Resiliency for Today's Cyber-Ecosystems

Association of Environmental Authorities

March 14, 2018

MERCADIEN

Lets Get Started

- Presenter(s)
- Mercadien Overview
- Datto Overview

How did we get here?
....The Internet of Things / Big Data

The things around us are increasingly computerized, and increasingly connected to the Internet. And most of them are listening. Our smartphones and computers listen to us when we're making audio and video calls...your microphones are always there, and there are ways hackers, government or a clever company can turn those microphones on without our knowledge. If you have an iPhone, the voice-processing system Siri listens, if you have an Android, "OK Google" is listening, and so does Amazon's voice-activated system Echo (Alexa – Dollhouse incident). Facebook has the ability to turn your smartphone's microphone on when you're using the app.

How did we get here?
....The Internet of Things / Big Data

If you have an Internet-connected smart TV, you can turn on a voice command feature that saves you the trouble of finding the remote, pushing buttons and scrolling through Menus...BUT... making that feature work requires the television to listen to everything you say. And what you say isn't just processed by the television; it’s forwarded over the internet for remote processing.

How did we get here?
....The Internet of Things / Big Data

Our computers are paying attention. Google "listens" to everything you write, and shows you advertising based on it. Facebook does the same with everything you write on that platform, and even listens to the things you type but don't post.

Skype data has been accessible to the NSA's “snoops" since 2011. It's not just the devices that listen; most of this data is transmitted over the Internet. Samsung sends it to a "third party" in its policy statement.

That third party (most have never heard of) – Nuance....turns the voice into text, which is retained. Most of the other companies that are listening save your data for an indefinite period of time as well.

How did we get here?
....The Internet of Things / Big Data

This data is a treasure trove for criminals....we are learning again and again as hundreds of millions of customer records are repeatedly stolen. The Internet of Things is full of listeners. Newer cars contain computers that record speed, steering wheel position, pedal pressure, even tire pressure – insurance companies are listening.
And, of course, your cell phone records your precise location at all times you have it on – and even when you turn it off. If you have a smart thermostat, it records your house's temperature, humidity, ambient light. Fitness trackers record your movements and vital signs. Add security cameras, drones and other surveillance, and we're being watched, tracked, measured and listened to almost all the time.

How did we get here?
…"Big Data" gathering

Pentagon Data Breach Shows Growing Sophistication Of Phishing Attacks

by Sarah Kuranda on August 7, 2015, 11:40 am EDT

U.S. officials confirmed this week that the Pentagon was hit by a spearphishing cyberattack last

> What makes them more effective is the amount of advance knowledge the attackers have in order to trick the recipient into clicking on the link," Patterson said.

The attack occurred around July 25 and used what officials called a "sophisticated cyberattack." The suspected Russian hackers, which may or may not be connected with the Russian government, used automated social engineering tactics to gain information from employee social media accounts and then used that information to conduct a spearphishing attack, according to CNN, which first reported the attack.

Internet of Things...a little scary

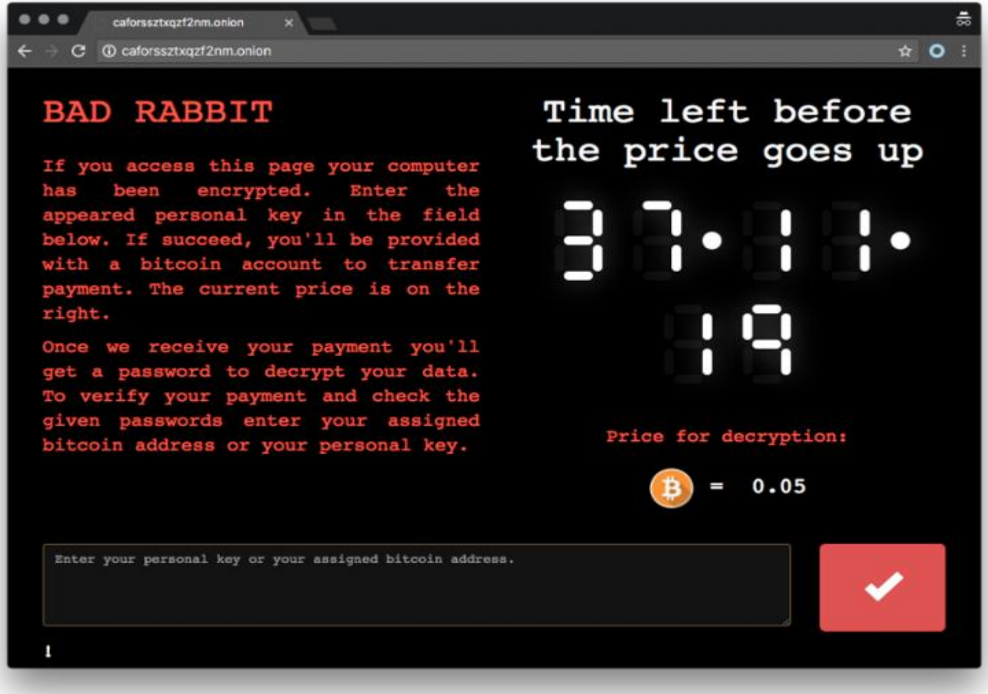
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAFE!

Escalation of events…

- Last Spring , the world experienced the wrath of a well-coordinated ransomware attacks, known as WannaCry and PetyaWrap. The attack caused Britain's HS to cancel surgeries and a wide array of Russian and Chinese private and public institutions to be crippled most of the day.
- Last May through July…Equifax had 143 million records breached due to an open-source software designed to create Java web-applications. We now know it was an older vulnerability that could have been “patched”.

Escalation of events…

On Tuesday, Oct. 24th, 2017 a strand of ransomware named Bad Rabbit appeared in Russia and the Ukraine and spread throughout the day.
The outbreak appears to have started via files on hacked Russian media websites, using the popular social engineering trick of pretending to be an Adobe Flash installer.
The ransomware demands a payment of about $275 (Bitcoin), from its victim; you have just 40 hours to pay.



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

37:11:19

Price for decryption:

₿ = 0.05

Enter your personal key or your assigned bitcoin address.

✓

Enter…23 NYCRR 500

NEW YORK STATE
DEPARTMENT of
FINANCIAL SERVICES

Regulation Background

- Enacted on March 1, 2017, the New York Department of Financial Services (DFS) issued a regulation designed to promote the protection of financial customer information, as well as the information technology systems of regulated entities.
- This regulation, 23 NYCRR 500 (DFS 500), requires each regulated entity to assess its specific risk profile and design a program that addresses its risks in a robust fashion.
- Regulated entities involve a broad range of businesses, including Credit-Unions, Banks, Credit-Card companies, Insurance companies, Consumer-Finance companies, Stock Brokerages, Investment Funds, Charitable Foundations, State-Regulated corporations and some Government-Sponsored enterprises.

The Basics

What is Ransomware?

YOUR MONEY OR YOUR DATA

The Basics…

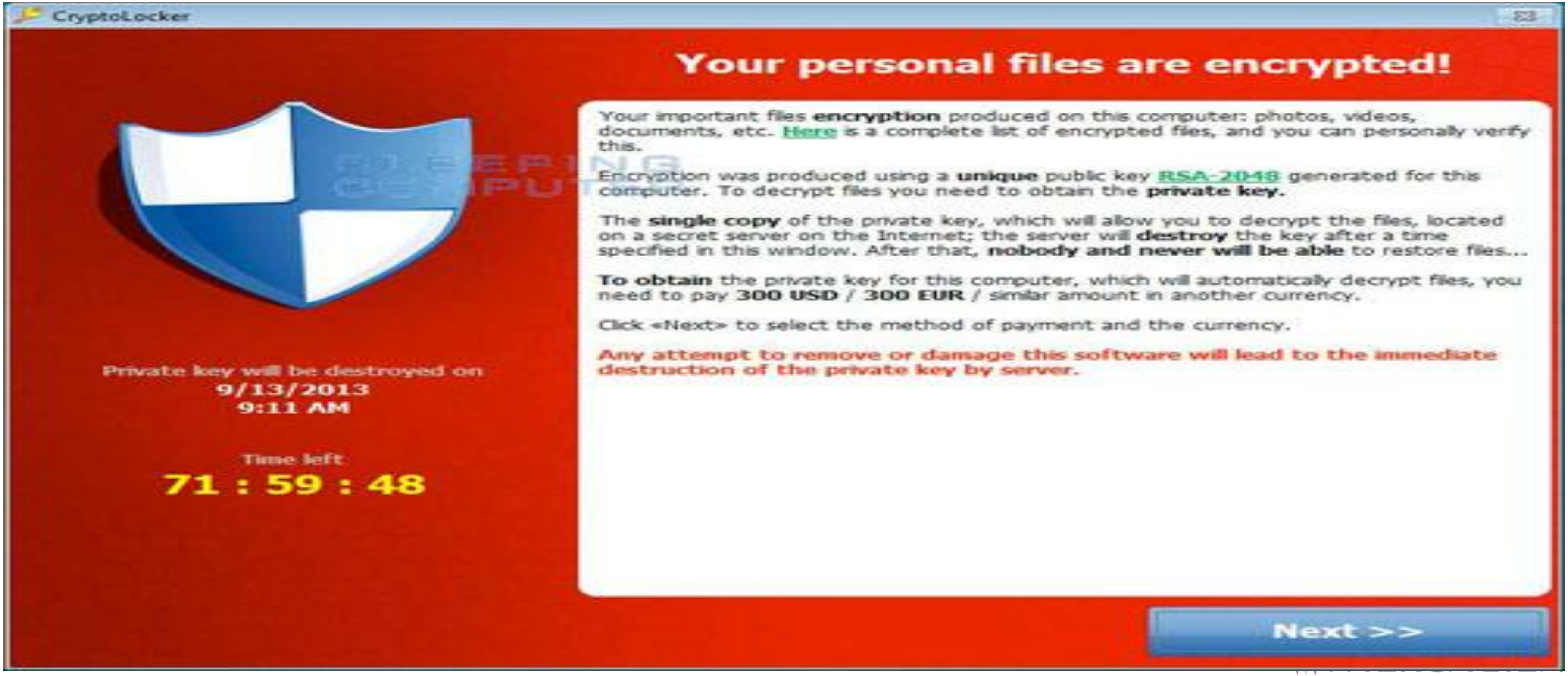
What is Ransomware?

- ✓ Advanced Algorithm is programmed
- ✓ Encrypts files so you can’t use them
- ✓ Encrypts all network shares
- ✓ Demands money (in Bitcoin) so you can gain access

Currency…

- Bitcoin is a digital, peer-to-peer payment system. Unlike traditional currency, Bitcoin does not rely on a central authority; it’s controlled by its users. Bitcoins can be acquired as a payment for goods and services, purchased on Bitcoin exchanges, or exchanged with others.
- The rise of Bitcoin and other crypto currencies has made it possible, safe, and easy, to demand and receive payments and transfer money anonymously. This has had a dramatic impact on the number and type of cybercrime opportunities; it’s the engine of cybercrime.

Ransomware…



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 files you 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 **300 USD / 300 EUR** / similar amount in another currency.

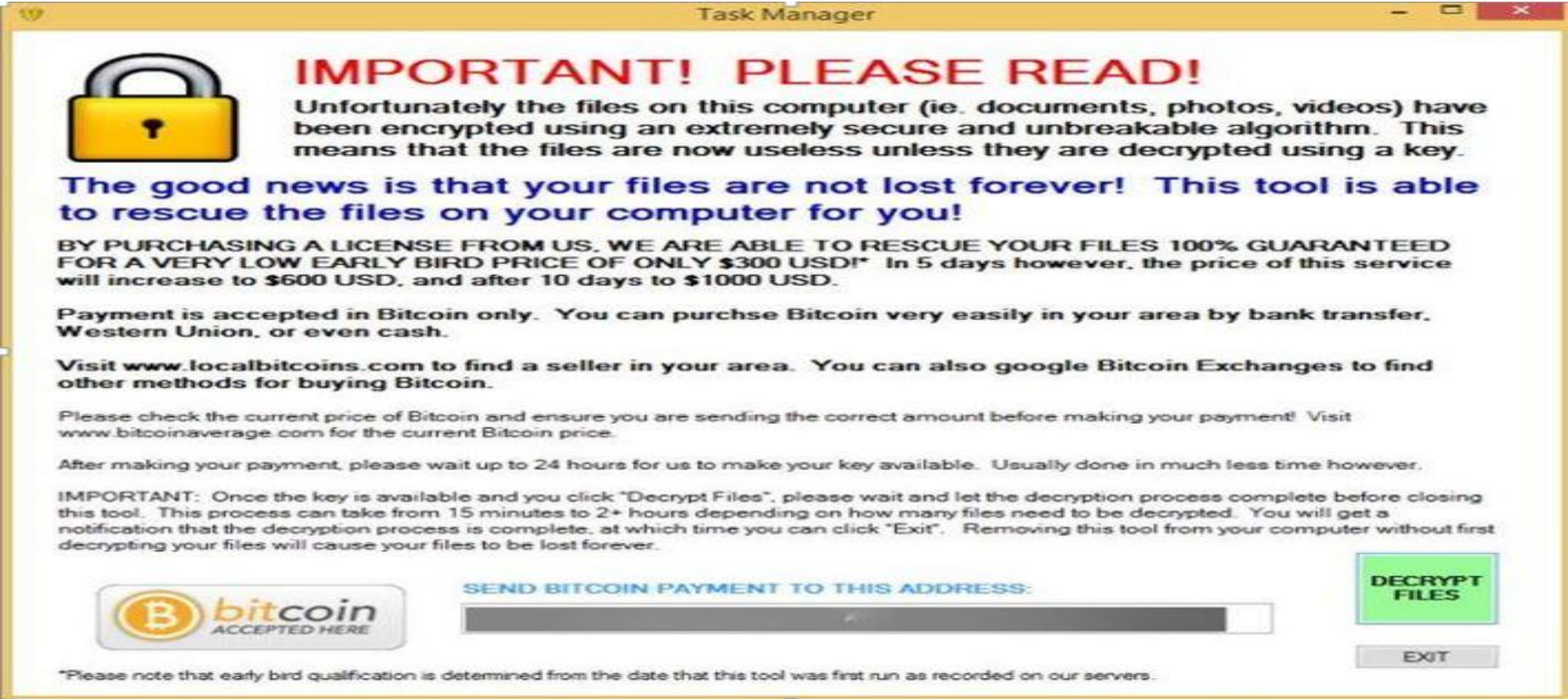
Click «Next» to select the method of payment and the currency.

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

Private key will be destroyed on
9/13/2013
9:11 AM

Time left
71 : 59 : 48

Ransomware…



IMPORTANT! PLEASE READ!

Unfortunately the files on this computer (ie. documents, photos, videos) have been encrypted using an extremely secure and unbreakable algorithm. This means that the files are now useless unless they are decrypted using a key.

The good news is that your files are not lost forever! This tool is able to rescue the files on your computer for you!

BY PURCHASING A LICENSE FROM US, WE ARE ABLE TO RESCUE YOUR FILES 100% GUARANTEED FOR A VERY LOW EARLY BIRD PRICE OF ONLY $300 USD!* In 5 days however, the price of this service will increase to $600 USD, and after 10 days to $1000 USD.

Payment is accepted in Bitcoin only. You can purchse Bitcoin very easily in your area by bank transfer, Western Union, or even cash.

Visit www.localbitcoins.com to find a seller in your area. You can also google Bitcoin Exchanges to find other methods for buying Bitcoin.

Please check the current price of Bitcoin and ensure you are sending the correct amount before making your payment! Visit www.bitcoinaverage.com for the current Bitcoin price.

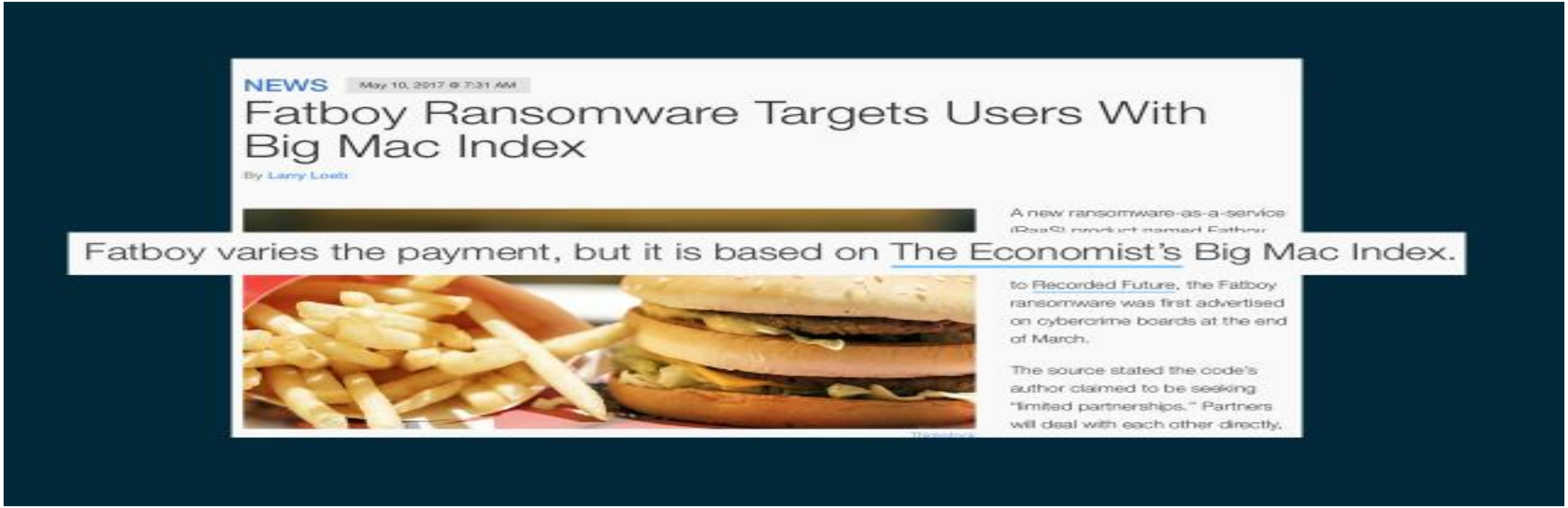
After making your payment, please wait up to 24 hours for us to make your key available. Usually done in much less time however.

IMPORTANT: Once the key is available and you click "Decrypt Files", please wait and let the decryption process complete before closing this tool. This process can take from 15 minutes to 2+ hours depending on how many files need to be decrypted. You will get a notification that the decryption process is complete, at which time you can click "Exit". Removing this tool from your computer without first decrypting your files will cause your files to be lost forever.

SEND BITCOIN PAYMENT TO THIS ADDRESS: [redacted]

*Please note that early bird qualfication is determined from the date that this tool was first run as recorded on our servers.

Types of Ransomware...



NEWS May 10, 2017 @ 7:31 AM

Fatboy Ransomware Targets Users With Big Mac Index

By Larry Loeb

A new ransomware-as-a-service (RaaS) product named Fatboy

Fatboy varies the payment, but it is based on The Economist's Big Mac Index.

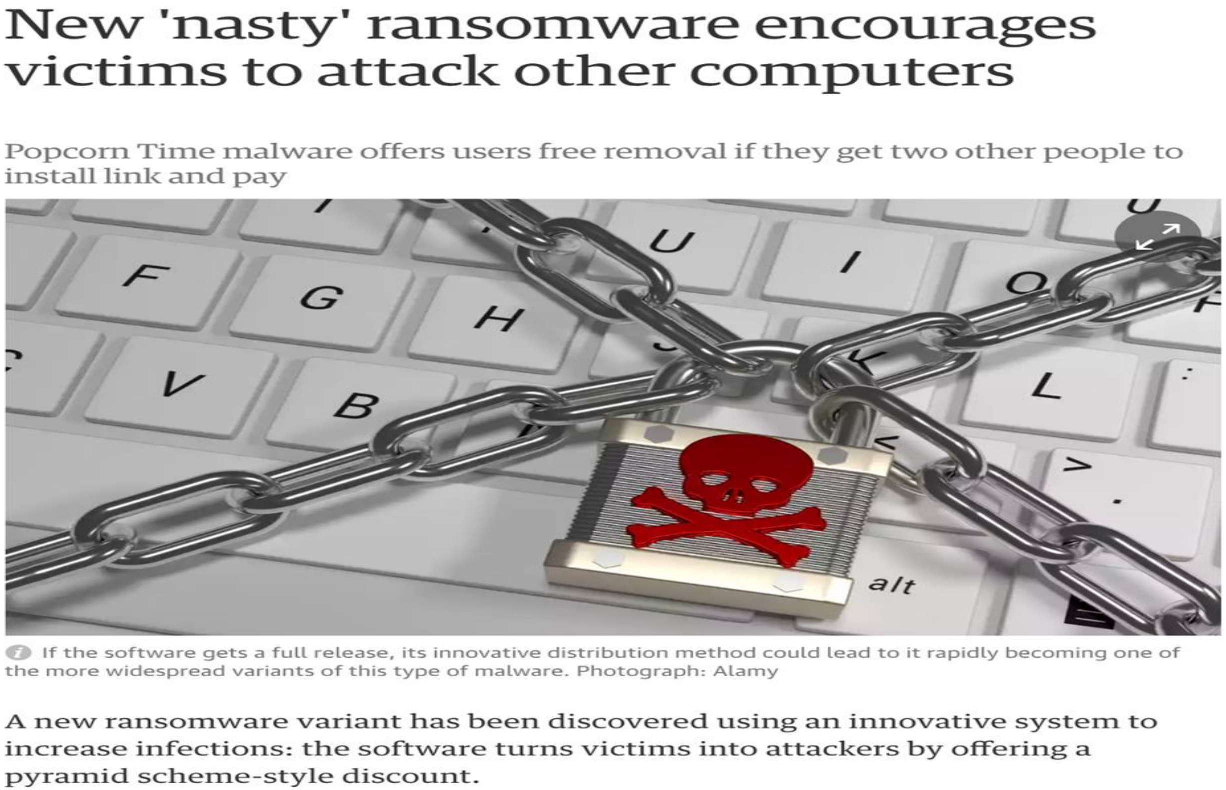
to Recorded Future, the Fatboy ransomware was first advertised on cybercrime boards at the end of March.

The source stated the code's author claimed to be seeking "limited partnerships." Partners will deal with each other directly.

Thinkstock

Attacking With Location-Specific Pricing...the malware has a novel way of pricing its bitcoin ransom: It's determined by the victim's location.

Types of Ransomware...



New 'nasty' ransomware encourages victims to attack other computers

Popcorn Time malware offers users free removal if they get two other people to install link and pay

If the software gets a full release, its innovative distribution method could lead to it rapidly becoming one of the more widespread variants of this type of malware. Photograph: Alamy

A new ransomware variant has been discovered using an innovative system to increase infections: the software turns victims into attackers by offering a pyramid scheme-style discount.

Actual Scam…

Verify your Security Information

9/21/2017 9:07 AM

PNC Alerts

PNC -recipients:;

Dear Customer **,**

We **resently** determined that **diferent** computers have tried to log on your account.

Multiple password failures automatically place your account on hold.

We now need more information to help us provide you with our secure service.

Click the link below to open a secure **browers** windows.

- **http../www.pnc.com/server/users/default/confirm**

You will need to fill out all the information required in order to protect your account.

Skype…

Be careful of ransomware-infested Skype ads!

Skype is a free service for consumers; it relies on advertising to turn a profit. As a result, most users regularly see banner ads on the video calling interface. Hackers have begun to exploit these advertisements by distributing fake ads that contain ransomware. Initial reports found that the fake ad was disguised as a critical Flash update. Clicking on the ad triggers a download of a seemingly innocuous HTML application named “FlashPlayer.hta”. If opened, the app would download malicious code that encrypts the victim’s files and holds them hostage until a ransom is paid.

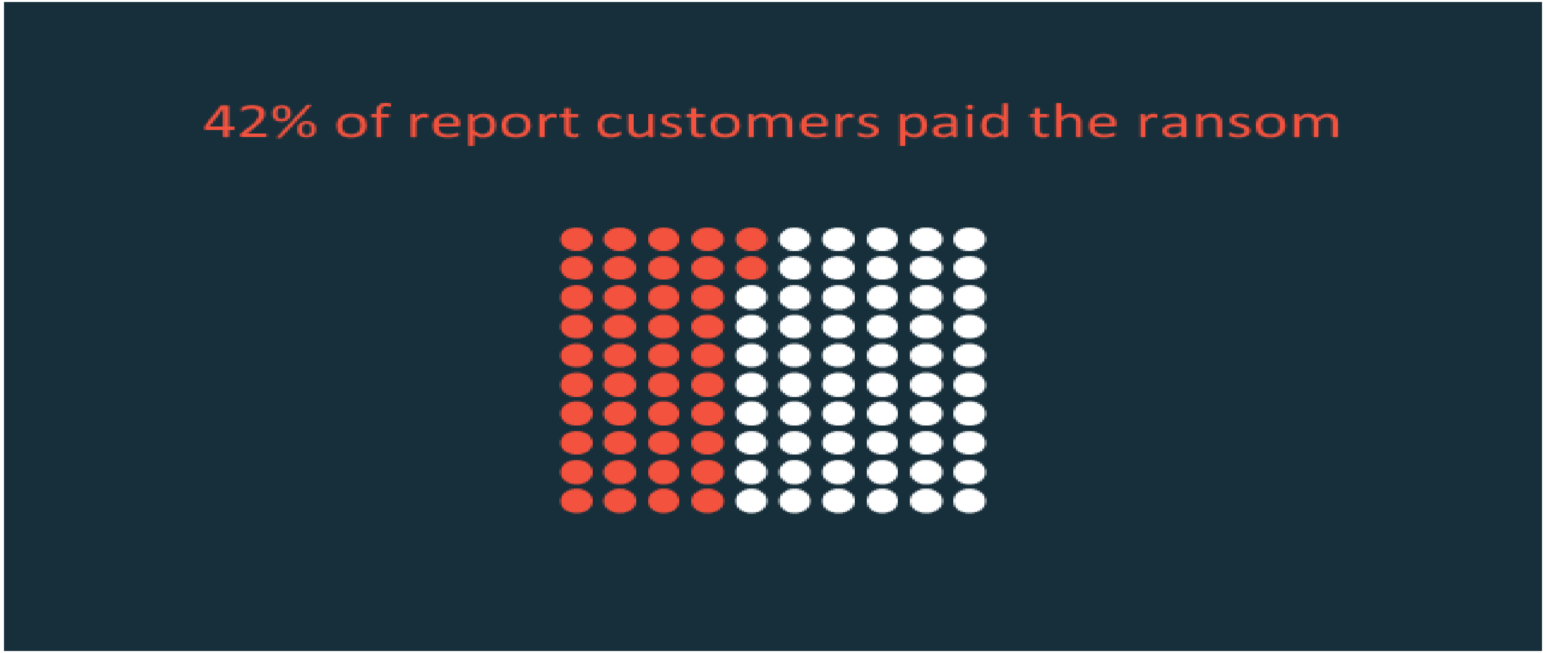
It’s not this guy anymore...

It’s a sophisticated network of highly skilled criminals….Global Criminal Economy

Costing Org’s over 75 Billion / year... Numbers are actually worse...

Less than 1 in 4 ransomware incidents are reported to the authorities

Outcomes...

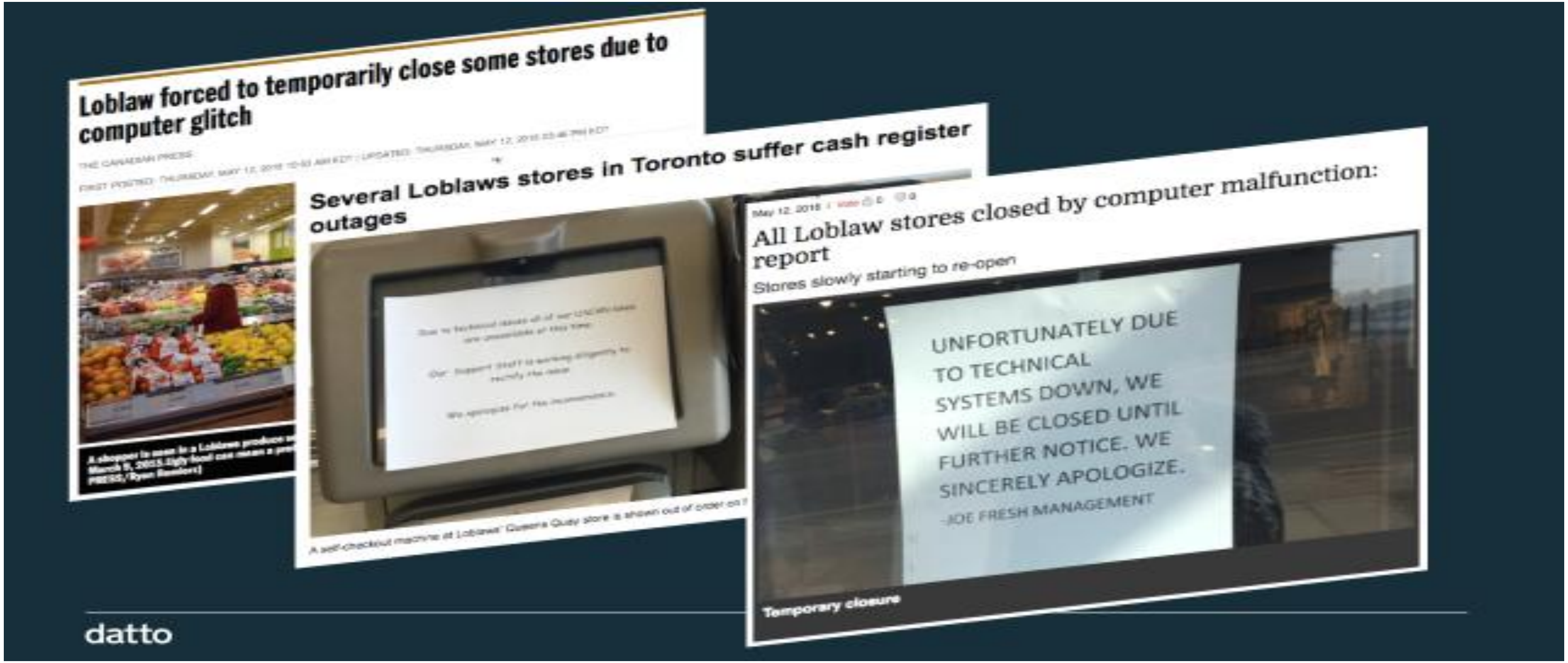


42% of report customers paid the ransom

Ethical Criminals...

1 in 4 who did so never recovered the data

Canadian Grocery…



Loblaw forced to temporarily close some stores due to computer glitch

THE CANADIAN PRESS

FIRST POSTED: THURSDAY, MAY 12, 2016 10:53 AM EDT | UPDATED: THURSDAY, MAY 12, 2016 03:46 PM EDT

A shopper is seen in a Loblaws produce s
March 9, 2015.Ugly food can mean a pro
PRESS/Ryan Remiorz)

Several Loblaws stores in Toronto suffer cash register outages

A self-checkout machine at Loblaws' Queens Quay store is shown out of order on t

May 12, 2016 | Vote 0 0

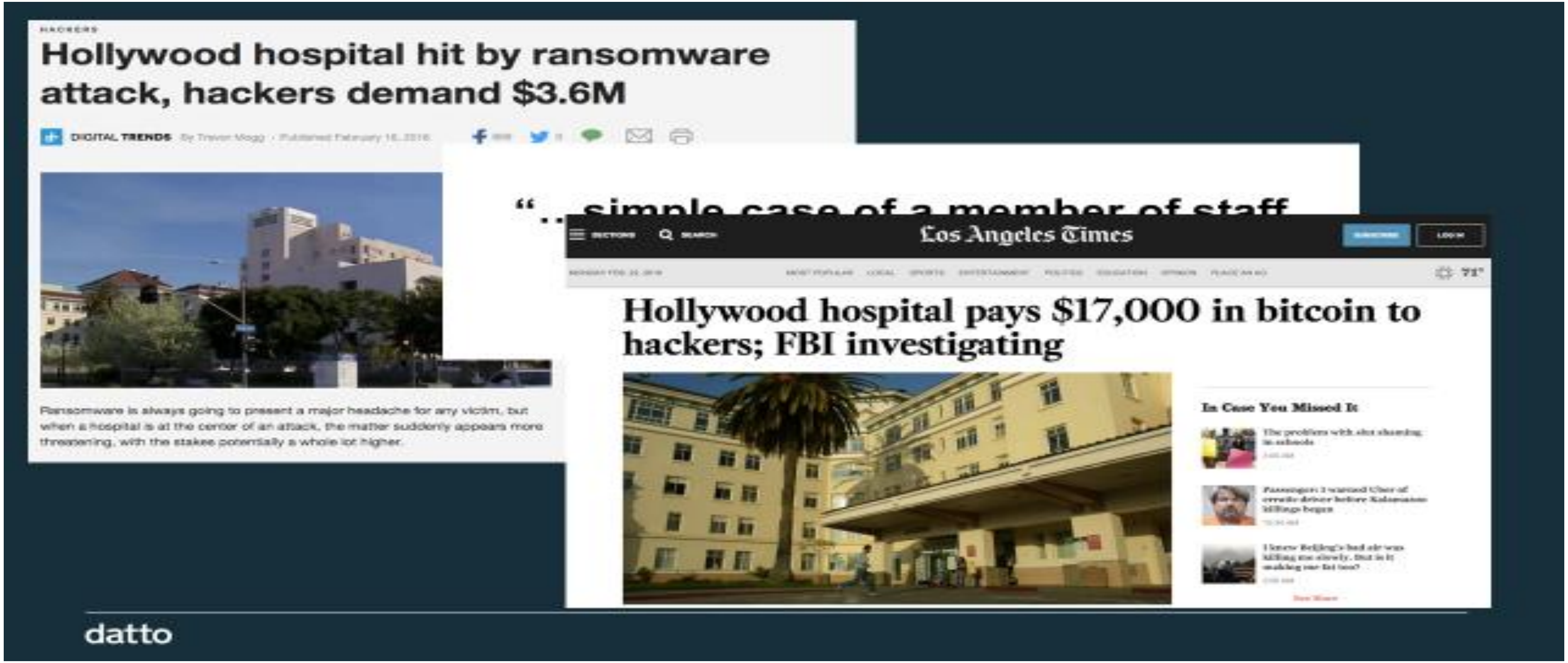
All Loblaw stores closed by computer malfunction: report

Stores slowly starting to re-open

Temporary closure

Due to technical issues all of our U-SCAN lanes are unavailable at this time.
Our Support Staff is working diligently to rectify the issue.
We apologize for the inconvenience.
UNFORTUNATELY DUE TO TECHNICAL SYSTEMS DOWN, WE WILL BE CLOSED UNTIL FURTHER NOTICE. WE SINCERELY APOLOGIZE.
-JOE FRESH MANAGEMENT
datto

Hollywood Hospital...



HACKERS

Hollywood hospital hit by ransomware attack, hackers demand $3.6M

DIGITAL TRENDS By Trevor Mogg · Published February 16, 2016

Ransomware is always going to present a major headache for any victim, but when a hospital is at the center of an attack, the matter suddenly appears more threatening, with the stakes potentially a whole lot higher.

"...simple case of a member of staff

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

In Case You Missed It

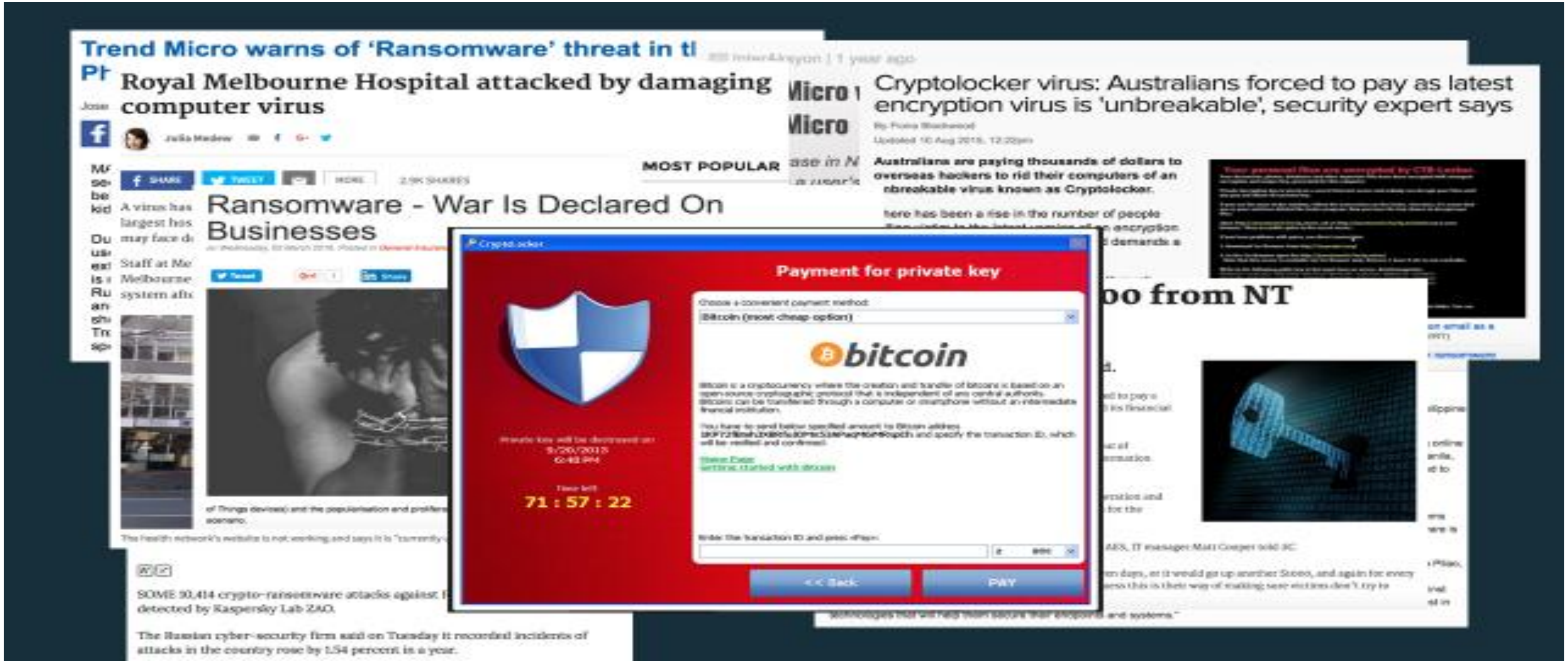
The problem with slut shaming in schools

Passenger: I warned Uber of erratic driver before Kalamazoo killings began

I knew Beijing's bad air was killing me slowly. But is it making me fat too?

See More

Melbourne Hospital...



Trend Micro warns of ‘Ransomware’ threat in tl

Royal Melbourne Hospital attacked by damaging computer virus

Julia Medew

MOST POPULAR

2.9K SHARES

A virus has largest hos may face d

Staff at Me Melbourne system aft

The health network's website is not working and says it is "currently

Ransomware - War Is Declared On Businesses

of Things devices) and the popularisation and prolifera scenario.

SOME 30,414 crypto-ransomware attacks against detected by Kaspersky Lab ZAO.

The Russian cyber-security firm said on Tuesday it recorded incidents of attacks in the country rose by 154 percent in a year.

Cryptolocker virus: Australians forced to pay as latest encryption virus is 'unbreakable', security expert says

Updated 10 Aug 2015, 12:22pm

Australians are paying thousands of dollars to overseas hackers to rid their computers of an nbreakable virus known as Cryptolocker.

here has been a rise in the number of people encryption demands a

Your personal files are encrypted by CTB-Locker.

oo from NT

AES, IT manager Matt Cooper told SC

en days, as it would go up another $1000, and again for every

technologies that will help them secure their endpoints and systems."

CryptoLocker

Payment for private key

Private key will be destroyed on 5/20/2015 6:48 PM

Time left

71 : 57 : 22

Choose a convenient payment method:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address and specify the transaction ID, which will be verified and confirmed.

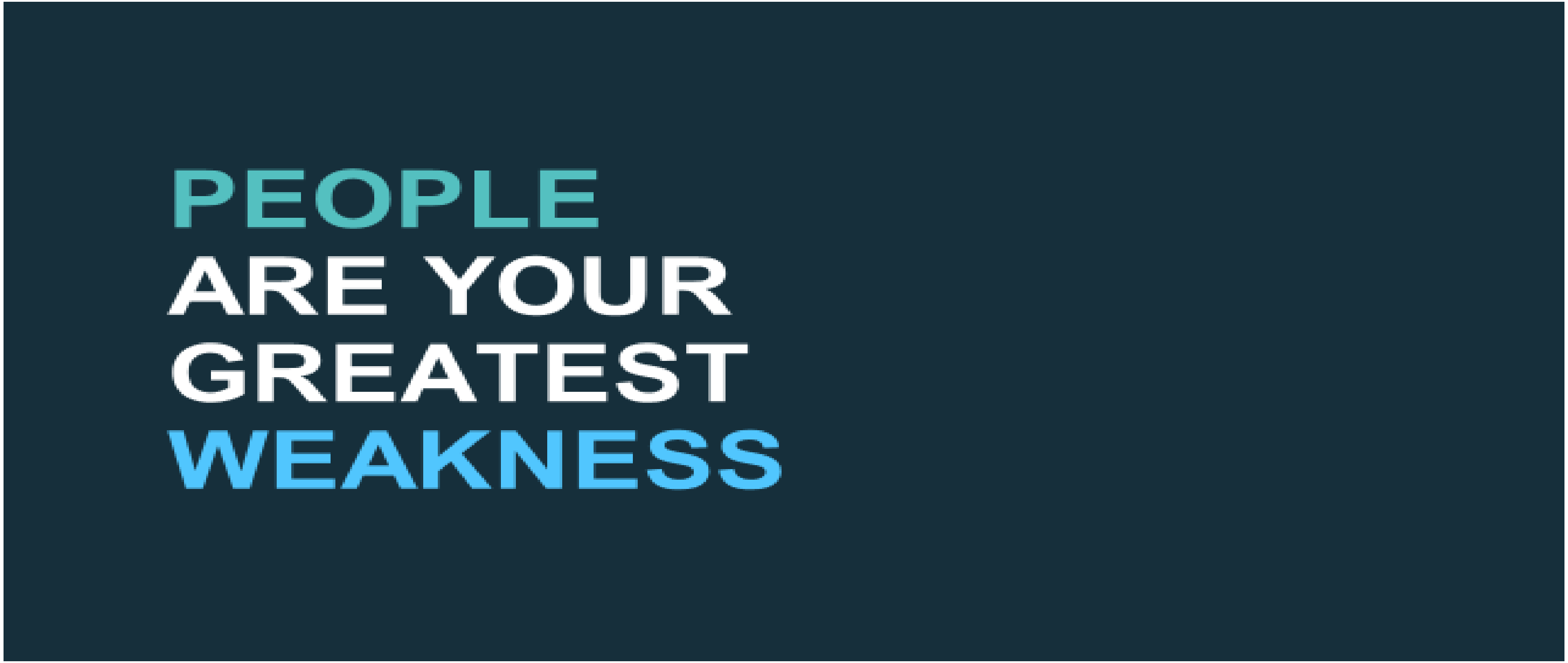
Home Page
Getting started with Bitcoin

Enter the transaction ID and press «Pay»:

Safe-Guarding....

How can you safe guard against Ransomware?

Not Outside but Inside...



PEOPLE
ARE YOUR
GREATEST
WEAKNESS

Protection from your own Staff

Safeguarding against Ransomware...

- Insiders are the cause of 91% of all incidents
- Of those, 71% are unintentional

Adoption of Prevention...

Safeguarding against Ransomware...

- Perform on-going education with employees
- Learn to identify Phishing schemes
- Stress the importance of caution when opening attachments and/or hyperlinks
- Create a culture of security

Crafting a Business Continuity Management (BCM) plan...

Business Impact Analysis (BIA)...the results of the BIA will form the foundation of the BCM plan ultimately put in place.

BCM plans should include (at a minimum)...

- Formal Risk Assessment
- Formal User-Awareness-Training
- Cyber-Liability-Insurance Coverage
- Mobile-Device-Management (MDM)
- Backup-Disaster-Recovery (BDR) program/service

Risk Assessment

- A Risk Assessment is NOT a Vulnerability Assessment...a VA is surface-level review of basic risks and points of entry – example...a walk around your home.
- Based on this example, a Risk Assessment allows entry into your home, movement around all rooms and seizure/removal/control of your posessions.
- A Risk Assessment is a MANDATORY requirement for nearly all audits in the private and now government sectors.

User-Awareness-Training

Cyber-attacks are quickly becoming more sophisticated. Regardless of the safety measures put in place, whether it be virus protection & malware software or physical firewalls, the weakest link in any organization is its employees. 91% of successful data breaches start with a spear-phishing attack. Users are targeted via email or embedded web links that are designed to cripple organizations. Our goal is to help train your employees to better understand how they are being targeted on a daily basis and what to avoid.

User Awareness Training

MCare User-Awareness-Training begins by gathering a base line of your user environment to help you understand how vulnerable you are to outside threats. Statistics are provided on how vulnerable your organization is to external phishing attempts. Users are then provided a series of interactive training videos that include demonstrations and examples of what to look for. Users are given a behind the scenes look on how hackers attempt to infiltrate an organization through them. Phishing tests are conducted monthly to not only help keep your employees on their toes, but also provide feedback on your user base and their ability to safely manage technology. Those users that fail to effectively identify phishing emails, will automatically be enrolled in additional training sessions.

What Can Cyber Insurance Cover?

Business Interruption

(1st Party)

- Restoration of data and systems
- Loss of income
- Extra expenses
- Dependent business interruption
- Reward expenses
- Ransom expenses

Crisis Management

(1st Party)

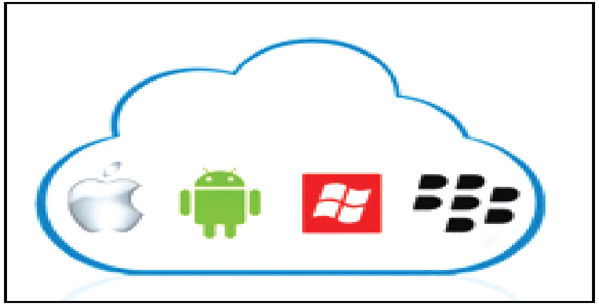
- Forensic analysis
- Legal costs
- Notification (state specific)
- Credit monitoring
- Call centers
- Reputation management

Lawsuits, Fines, and Penalties

(3rd Party)

- Invasion of privacy
- Negligence
- Failure to keep data secure
- Breach of implied contract
- Intellectual property infringement
- Libel or defamation
- PCI fines and penalties
- Regulatory defense & fines (HIPAA, HITECH, FACTA)

MCare-Mobile-Device-Management (MDM)



MDM is an easy-to-use cloud platform with all of the essential functionality for end-to-end management of today’s mobile devices including iPhones, iPads, Androids, Kindle Fire devices, Windows Phones and Blackberry smartphones.

MCare-Mobile-Device-Management (MDM)

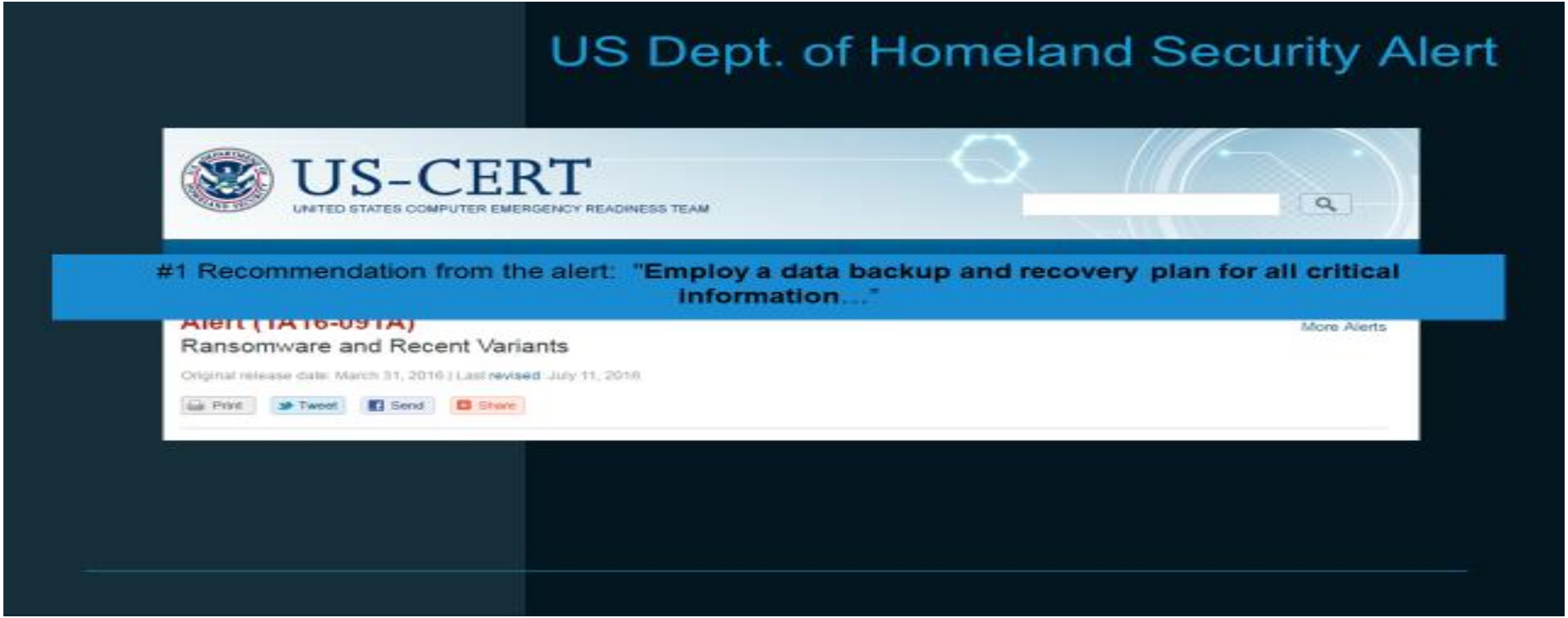
Mobile malware is the next big security threat to every enterprise. With the trend towards Bring Your Own Device (BYOD) and proliferation of mobile apps, your enterprise data is especially vulnerable to rogue apps and malicious websites. Organizations need a modern and comprehensive mobile security solution to detect, block and manage mobile malware and proactively address these concerns.

Key Benefits

- Safely and securely support both BYOD and corporate-owned devices
- Proactively manage mobile threats in real-time
- Reduce risk of sensitive data leakage of corporate and personal information
- Take automated actions to remediate mobile security risks

So...Reminders

A Disruption / Infection has occurred…Now What?



US Dept. of Homeland Security Alert

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

#1 Recommendation from the alert: **"Employ a data backup and recovery plan for all critical information…"**

Alert (TA16-091A)

Ransomware and Recent Variants

Original release date: March 31, 2016 | Last revised: July 11, 2016

Mike DePalma...