Internet Security Threat Report

ISTR

Volume

22

Ajay K. Sood
VP, Symantec Canada

Symantec

Copyright 2017, Symantec Corporation

Is This Ladder a Threat?

Copyright 2017, Symantec Corporation

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.

Copyright 2017, Symantec Corporation

Targeted Attacks

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

Copyright 2017, Symantec Corporation

Timeline of notable targeted attack incidents during 2016

SABOTAGE

SUBVERSION

Destructive malware used in cyberattacks against power stations in Ukraine

Buckeye begins campaign against targets in Hong Kong

Microsoft patches IE zero day which was being used in targeted attacks in South Korea

Equation Breach—exploits and malware dumped online

Disk-wiping malware Shamoon reappears after four years

JAN — FEB — MA — APR — MAY — JUN — JUL — AUG — SEP — OCT — NOV — DEC

R

Seven Iranians charged in relation to cyberattacks against US targets

Data stolen from Democratic National Committee (DNC) intrusion released online

Symantec uncovers Strider cyberespionage group

WADA

Data stolen from World Anti-Doping Agency (WADA) intrusion released

Power outages in Ukraine suspected to be linked to cyberattack

Copyright 2017, Symantec Corporation

Resurgence of sabotage

Sabotage campaigns represent another form of politicized and disruptive attack

Shamoon

est. 2012

Possible region of origin: Middle East

Aliases / Distrack

Tools, tactics & procedures (TTP)

- Stage one: Spear-phishing, credential theft
- Stage two: Disk-wiping payload

Motives

- Aggressive and highly disruptive campaigns
- Political: payload includes political imagery

Target categories & regions

- Energy
- Saudi Arabia

Known for

- 2012 campaign against Saudi and Qatari energy sector
- Reappearance with broader campaign in 2016

Sandworm

est. 2014

Possible region of origin: Russia

Aliases / Quedagh, BE2 APT

Tools, tactics & procedures (TTP)

- Killdisk disk-wiping threat
- Stealth: deletes logs, removes attack artifacts
- Maximum disruption: blocks access to recovery systems

Motives

- Political, military: cyber wing of ongoing Russian activity against Ukraine

Target categories & regions

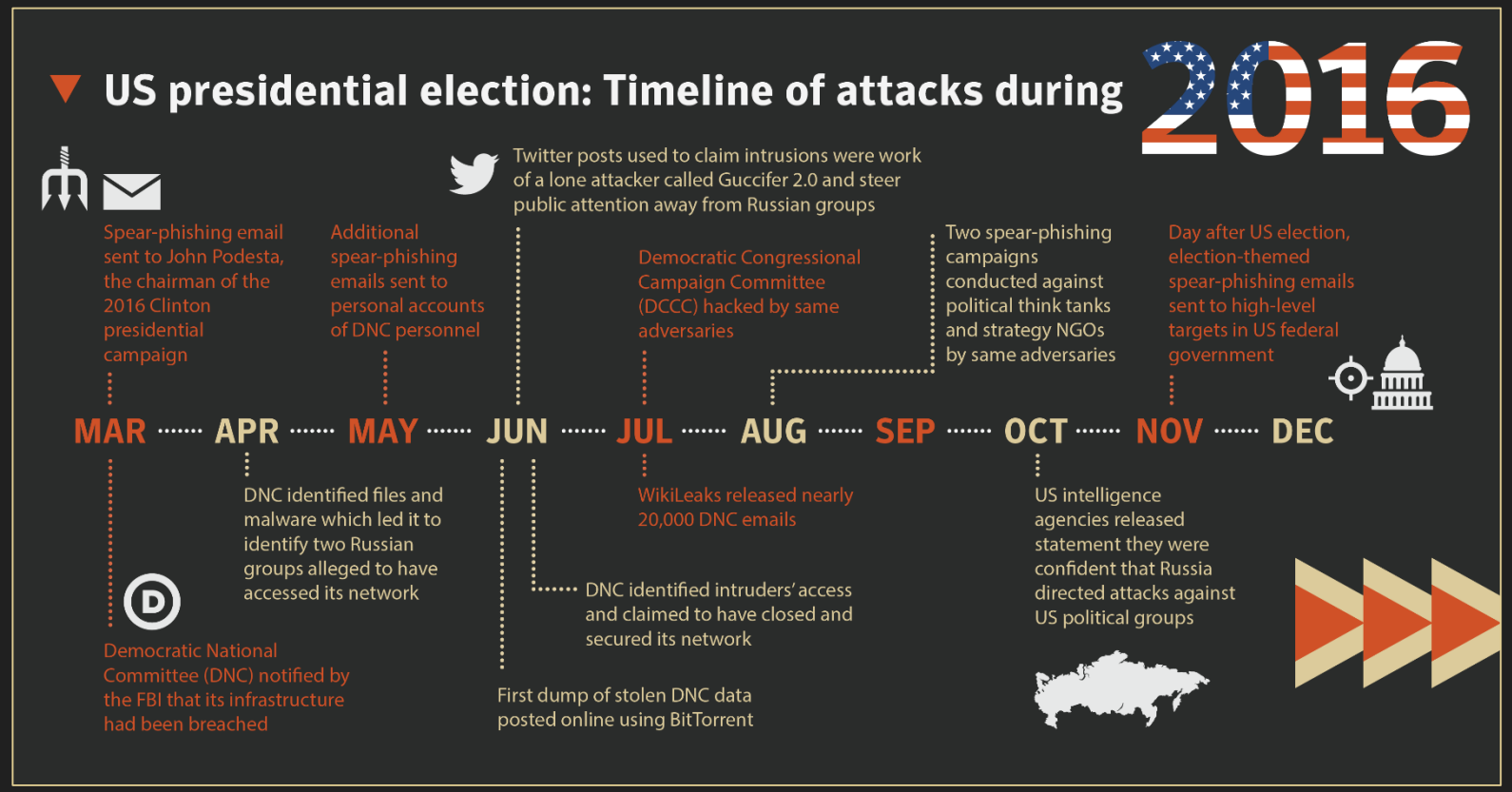
- Critical infrastructure, energy, media, finance
- Ukraine

Known for

- Late 2015 power outage in Ukraine
- War-dialing of energy companies

Copyright 2017, Symantec Corporation

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**

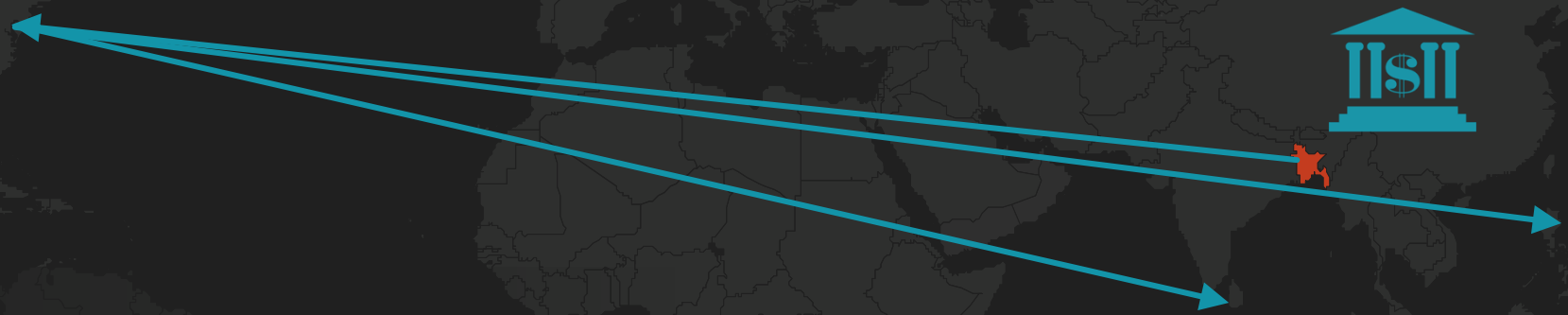
Copyright 2017, Symantec Corporation

Cyber Bank Heists

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

Copyright 2017, Symantec Corporation

Bank in Bangladesh compromised



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

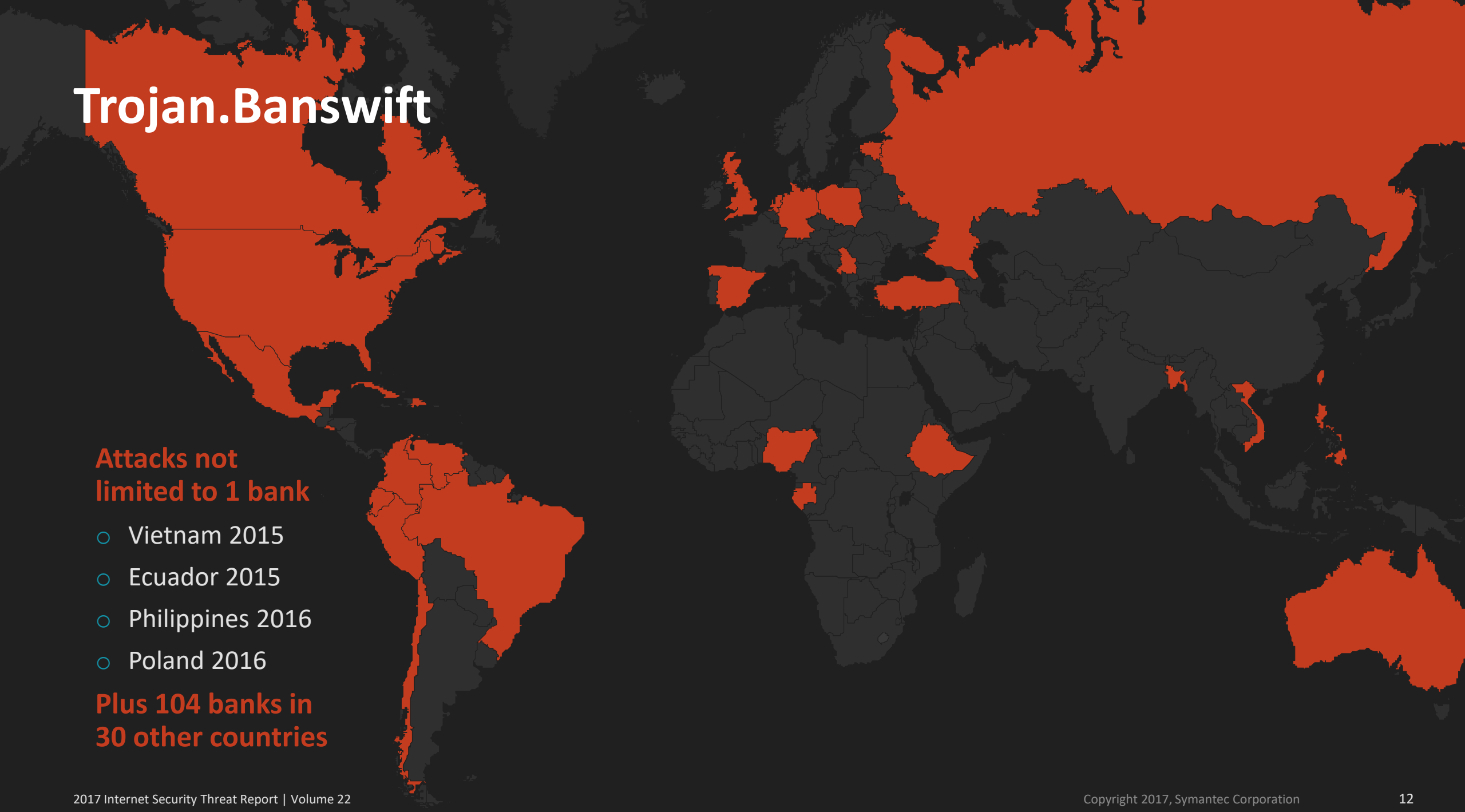
Copyright 2017, Symantec Corporation

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

Copyright 2017, Symantec Corporation

Trojan.Banswift



Attacks not limited to 1 bank

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

Plus 104 banks in 30 other countries

Copyright 2017, Symantec Corporation

Email Attacks

Email Becomes the Weapon of Choice for 2016

Copyright 2017, Symantec Corporation

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

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

Copyright 2017, Symantec Corporation

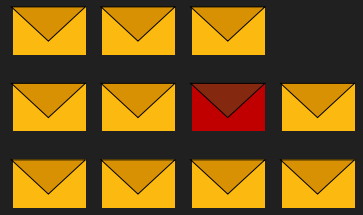
Malicious Emails Hit the Highest Rate in Five Years

1 out of

244

1 out of

220

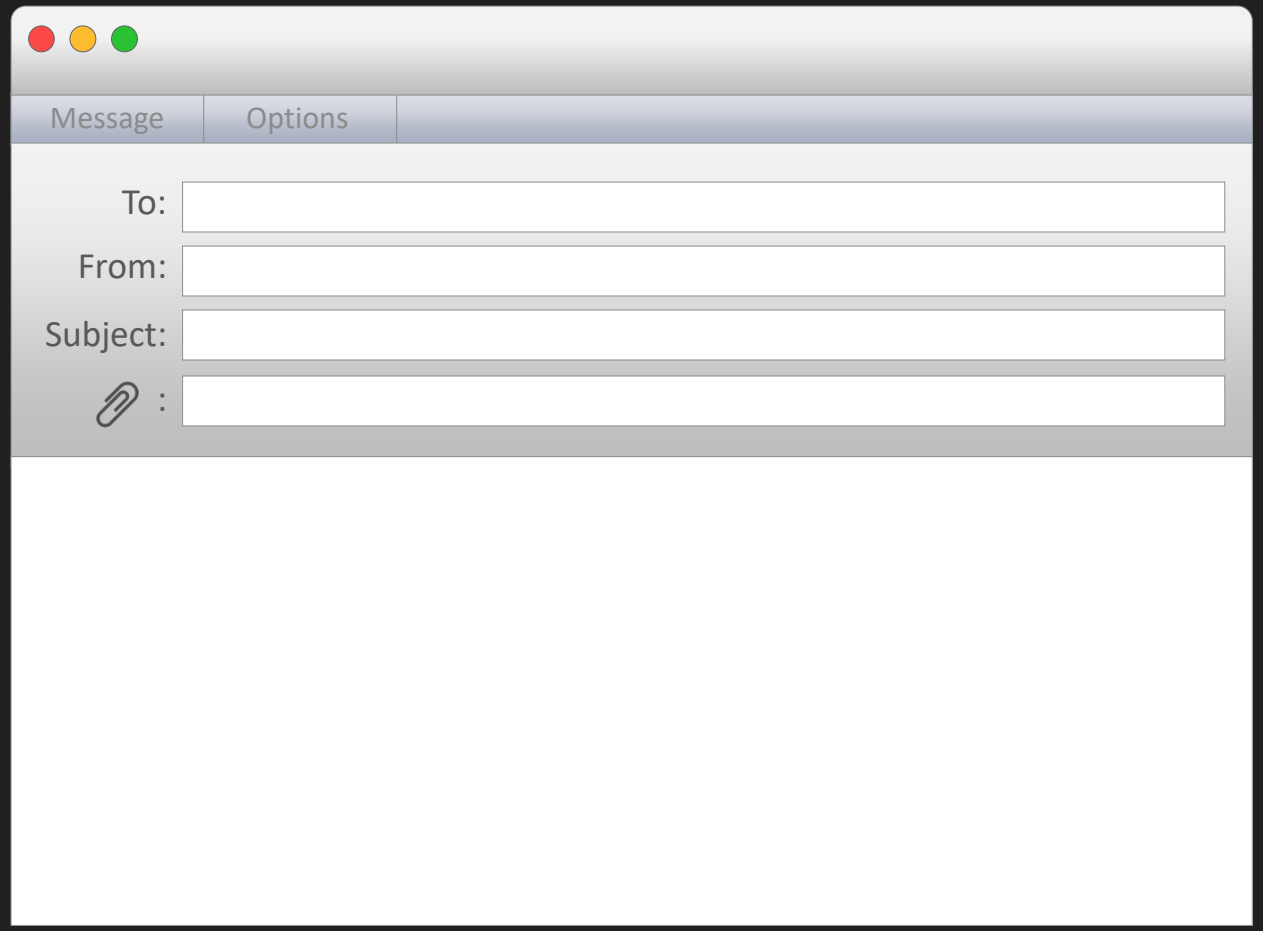


1 out of

131

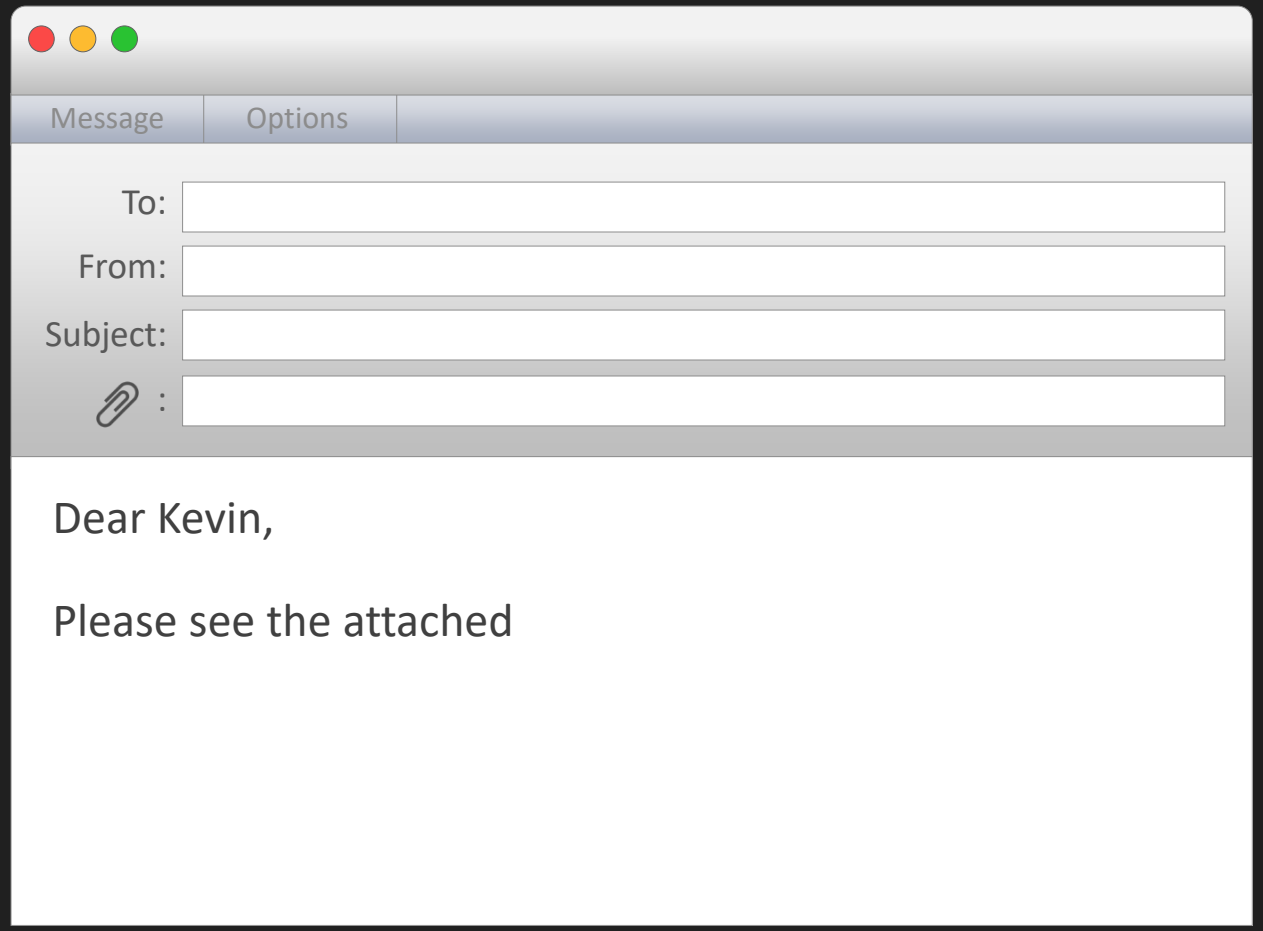
Copyright 2017, Symantec Corporation

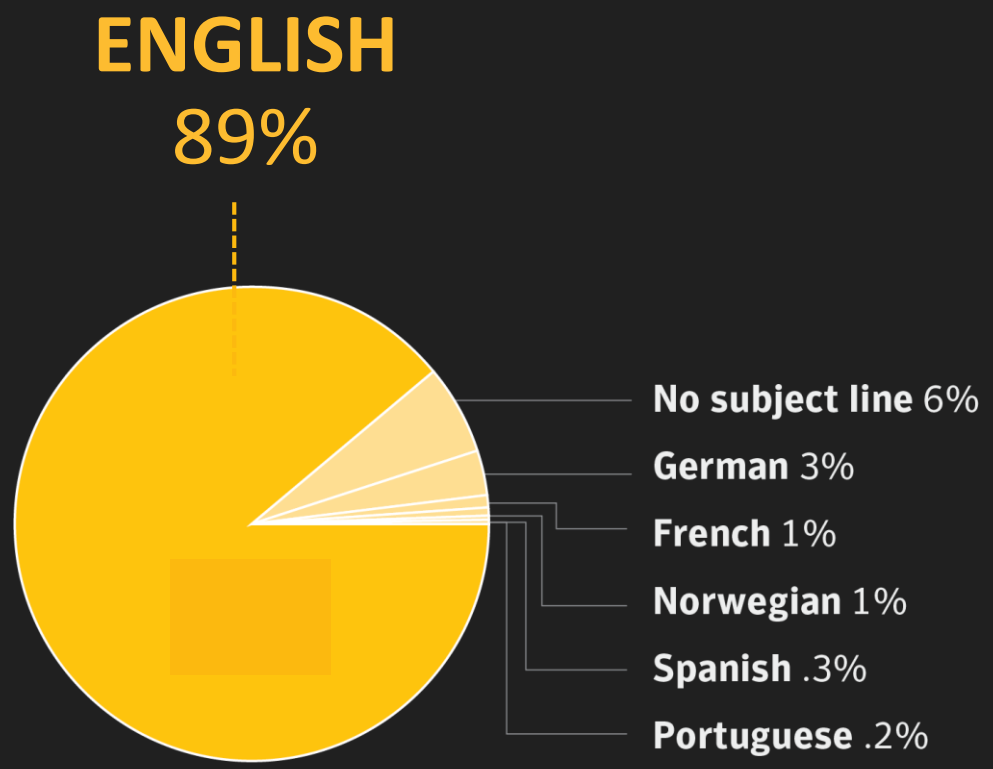
Building Malicious Email



Copyright 2017, Symantec Corporation

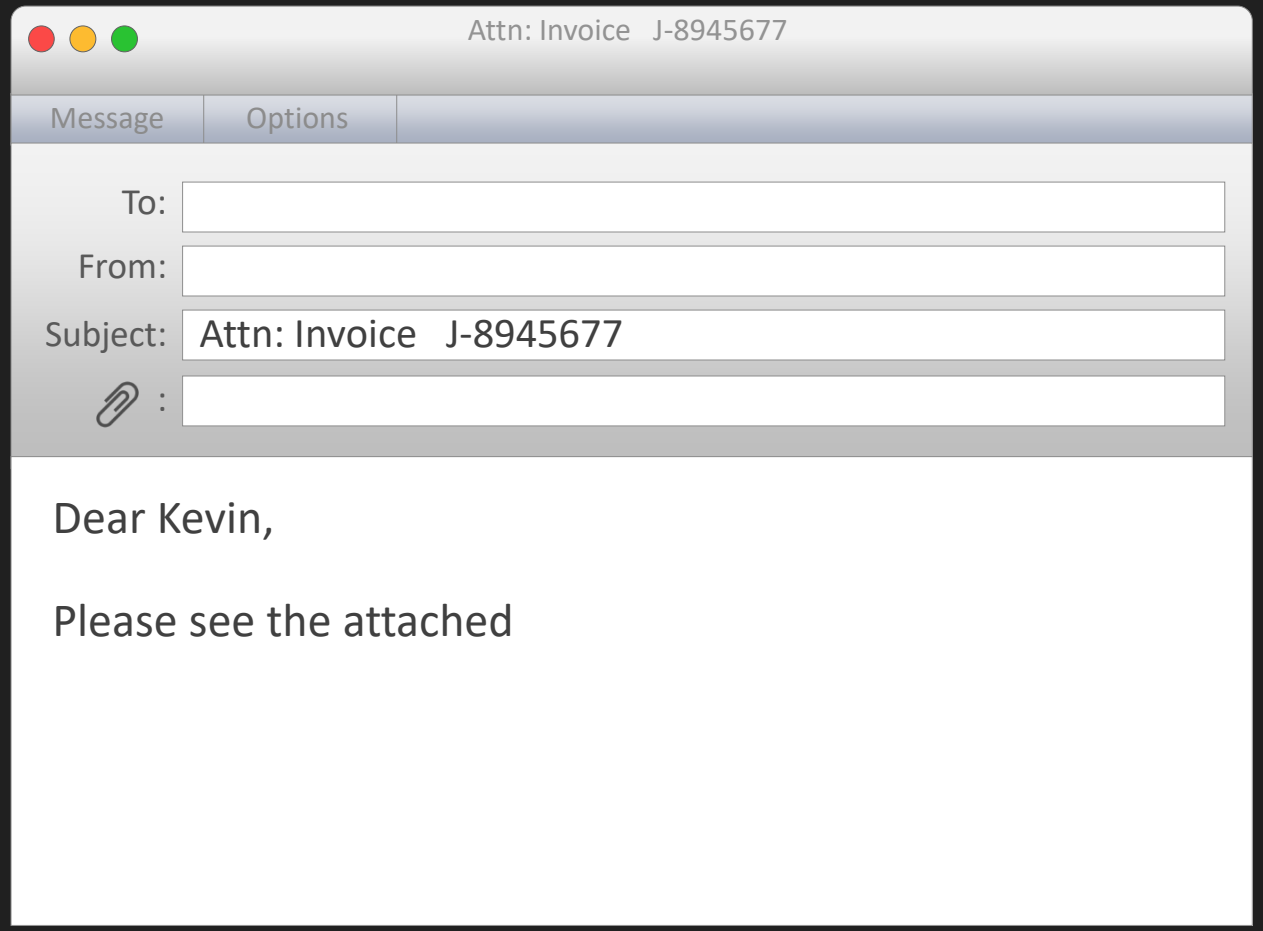
Building Malicious Email: Language

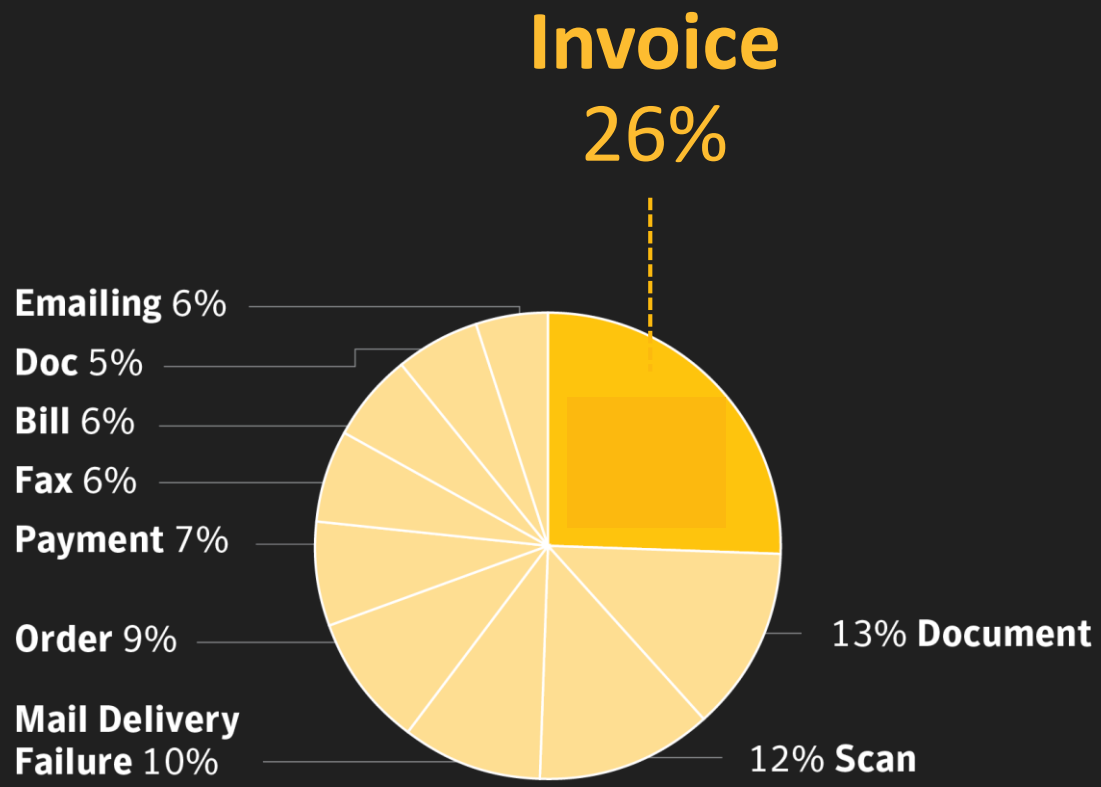




Copyright 2017, Symantec Corporation

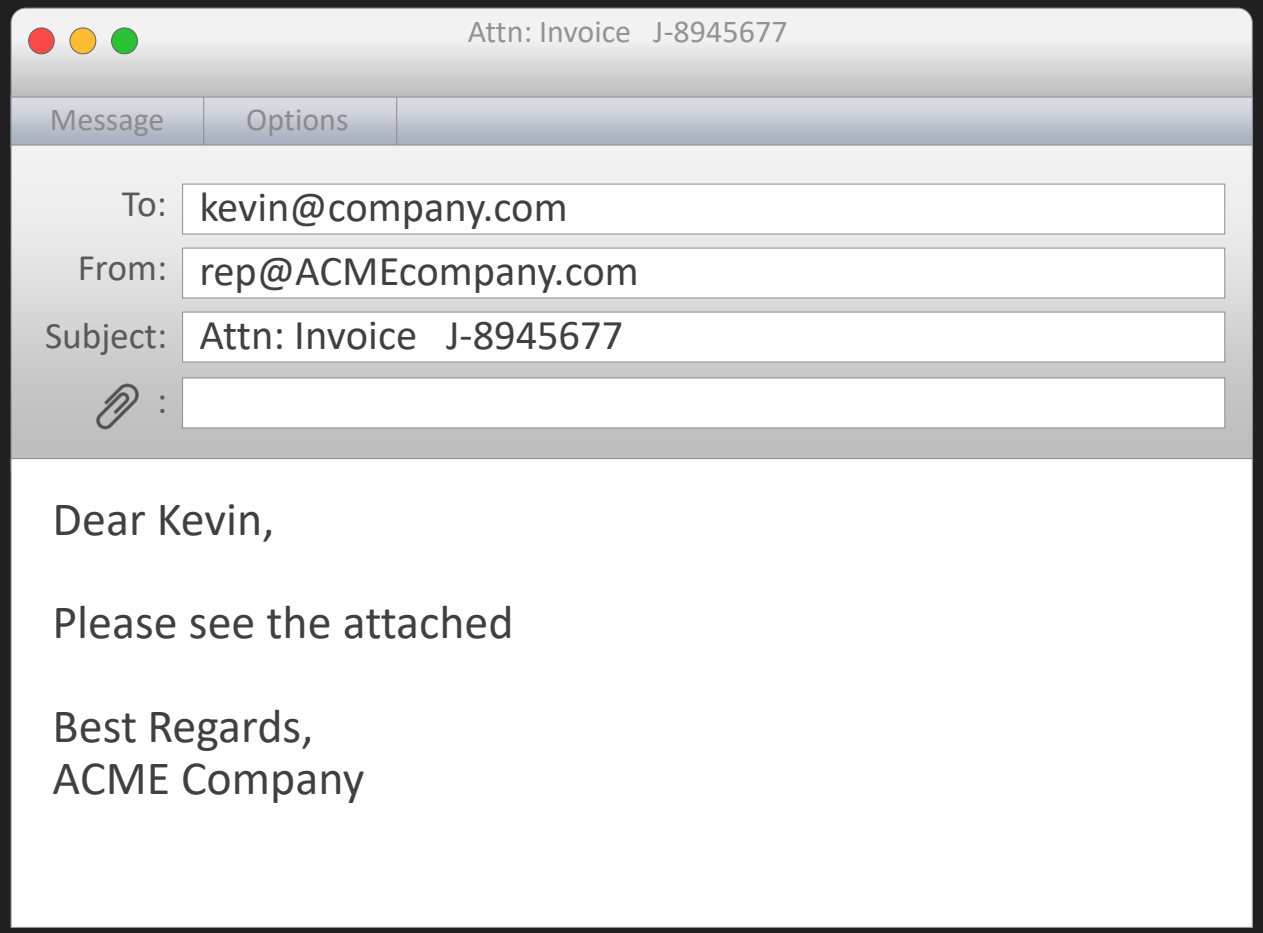
Building Malicious Email: Subject





Copyright 2017, Symantec Corporation

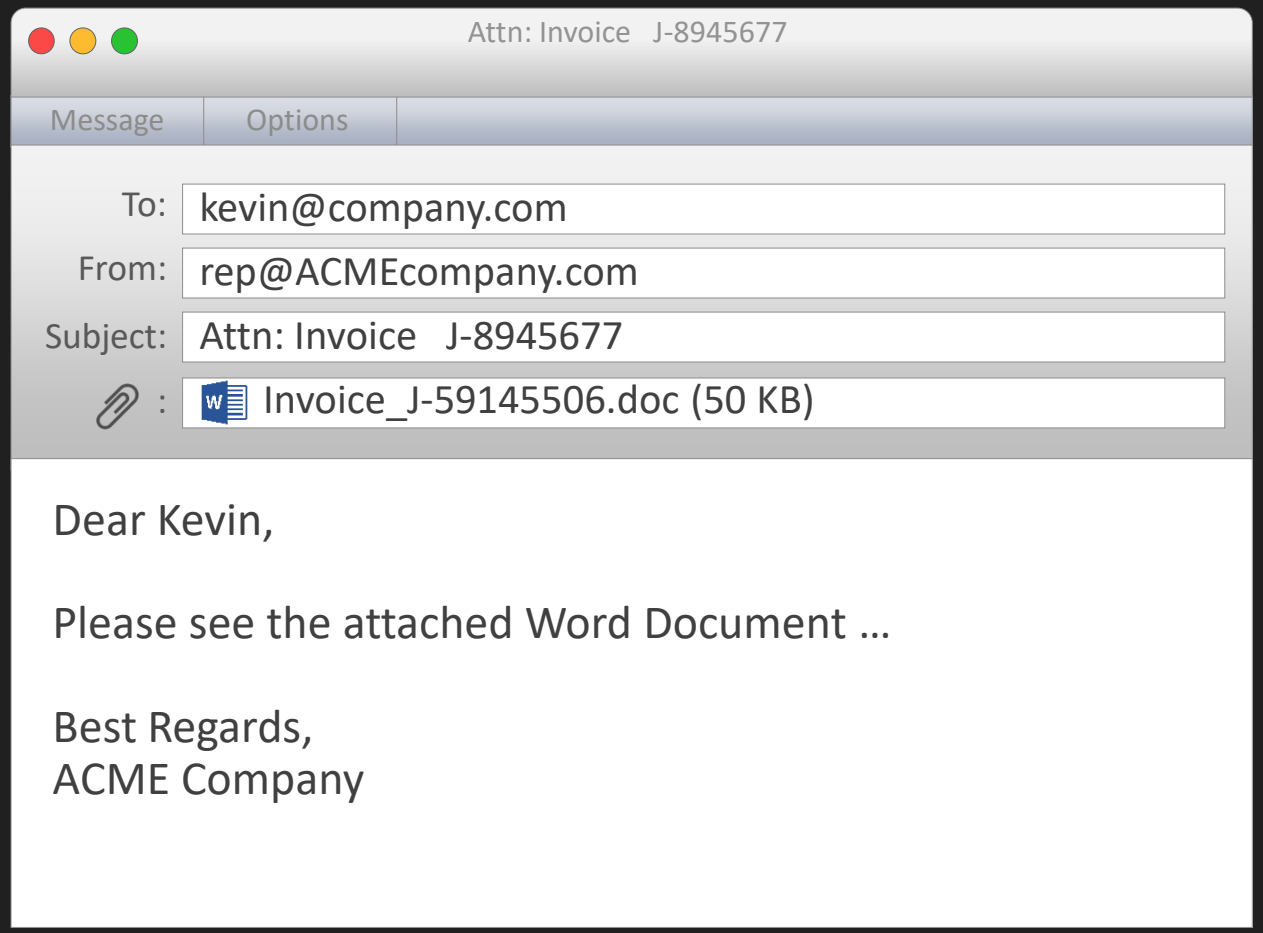
Building Malicious Email: To/From



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

Copyright 2017, Symantec Corporation

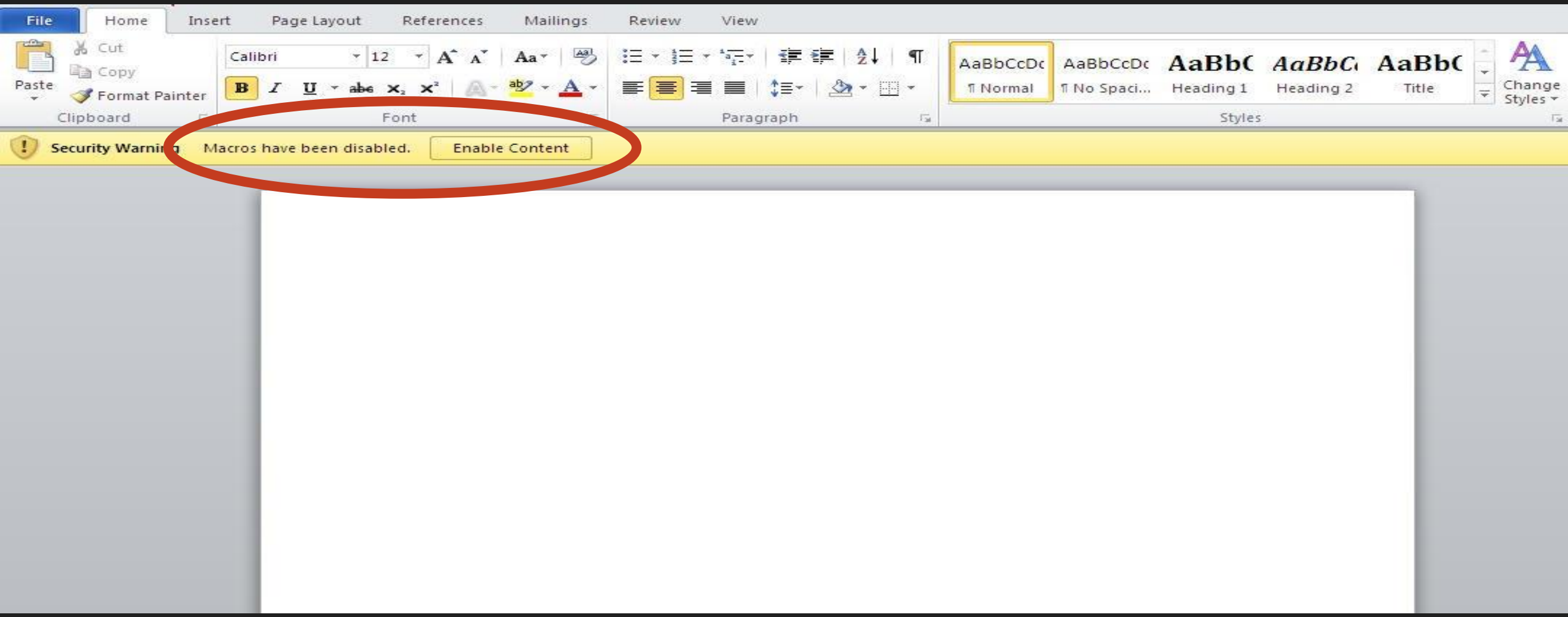
Building Malicious Email: Attachment



- 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

Copyright 2017, Symantec Corporation

Building Malicious Email: Social Engineering



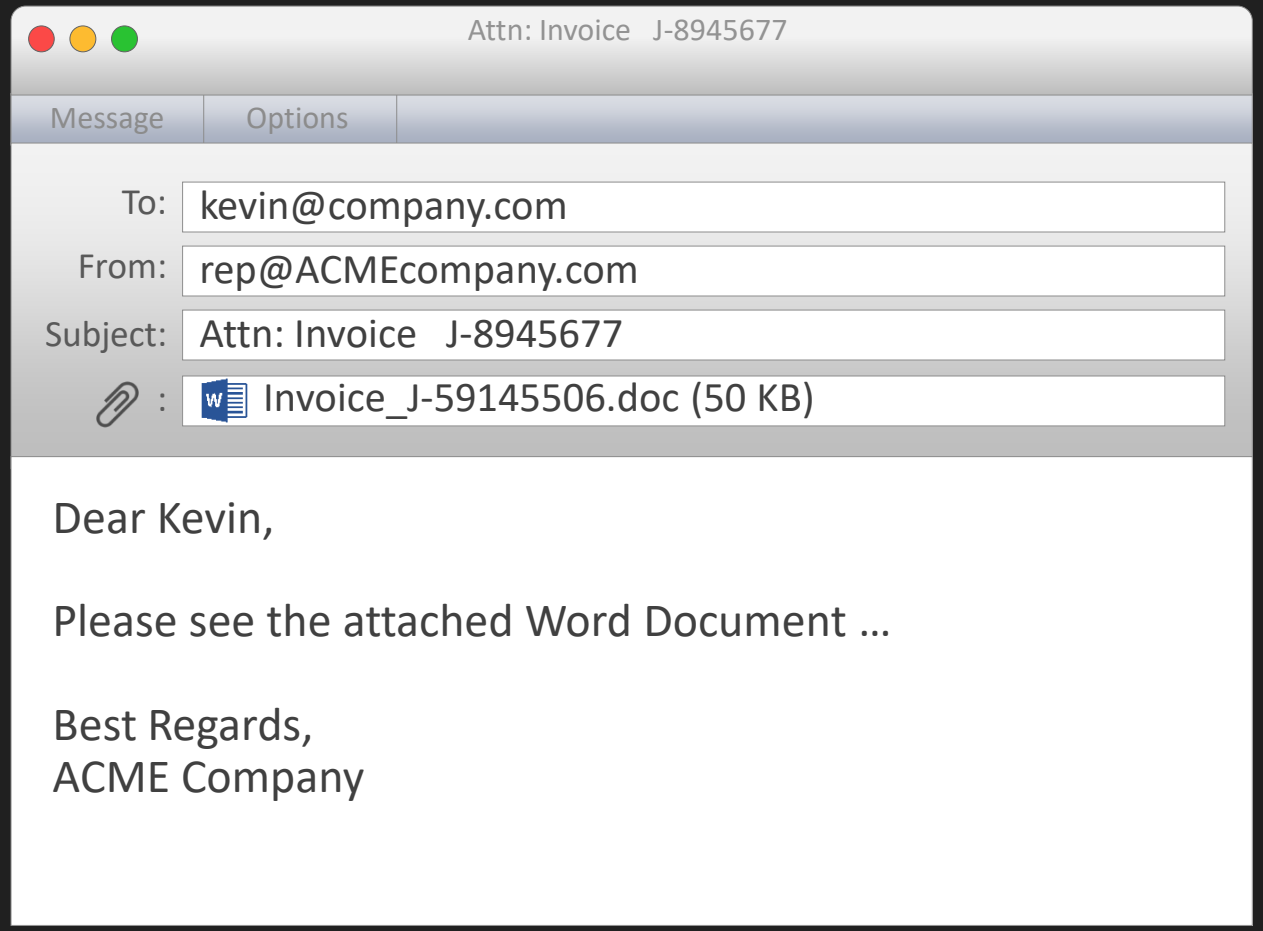
Copyright 2017, Symantec Corporation

Macros, IT tools & Malware

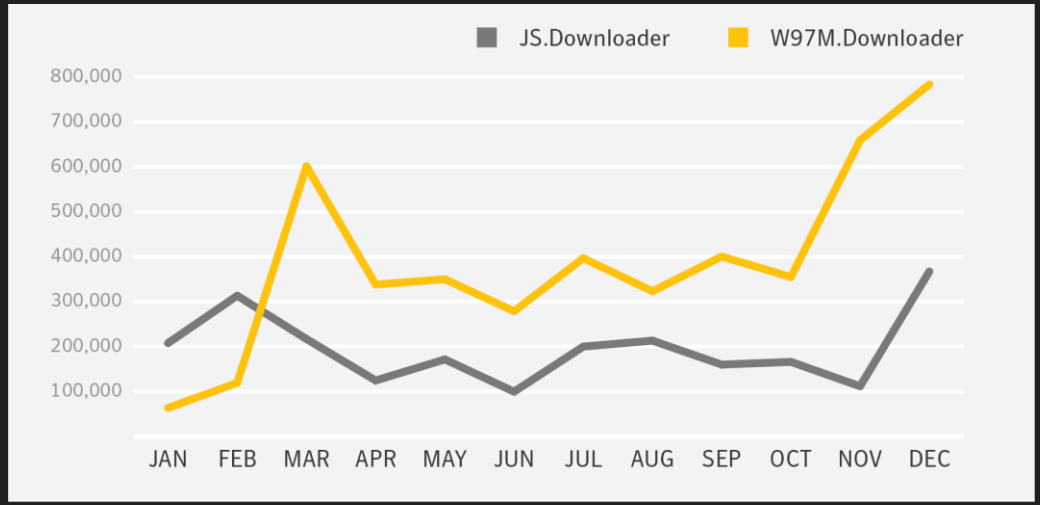
Attackers Weaponize Common IT Tools

Copyright 2017, Symantec Corporation

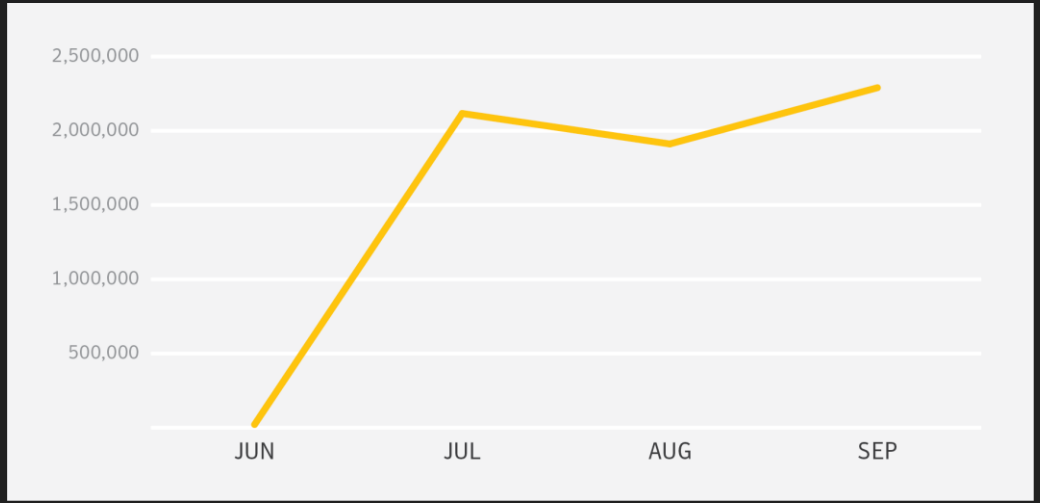
Macros



Downloader detections by month



Blocked emails with WSF attachments



Copyright 2017, Symantec Corporation

Powershell

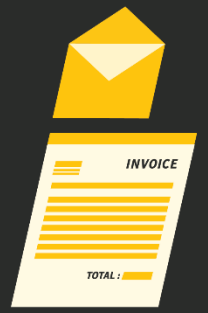
95% of Powershell scripts found in the wild were malicious

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*

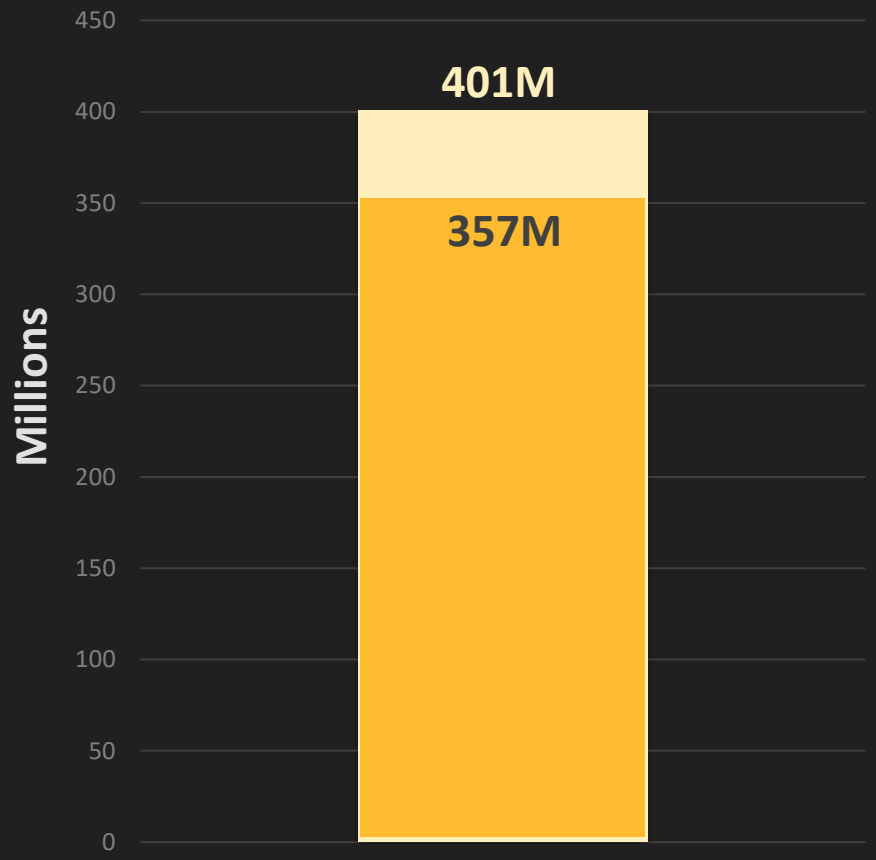


02 Includes attachment, typically JavaScript (JS) file or Office file containing malicious macro

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

Copyright 2017, Symantec Corporation

Cloud

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

Copyright 2017, Symantec Corporation

John Podesta

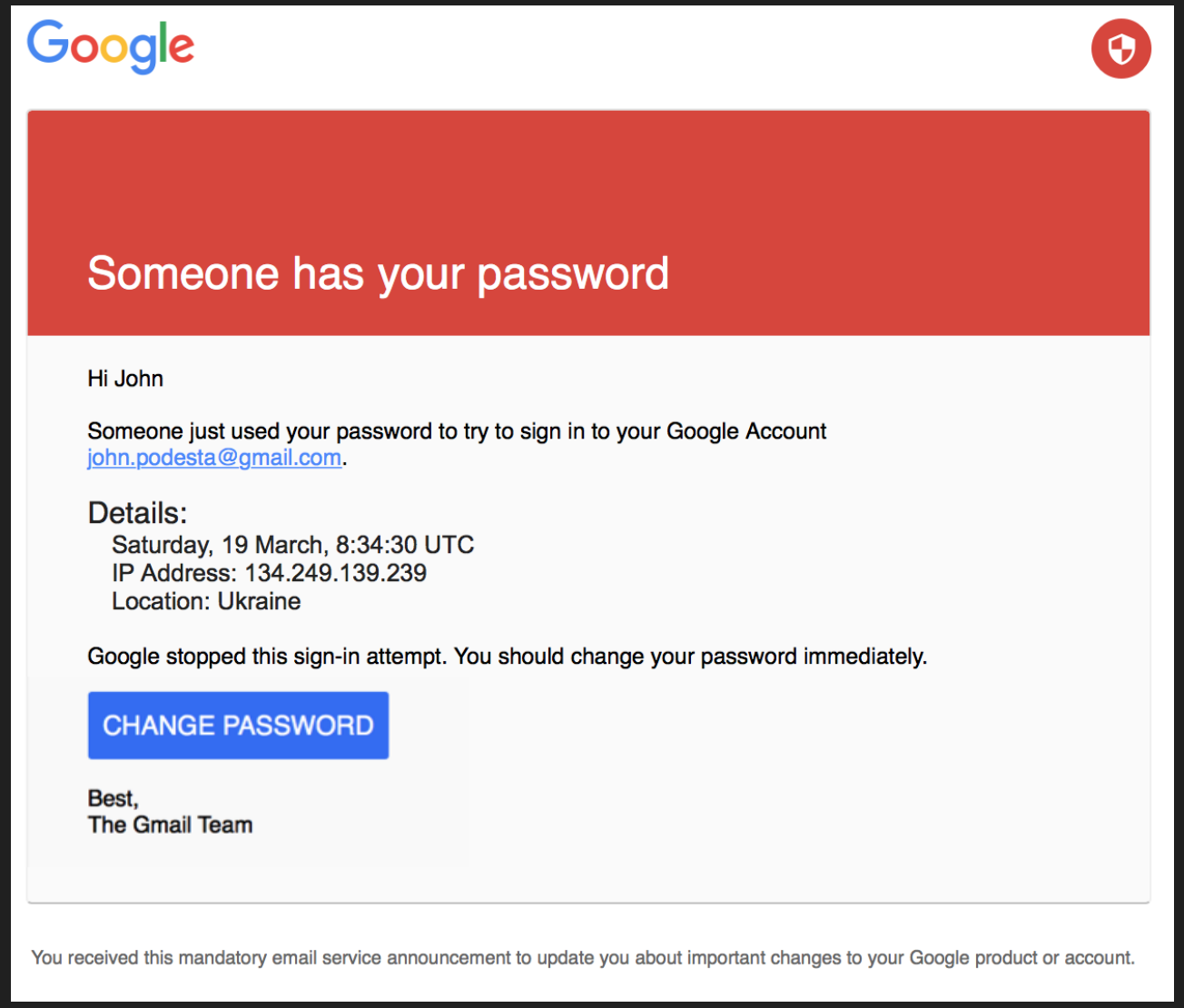
From Wikipedia, the free encyclopedia

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]

Copyright 2017, Symantec Corporation

Anatomy of a Targeted Phishing Attack



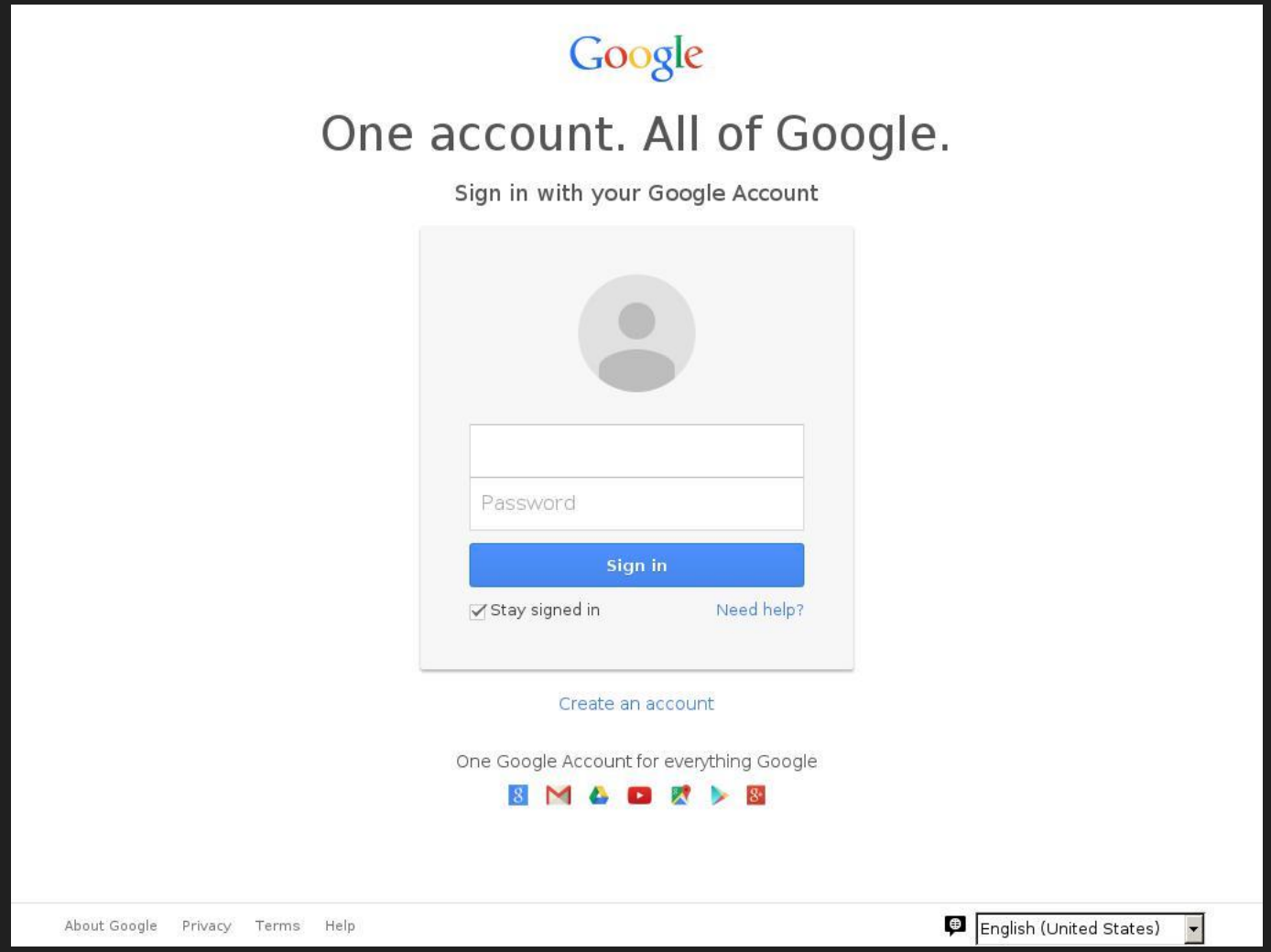
- The branding looks consistent (Google logo, shield logo)
- The email is addressed to the recipient (not “Dear Sir”)
- The English is not broken

Copyright 2017, Symantec Corporation

Anatomy of a Targeted Phishing Attack

Copyright 2017, Symantec Corporation

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

Copyright 2017, Symantec Corporation

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.

Copyright 2017, Symantec Corporation

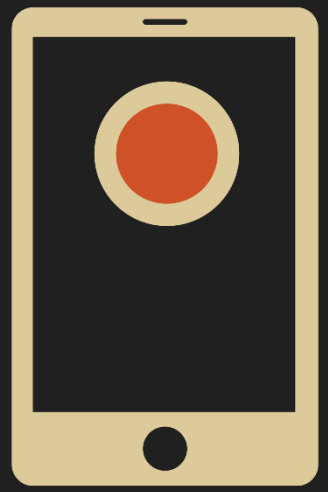
Two Factor Authentication Should Not Be An Option for Cloud Apps

Copyright 2017, Symantec Corporation

The Cloud in the Average Enterprise

How many Cloud Apps are used?

Copyright 2017, Symantec Corporation



Internet of Things

IoT Devices Attacked Within Two Minutes of Connecting to the Internet

Copyright 2017, Symantec Corporation

In 2004 security researchers put a PC on the internet

- Without any patches installed
- Without any security software

It was attacked within

4 minutes

Copyright 2017, Symantec Corporation

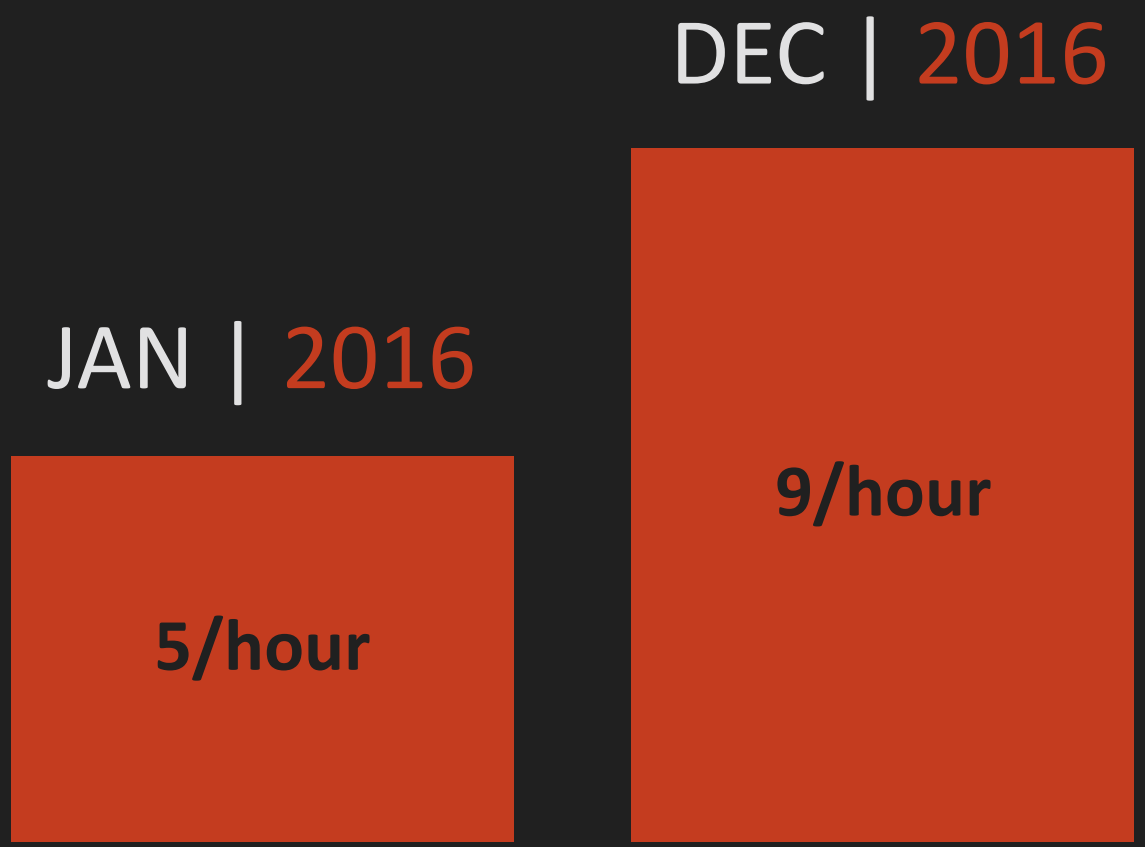
In 2016 Symantec researchers put an IoT device on the internet

It was attacked within

2 minutes

Copyright 2017, Symantec Corporation

Attacks against Symantec IoT honeypots doubled from January to December 2016

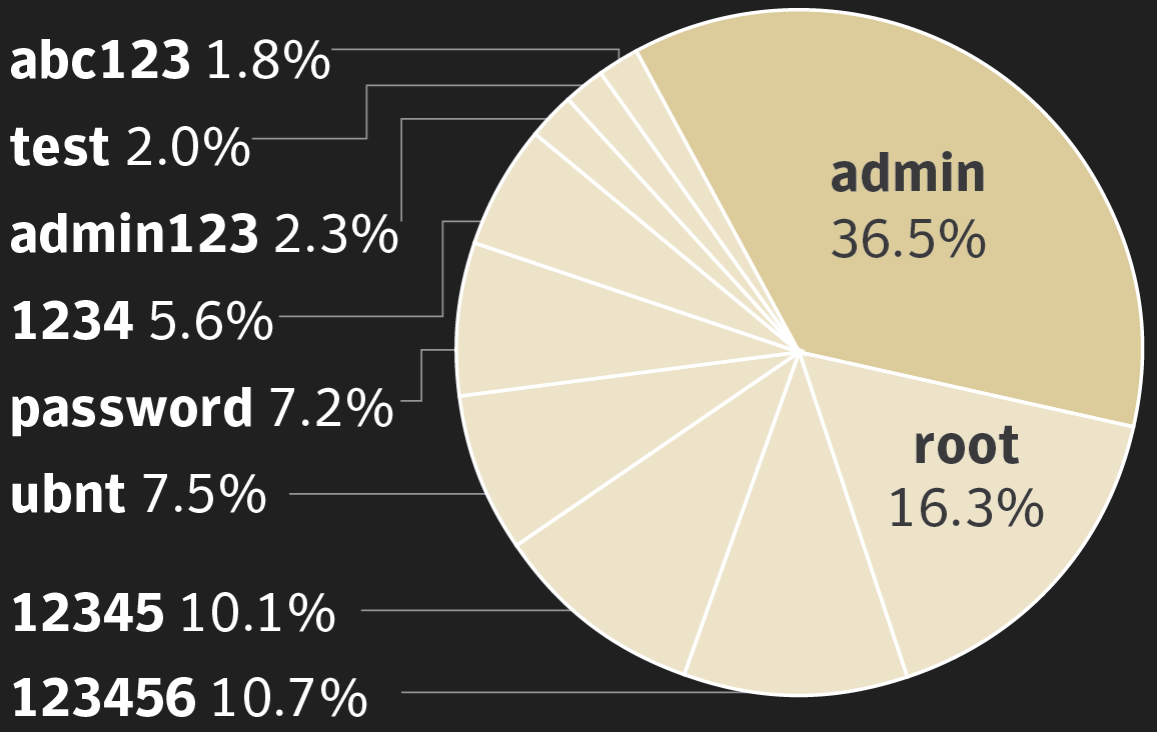


Copyright 2017, Symantec Corporation

The security shortcomings of IoT

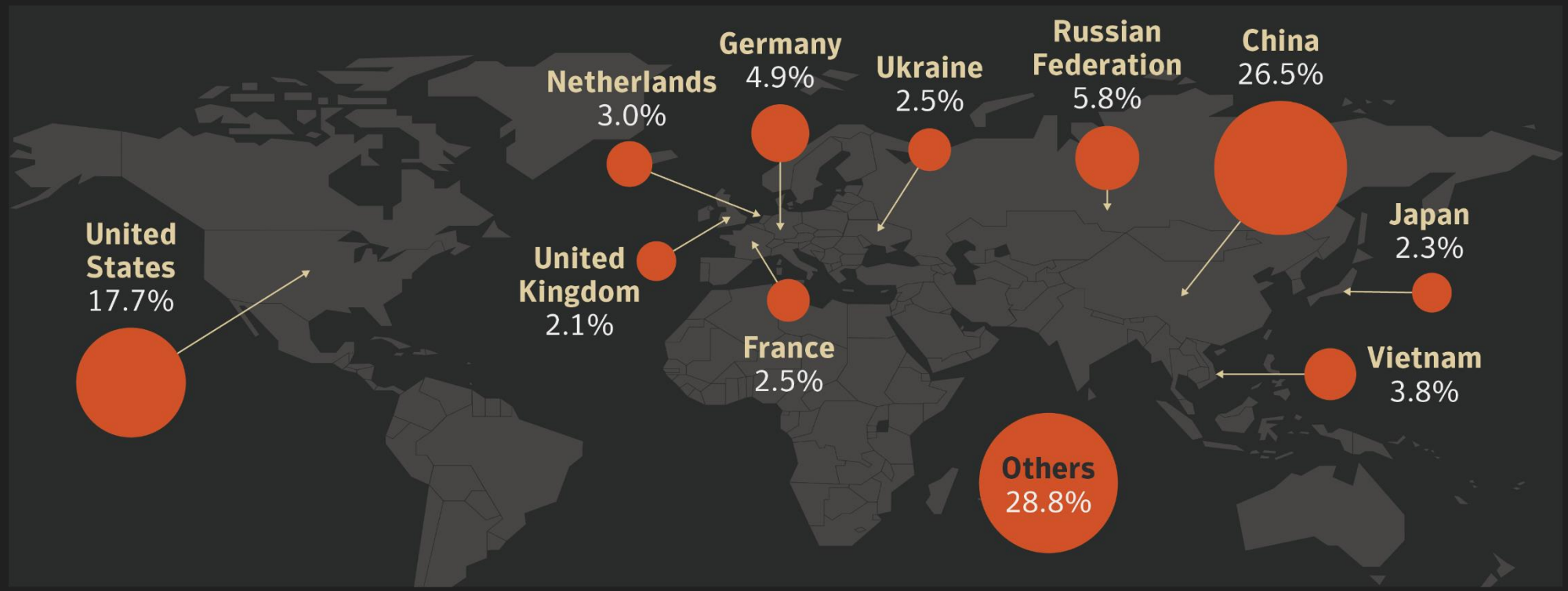
- No system hardening
- No update mechanism
- Default/hardcodes passwords

Top 10 passwords used by malware to break into IoT devices



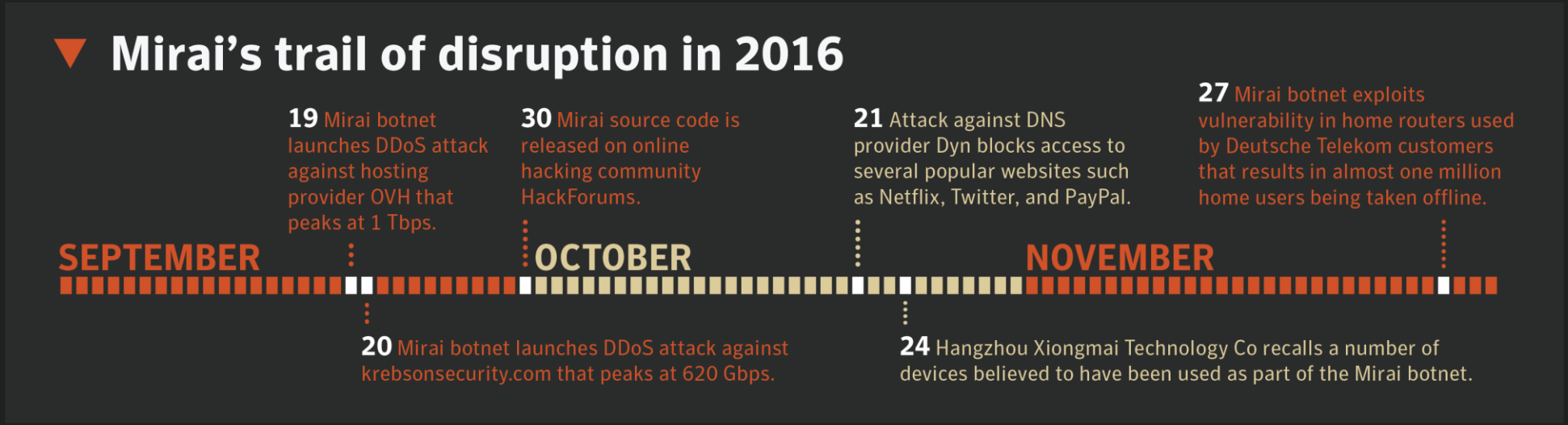
Copyright 2017, Symantec Corporation

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



Copyright 2017, Symantec Corporation

The Consequences of Poor IoT Security



- 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)

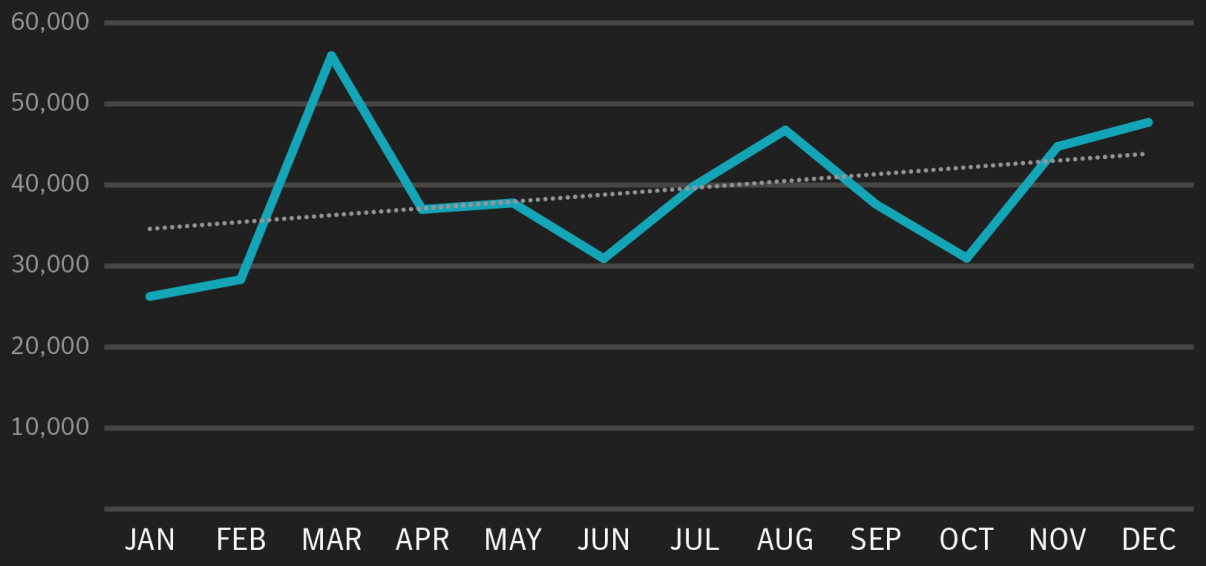
Copyright 2017, Symantec Corporation

Ransomware

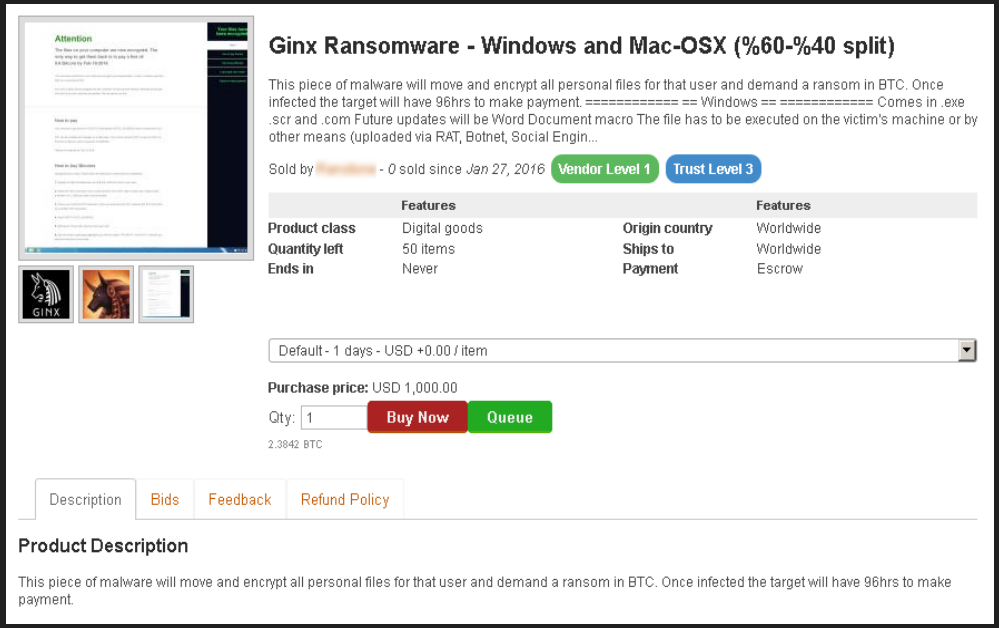
Caving to Digital Extortion: Americans Most Likely to Pay Ransom Demands

Copyright 2017, Symantec Corporation

36% Increase in Ransomware Attacks

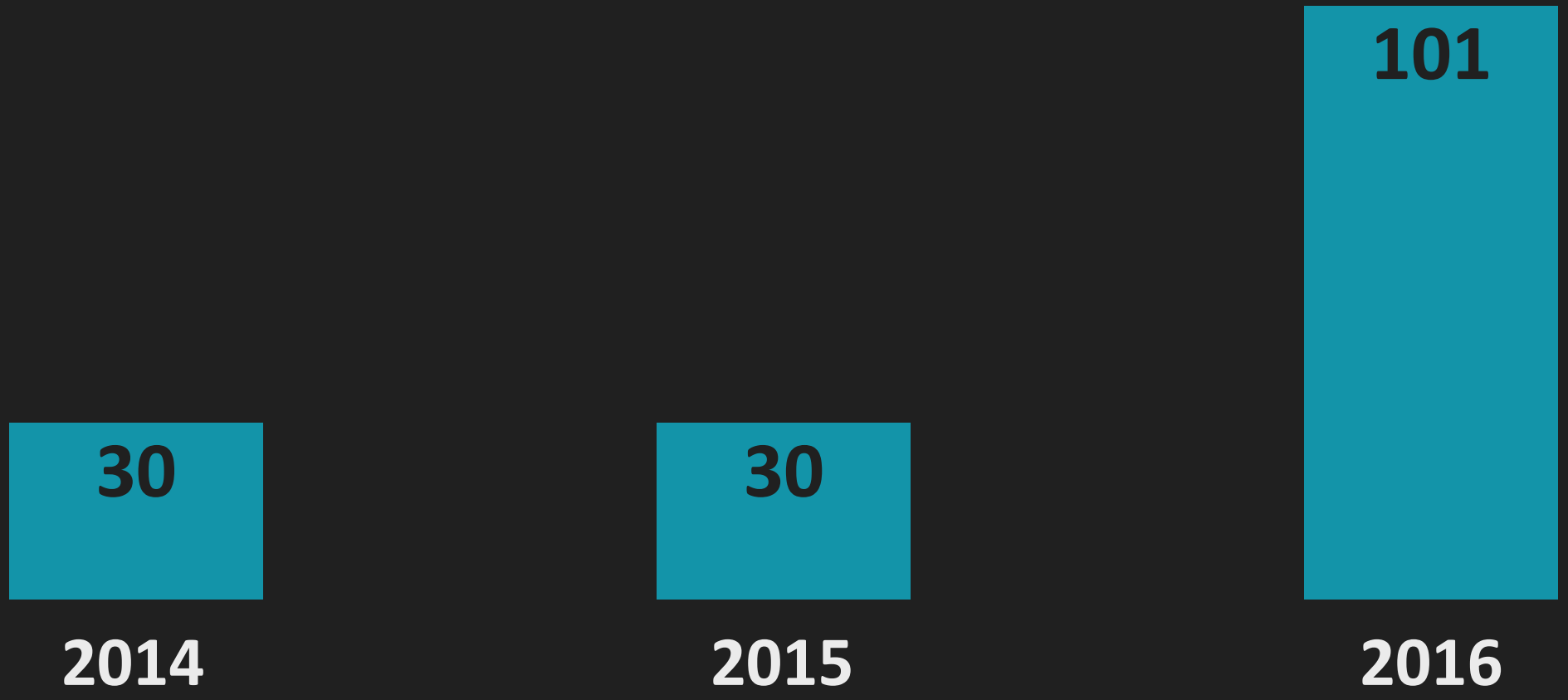


- Highly profitable
- Low Barrier to Entry
  - Multiple Software as a Service offerings available



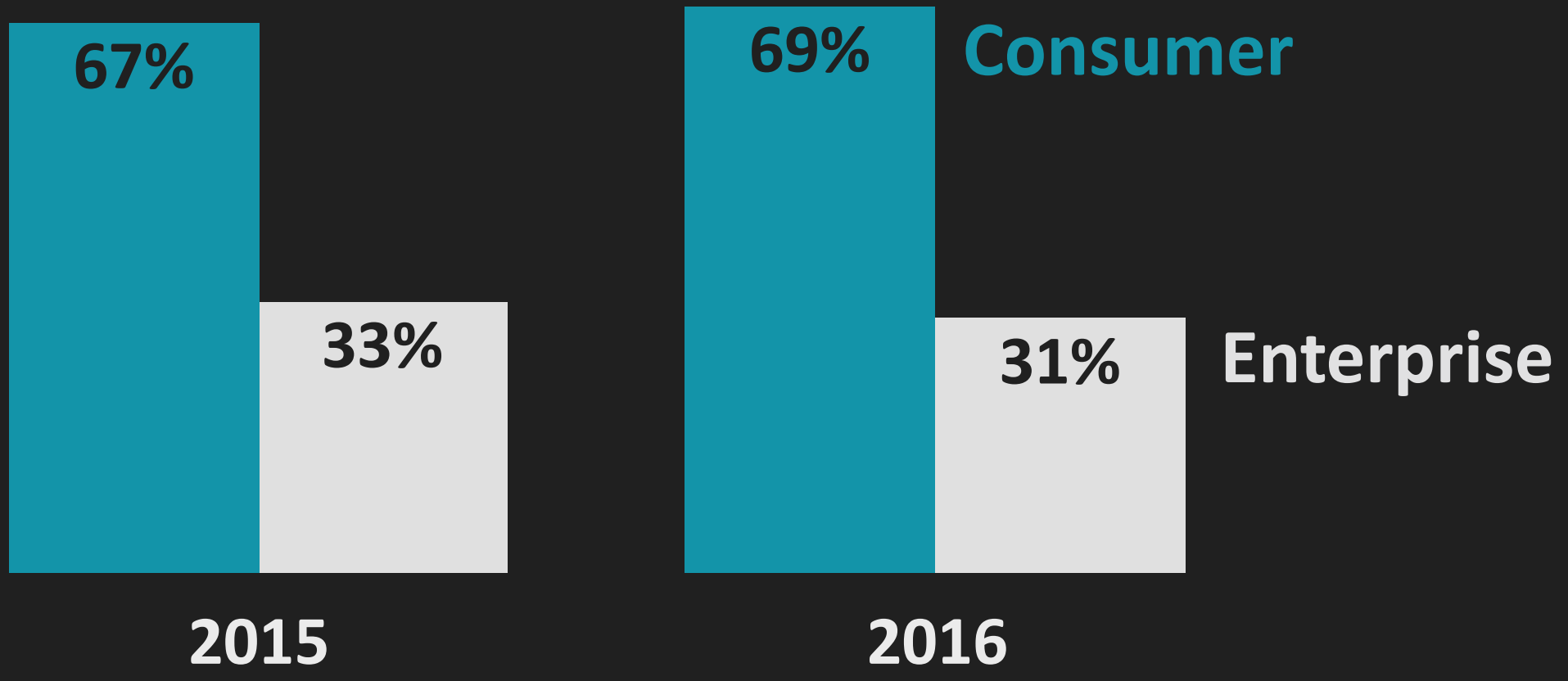
Copyright 2017, Symantec Corporation

3x as many new ransomware families in 2016



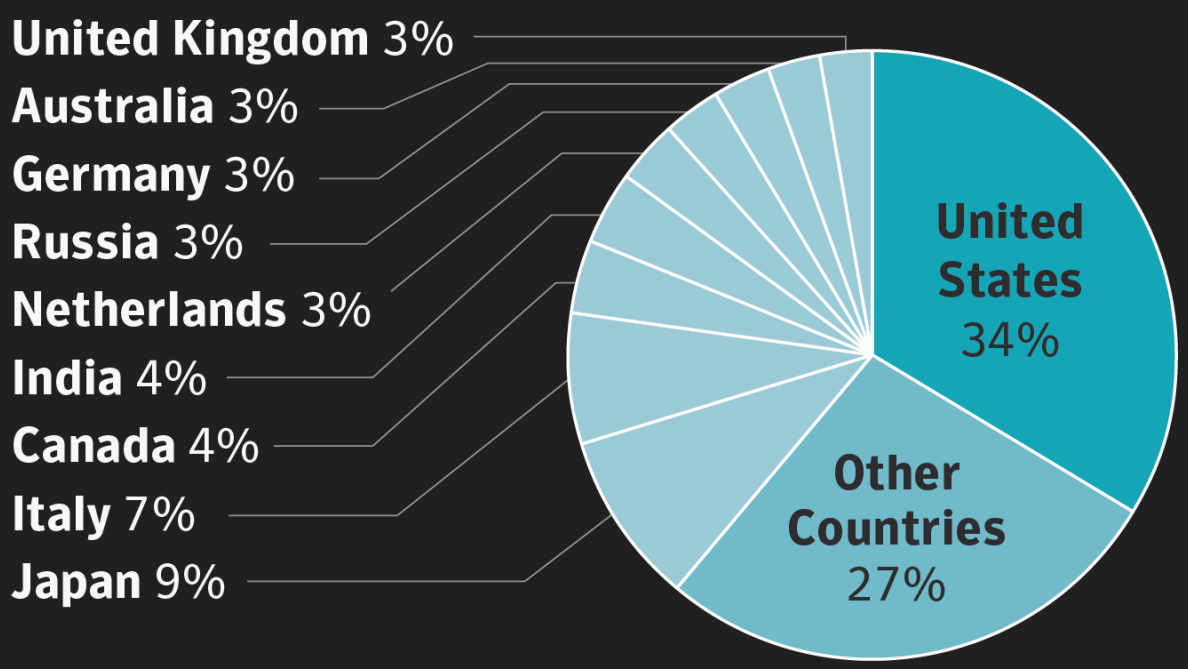
Copyright 2017, Symantec Corporation

Consumers Continue to see the Majority of Attacks



Copyright 2017, Symantec Corporation

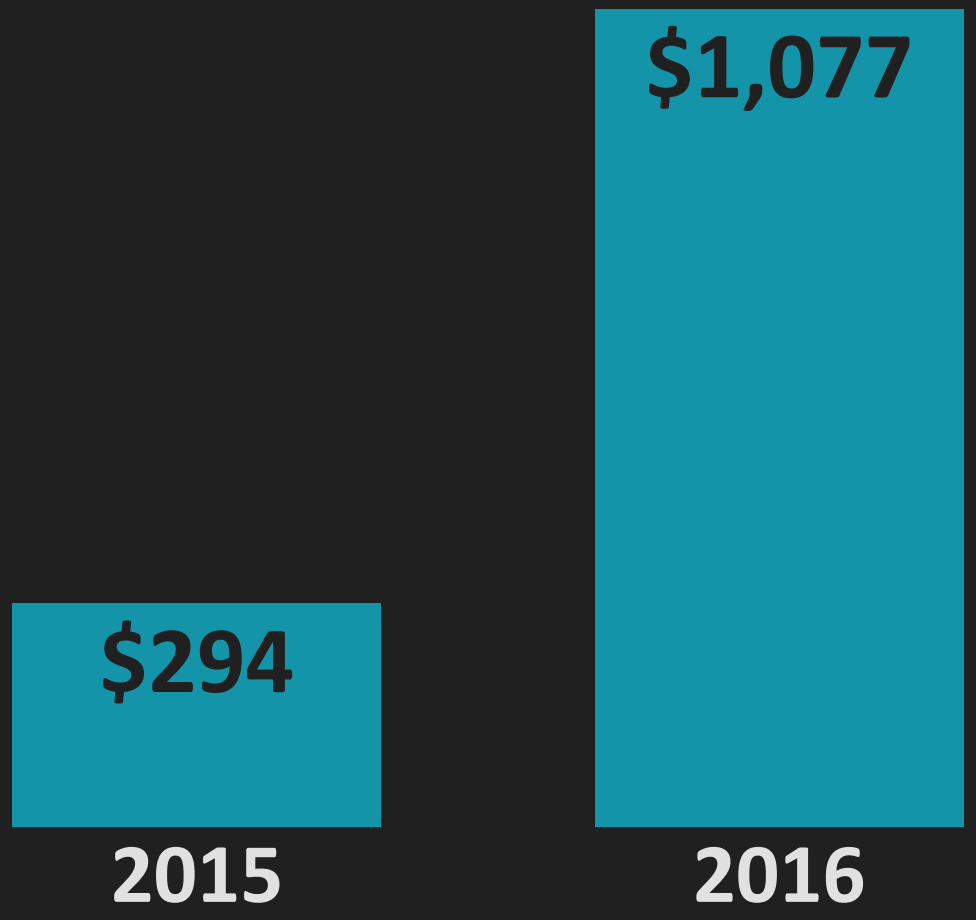
Ransomware Detections by Country



- 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

Copyright 2017, Symantec Corporation

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)

Copyright 2017, Symantec Corporation

What is Driving Up the Ransom Demand?

Percentage of Consumers Who Pay Ransom

34%
Globally

64%
US

- 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

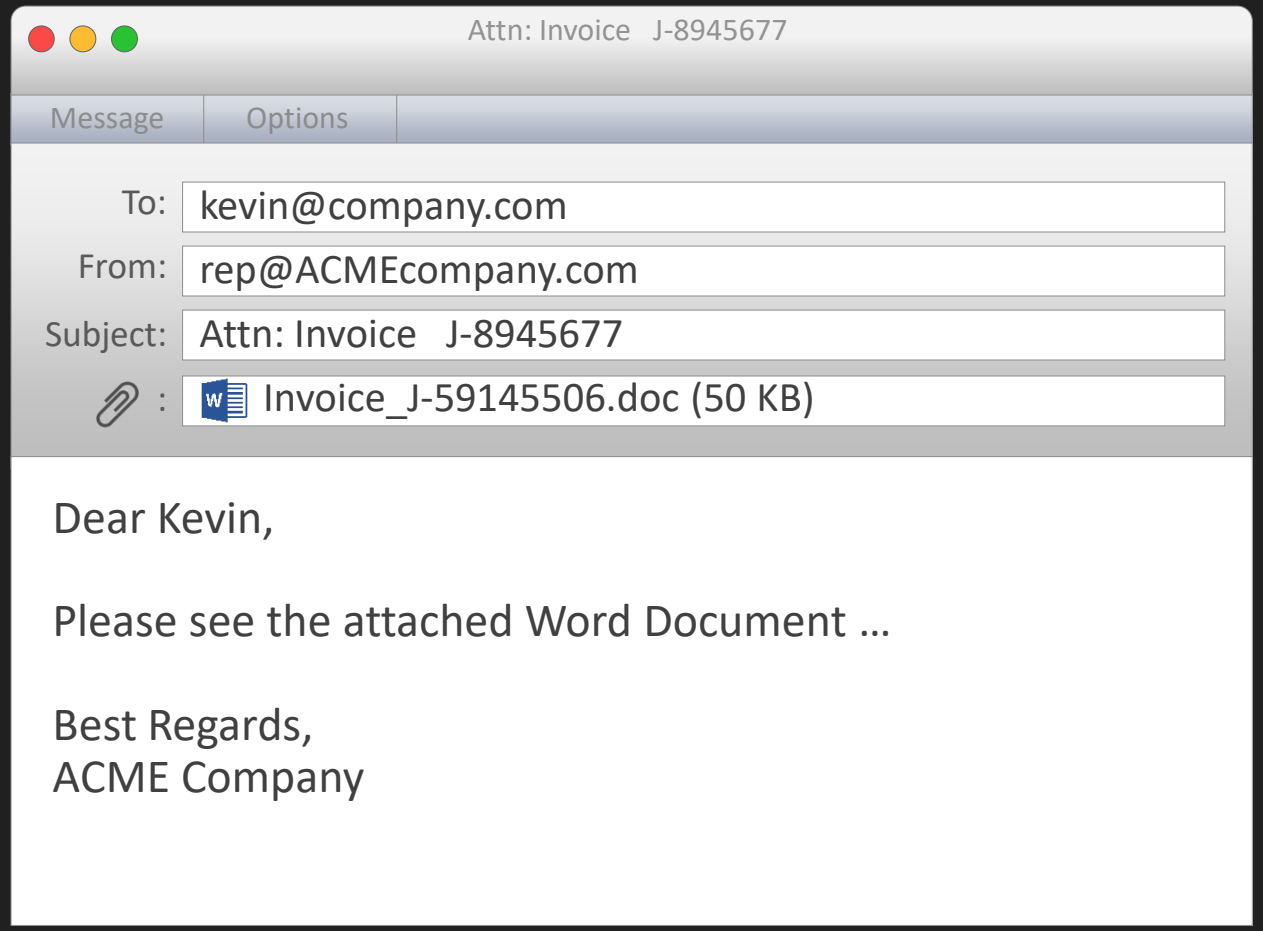
Copyright 2017, Symantec Corporation

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.Lockdrod.E
- **Social Networking** – ex. Locky
- **Exploit Kits** – 388k attacks blocked a day in 2016
- But mainly ransomware spreads via…

Copyright 2017, Symantec Corporation

Email Attacks



Symantec Sees Millions of Attacks per day sent via **Malicious Email**

Copyright 2017, Symantec Corporation

Internet Security Threat Report

ISTR

Best Practices & Solutions

Volume

22

Symantec

Copyright 2017, Symantec Corporation