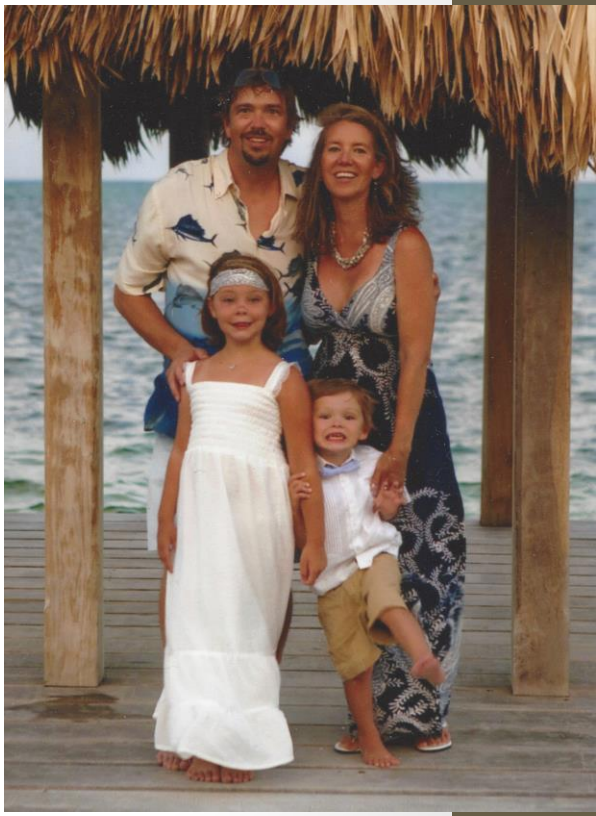
Malspam and Ransomeware

Dave Brockmyer
Incident Response Manager
October 2016

Introduction

- Dave Brockmyer is a Manager in IT Information Security at Intel Corporation. He has been in various functions in IT for over 20 years there, with the last 6 in Information Security. He has managed a team called Threat Management throughout this 6 years. He has a background in Computer Science and considers himself a bit of a geek with a management focus. In his free time, he enjoys spending time with his family and traveling.



Why do you care?

- Audit is focused on identifying gaps in the security of the environment before an incident occurs
- Cyber attacks continue to rise – nobody is safe
- Strengthening Protect, Detect and Respond is critical to the Information Security Function

Background

- Malspam is the combination of “Malware” and “Spam”
  - Usually delivered through Phishing or Spear Phishing
  - New technique: targeted to an organization
  - the latest version of attacking victims with the goal of exploiting their computer for financial gain
- Ransomware is malware that encrypts the contents of the victims computer
  - It is more frequently becoming active as a payload of Malspam attacks – 93% according to CSO Online
  - The first case was in 1989!
  - a common payload in malspam, focused on encrypting a users’ files to extract a payment to get them back

How Malspam works

- Spoofed email address
- Legitimate looking internal appearing memo in email
- Either a malicious attachment or an obfuscated hyperlink to malicious internet content

Example:

Note how the actual email address is Meaningless (randomized). This is an Indicator that the email did not originate From the sender (Jean Lucas in this case)

From: Jean Lucas [mailto:Eve.b4a0@dnt-gw-rus-savitar2.dnttm.ro]
Sent: 10 December 2014 11:15
To:
Subject: Remittance Advice for 190.85 GBP

Please find attached a remittance advice for recent BACS payment.

Any queries please contact us.

Jean Lucas
Senior Accounts Payable Specialist
K J Watking & Co
Tel: 01469 492182

How Ransomware works

- Silently encrypts files in the background while you continue about your business
- When the encryption has gone far enough, a pop-up occurs, demanding payment for the encryption key

But we have protection, right?

- Email gateways offer a level of protection
- Antivirus offers a level of protection
- Proxies offer a level of protection
- But it’s not enough!

Shortfalls of Existing Protection

- Almost all forms of protection on the previous slide depend on IOC's (signatures or known bad artifacts)
- IOC's are developed after the fact
- There is a window of opportunity between the time a new attack vector is developed and protection is in place
- Aggressive email blocking at the gateways results in blocking critical business emails


LIVE LONDON
CYBERSEC NEWS
THERE IS SOMETHING YOU CAN DO!
14/10/2016
IMPROVING YOUR CYBER RESPONSE PROGRAM WILL HELP
classtools.net

So, how do we respond then?

- User awareness!
  - User awareness programs can reduce exposure
    - Anti-clicking campaigns
    - Prompt reporting with rewards
  - Open and honest conversation with IS from individual contributors through the BOD
- Develop better Incident Response

What can we do?

- It starts with the User!
  - Train them
  - Encourage them to report
  - Fast reporting to the SOC or trained responders is key
- Train your Incident Response team
  - Phishing Email characteristics
  - Malspam payload characteristics
- Prioritize appropriately – assume there are more than one
- Partner with the teams that can fix this
  - Clean the mailboxes that received the message
  - Find the systems that clicked & inspect for infection
  - Fix your filters on email and web gateways

In Conclusion

- Malspam is a fast-growing threat to every organization
- Threat actors are targeting organizations directly
- Ransomware can ruin more that photos and music files
- User awareness is key to fast detection
- Knowing the full extent of the attack and remediating it quickly requires coordination with messaging and web gateway teams
- Incident response teams need to have a network in the organization and IT

Reference

- https://blog.malwarebytes.com/threats/malspam/
- https://inews.co.uk/essentials/news/dozens-nhs-hospitals-targeted-cyber-blackmailers/
- https://hbr.org/2016/10/is-your-company-ready-for-a-ransomware-attack
- http://www.csoonline.com/article/2133408/network-security/network-security-the-7-elements-of-a-successful-security-awareness-program.html
- http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/
- https://blog.continuum.net/uncovering-and-guarding-against-the-ransomware-revolution?sf34996425=1
- https://blogs.mcafee.com/consumer/spot-phishy-email/