RSAConference2017
Singapore | 26–28 July | Marina Bay Sands

POWER OF OPPORTUNITY

SESSION ID: GPS-R08A

Adventures in Threat Intelligence: Why Organizations Fall Prey to Cyberthreats

Guy Rosefelt
Dir, Threat Intelligence & Web Application Security
NSFOCUS, Inc.
@otto38dd

RSA Conference 2017
Singapore

"Those who cannot remember the past are condemned to repeat it."

- George Santayana

Some history

- 1903 1st secure communications hack
  - Magician and inventor Nevil Maskelyne disrupts John Ambrose Fleming's public demonstration of Guglielmo Marconi's purportedly secure wireless telegraphy technology, sending insulting Morse code messages through the auditorium's projector.
- 1957 1st Phreaking call
  - Joe "Joybubbles" Engressia, a blind seven-year-old boy with perfect pitch, discovered that whistling the fourth E above middle C (a frequency of 2600 Hz) would interfere with AT&T's automated telephone systems
- 1979 1st Modern hacker
  - Kevin Mitnick breaks into his first major computer system, the Ark, the computer system Digital Equipment Corporation (DEC) used for developing their RSTS/E operating system software.
- 1998 1st internet cyber attack
  - Morris Worm inadvertently released bringing down 10% of the internet

RSA Conference 2017
Singapore

So what is the problem?

What do these events have in common?

- July 2001 Code Red
- SQL Slammer Worm Jan 2003
- May 2017 Wannacry/Petya

What do these events have in common?

- July 2001 Code Red
  - Microsoft Security Bulletin MS01-033 patch released June 2001
- SQL Slammer Worm Jan 2003
  - Microsoft Security Bulletin MS02-039 - Critical July 2002
- May 2017 Wannacry/Petya
  - MS17-010 patch released Mar 2017

What do these events have in common?

- Spring 2008 Democratic & Republican National Committees Chinese email hack
- 2012-2015 Sony email hack
- Spring 2016 Democratic & Republican National Committees Russian email hack

What do these events have in common?

- Spring 2008 Democratic & Republican National Committees Chinese email hack
  - Phishing -> Malware
- 2012-2015 Sony email hack
  - Phishing
- Spring 2016 Democratic & Republican National Committees Russian email hack
  - Phishing

What have we learned?

Apparently nothing…..

It cannot be due to lack of awareness

- 1 Feb 1988 Star Trek: The Next Generation
  - Episode 15: "**11001001**" First annual "backup your hard drive" episodes
- May 2007 Information Se ok, 6th Edition
  - Chapter 16: "Patch Manager nse!"
- 10 October 2011 CNET
  - "Only you can prevent phish
- 26 Jan 2016 CSO Online
  - "Why patching is still a prob
- And so many more…..

It cannot be due to lack of awareness

- 1 Feb 1988 Star Trek: The Next Generation
  - Episode 15: "**11001001**" First annual "backup your hard drive" episodes
- May 2007 Information Se ok, 6th Edition
  - Chapter 16: "Patch Manager nse!"
- 10 October 2011 CNET
  - "Only you can prevent phish
- 26 Jan 2016 CSO Online
  - "Why patching is still a prob
- And so many more…..

What should we be doing?

- Regular patching to remove critical vulnerabilities
- Regular backups of data
  - Easiest way to make ransomware a nuisance
- Don’t open suspicious emails to prevent phishing
- None of this is news to you….

So why don’t organizations patch?

- There are hundreds of automated patch management solutions
- But there a thousands of patches….

#1 Reason organizations do not patch

Drum roll….

Anything that impacts revenue

In fairness to organizations…

- Patches have caused critical outages in the past
- There is ZERO guarantee that it will not happen in the future
- So now you have a rock…
  - Critical vulnerability
- And a hard place…
  - Potential outage from a patch
- There are too many patches to validate before install…

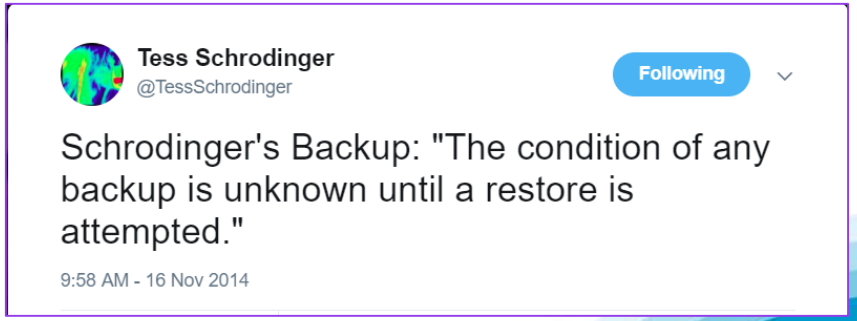
So why don’t organizations back up data?

- There are hundreds of automated data backup solutions
- Many are not that expensive….
- Many organizations do back up data

Top 2 Reasons organizations do not back up data

Drum roll….

2. Not a priority for ~~smaller~~ most organizations
1. Backups do not always restore



Really, there is no excuse for being phished!

- Everyone should know
  - DO NOT open emails from strangers
  - DO NOT accept attachments from even people you know unless previously notified they are being sent
  - DO NOT click on embedded links in emails from even people you know unless you verify that they are being sent
- Yet, people still fall prey…
  - Especially spear phishing Whales (execs)…

Top 2 Reasons people fall prey to phishing

Drum roll….

2. People are not able to recognize phishing emails (seriously!!)
1. Self-identified "tech-savvy" people are actually 18% more likely to fall prey to identity theft.
    - CBT Nuggets study

BTW

Phishing is #1

- mechanism used for stolen credentials
- delivery mechanism for ransomware and other malware
  - Email attachments

- 30% of phishing emails are opened and 12% of the links are clicked.
  - Verizon DBIR 2017

What should we do differently about patching?

- If you want to be hip and cool
  - Leverage the cloud!
  - Let someone else worry about patching!
- If you want to be traditional
  - Investigate cool vulnerability management tools
    - Cloud solutions
    - On premise appliances
    - Open source
  - Tools that can help you prioritize vulnerability remediation based on business criticality

What should we do differently about backups?

- If you do not have one, DEVELOP a Disaster Recovery Strategy
  - You know you do not have one!
- Investigate new backup technologies and strategies
  - “we don’t need no stinkin’ tapes!”
  - “again with the cloud….”
- Automate daily backups of critical data
  - You cannot afford to lose more that a day’s data
- Test random system restore at least quarterly
  - What good is all this if you cannot bring back the data

What should we do differently about phishing?

- Educate, Educate! EDUCATE!!
  - Annual training classes on how to identify phishing tactics
  - Additional training for execs on how to better limit and protect personal and professional information online
- Conduct semi-annual phishing drills
  - Lots of open source and commercial phishing simulators
  - However, provide positive feedback to all participants to reinforce better behavior
    - Calling out participants that were susceptible: **bad**
    - Helping them understand what they did well: **good**

What should we do differently about phishing?

- Anti-phishing technology
  - Email Gateways
  - Threat intelligence blacklists of spammers, phishers, and malware hashes
  - Integration with sandboxes

How do we apply what we have learned today?

"Those who cannot remember the past are condemned to repeat it."

- George Santayana

Learn from others' mistakes…

How should you apply what you learned next 30 days?

- Patching
  - Inventory patch status of critical business systems
  - Determine if any vendor identified critical patches have not been installed
  - Research if any issues identified with patches.
    - If so significant issues, schedule installation!

How should you apply what you learned next 30 days?

- Data backup
  - BACKUP CRITICAL DATA ASAP!
  - Verify restore on at least one system
  - Review and update current backup strategy & policies

How should you apply what you learned next 30 days?

- Phishing
  - Research how many successful phishing attacks occurred
    - Any malware infestations due to phishing?
  - Start developing an education plan
  - Start developing an awareness campaign
  - Research anti-phishing technologies

How should you apply what you learned next 90 days?

- Patching
  - Research vulnerability scanning and management solutions
  - Develop methodologies for better patch remediation and metrics
  - Develop a mantra to accept that you need to patch
    - "Help me accept that I need to patch and not be afraid of an outage…"

How should you apply what you learned next 90 days?

- Data backup
  - Develop/review/update Disaster Recovery strategy and policies
    - What needs to be done in the event of ransomware infestation?
  - Investigate newer more robust backup technologies
  - Verify restore of random critical system

How should you apply what you learned next 90 days?

- Phishing
  - Conduct anti-phishing education training
  - Conduct simulated phishing drill
  - Develop remediation plan for personnel that did not pass the drill
  - Implement awareness campaign
  - POC anti-phishing technologies

How should you apply what you learned next 6 months?

- Patching
  - Implement vulnerability scanning and management solutions
  - Implement methodologies for better patch remediation and metrics
  - Develop as part of Disaster Recovery what actions need to be taken in the event of system impact due to patch installation
    - Can you back out patch?
    - Can you restore previous version?
    - Is there a warm or cold spare of critical systems?

How should you apply what you learned next 6 months?

- Data backup
  - Conduct Disaster Recovery drill
    - What needs to be done in the event of ransomware infestation?
    - What needs to be done in the event of critical system failure?
  - Investigate newer more robust backup technologies
  - Verify restore of random critical system

How should you apply what you learned next 6 months?

- Phishing
  - Research how many successful phishing attacks occurred
    - Any malware infestations due to phishing?
  - Maintain metrics to determine effectiveness of education and awareness activities
  - Update awareness campaign as needed
  - Implement anti-phishing technologies

RSA® Conference 2017

Singapore

Thank you!