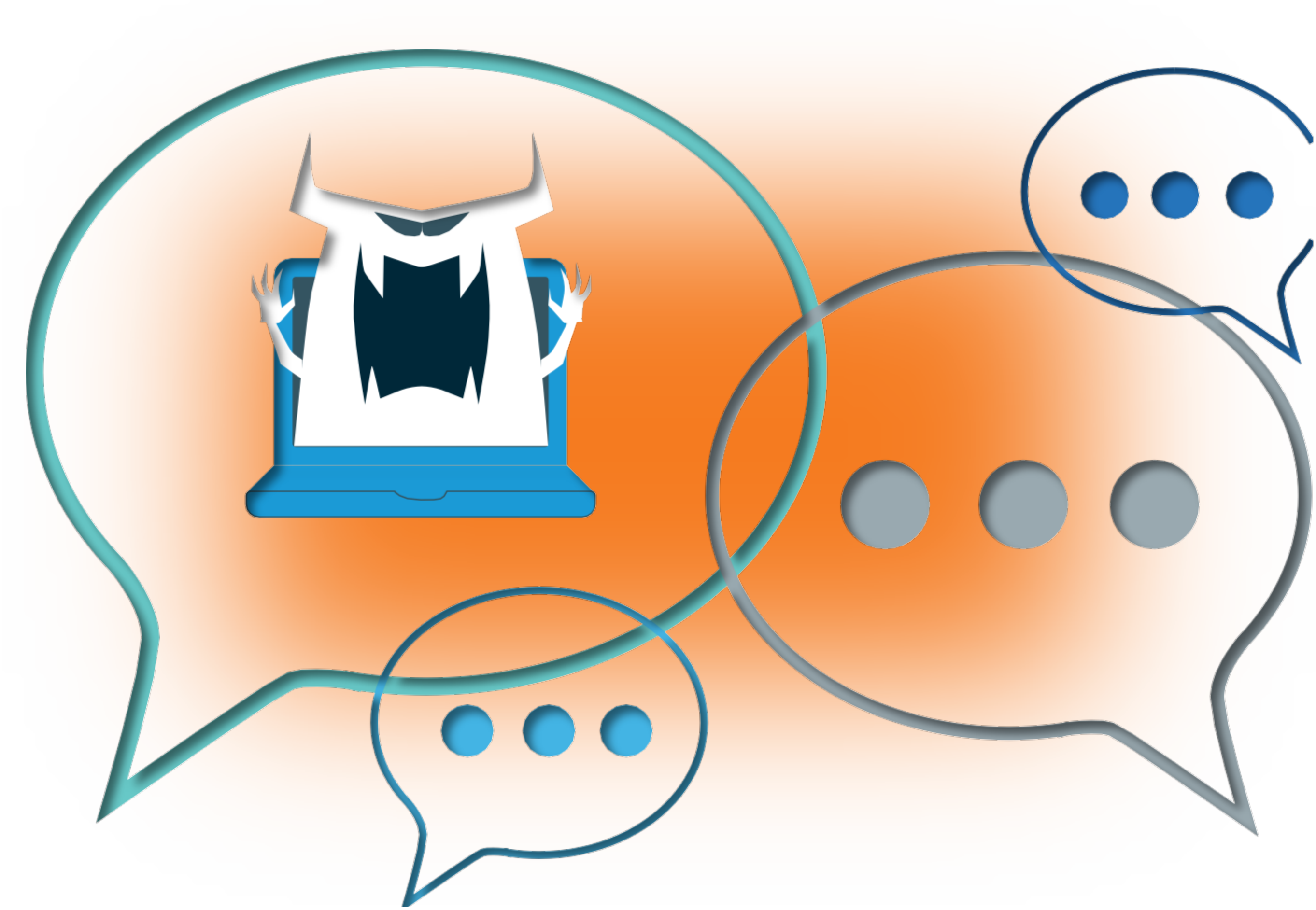
NLN
NEX LEVEL NETWORKS

WHAT IS RANSOMWARE?

A quick guide to help you understand Ransomware and its dangers

RANSOMWARE IS:

A type of malicious software that blocks access to data or threatens to publish it until a ransom is paid. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse.



NEX LEVEL NETWORKS

RANSOMWARE IS NOT LOSING ANY MOMENTUM

Attacks on various industries are becoming daily occurrences. There are companies paying huge sums to retrieve their data from the malicious software. Often, the companies affected aren't familiar with ransomware until it's too late. So, allow us to introduce you to the infamous ransomware.

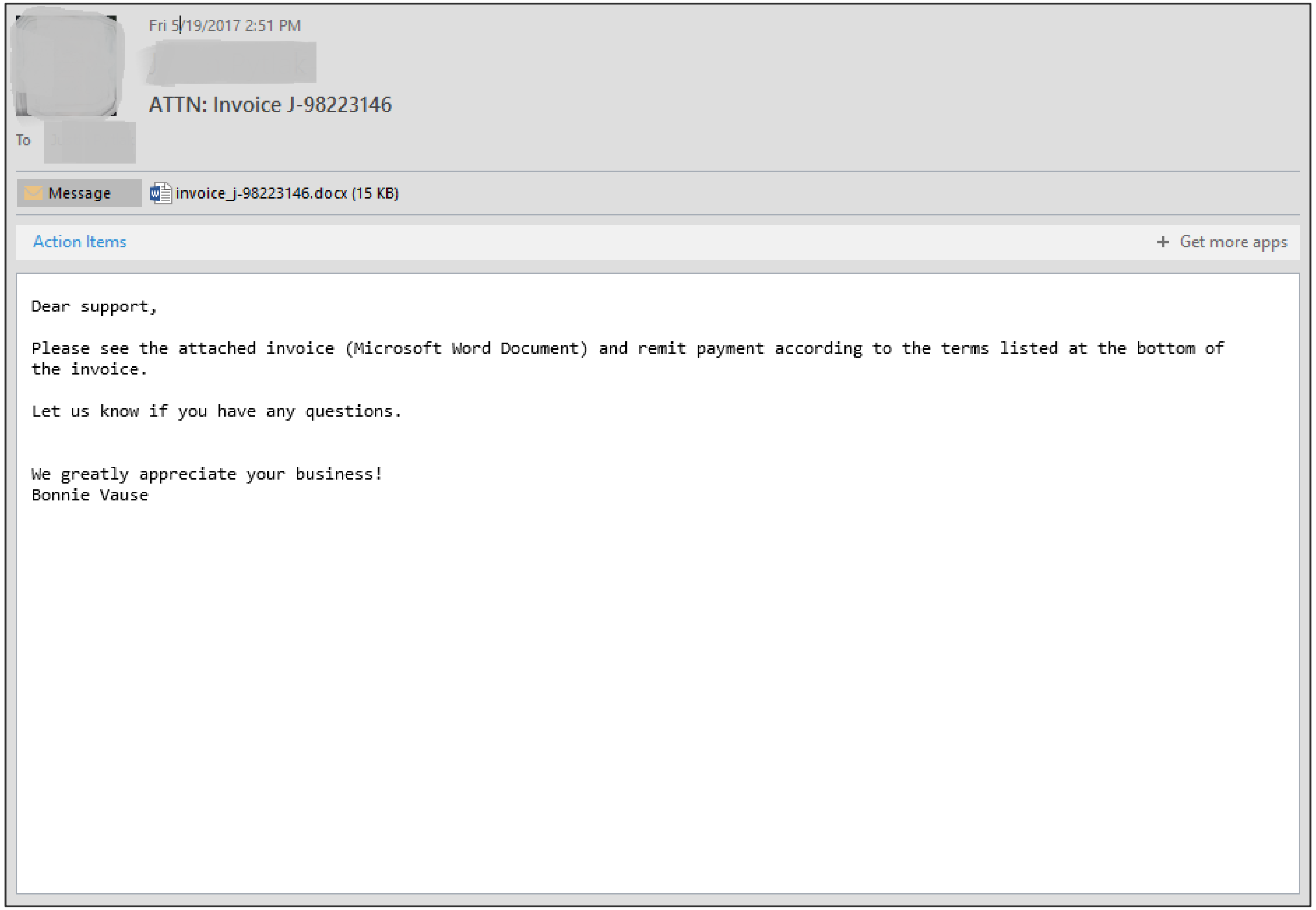
While ransomware is a form of malware, it's definitely unique in what it does.

Sprinkle in some 'ransom' and you've got a malicious virus that keeps your data encrypted until ransom is paid.

SO WHY SHOULD YOU CARE? THE NUMBERS TELL A DARK TALE!

INBOX SCAMS

This image is a prime example of a phishing email used to spread "Locky," a common strain of ransomware. To the recipient, the email appears to come from a business partner asking the reader to "see the attached invoice" by clicking on the attached Word doc. Note how harmless this email appears and how easy it would be for a user to absentmindedly open and click, an action that would result in an instant ransomware infection. It happens every single day.



Fri 5/19/2017 2:51 PM

[redacted]

ATTN: Invoice J-98223146

To [redacted]

invoice_j-98223146.docx (15 KB)

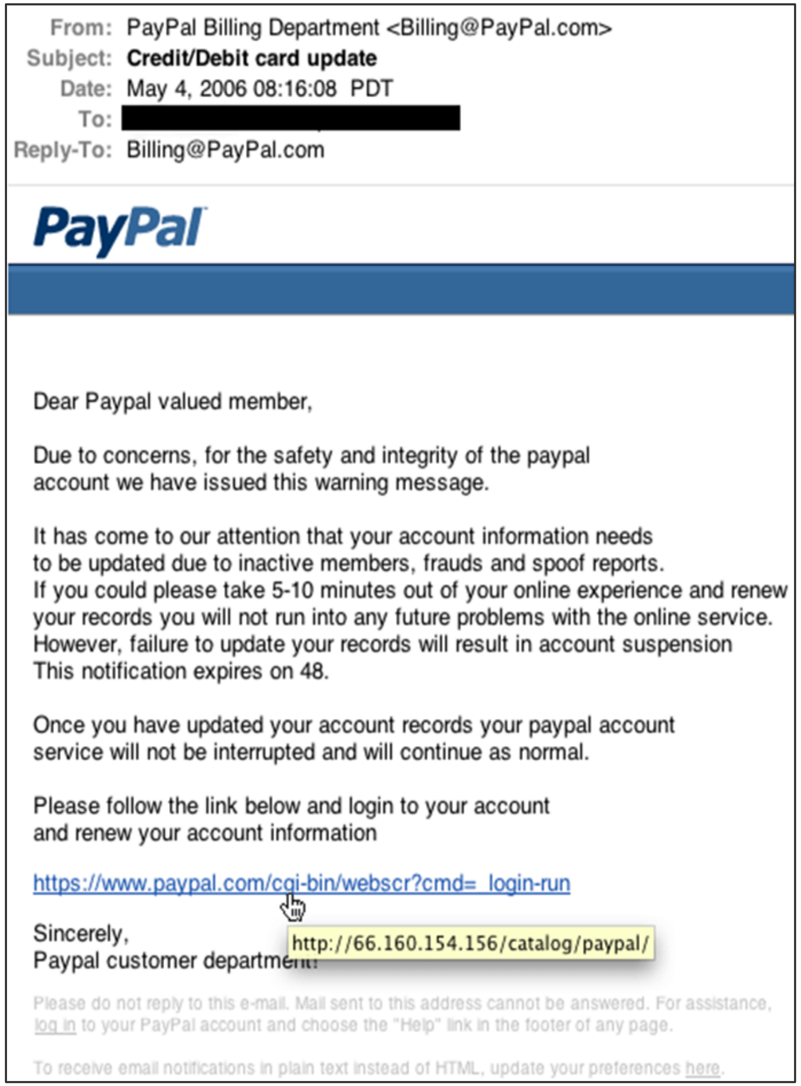
Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your business!
Bonnie Vause

Image 1



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date: May 4, 2006 08:16:08 PDT
To: [redacted]
Reply-To: Billing@PayPal.com

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

Image 2

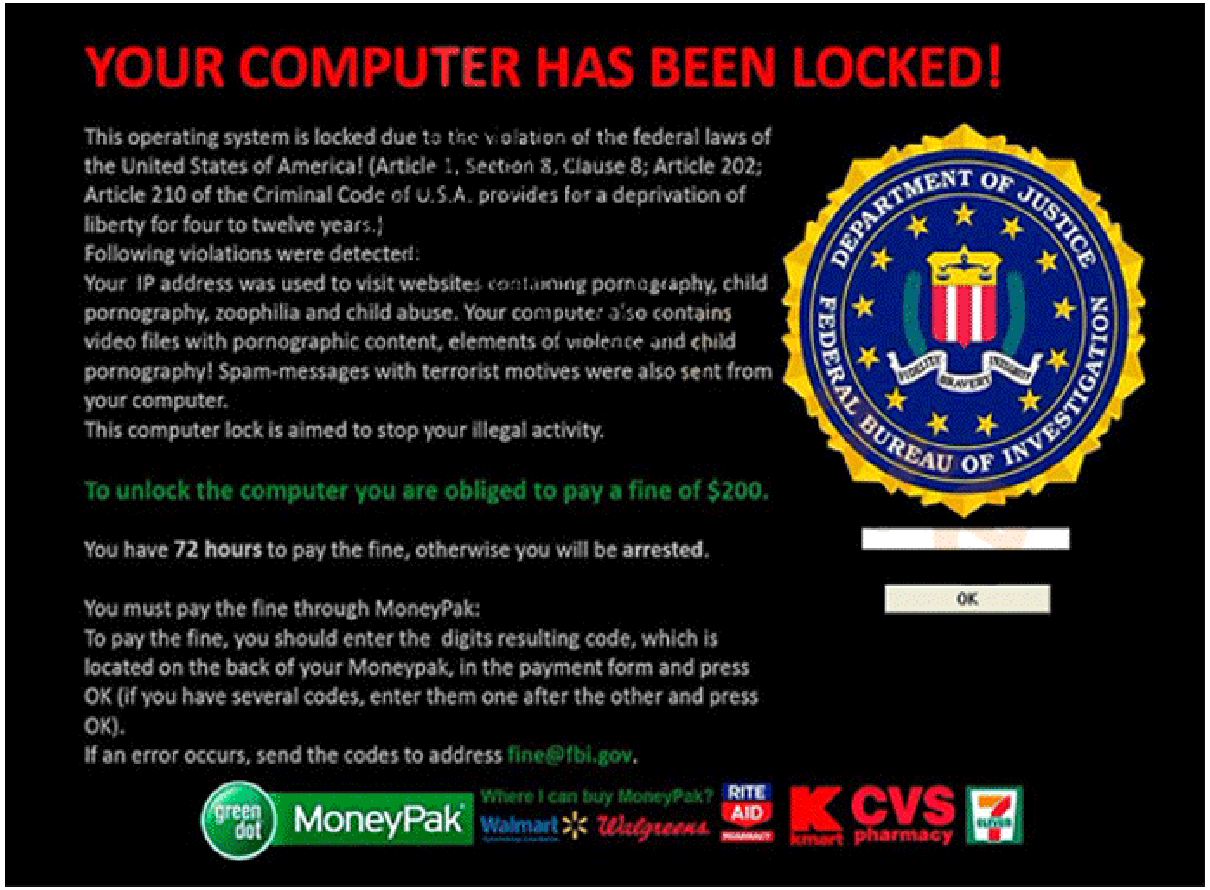
In image 2, note the link appears to direct the reader to a legitimate PayPal web page and yet, when the mouse is hovered over the link, you see that it actually directs to a different site designed to inject malware or illegally collect personal information.

RED FLAGS: Missing sender or recipient information, generic greetings, misspelled email addresses, (e.g. billing@amzaon.com), and email addresses that don't match the company name. Any emails that ask the recipient to download a form or macro in order to complete a task are highly suspicious and an employee should NOT click on anything. Instead, report the email to IT immediately.

POP UPS

Another common lure is a pop-up that claims that a user's computer has been locked by the FBI because it was used to access illegal material such as child pornography (Image 3). The lure instructs users to click a link in order to pay a fine, which is bogus.

RED FLAGS: Links that redirect to a different domain, pop-ups that require you to enter personal information, or misspelled URLs. This type of attack can be very hard to detect, even if employees are highly vigilant.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:

To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.

Image 3

MOST IMPORTANTLY, IF YOU SEE SOMETHING, SAY SOMETHING!

For more information, please contact:

Nex Level Networks

315.426.8800

helpdesk@nlnit.com