CryptoLocker FREE Report

For

Anyone

January 2015

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

Contents

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

Preface

This FREE report was written to help your company to defend itself from a very well defined attack – the ability to encrypt or steal your data.

CryptoLocker and similar ‘ransomware’ viruses are spreading by Emails, social media, and browsing the web. Currently the security community is trying to find ways to protect customers by this growing threat.

The CryptoLocker virus and its various versions, work by infecting your computer and encrypting all your data so you can no longer access it. It then demands a ransom in Bitcoin in order to decrypt your data to its original readable state. You have very limited options: pay the ransom or restore from a backup. There is no practical way to decrypt it yourself.

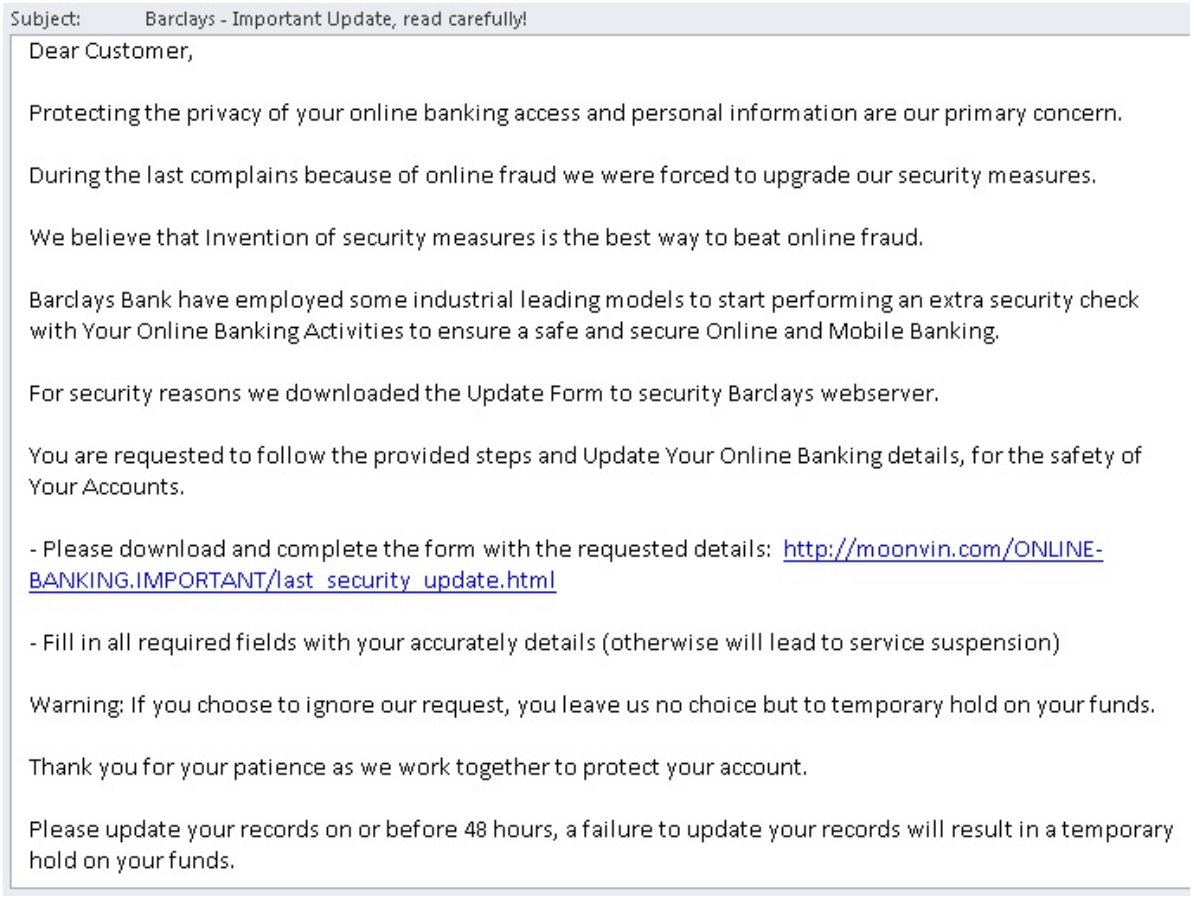
Objectives

Educate IT Administrators and users about this threat, helping them to better defend themselves.

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

How IT Works

A user may be infected by receiving what appears to be a “real” email from a bank, their company, or any familiar/trusted source alerting them about a fraud, see below sample from “Barclays Bank”



Subject: Barclays - Important Update, read carefully!

Dear Customer,

Protecting the privacy of your online banking access and personal information are our primary concern.

During the last complains because of online fraud we were forced to upgrade our security measures.

We believe that Invention of security measures is the best way to beat online fraud.

Barclays Bank have employed some industrial leading models to start performing an extra security check with Your Online Banking Activities to ensure a safe and secure Online and Mobile Banking.

For security reasons we downloaded the Update Form to security Barclays webserver.

You are requested to follow the provided steps and Update Your Online Banking details, for the safety of Your Accounts.

- Please download and complete the form with the requested details: http://moonvin.com/ONLINE-BANKING.IMPORTANT/last_security_update.html

- Fill in all required fields with your accurately details (otherwise will lead to service suspension)

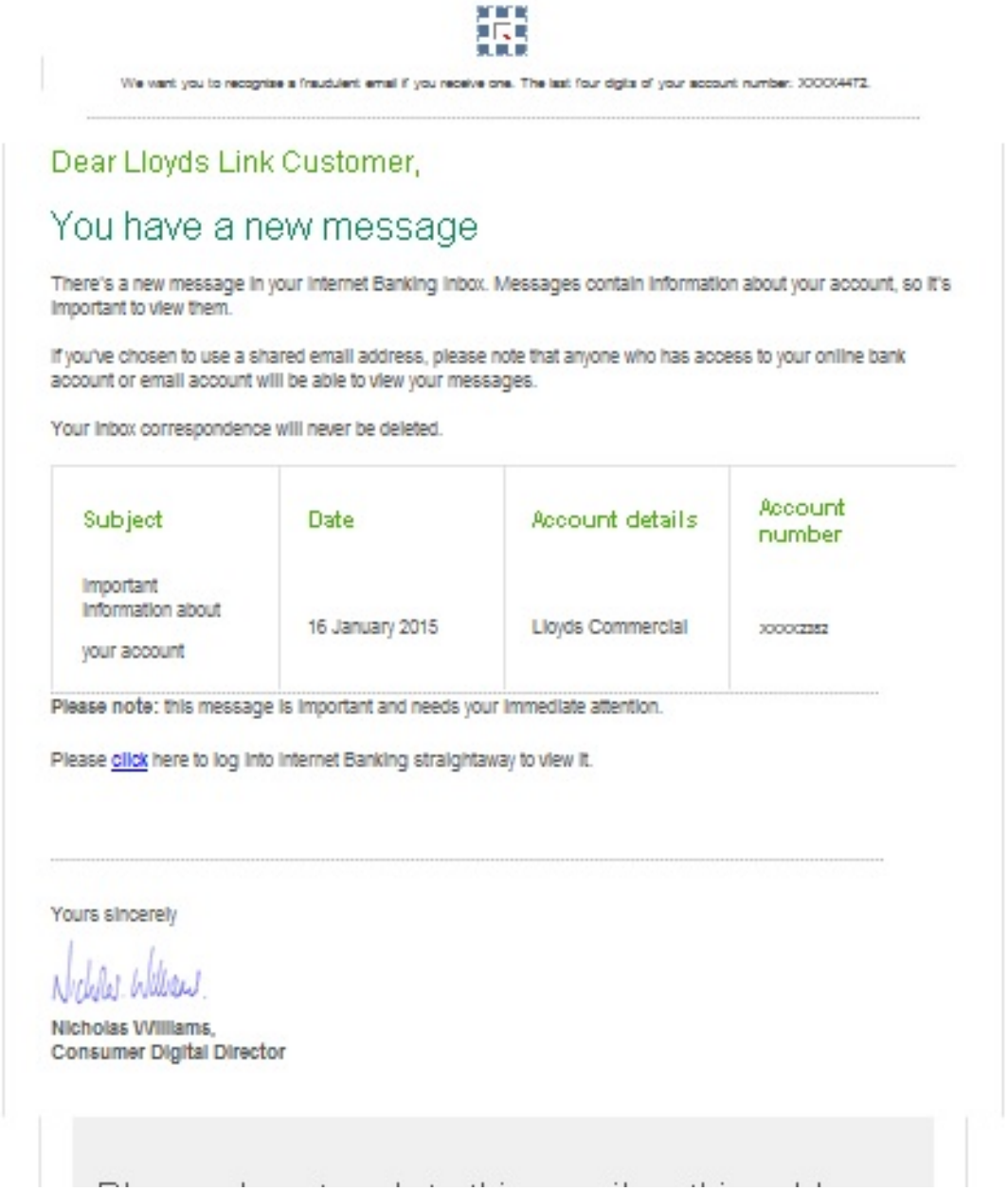
Warning: If you choose to ignore our request, you leave us no choice but to temporary hold on your funds.

Thank you for your patience as we work together to protect your account.

Please update your records on or before 48 hours, a failure to update your records will result in a temporary hold on your funds.

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

Here, is another example of an Email from “Lloyds Bank”



We want you to recognise a fraudulent email if you receive one. The last four digits of your account number: XXXX4472.

Dear Lloyds Link Customer,

You have a new message

There's a new message in your Internet Banking inbox. Messages contain information about your account, so it's important to view them.

If you've chosen to use a shared email address, please note that anyone who has access to your online bank account or email account will be able to view your messages.

Your inbox correspondence will never be deleted.

Subject	Date	Account details	Account number
Important Information about your account	16 January 2015	Lloyds Commercial	xxxxzzzz

Please note: this message is important and needs your immediate attention.

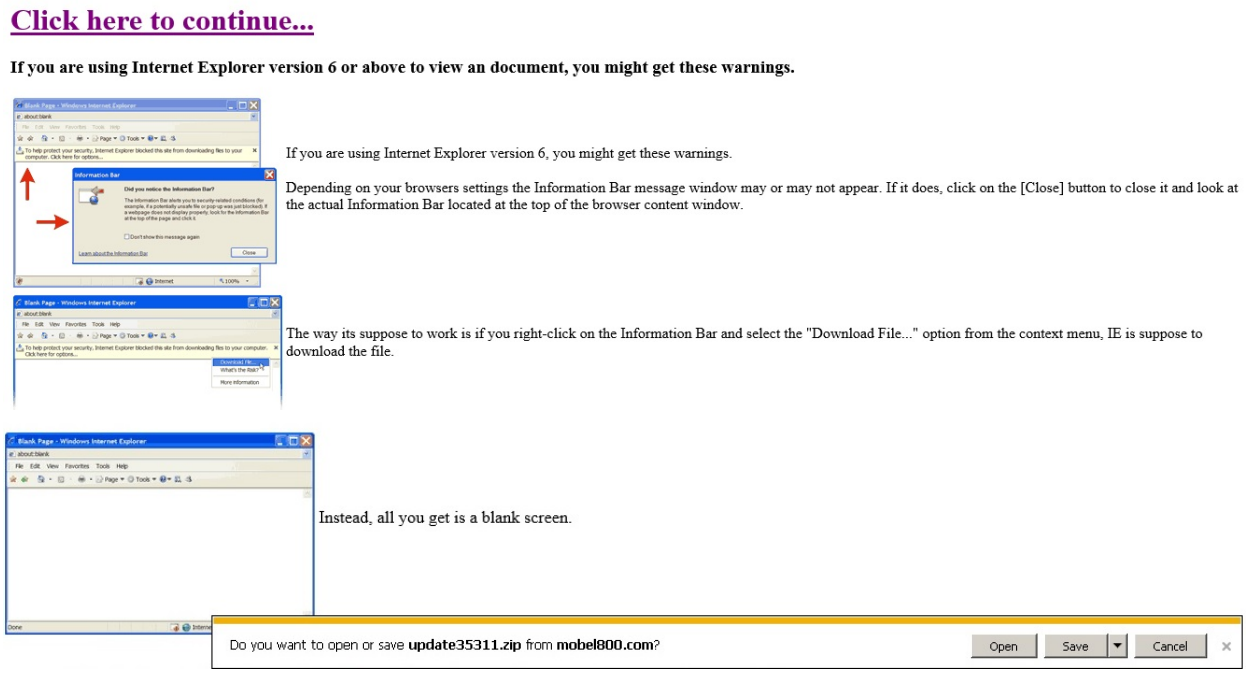
Please click here to log into Internet Banking straightaway to view it.

Yours sincerely

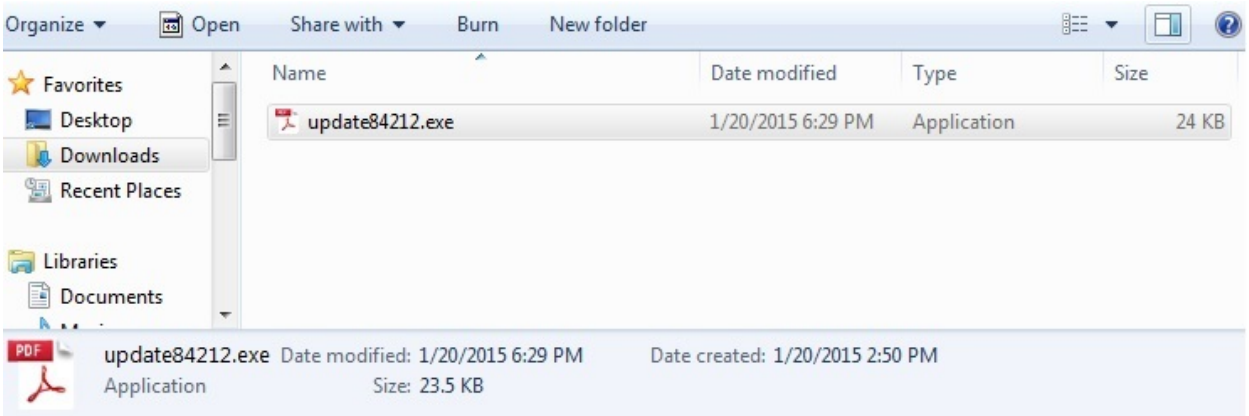
Nicholas Williams,
Consumer Digital Director

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

Clicking the link will cause the browser to open and show a message to download a zip file, see below picture.



Unzipping and double-clicking the file will cause the file to be executed, see picture:



The file will be seen as “innocent” to the user, as it presents itself as a PDF file, not a threat.

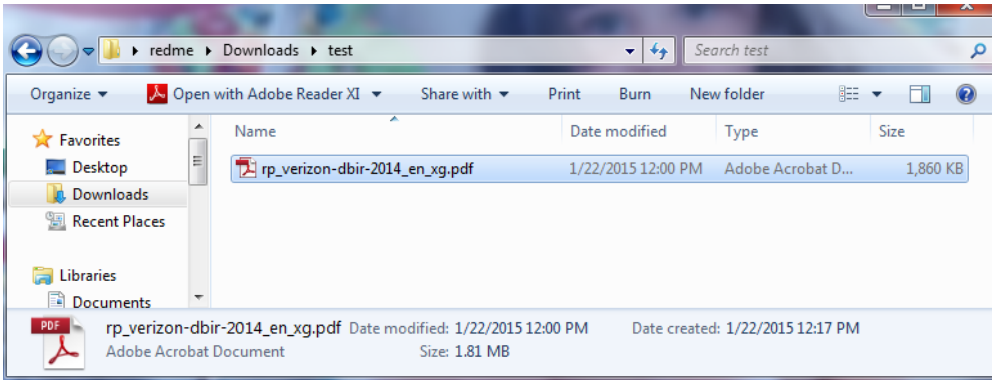
80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

The Outcome

Once file is executed, all files in alphabetically order will be encrypted on local drives and or network shares.

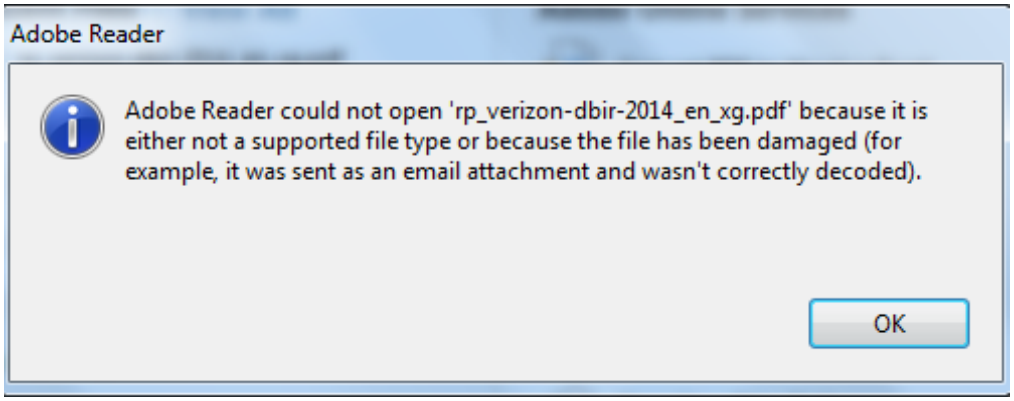
To better illustrate this, below is a snapshot of pdf file before the encryption:

The file after the encryption



80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

The same file not accessible anymore …



80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

How To Reduce The Risk

As you know, good security includes the onion-approach, having layers of protection that increases the safety and efficiency of your users.

There are four steps that can reduce and improve your ability to defend your organization in an efficient way.

1. Incoming Filtering & Blocking Mechanisms
2. Workstation Protection Levels: File Permissions & Execution
3. Antivirus & Anti-Malware
4. Incident Response Teams

In the following pages we will provide detailed information for each step.

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

Step #1: Incoming Filtering & Blocking Mechanisms

Review incoming filtering systems for:

1. Update every hour.
2. Block attachment types, such as exe, com, bat, zip, rar, scr etc.
3. If possible, enable dual incoming scanning by two systems from different vendors.
4. Reject invalid HELO/missing RDNS.
5. Do strict RDNS checks.
6. Use Greylisting.
7. Use BATV - Bounce Address Tag Validation.
8. Perform SPF (Sender Policy Framework) check.

Step #2: Workstations Protection Levels: File Permissions & Execution

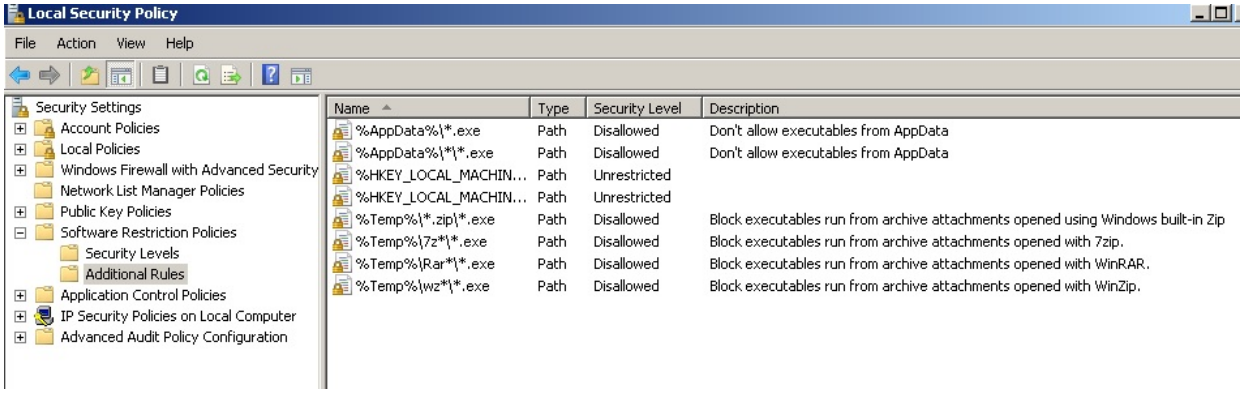
If you have a Windows domain, it's possible to setup a group policy or for local installations just use the Local Security Policy.

Windows XP: use the base path:

C:\Documents and Settings\User\Application Data

Windows Vista & Above:

Security Settings > Software Restriction Policies > Additional Rules



80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

Name	Type	Security Level	Description
%AppData%*.exe	Path	Disallowed	Don't allow executables from AppData
%AppData%**.exe	Path	Disallowed	Don't allow executables from AppData
%Temp%\Rar**.exe	Path	Disallowed	Block executables run from archive attachments opened with WinRAR.
%Temp%\7z**.exe	Path	Disallowed	Block executables run from archive attachments opened with 7zip.
%Temp%\wz**.exe	Path	Disallowed	Block executables run from archive attachments opened with WinZip.
%Temp%*.zip*.exe	Path	Disallowed	Block executables run from archive attachments opened using Windows built-in Zip

Step #3: Antivirus & Anti-Malware

1. Since Antivirus & Anti-Malware solutions are signature based, detecting threats, it is impossible to detect and remove this threat.
2. Make sure you configure your endpoint solution to get updates every hour.

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355

Step #4: Incident Response Team

1. It's highly recommended to 1st establish an appropriate policy to handle problems and more specifically handling incidents as these will be routine, then:
2. Build an incident response team.
3. Educate your users with a security awareness program.
4. Ensure that you have at least:
    a. Two backup methods, ensuring integrity and availability
    b. You can restore successfully

Conclusion

The CryptoLocker virus is not a new attack vector. It has been in existence for several years and has morphed over time, becoming stronger and more sophisticated. We expect to see it continue over time in the form of new and more powerful versions.

About

2Secure specializes in the design and development of secure systems and the research of the latest security threats and how to best protect yourself.

Sincerely,

Yigal Behar
Principle IT Security Consultant
2Secure Corp

80 Broad Street, 5th Floor
New York, NY 10004
www.2secure.biz
info@2secure.biz
Tel: 646-666-9601
Fax: 718-942-5355