Malware in Email

Why this document:

In recent weeks we have seen a large increase in a particular type of Malware known as Ransomware, this document is aimed at giving you the tools to spot a potential infection.

What is Malware?

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency.

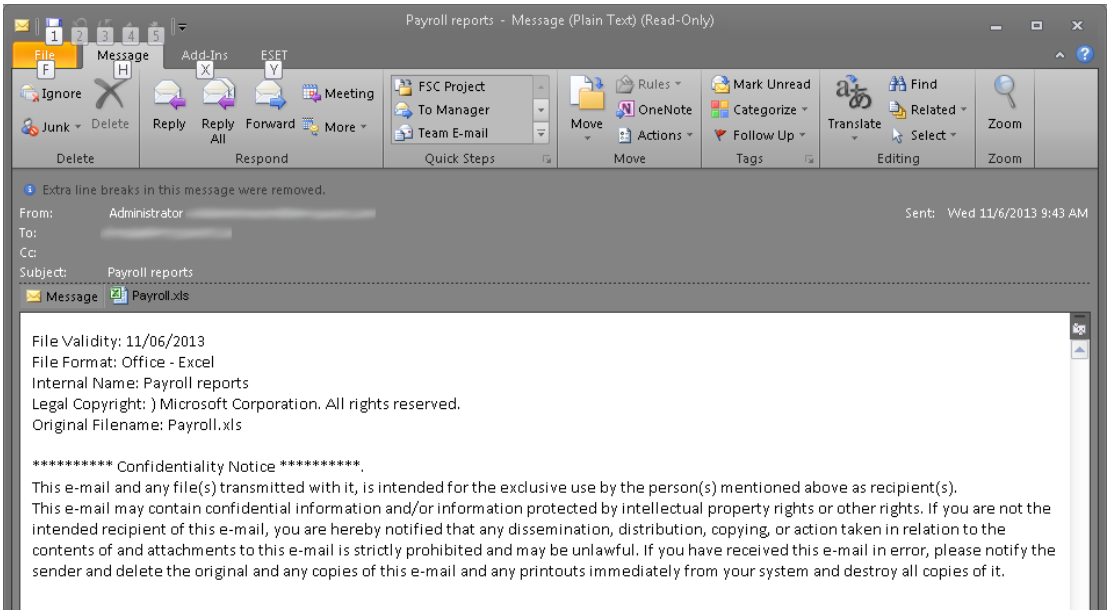
What is Ransomware?

Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying.

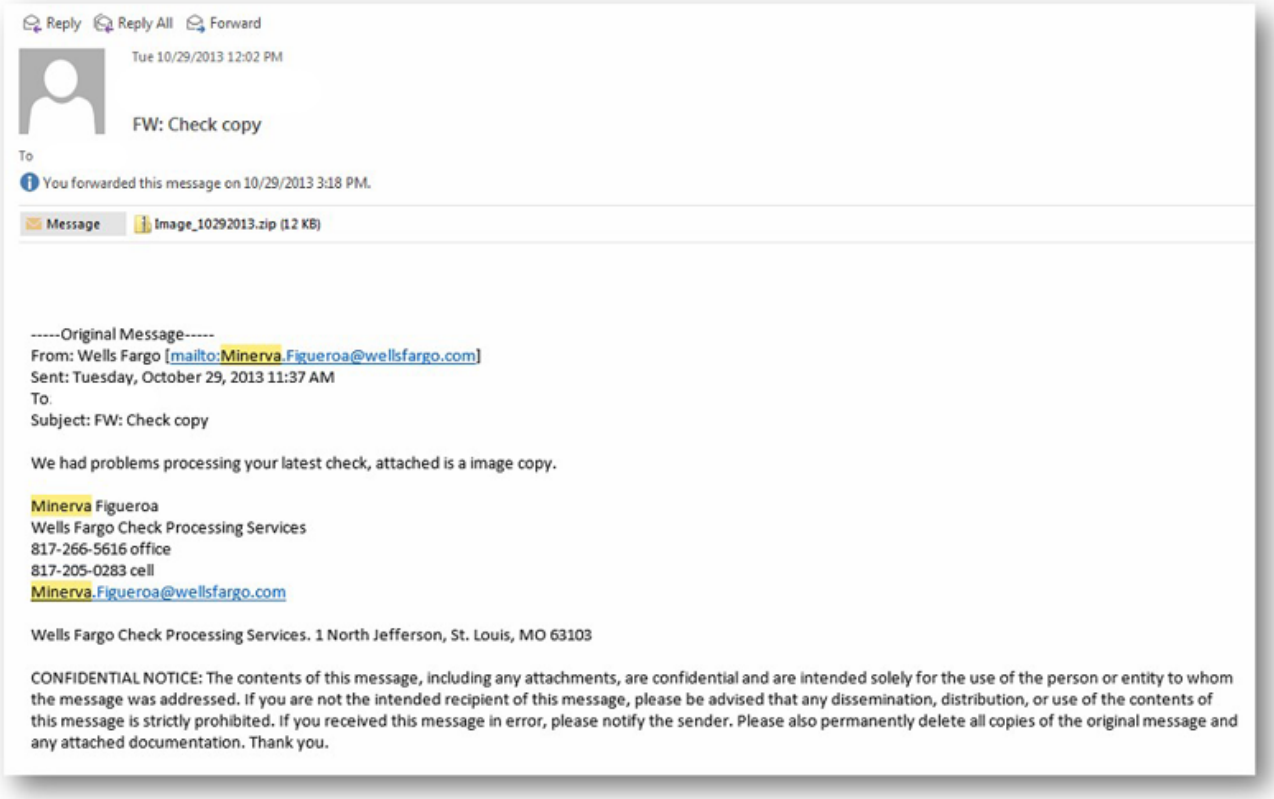
What to look for?

Ransomware uses multiple vectors to infect a system the most common is email, the email will generally come from a known infected source (friend, co-worker, supplier, etc.) or via an enticing header (resume, invoice, bill, holiday pictures, etc.). They rely on trust, below are a few emails I have collected over the last few weeks with malware attached:

In this one the email has come with the subject of Payroll and looks very official, the Excel document attached contains the ransomware.



This one is a little easier to spot, notice the email is referencing Wells Fargo (an American finance company) within the attachments is a zip file, zip files are often use as many email scanners can't process them and thus become in easy way to package the ransomware.



Reply Reply All Forward

Tue 10/29/2013 12:02 PM

FW: Check copy

To

You forwarded this message on 10/29/2013 3:18 PM.

Message Image_10292013.zip (12 KB)

-----Original Message-----
From: Wells Fargo [mailto:Minerva.Figueroa@wellsfargo.com]
Sent: Tuesday, October 29, 2013 11:37 AM
To:
Subject: FW: Check copy

We had problems processing your latest check, attached is a image copy.

Minerva Figueroa
Wells Fargo Check Processing Services
817-266-5616 office
817-205-0283 cell
Minerva.Figueroa@wellsfargo.com

Wells Fargo Check Processing Services. 1 North Jefferson, St. Louis, MO 63103

CONFIDENTIAL NOTICE: The contents of this message, including any attachments, are confidential and are intended solely for the use of the person or entity to whom the message was addressed. If you are not the intended recipient of this message, please be advised that any dissemination, distribution, or use of the contents of this message is strictly prohibited. If you received this message in error, please notify the sender. Please also permanently delete all copies of the original message and any attached documentation. Thank you.

This one pretends to be from Australia Post, but a quick look at the "From" address clearly shows it's not from Australia Post. This one is a little different it pushes you to a third party website and requests you download a file (usually a Word document) that contains the ransomware.

From: 7981 Post Service [mailto:admin2@ustr-post.net]
Sent: Wednesday, 4 March 2015 10:48 AM
To: [redacted]
Subject: 919188 Acceptance of the Order Completion Letter

Hello!
Your package was not delivered to the delivery address on 25 February 2014, because nobody was at home. Please, click the link below to get the information about your order at our official website. Be sure to print out the information about your package so that you could collect it at our Company's nearest office.
Get the information about your parcel
Attention!
Penalties are imposed for storage of the parcel if you fail to collect it within 30 days. The detailed information about storage and payment is available at our website.
Best regards,
Australia Post.
This is an automated email, please do not respond. unsubscribe

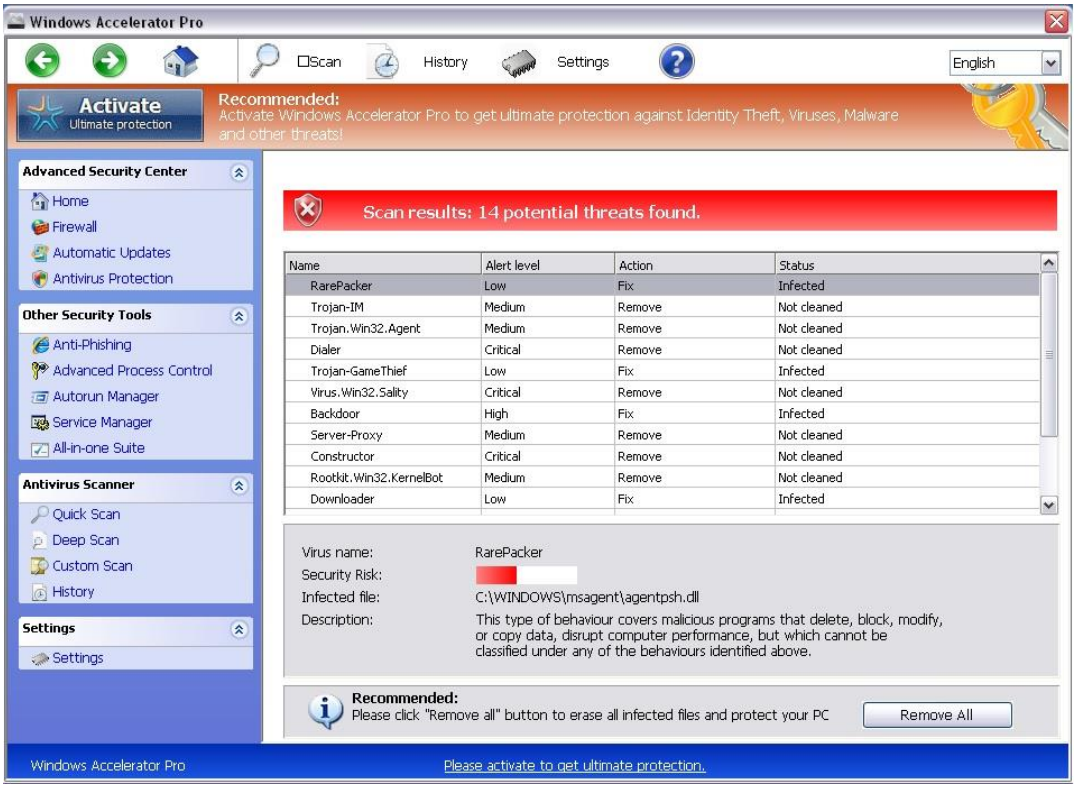
---

2015 Australia Post

What does malware look like?

Crypto-locker – A piece of malware that will encrypt files on your system and any network drives and ransom the key to access them back to you. If you get this specialist advice is required.

Fake-AV – An apparently free antivirus that always picks up between 10 and 40 viruses, corrupts several critical windows files to make the ruse more viable



What can you do?

On the company level you should ensure:

- All users are aware of how Malware and Viruses travel and the basics of what to look out for
- Making sure all PC's & servers have anti-viruses and that the anti-virus is fully patched and definitions updated (virus definitions are usually automatic, patches are usually installed manually)
- All critical data is backed up and the backups are not stored in a location the virus can affect, e.g. offsite, NAS, tape, secluded LUN, etc.
- Installing and testing any anti-spam / email anti-virus solutions
- Conducting system audits to confirm compliance issues and to determine where further action may be required
- Should you become compromised, isolate the system infected, determine the spread, begin cleanup of the PCs and restore data from known clean copies.

On the user level what can be done?

- Avoid sharing USB disks between home and work
- Don't ignore that "it seems fishy" feeling, e.g. if an invoice comes in from someone completely unexpected, phone and ask if it's correct don't assume all is well.
- Ensure software is updated, e.g. Windows updates, Acrobat updates, etc.
- If you believe you have been infected isolate the PC as soon as possible, and get someone to check over the PC

A few statistics:

- Viruses / Malware released in 2014: ~ 317,000,000
- Upon release of a new piece of malware the first infection is reported about 82 seconds later
- Amount cryptolocker (type of ransomware) acquired in ransom ~$30,000,000
- The first piece of malware was created in 1971, all it did was bring up a simple message saying "The creeper". This led to the first anti-virus being developed aptly named "The reaper".

Conclusions:

It's inevitable at some point in time you will come in contact with some form of malware, what important is to get on top of it early and halt it before it can get a foothold on the system. Hopefully this document will arm you with the information to help you make the correct call when the time comes.