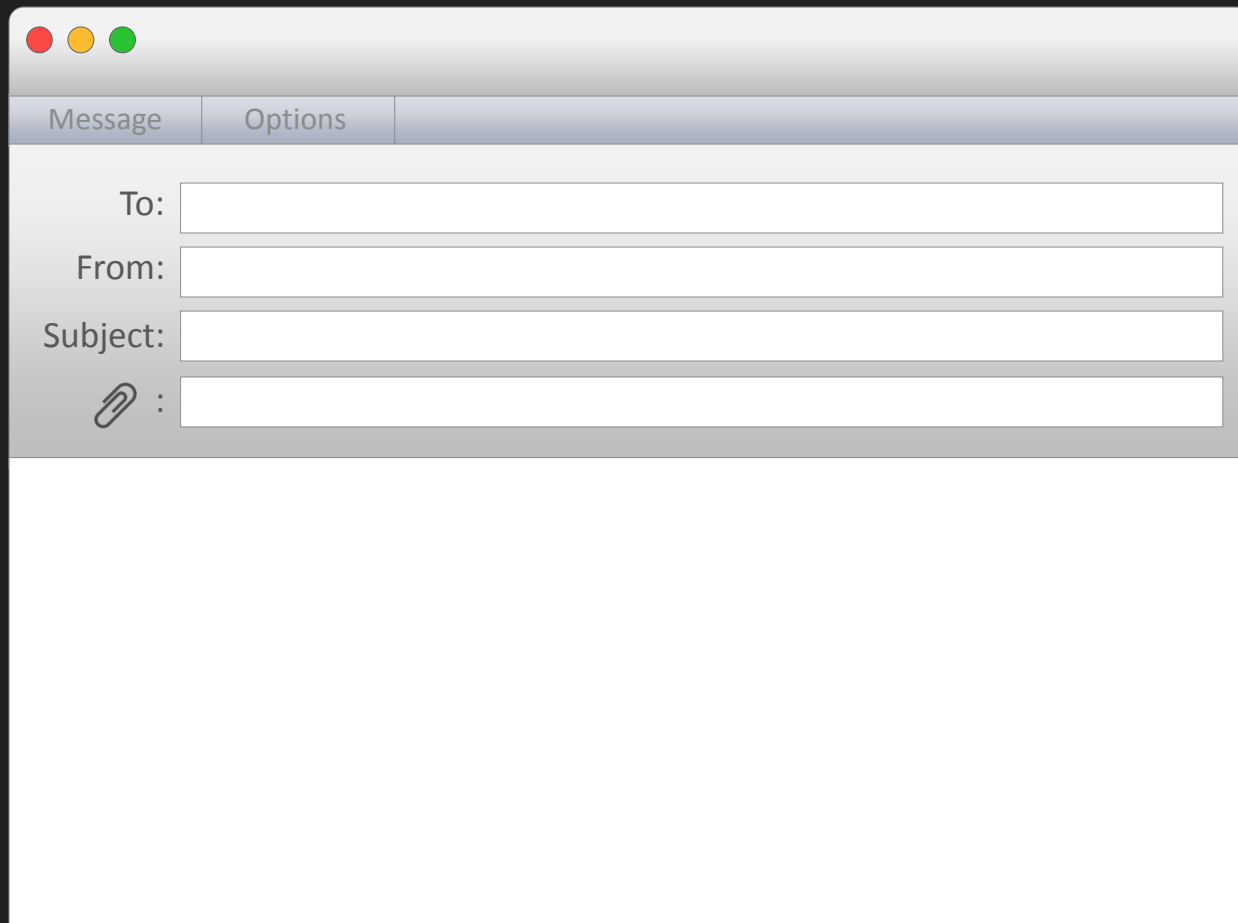
220



1 out of

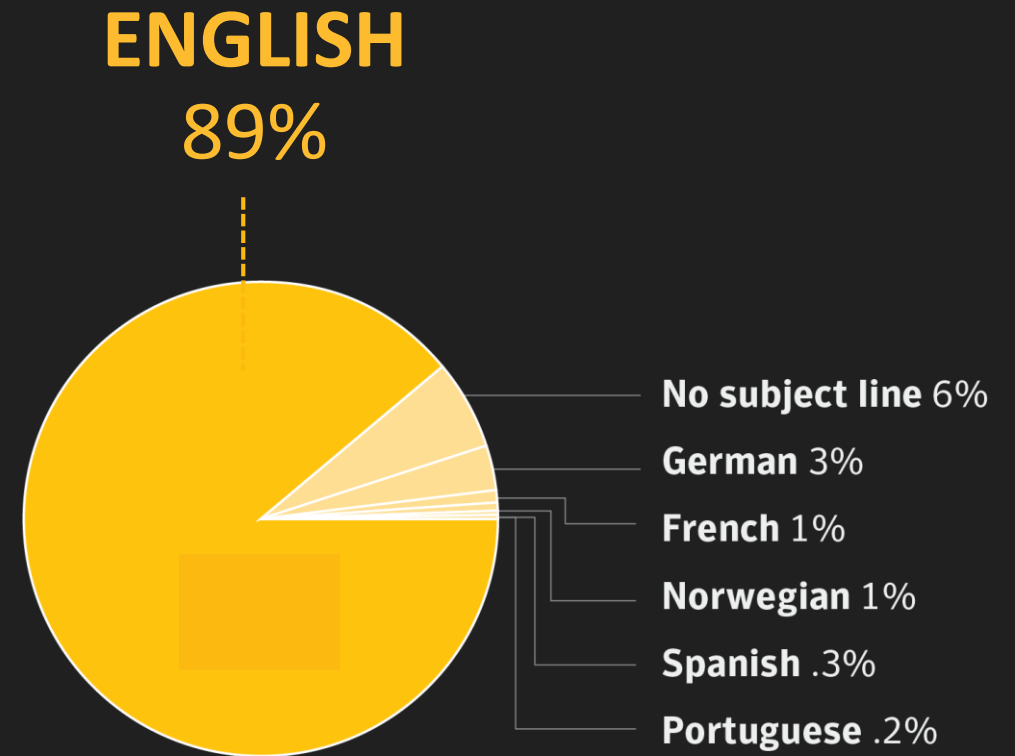
131

Building Malicious Email

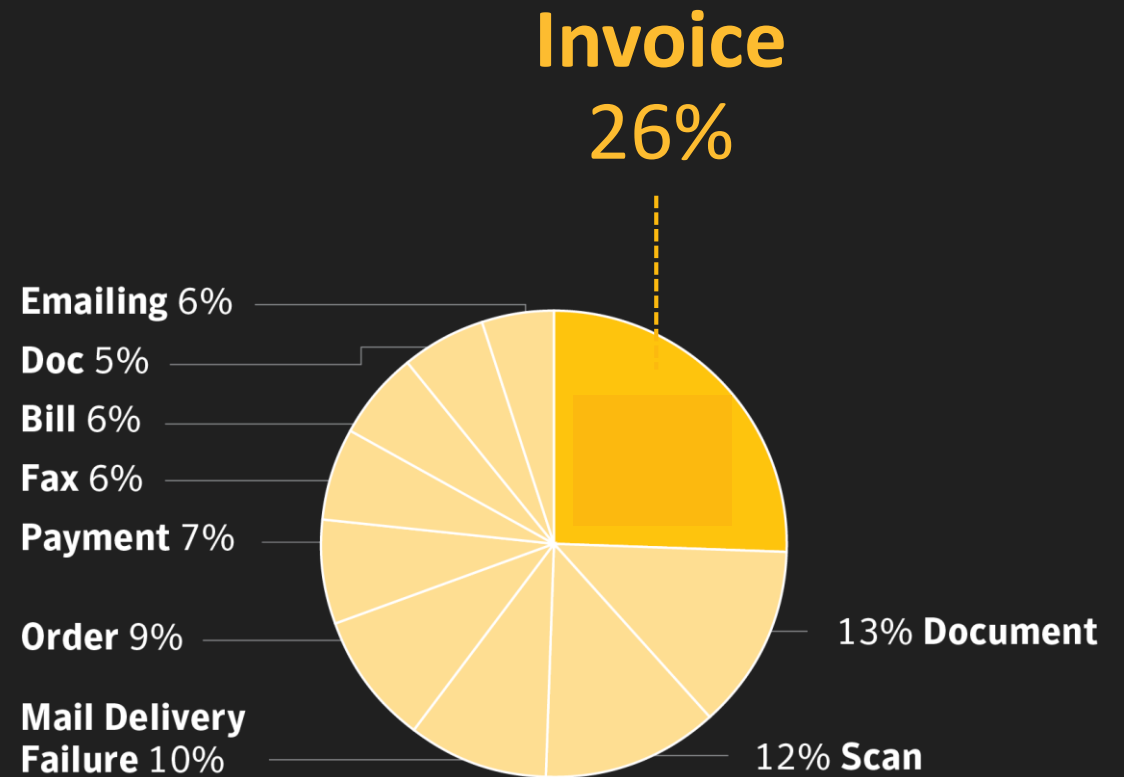
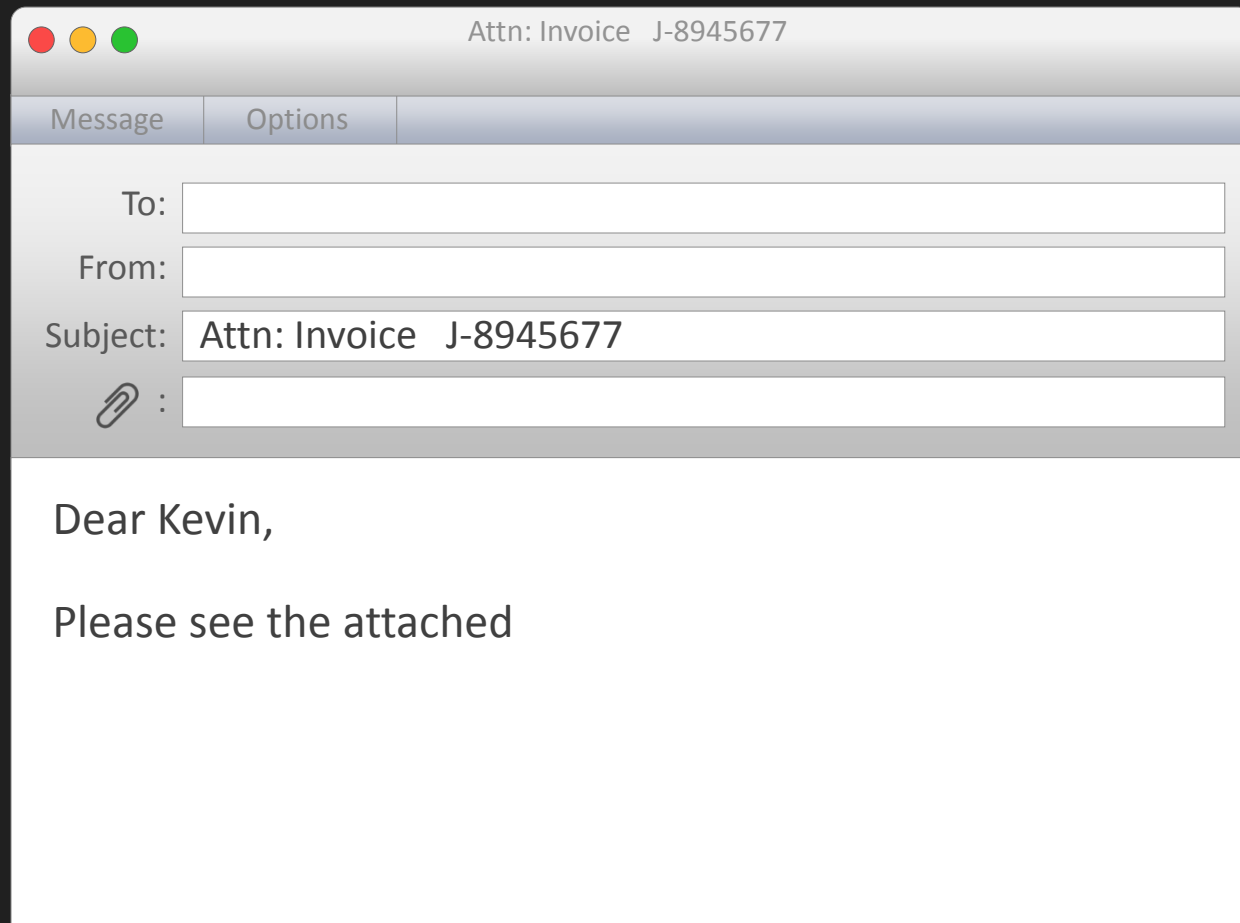


The image shows a screenshot of an email composition window. At the top, there are three colored window control buttons (red, yellow, green). Below them is a header bar with two tabs: "Message" and "Options". The main area contains four input fields: "To:", "From:", "Subject:", and "Attachments:" (indicated by a paperclip icon). The "Attachments:" field is currently empty, while the others contain placeholder text. The bottom half of the window is a large, empty white area for the email body.

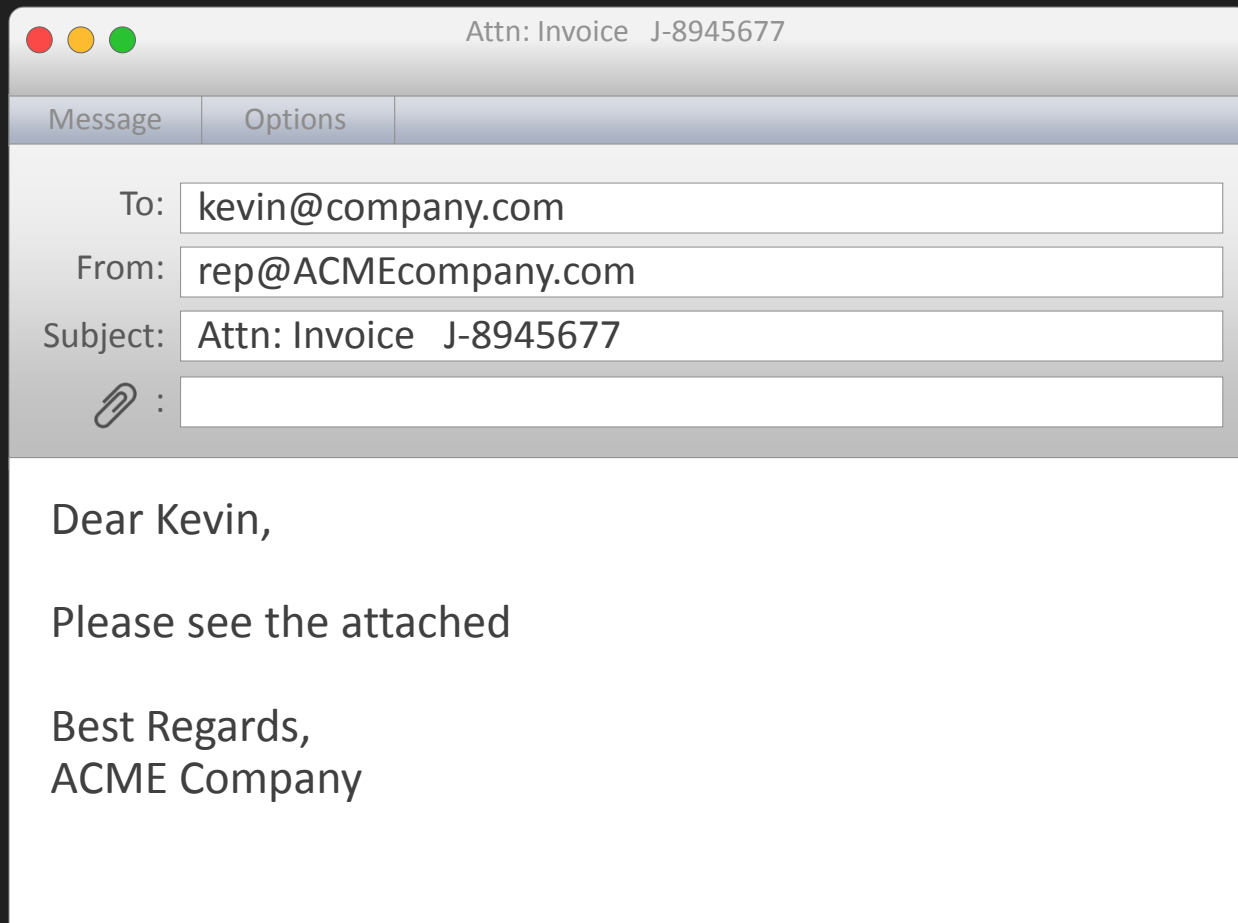
Building Malicious Email: Language



Building Malicious Email: **Subject**

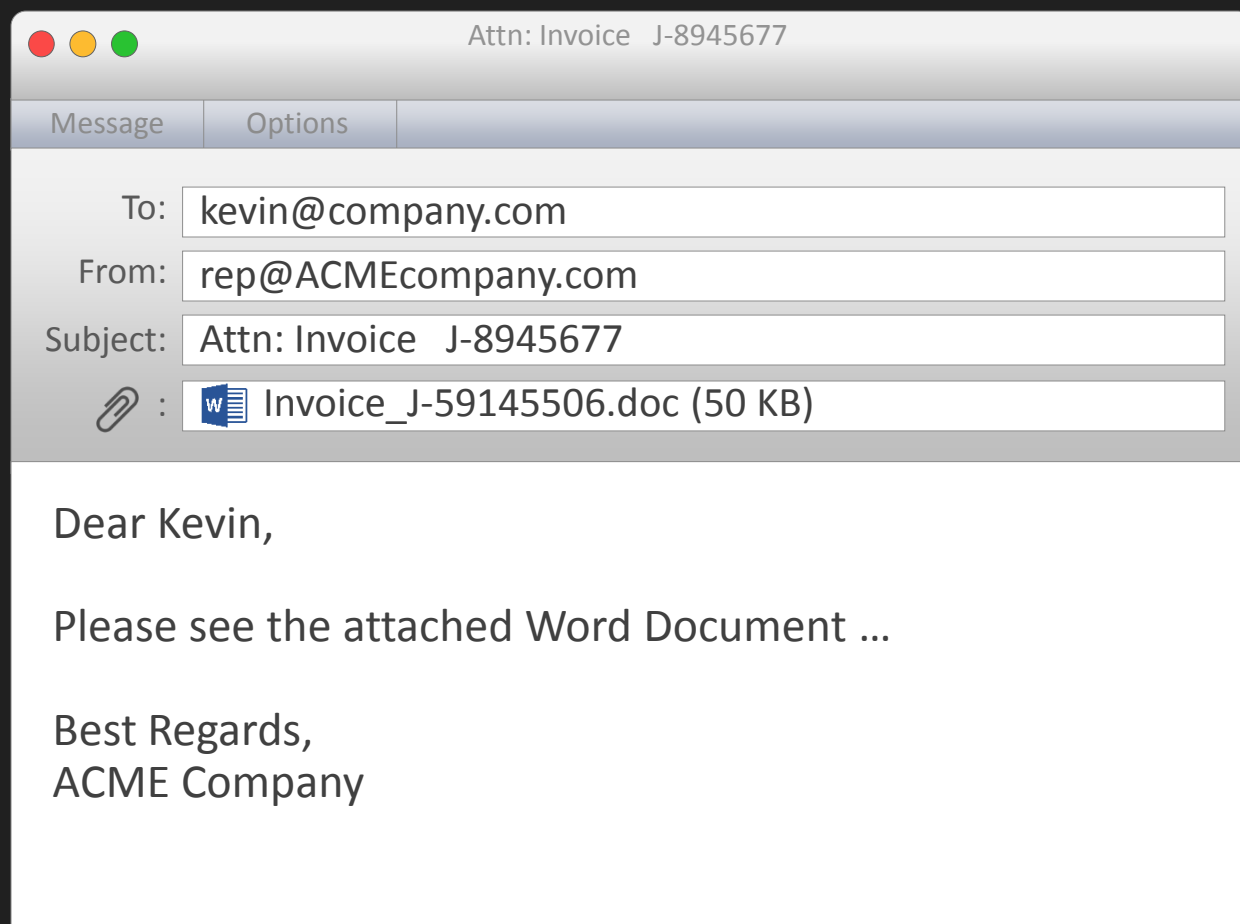


Building Malicious Email: **To/From**



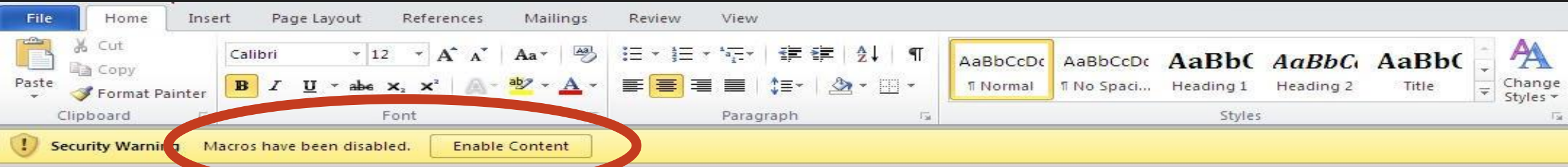
- The Sender is often spoofed to be a well known company, region specific.

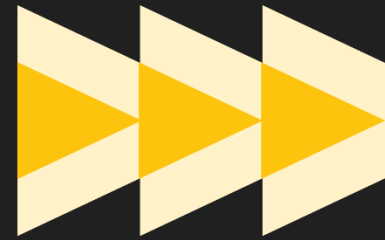
Building Malicious Email: Attachment



- Most users are not suspicious of a Word file
- And they are harmless unless users can be tricked into enabling macros
- Social Engineering becomes more important to bad guys as defenses get better

Building Malicious Email: Social Engineering

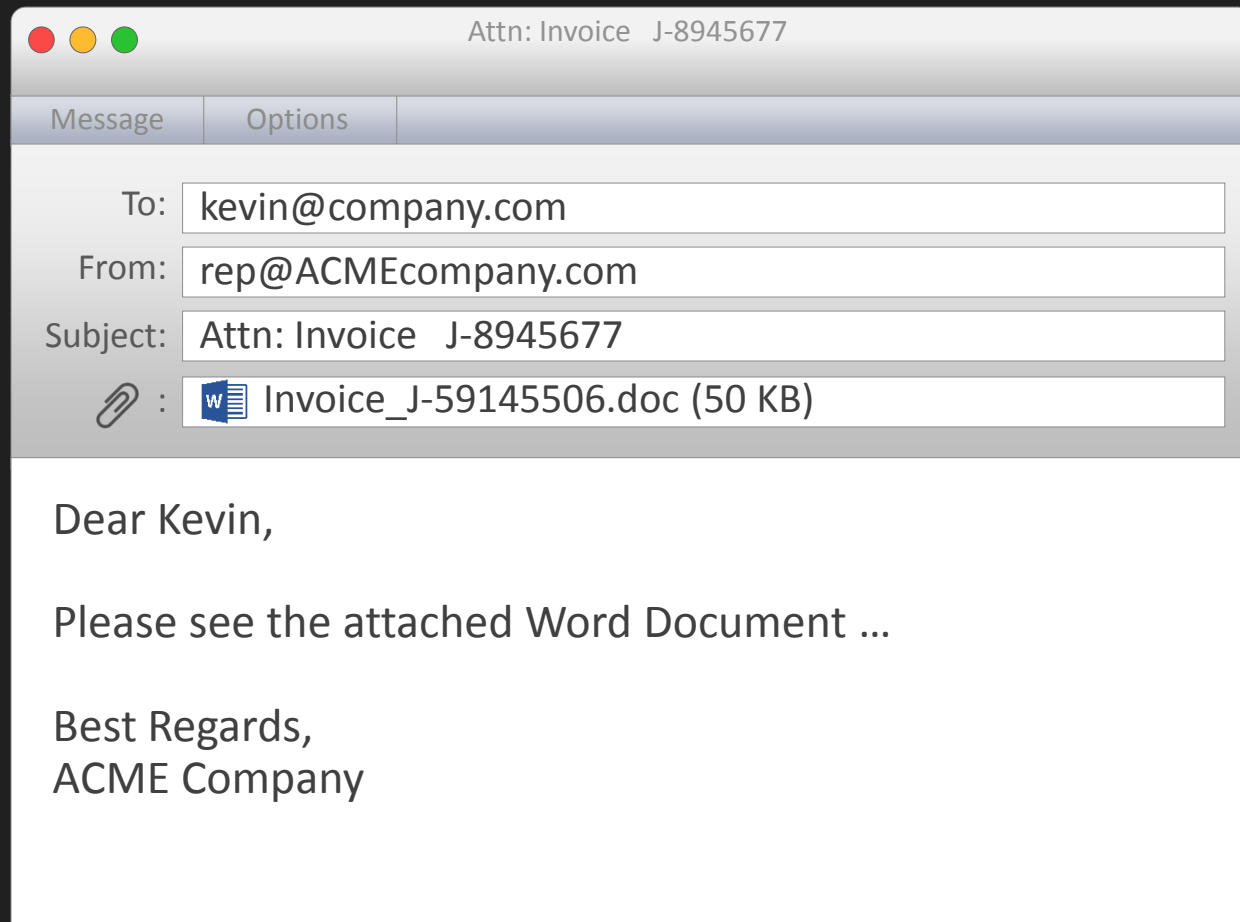




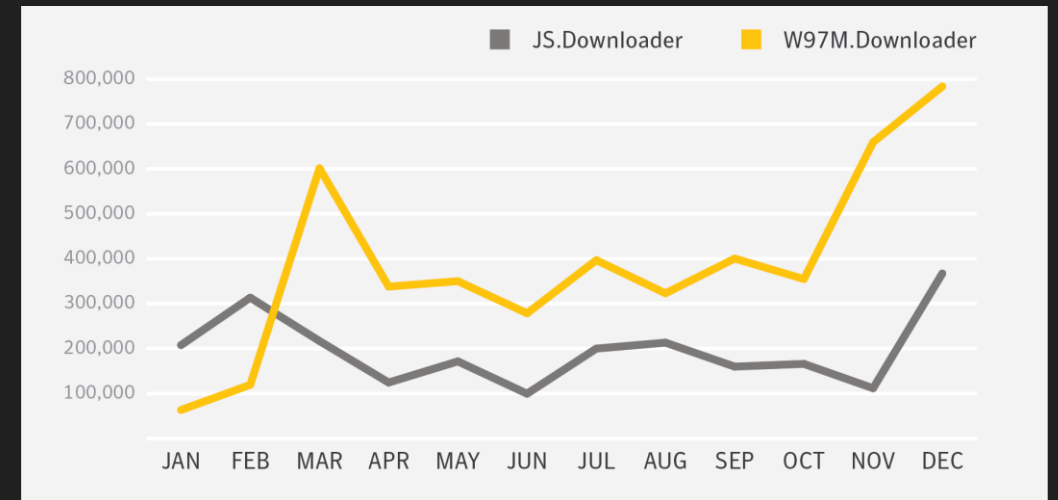
Macros, IT tools & Malware

Attackers Weaponize Common IT Tools

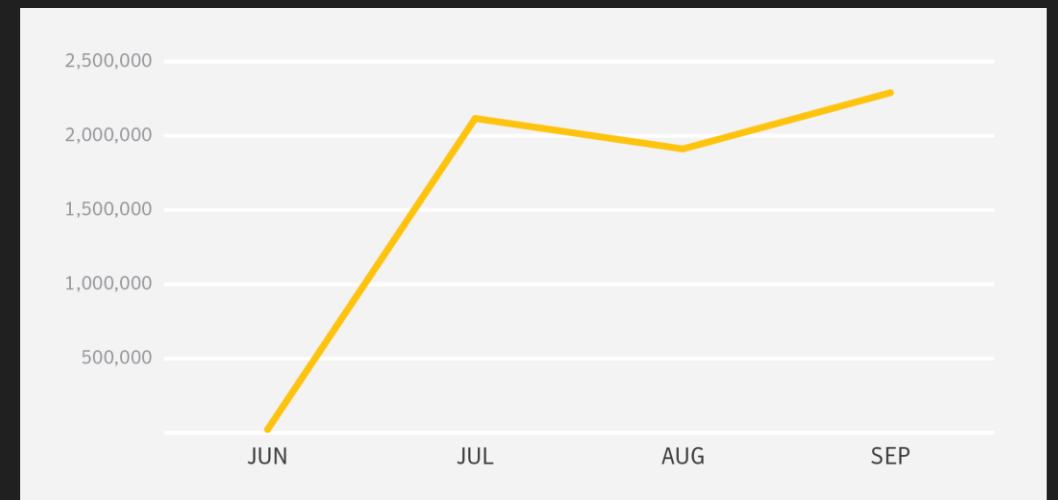
Macros



Downloader detections by month



Blocked emails with WSF attachments



Powershell

95% of Powershell scripts found in the wild were malicious



PowerShell

PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language built on the .NET Framework. [More at Wikipedia](#)

Typical emailed malware infection process

01 Email received disguised as routine notification, most commonly an **INVOICE** or **RECEIPT**



02 Includes attachment, typically JavaScript (JS) file or Office file containing malicious macro



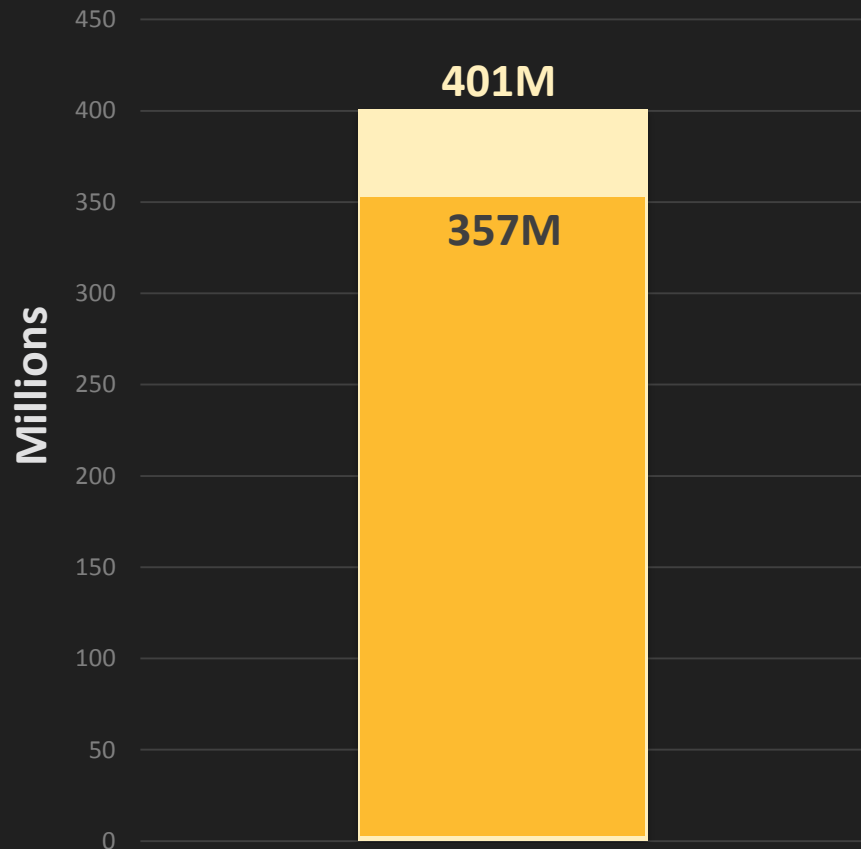
03 Opened attachment executes PowerShell script to download malware



04 Malware downloaded is typically Ransomware



Unique Malware in 2016



401M Unique Pieces of Malware

- **89%** of that malware first seen in 2016
- **20%** of all malware VM aware
- **4%** use cloud services
- **3%** use SSL for C&Cs communication (79% increase)
- **1%** use Tor



Cloud

Cracks in the Cloud: The Next Frontier for Cybercrime is Upon Us

John Podesta



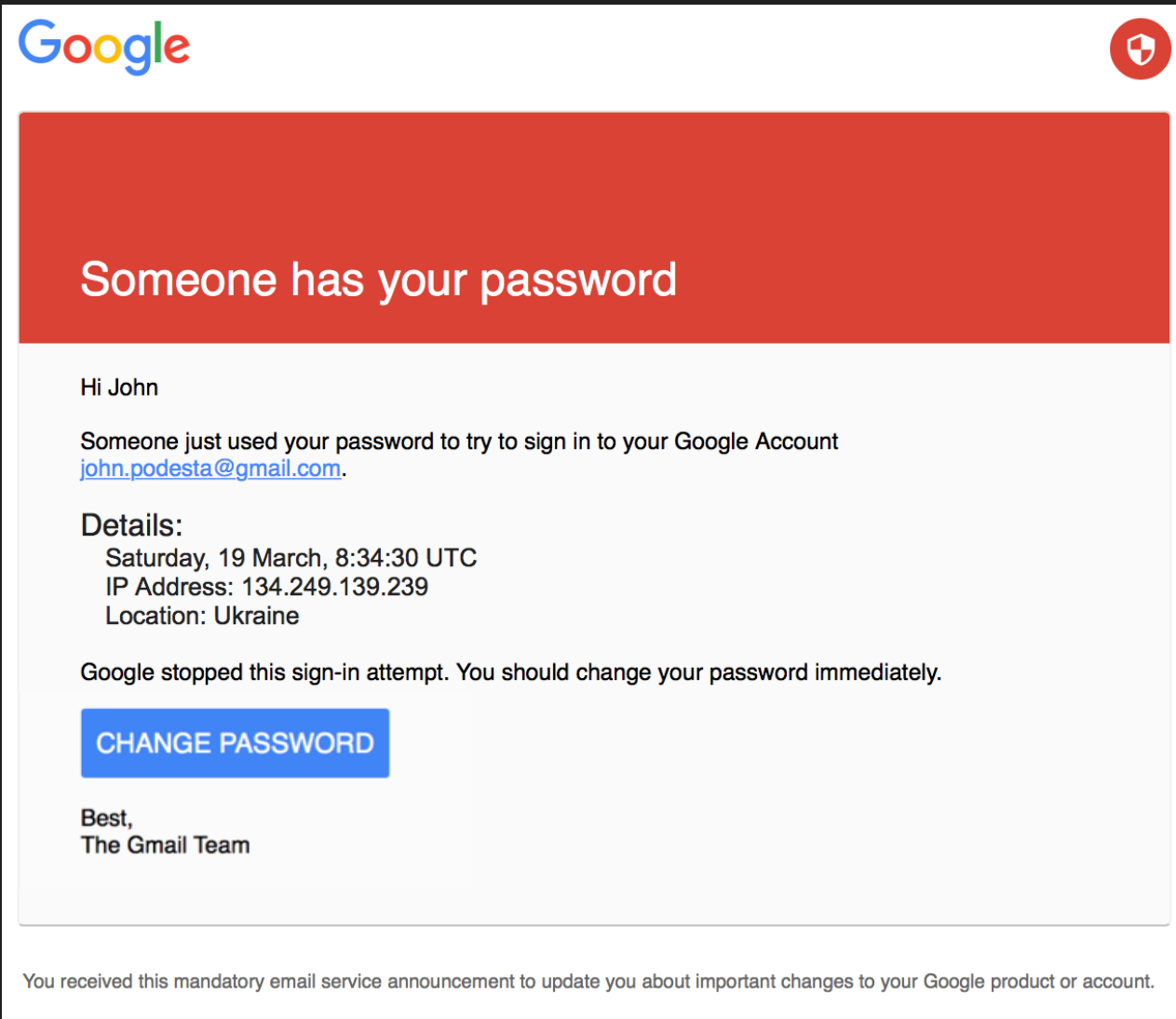
From Wikipedia, the free encyclopedia

John David Podesta (born January 8, 1949) is a columnist and former chairman of the [2016 Hillary Clinton presidential campaign](#).^[1] He previously served as [chief of staff](#) to [President Bill Clinton](#) and [Counselor](#) to [President Barack Obama](#).^[2]

He is the former president, and now Chair and Counselor, of the [Center for American Progress \(CAP\)](#), a [liberal think tank](#) in Washington, D.C., as well as a [Visiting Professor of Law](#) at the [Georgetown University Law Center](#). Additionally, he was a co-chairman of the [Obama-Biden Transition Project](#).^{[3][4]}



Anatomy of a Targeted Phishing Attack



- The branding looks consistent (Google logo, shield logo)
- The email is addressed to the recipient (not “Dear Sir”)
- The English is not broken

Anatomy of a Targeted Phishing Attack

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29w...xldXNlcmNvbnRibnQuY29tLy1RZVIPbHJKVGp2WS9BQUFB...

myaccount.google.com-**securitysettingpage.tk**

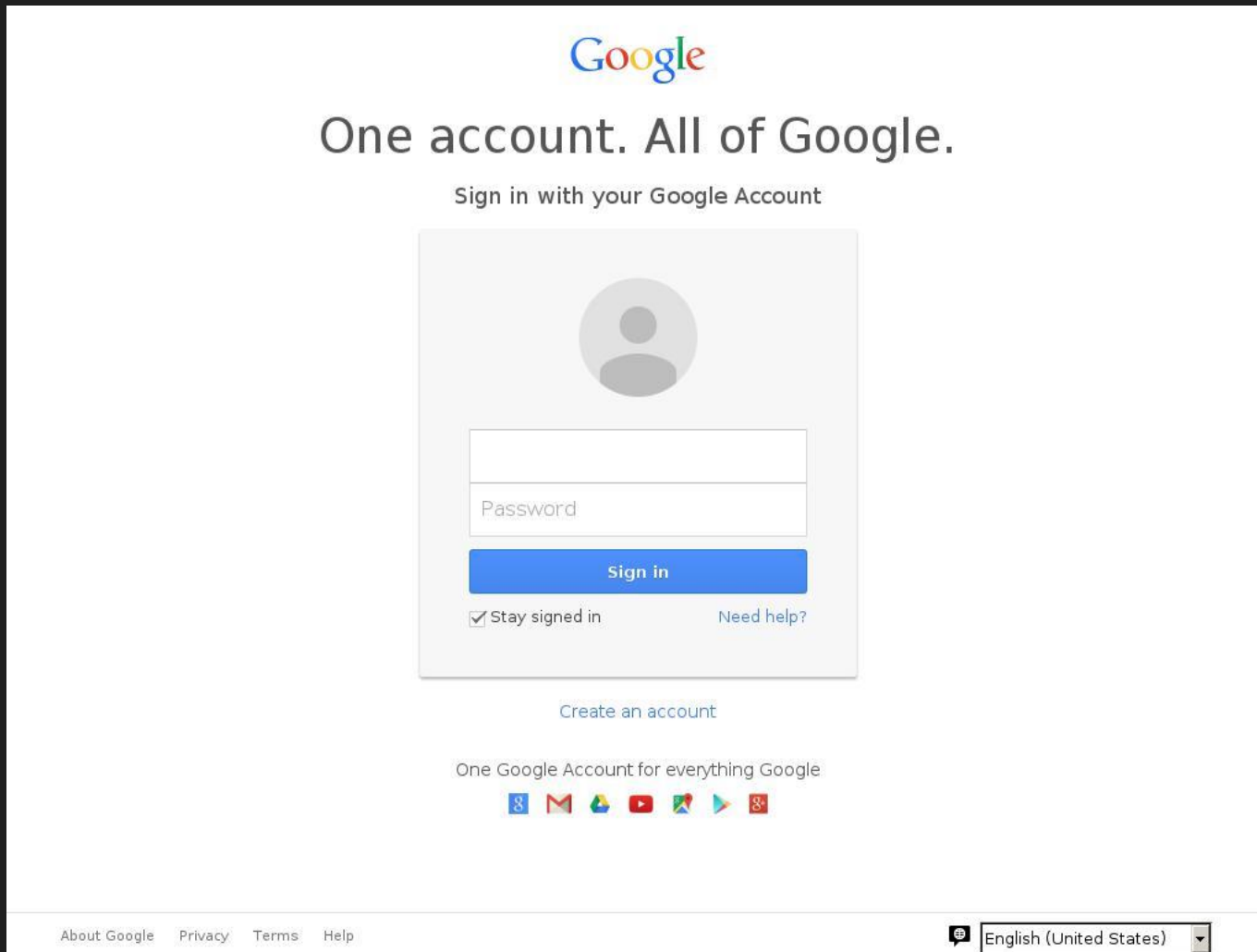
<http://bitly.com/gblgook>

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

Anatomy of a Targeted Phishing Attack



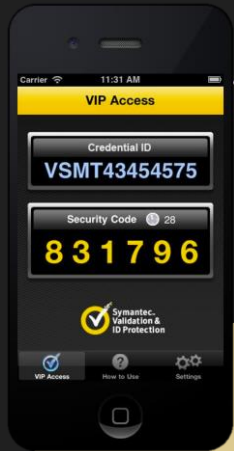
- The login page looks identical to the actual login page (HTML was cloned)
- Once the user submits the username/password combination, it doesn't matter what happens next
 - Typically, the phishing page redirects users back to Google.com

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: <https://myaccount.google.com/security> to do both. It is absolutely imperative that this be done ASAP.

Two Factor Authentication Should Not Be An Option for Cloud Apps

Login:
Password:



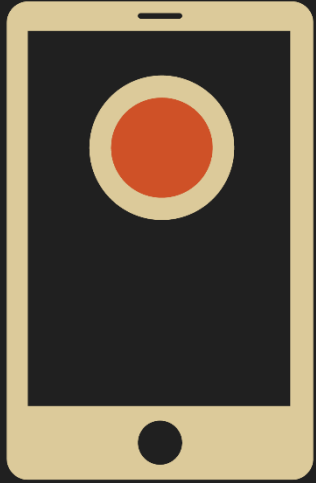
Login:
Password:



The Cloud in the Average Enterprise

How many Cloud Apps are used?





Internet of Things

IoT Devices Attacked Within Two Minutes of Connecting to the Internet

In **2004** security researchers put a PC on the internet

- Without any patches installed
- Without any security software

It was attacked within
within

4 minutes



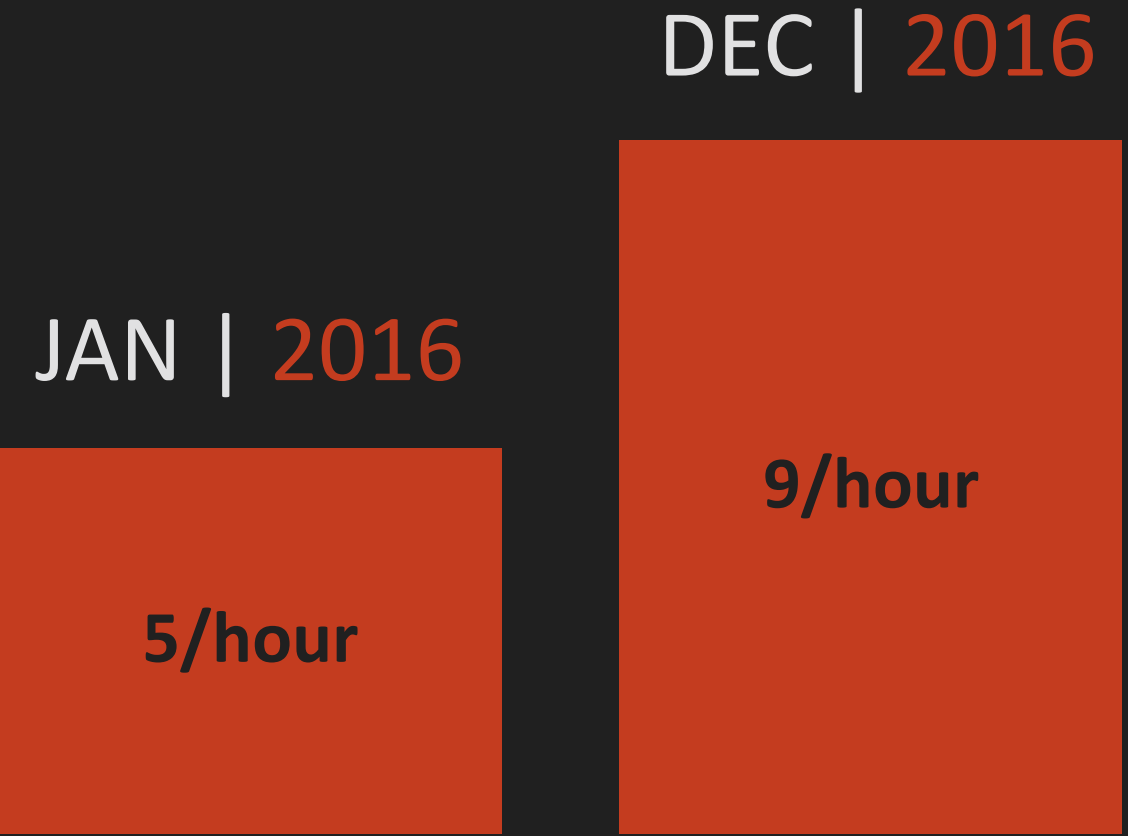
In **2016** Symantec researchers put an IoT device on the internet



It was attacked
within
2 minutes



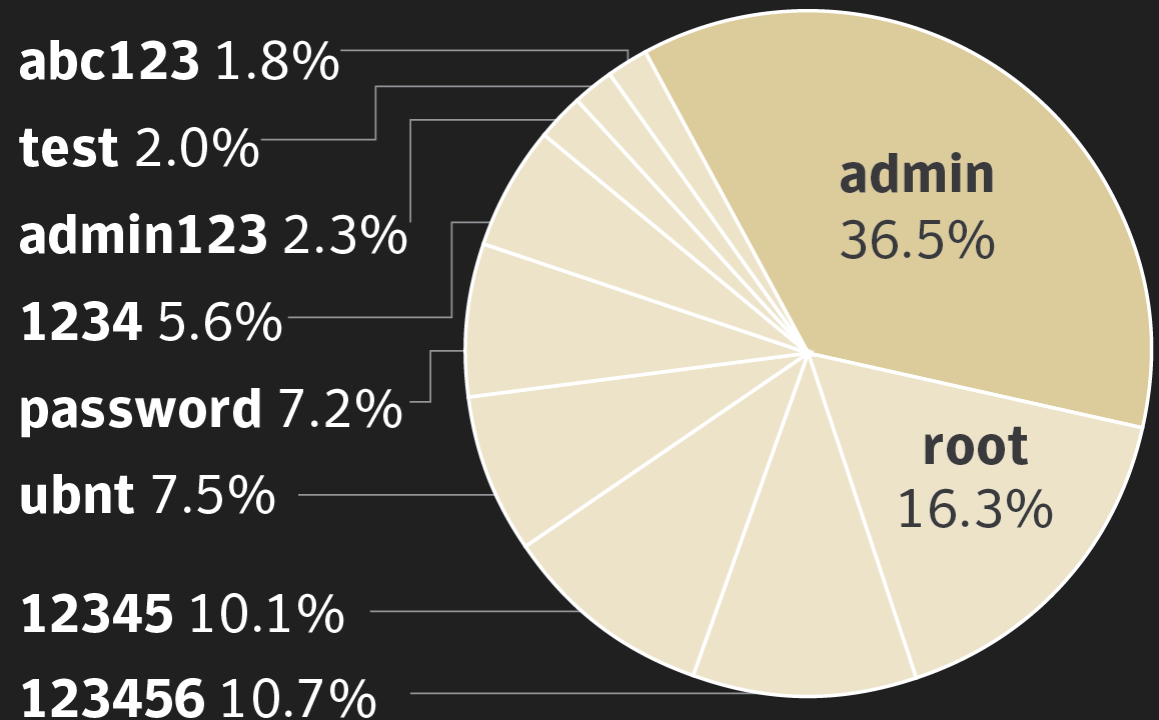
Attacks against Symantec IoT honeypots doubled from January to December 2016



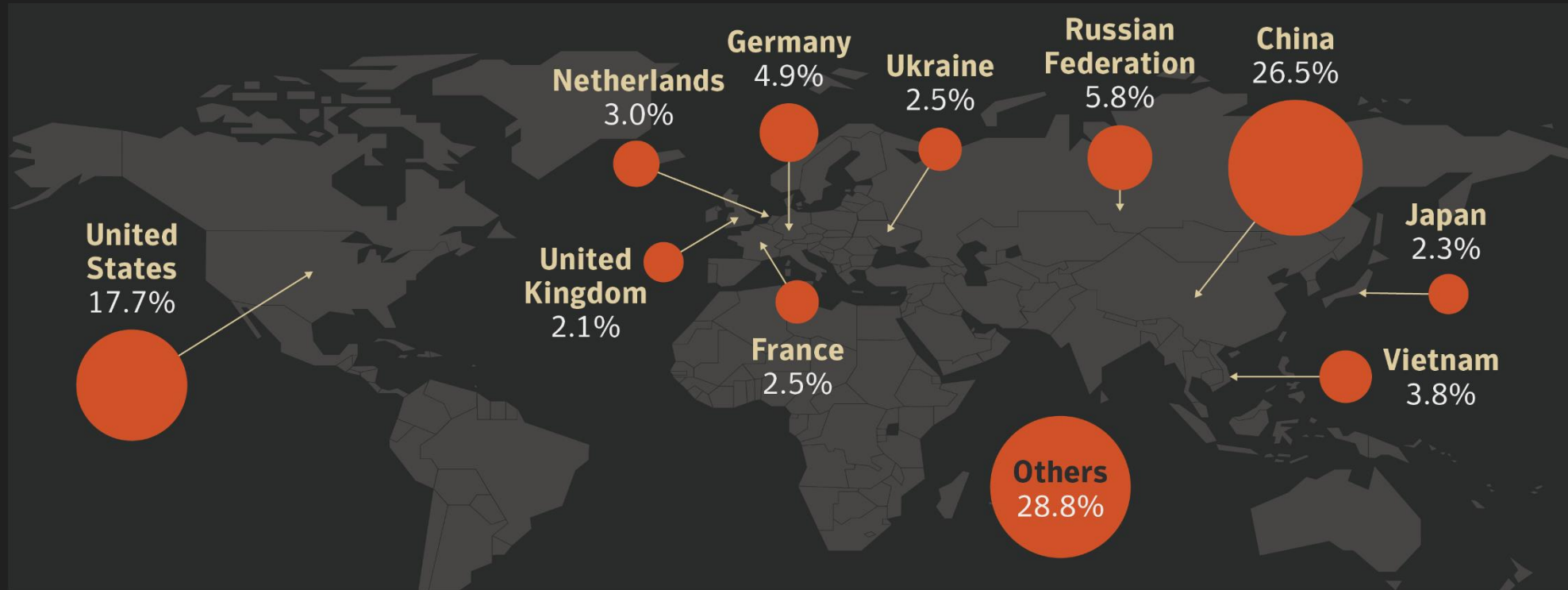
The security shortcomings of IoT

- No system hardening
- No update mechanism
- Default/hardcodes passwords

Top 10 passwords used by malware to break into IoT devices

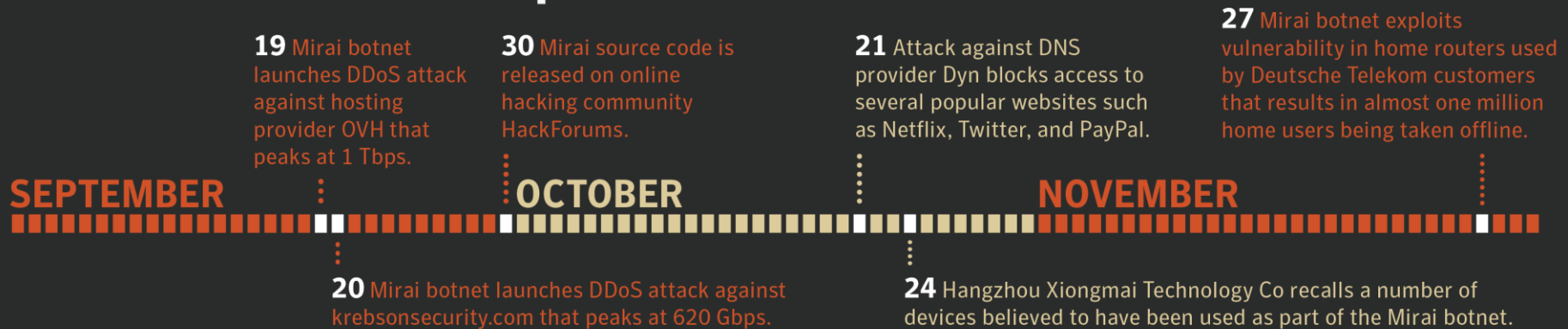


Top 10 countries where attacks on the Symantec IoT honeypot were initiated



The Consequences of Poor IoT Security

▼ Mirai's trail of disruption in 2016



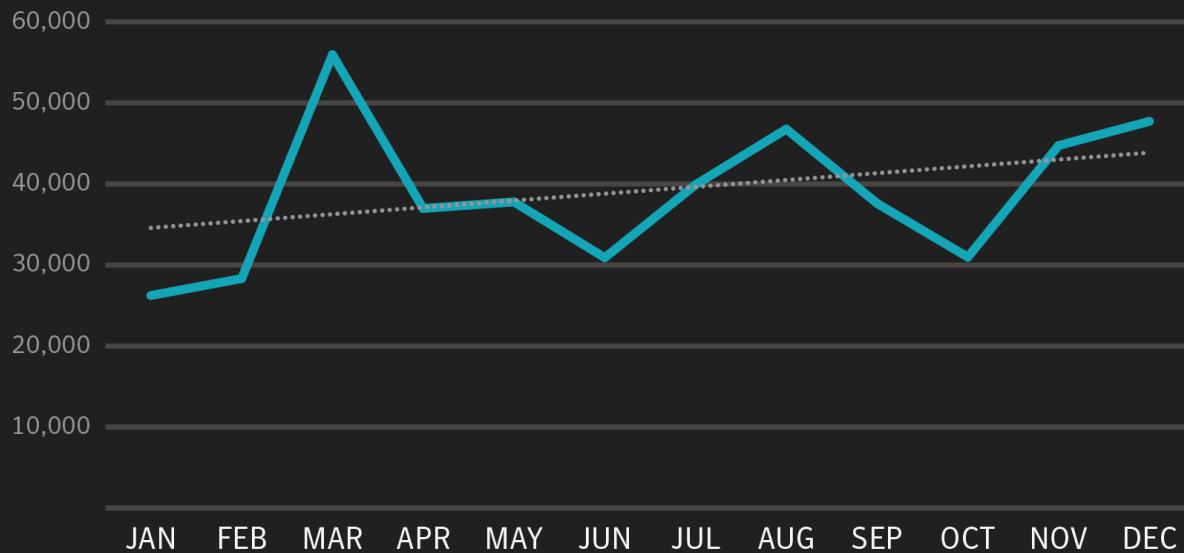
- Mirai source code has been released into the wild
- Variants appeared within two months
- Estimates of Mirai bots – 493,000
- Gartner estimates 20 Billion IoT devices in world by 2020
- At least 17 other malware families targeting IoT (including home routers)



Ransomware

Caving to Digital Extortion: Americans Most Likely to Pay Ransom Demands

36% Increase in Ransomware Attacks



- Highly profitable
- Low Barrier to Entry
 - Multiple Software as a Service offerings available

Ginx Ransomware - Windows and Mac-OSX (%60-%40 split)

This piece of malware will move and encrypt all personal files for that user and demand a ransom in BTC. Once infected the target will have 96hrs to make payment. ===== Windows ===== Comes in .exe .scr and .com Future updates will be Word Document macro The file has to be executed on the victim's machine or by other means (uploaded via RAT, Botnet, Social Engin...

Sold by [Avatar] - 0 sold since Jan 27, 2016 **Vendor Level 1** **Trust Level 3**

	Features	Origin country	Features
Product class	Digital goods		Worldwide
Quantity left	50 items	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 1,000.00

Qty: 1 **Buy Now** **Queue**

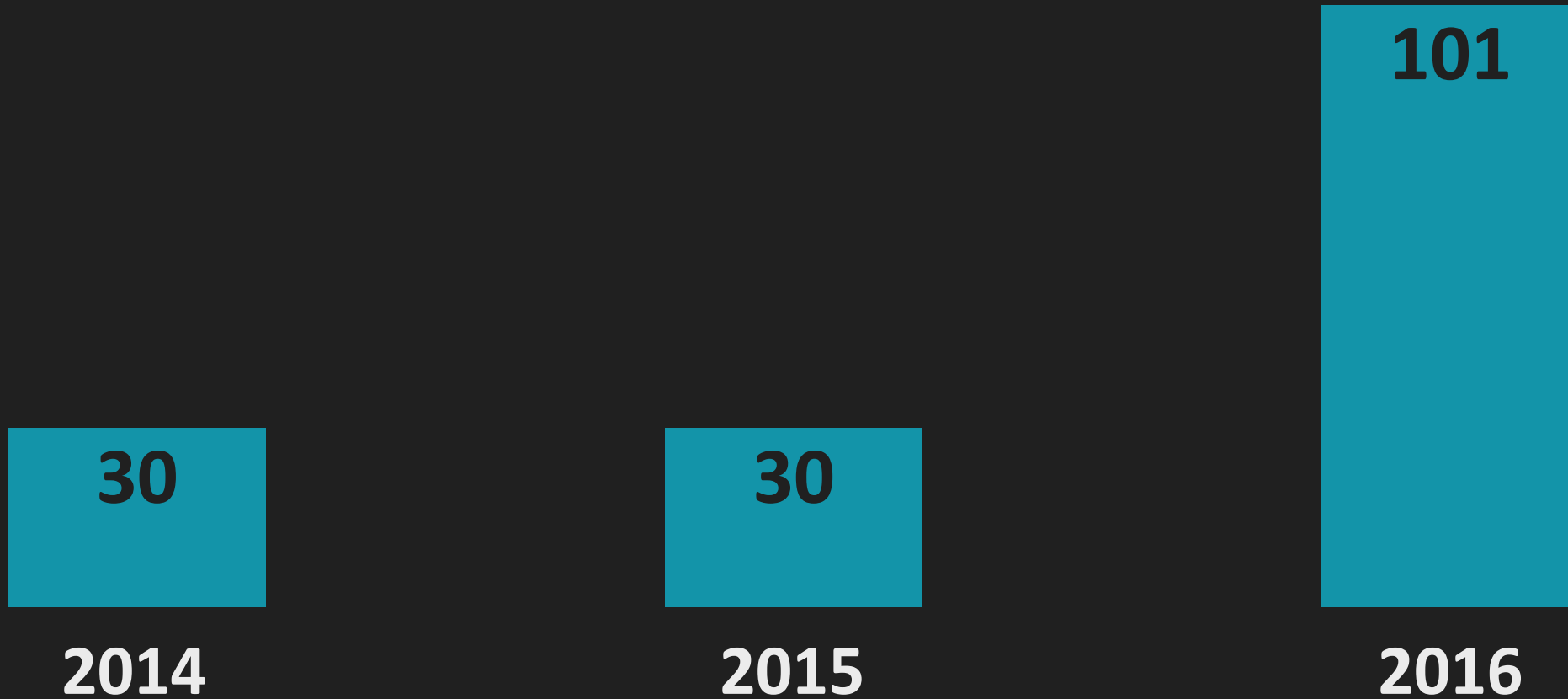
2.3842 BTC

Description Bids Feedback Refund Policy

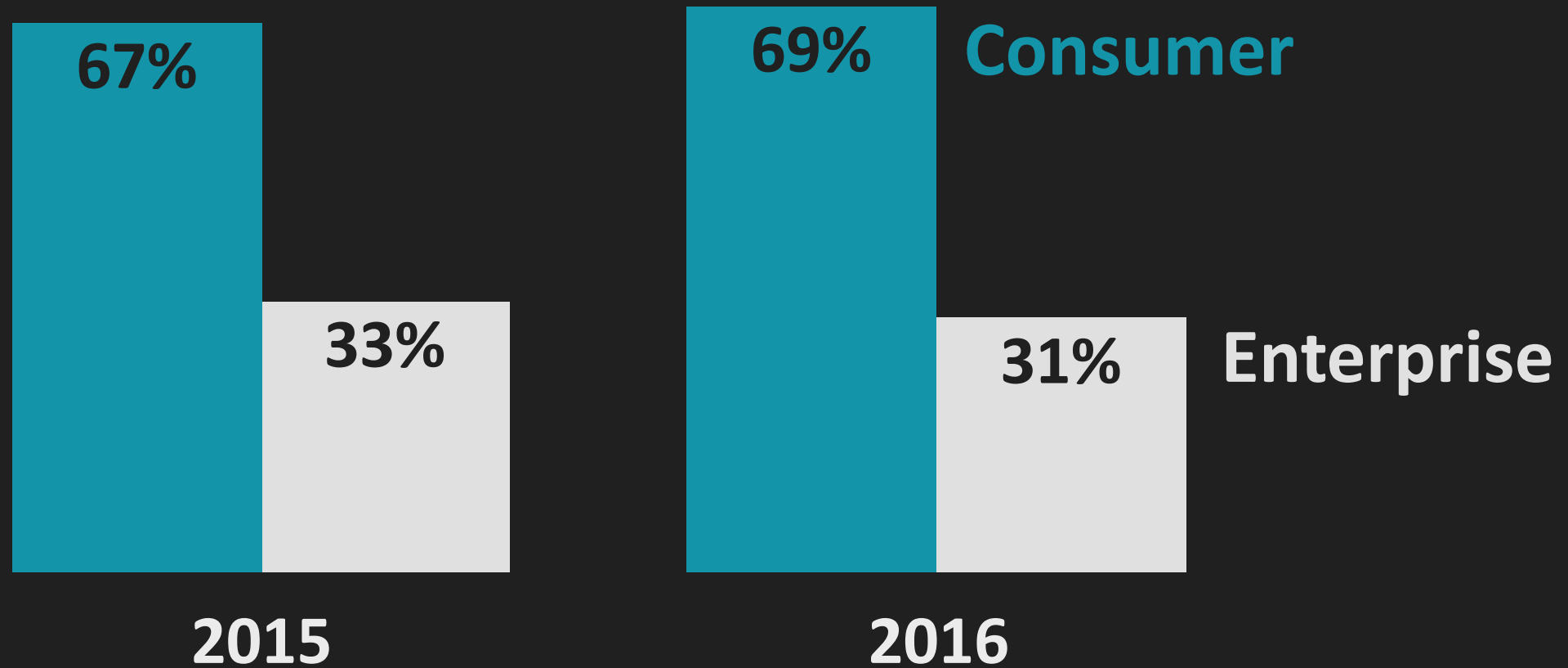
Product Description

This piece of malware will move and encrypt all personal files for that user and demand a ransom in BTC. Once infected the target will have 96hrs to make payment.

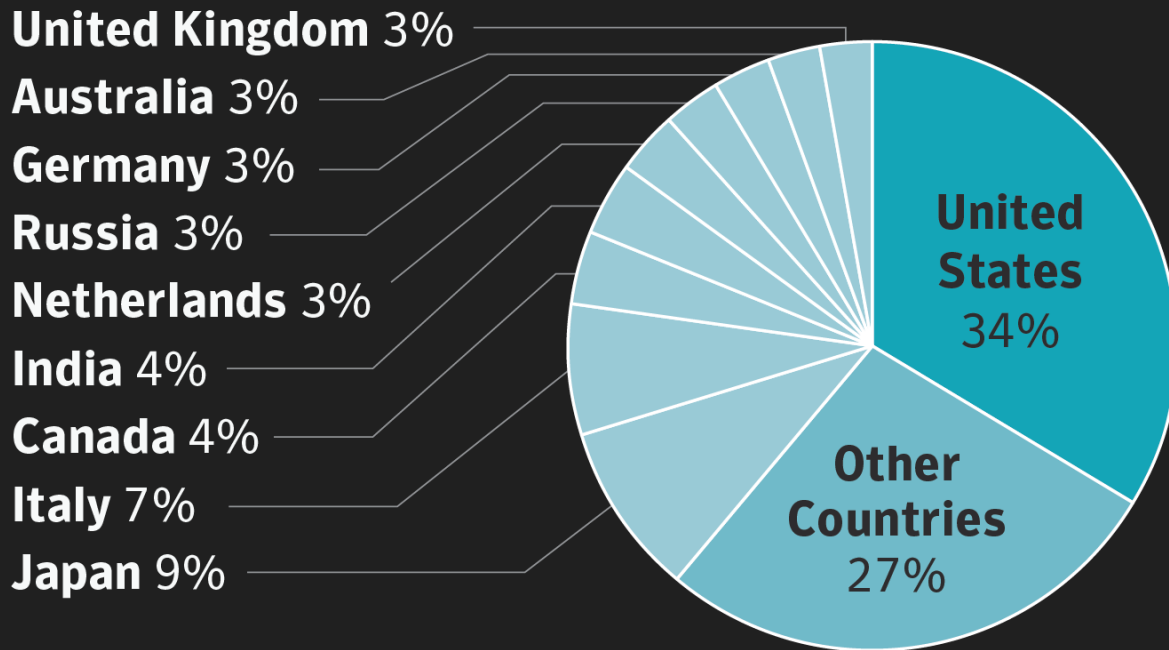
3x as many new ransomware families in 2016



Consumers Continue to see the Majority of Attacks

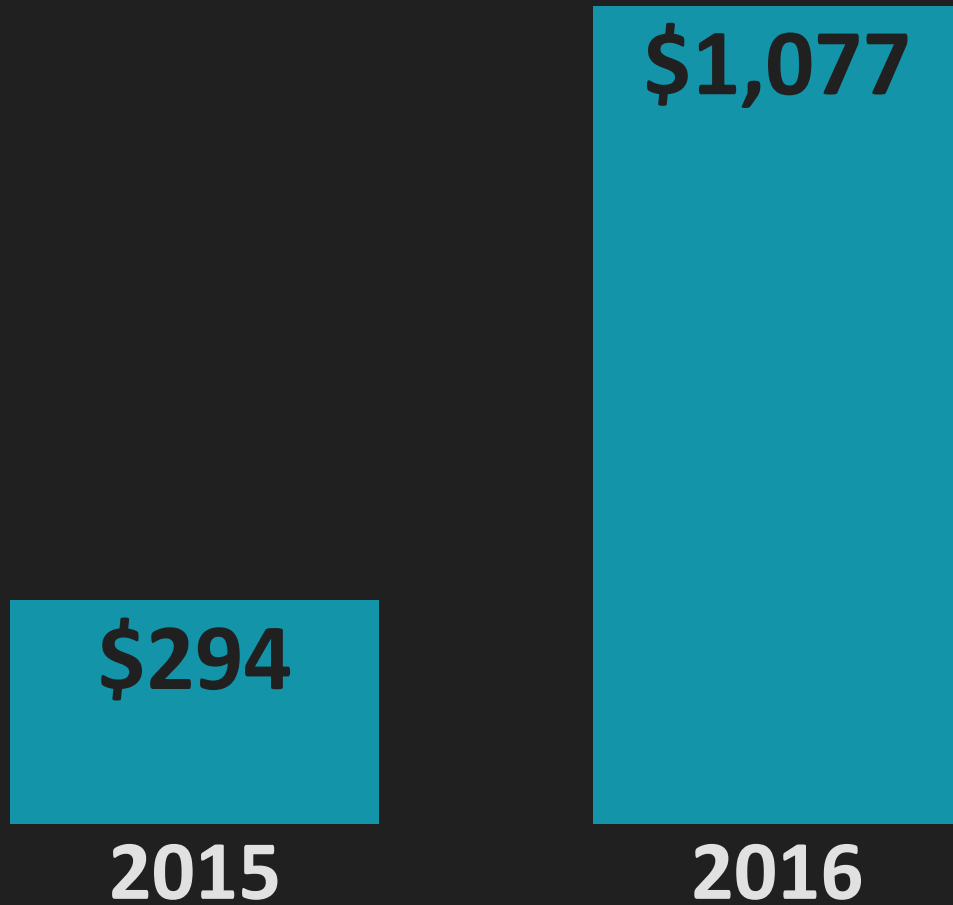


Ransomware Detections by Country



- With 34% of all attacks, US the region most affected by Ransomware
- Attackers target countries that can pay the largest ransom
- Number of internet connected computers also effect the numbers
- But US also has characteristic that is driving up the cost of the ransom

Average Ransom Demand



- The average starting ransom demand soared in 2016.
- Once infected many threats raise price if ransom not paid by deadline
- Some criminals will negotiate
- Targeted businesses will see higher demands
- Highest ransom demand for single machine seen in 2016 - \$28,730 (Ransom.Mircop)

What is Driving Up the Ransom Demand?

Percentage of Consumers Who Pay Ransom



34%

Globally

- There does not appear to be price sensitivity among victims, especially in the US
 - As long as victims willing to pay, criminals can raise the price



64%

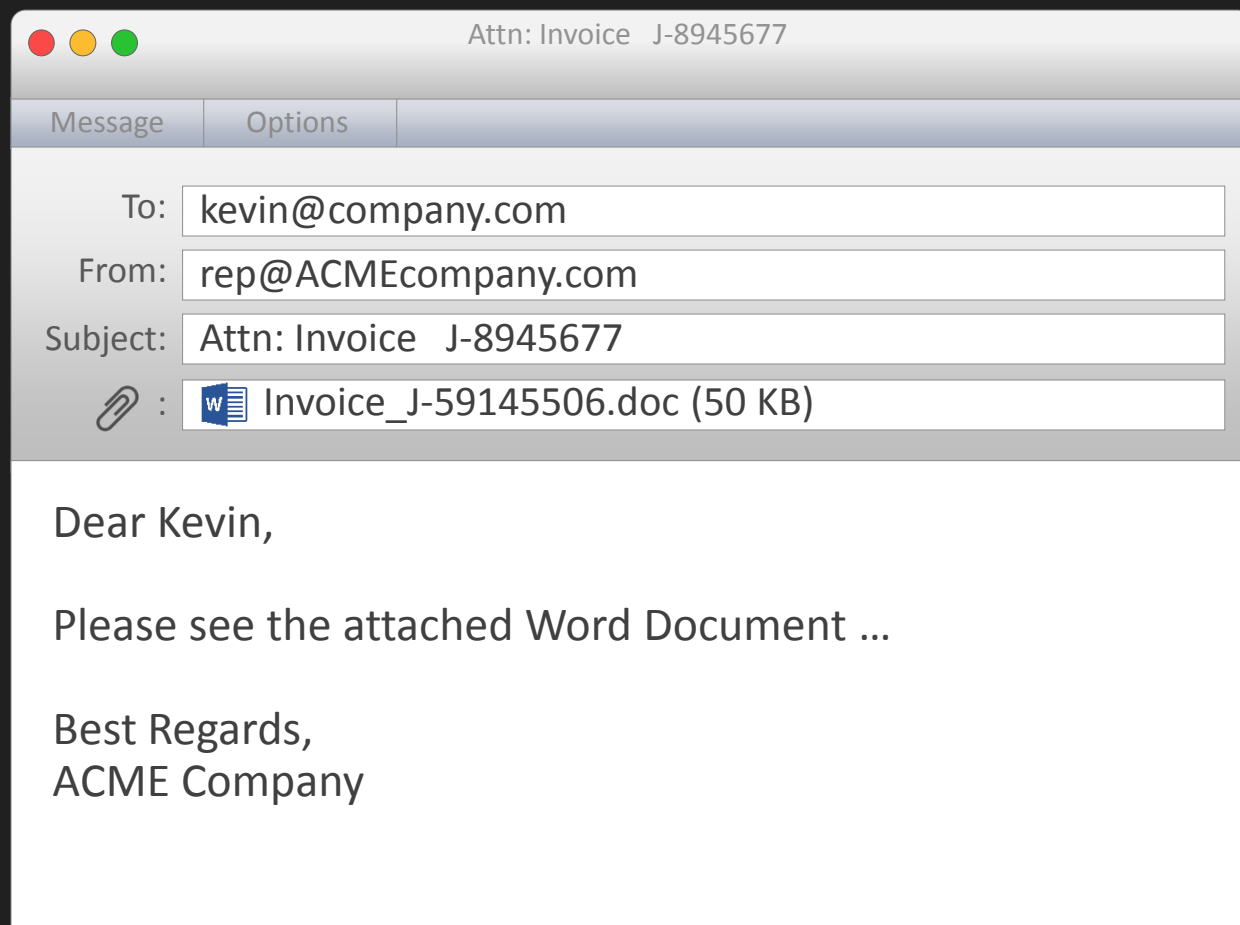
US

How is Ransomware Spreading

- **Secondary Infections** – infected machines download additional threat
- **Brute-force passwords** – ex. Ransom.Bucbi
- **Exploiting servers** – ex. Ransom.SamSam
- **Self-Propagation** – ex. W32.ZCrypt
- **3rd party app stores** – Android.Lockdroid.E
- **Social Networking** – ex. Locky
- **Exploit Kits** – 388k attacks blocked a day in 2016
- **But mainly ransomware spreads via...**



Email Attacks



Symantec Sees Millions
of Attacks per day sent via
Malicious Email

Internet Security Threat Report

ISTR

Best Practices & Solutions

Volume

22

