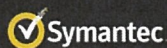


Threats, Trends, and Implications?

Presentation to:
New Mexico
Science, Technology & Telecommunications Committee

Thomas M. MacLellan
Director
Policy & Government Affairs
November 29, 2018
Thomas_MacLellan@Symantec.com



Symantec 2018

Copyright 2017, Symantec Corporation

Symantec's Unique Visibility into Today's Threat Landscape



200M
endpoints



70M attack sensors in
157 countries



182M web attacks
blocked last year



3.7T rows
of telemetry

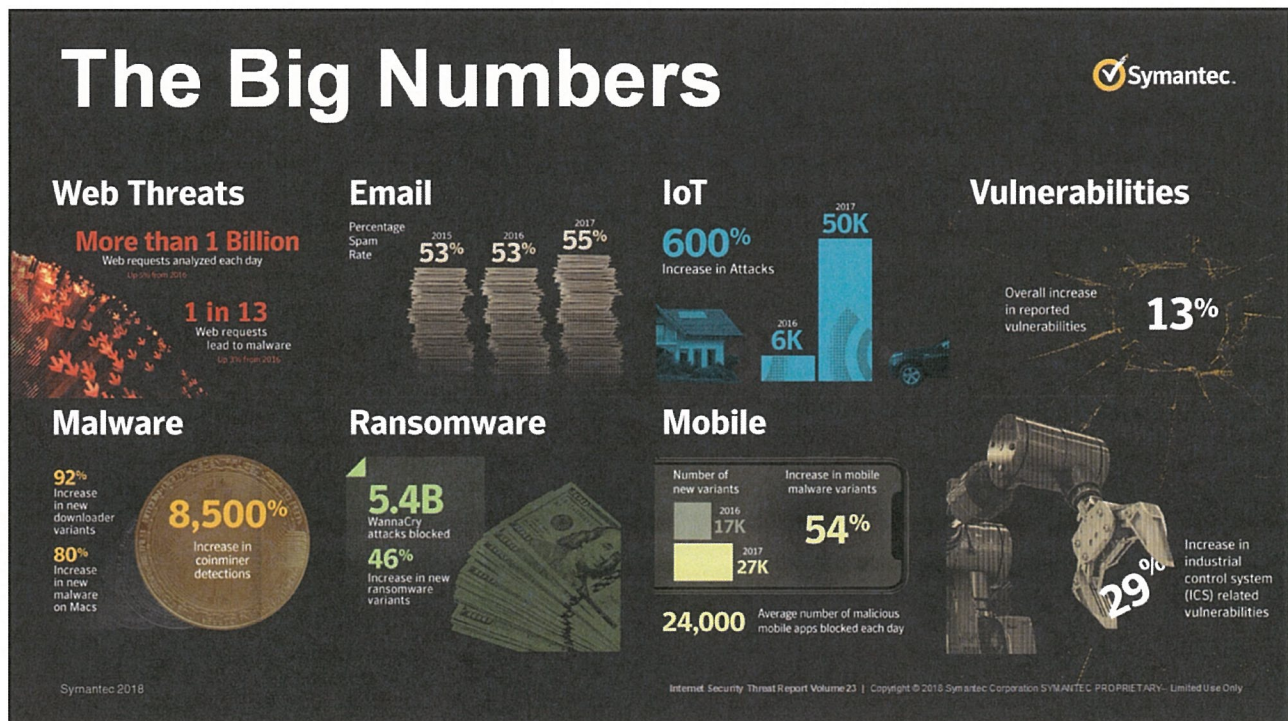
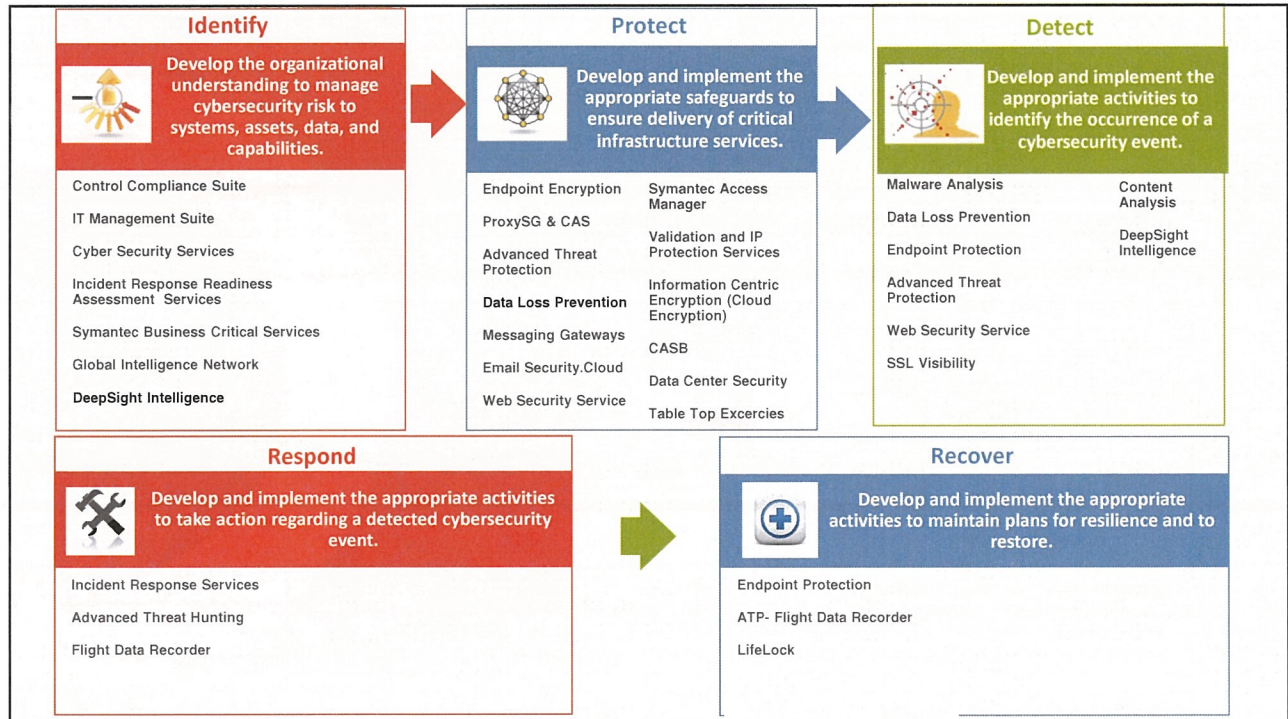


30% of world's enterprise
email traffic scanned/day



9 threat response centers
6 SOCs
3,500 FTEs Intel Analysts

Copyright © 2017 Symantec Corporation



New and Emerging Threats

- Ransomware and Cryptojacking
- Supply Chain
- Mobile
- Cloud
- IoT
- Critical Infrastructure
- Elections Security

ICTD
ICTD
ICTD
ISTR

Internet Security
Threat Report

Volume

23

 Symantec.

Ransomware and CryptoJacking

 Symantec.

Ransomware and Cryptojacking



Cybercriminals try to find new ways to generate revenue

Ransomware

- Detections stable at 1,242 per day in 2017 (-2%)
- Downloader detections increased by 92%
- 46% increase in new ransomware variants
- Average ransom down to \$522 from \$1,070

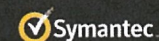
Shift to other attacks

- To coin mining e.g. VenusLocker shifted from ransomware to crypto mining
- To financial Trojans e.g. Emotet activity increased by 2,000% in Q4



Internet Security Threat Report Volume 23 | Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY - Limited Use Only Intel

Cryptocurrency malware



Coin mining malware:

- Misuse local resources to mine cryptocurrencies with CPUs and GPUs
- Number of blocked samples **increased by 8,500%** in 2017
- Focus is not on Bitcoin
 - Preference for coins that can still be mined with a CPU e.g. Monero
 - Monero is also more anonymous than Bitcoin

Criminals adapt known scam schemes for the age of cryptocurrencies

- Attacks against crypto exchanges
- Wallet theft
- Phishing
- Tech support scams
- Fake mobile apps

Internet Security Threat Report Volume 23 | Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY - Limited Use Only

8

Three main impacts of crypto currency mining



DEVICE PERFORMANCE

- Slower device
- CPU usage at 100%



ENERGY CONSUMPTION

- High energy consumption
- Fast battery drain
- Hard on mobile devices



SECURITY POSTURE

- Reflects badly on security posture

2 out of 3 victims are consumers
but targeting of organizations is increasing

Internet Security Threat Report Volume 23 | Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY - Limited Use Only

9

Predictions for Cryptojacking



BOTNETS

Distributed mining, either through conventional **botnets** of malware-infected **computers** and **IoT devices** or browser-based coinminers, hosted on websites.



TARGETING ORGANIZATIONS

Targeting of **corporate** or organizational networks in order to harness the power of servers or supercomputers.



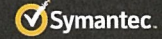
CLOUD HIJACKING

Cloud services offer the possibility of high-powered mining. This has a possible financial impact on **cloud customers** where they pay based on CPU usage.

Internet Security Threat Report Volume 23 | Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY - Limited Use Only

10

Ransomware Still a Real Threat



Petya Ransomware - Next Global Threat

+2

By: Mithun Sanghavi

Created 28 Jun 2017 0 Comments



Hello All,

On June 27th, 2017 we all became aware of a new variant of the Petya malware which is spreading over the Microsoft Windows SMB protocol. The malware appears to use the ETERNALBLUE exploit tool to accomplish this. This is the same exploit the WannaCrypt/WanaCry malware exploited to spread globally in May, 2017. Multiple organizations have reported network outages, including government and critical infrastructure operators.

Windows users should take the following general steps to protect themselves:

- Apply security updates in MS17-010
- Block inbound connections on TCP Port 445
- Create and maintain good back-ups so that if an infection occurs, you can restore your data.

Overview

Petya is a ransomware family that works by modifying the Windows system's Master Boot Record (MBR), causing the system to crash. When the user reboots their PC, the modified MBR prevents Windows from loading and instead displays an ASCII Ransom note demanding payment from the victim.



Corporation SYMANTEC PROPRIETARY - Limited Use Only

Ransomware Still a Major Threat



The screenshot shows a web browser displaying an Engadget article. The URL is https://www.engadget.com/2018/06/06/atlanta-ransomware-attack-its-truck-mission-critical-services/. The article title is "Atlanta ransomware attack may cost another \$9.5 million to fix". The author is Jon Fingas, @jonfingas, with a bio "06:06:18 in Security". The article has 8 comments and 564 shares. The main text discusses the "Samsam" ransomware attack on Atlanta's government, stating that more than a third of Atlanta's 424 necessary programs were knocked offline or partly disabled, and close to 30 percent of those affected apps were "mission critical" -- that is, vital elements like the court system and police. The government initially reckoned that essential programs were safe. Department leaders had elaborated on the damage earlier in the week. The City Attorney's office lost all but six of its 77 computers and 10 years' worth of documents, while the police lost their dash cam recordings. Crucially, the cost of cleaning up the attack is likely to balloon as well. Rackley estimated that Atlanta would need another \$9.5 million in the next year to recover, or well past the \$2 million it had spent as of April. There's a good chance the figures could keep growing, too. Deputy CFO John Gaffney warned that the city was still in the "ransomware phase" and had not yet...

Symantec

EC PROPRIETARY - Limited Use Only

Some Good (but rare) News.





THE UNITED STATES
DEPARTMENT OF JUSTICE

HOME ABOUT AGENCIES RESOURCES NEWS CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice
Office of Public Affairs

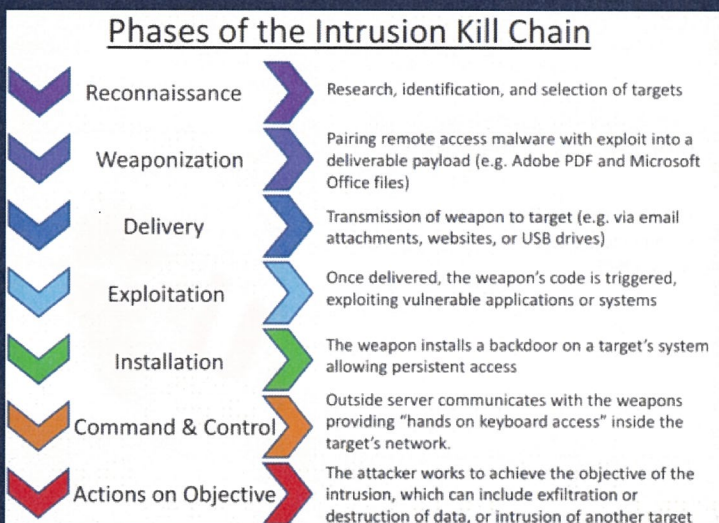
FOR IMMEDIATE RELEASE Wednesday, November 28, 2018

Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over \$30 Million in Losses

A federal grand jury returned an indictment unsealed today in Newark, New Jersey charging Faramarz Shahi Savandi, 34, and Mohammad Mehdi Shah Mansouri, 27, both of Iran, in a 34-month-long international computer hacking and extortion scheme involving the deployment of sophisticated ransomware, announced Deputy Attorney General Rod J. Rosenstein, Assistant Attorney General Brian A. Benzckowski of the Justice Department's Criminal Division, U.S. Attorney Craig Carpenito for the District of New Jersey and Executive Assistant Director Amy S. Hess of the FBI.

The six-count indictment alleges that Savandi and Mansouri, acting from inside Iran, authored malware, known as "SamSam Ransomware," capable of forcibly encrypting data on the computers of victims. According to the indictment, beginning in December 2015, Savandi and Mansouri would then allegedly access the computers of victim entities without authorization through security vulnerabilities, and install and execute the SamSam Ransomware on the computers, resulting in the encryption of data on the victims' computers. These more than 200 victims included hospitals, municipalities, and

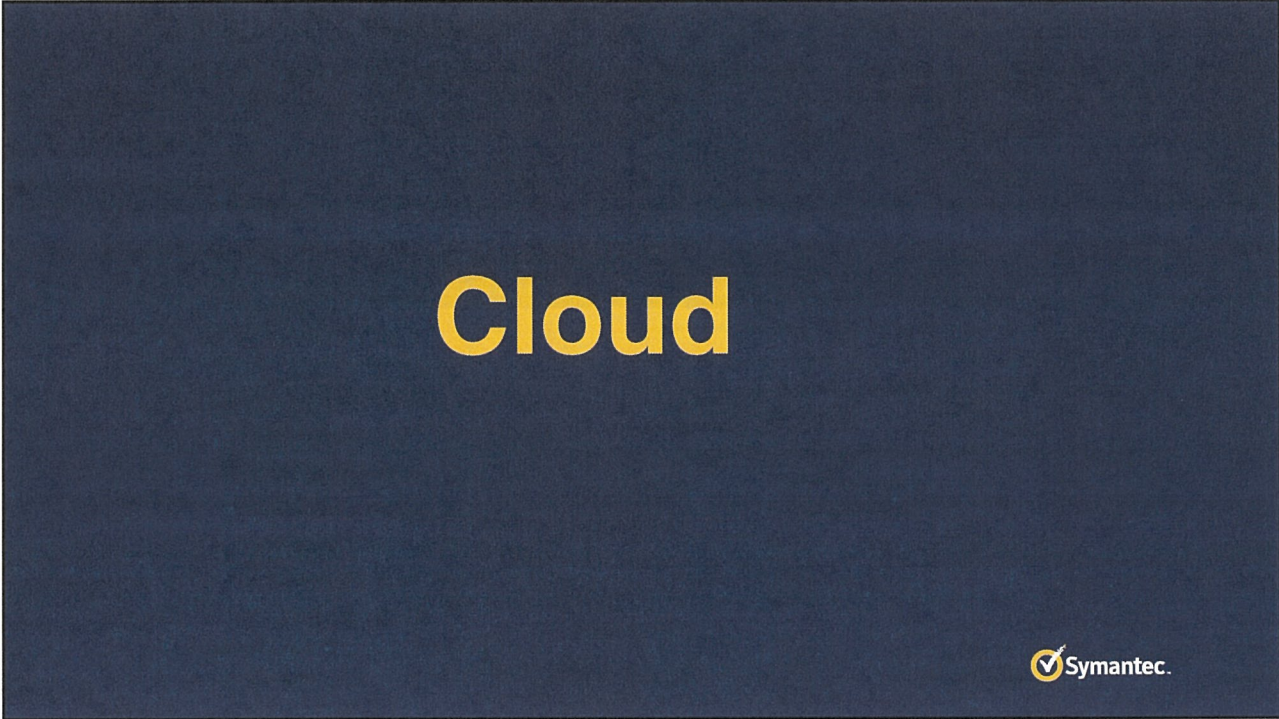
How the bad guys do it. (And why email isolation is so important.)

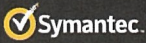


Some Names To Remember:

- ✓ Petya
- ✓ SamSam
- ✓ Emotet
- ✓ Mirai
- ✓ WannCry
- ✓ Qakbot

The List Will continue to grow.



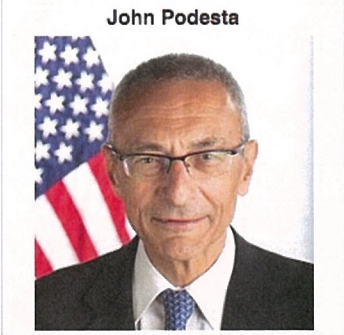


John Podesta

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]

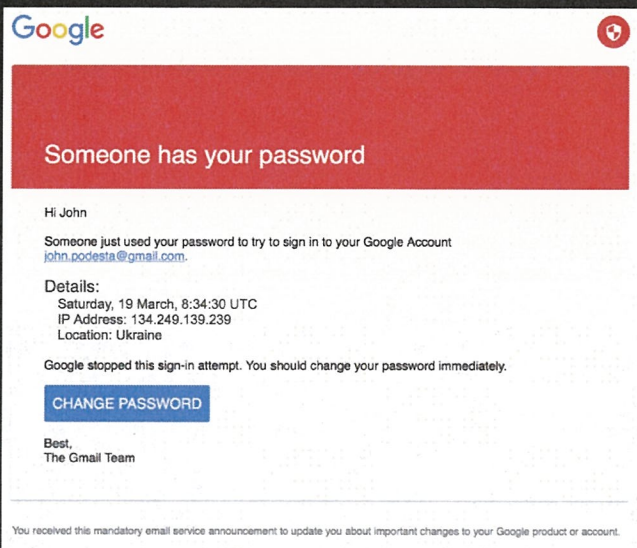
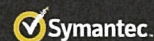
He is the former president, and now Chair and Counselor, of the Center for American Progress (CAP), a liberal think tank in Washington, D.C., as well as a Visiting Professor of Law at the Georgetown University Law Center. Additionally, he was a co-chairman of the Obama-Biden Transition Project.^{[3][4]}



John Podesta

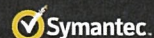
2017 Internet Security Threat Report | Volume 22
Internet Security Threat Report Volume 23 | Copyright © 2018 Symantec Corporation. SYMANTEC PROPRIETARY - Limited Use Only
16

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

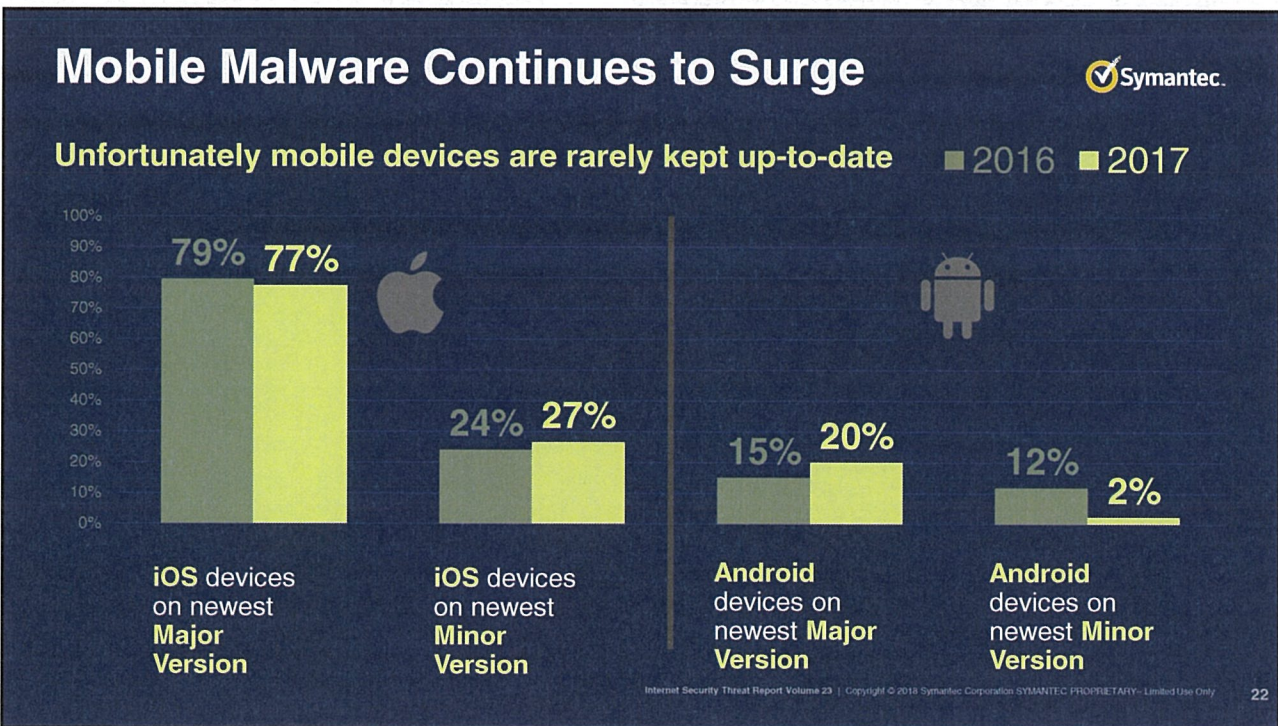
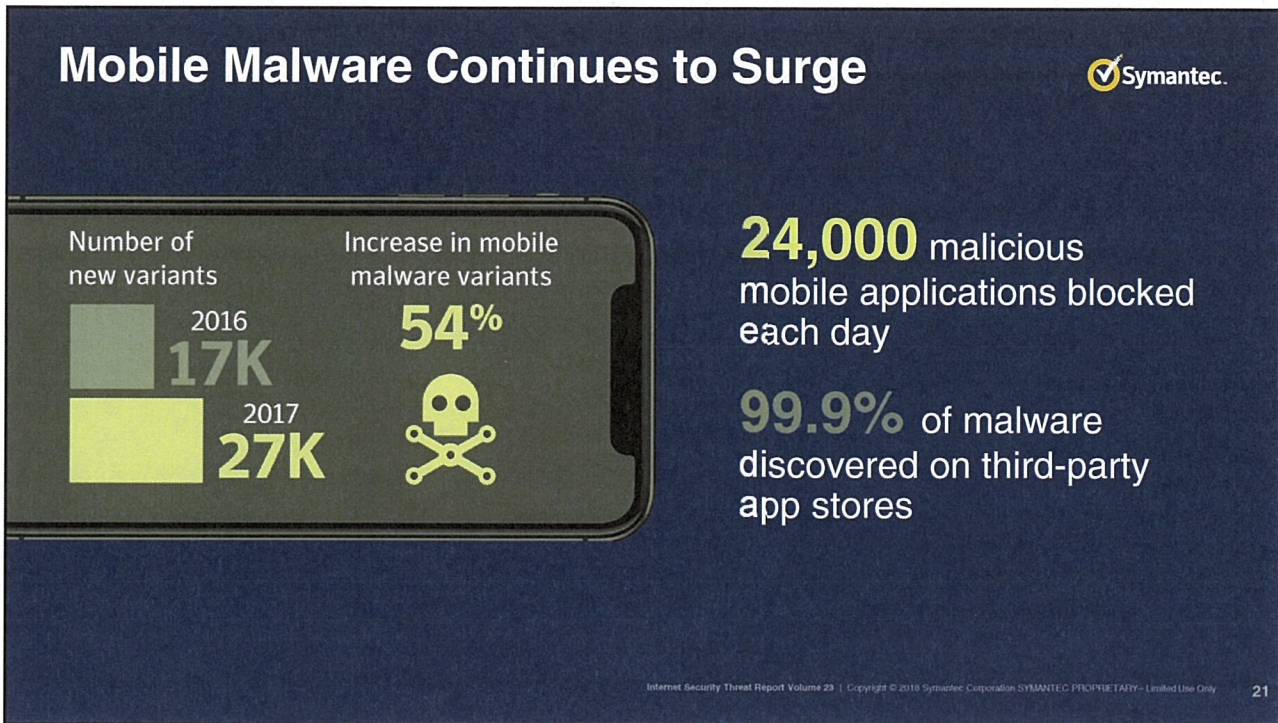
Anatomy of a Targeted Phishing Attack



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.

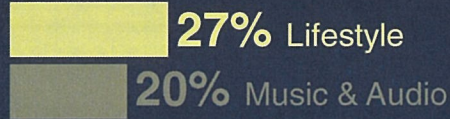
Mobile Threats



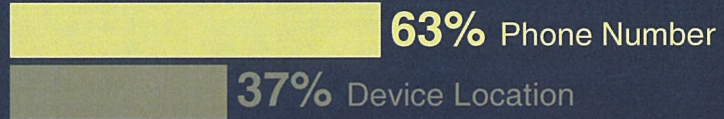
Privacy on mobile phones



App categories that have the most malicious mobile apps are:



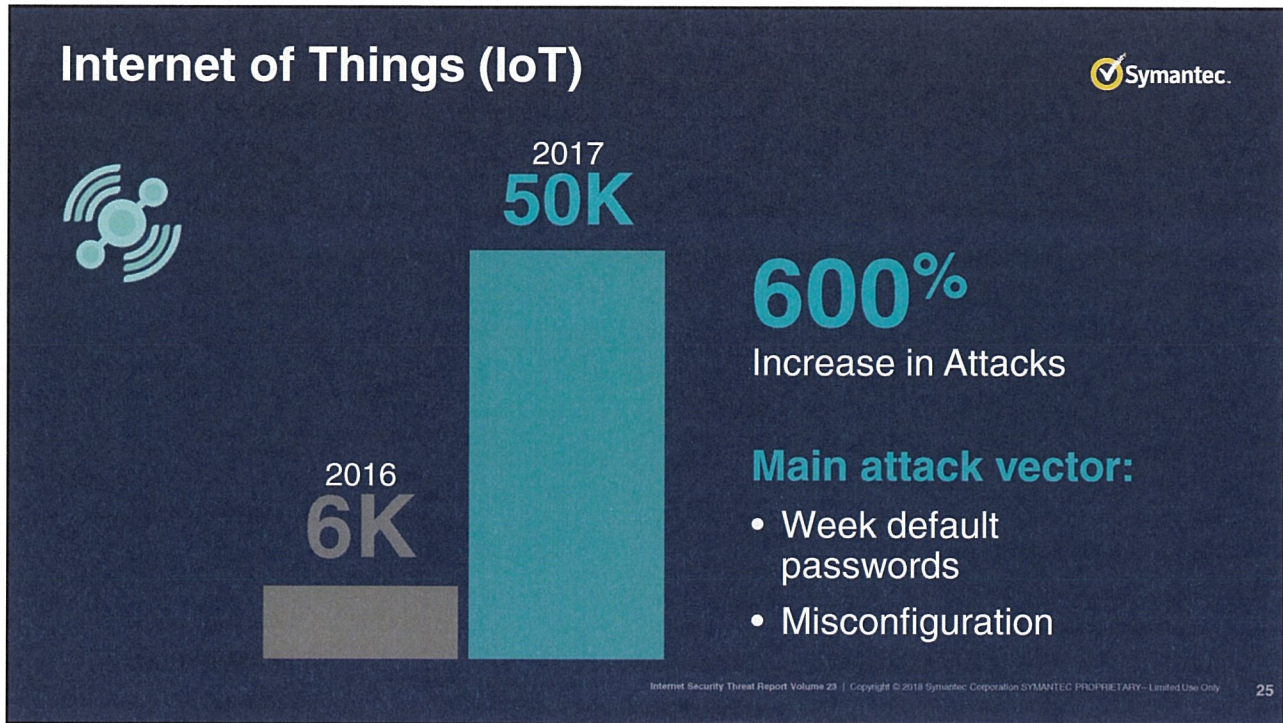
Leaky Apps – what sensitive information do they most often leak?



20% Percent increase in grayware in 2017

IoT





Supply Chain Attacks

Attacking the software supply chain ...



Definition: *Implanting a piece of malware into an otherwise legitimate software package at its usual distribution location; This can occur during production at the software vendor, at a third-party storage location, or through redirection.*

... Is an extension of the **“Living off the Land”** attack trend

Fewer exploitable zero day vulnerabilities available

Only **27%** of targeted attack groups ever used zero days

Trojanized updates are difficult to identify

Trusted domain, digitally signed, and trusted update process

Why?



Trust

Infiltration of well-protected organizations by leveraging a trusted channel

Fast

number of infections can grow quickly as users update automatically

Focus

Targeting of specific regions or sectors

Reach

Infiltration of isolated targets, such as those in industrial environments

Hidden

Difficult for victims to identify attacks as trusted processes are hijacked

Privileges

May provide attacker with elevated privileges during installation

Three different methods to achieve their goal

Compromising the software
supplier directly

Hijacking DNS,
domains, IP routing
or network traffic

Hijacking
third-party
hosting services



Symantec 2018

Internet Security Threat Report Volume 23
Copyright © 2018 Symantec Corporation
SYMANTEC PROPRIETARY - Limited Use Only

Critical Infrastructure





Home > Blogs > Security Response

Security Response

Symantec Official Blog +2

Symantec. **Dragonfly: Western energy sector targeted by sophisticated attack group**

Symantec Security Response
Resurgence in energy sector attacks, with the potential for sabotage, linked to re-emergence of Dragonfly cyber espionage group

By: Symantec Security Response **SYMANTEC EMPLOYEE**

Created 06 Sep 2017 0 Comments 简体中文, 日本語

0 1261

The energy sector in Europe and North America is being targeted by a new wave of cyber attacks that could provide attackers with the means to severely disrupt affected operations. The group behind these attacks is known as Dragonfly. The group has been in operation since at least 2011 but has re-emerged over the past two years from a quiet period following exposure by Symantec and a number of other researchers in 2014. This "Dragonfly 2.0" campaign, which appears to have begun in late 2015, shares tactics and tools used in earlier campaigns by the group.

The energy sector has become an area of increased interest to cyber attackers over the past two years. Most notably, disruptions to Ukraine's power system in 2015 and 2016 were attributed to a cyber attack and led to power outages affecting hundreds of thousands of people. In recent months, there have also been media reports of attempted attacks on the electricity grids in some European countries, as well as reports of companies that manage nuclear facilities

Symantec 2018 Written by ucs.a@symantec.com Internet Security | Annual Report Volume 23 | Copyright © 2018 Symantec Corporation. SYMANTEC PROPRIETARY - Limited Use Only

Elections Security



It's Not Just the Ballot Box.



Three Key Battlegrounds for Election Security

Election security is a key to maintaining our democracy. To preserve the integrity of our elections, three critical battlegrounds require focus and attention.



Election infrastructure

Protecting the hardware, software, databases, networks, and processes used for capturing and tallying votes is essential for maintaining elections integrity.

Election officials must institute best practices—with people, processes, and technology—to protect their voting infrastructure.



Election personnel

Since most attacks target individuals, it's important for elections officials and campaign managers to educate their employees and volunteers on potential threats and critical best practices.

Good news—these efforts require only good common sense, cost little to nothing, and help to lessen vulnerabilities.



Information warfare

Perhaps the most difficult threat to address. Education and best practice sharing are key to changing behaviors.

As a user of social media, taking care of your feed, vetting information you post for accuracy and ensuring a trusted and legitimate source from where they came, prevents you from being an unwitting pawn in a disinformation campaign.

Symantec 2018

Internet Security Threat Report Volume 23 | Copyright © 2018 Symantec Corporation. SYMANTEC PROPRIETARY - Limited Use Only

Cyber crime is changing ...

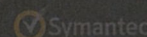


Trends to Consider

- Change in Motivation From Theft to Sabotage and Subversion
- Impact of Market Forces
- Professionalization and Commoditizing of Attacks
- Evolution of the Tactics, Techniques, and Procedures (TTPs) of Targeted Attackers
- Growing Threat Surface

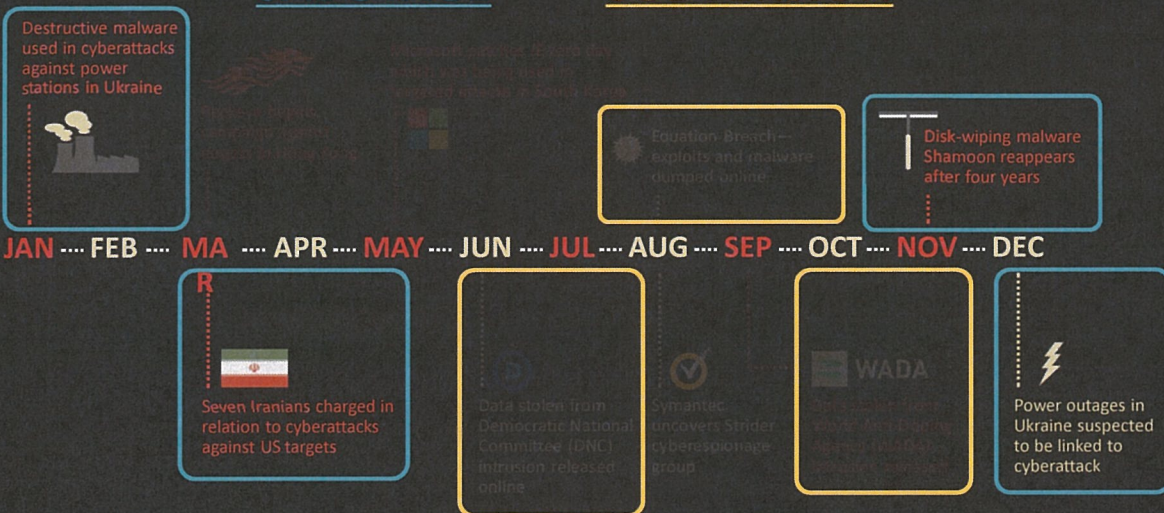


Changes in Motivation. Not just economic gain.

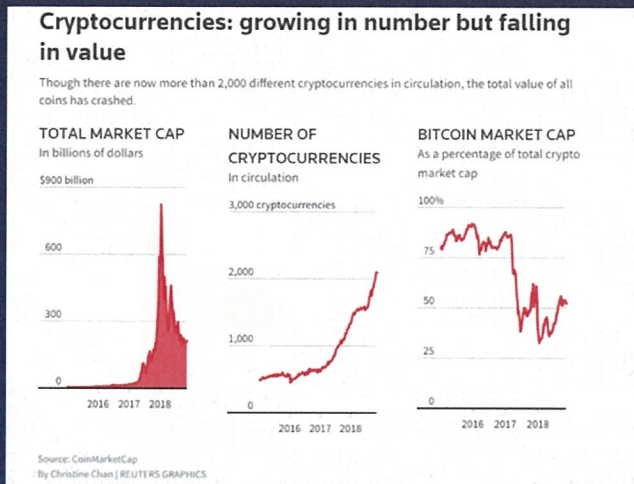


SABOTAGE

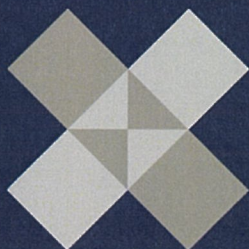
SUBVERSION



Emerging Market Forces to Consider: Where do the bad guys go next?



Targeted Attack Trends



“Attacks carried out by organized groups, directed at a specific target or targets”

- Analysis of TTPs of 140 groups tracked by Symantec
- 10% increase in targeted attacks in 2017
- Primary motive is espionage, followed by financial and disruption
- Continuing to opt for “Living off the Land” techniques

Targeted Attacks by the Numbers



Internet Security Threat Report Volume 23 | Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY – Limited Use Only 39

Growing Threat Surface



- Mobile
- IoT
- Smart Cities
- AI
- Autonomous Vehicles

Internet Security Threat Report Volume 23 | Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY – Limited Use Only 40

So What? What Should Policymakers Care About?

- Effective Enterprise Governance Structure
- Adoption of NIST Framework
- Changing Budgeting and Procurement Practices
- Platform-Based Approaches
- Elections Security
- Growth in Identity
- Know the Threats, Get Briefed



Questions?



