About ESET

• Leading security solution provider for companies of all sizes, home and phones
• Pioneered and continues to lead the industry in proactive threat detection
• Presence in more than 180 countries worldwide
• Protecting over 100 million users
• Twelve years of consecutive VB100 awards†
• 5th Largest Endpoint Security Vendor‡

†Source: Virus Bulletin Magazine
Agenda

• End of an era: The long tail of Windows XP
  – Windows 10 Cometh
• 2014’s Biggest Security Threats
  – Heartbreak, POODLE, Shellshock, et al
  – Honorable Mentions...
• 2014: The Year of the Data Breach
  – Lessons learned
• Security beyond anti-malware
  – What to keep an eye on/watch out for in 2015
Not on the Agenda

- this is not a deep dive

- I am not going to be going over these threats in detail – see ESET’s 2014 Mid-Year Threat Review for more info
End of an era: Windows XP

• Introduced in August 2001
• Support ended in April 2014 (but still going?)
End of an era: Windows XP

What did we learn?

• It was tough for some organizations to move off of Windows XP
  • legacy apps, failure to plan ahead and financial reasons contributed to Windows XP unplanned longevity

• Businesses upgraded mostly to Windows 7
  • Windows 8 a non-starter for most businesses
End of an era: Windows XP

- It is crucial to think about lifecycle management up front.

- Pay attention to vendor communications, especially those involving end of support dates.

- If need be, come up with a plan for securely using programs and operating systems after support ends.
Survey No. 1

How many of you still have Windows XP running somewhere in your organization?

- not in use anywhere
- in use on a few PCs
- in use on many PCs
- not sure / don’t know
What to expect from Windows in 2015

• Windows 10 to arrive... sometime in 2015
  – plans to fix issues with Windows 8, perceived or otherwise
    • Classic and Modern UIs to coexist better
    • Windows Desktop no longer a second-class citizen
  – security investments
    • encryption
    • improvements to deployment and manageability
    • locked down PCs from OEMs
    • multifactor authentication
    • VPN technology improvements
What to expect from Windows in 2015

But will this be enough for the Enterprise?

• Shared codebase means a zero-day could affect all your devices at once:
  – appliances, phones, tablets, laptops, desktops, servers...

• Tech Preview uses fast + slow update channels:
  – Consequences to patch quality if used in release (?)
  – Businesses could remain unprotected for longer
Survey No. 2

Have you looked at the Windows 10 Technical Preview yet?

- [ ] yes
- [ ] no
2014’s biggest security threats

- Heartbleed OpenSSL vulnerability identified, affects anywhere from 1/6\textsuperscript{th} to 2/3\textsuperscript{rd}s of web sites, networking gear, VPNs, etc.
- POODLE vulnerability in OpenSSL’s SSL 3.0 implementation allows decryption of data
- Shellshock bug in Bash shell affects UNIX-like systems
- Various network devices (routers, NAS, etc.) subject to worms, coin miners, DNS redirection DDoS...
- Windigo campaign affects 25,000 UNIX-like servers
2014’s biggest security threats

Common denominator in all of these attacks?

- Number of Windows-specific threats: **ZERO**

So, either:

- Microsoft has gotten its security together or
- Attackers are targeting other systems

Most likely some mixture of the two
Rise of the Androids

Malware authors take an interest in Android...

- but mostly an issue for 3rd-party app stores & downloads in CN + RU, not in Google Play

- still issues in Google Play with
  - Potentially Unwanted Applications
  - Adware... bordering on and up to Spyware
  - fake/counterfeit apps
But what about Apple?

Apple had two high-profile attacks affecting both Mac OS X and iOS:

- GotoFail – SSL vulnerability
- WireLurker – cross-platform malware
Honorable mention: Microsoft

Microsoft didn't escape entirely unscathed.

- MS14-064 vulnerability in OLE affects Internet Explorer 3.0 through 11 (Windows 95 – 8.1, RT, too)
- MS14-068 vulnerability in Kerberos allows elevation to domain admin
Lessons Learned, IT Dept. Edition

• Stay on top of patching
  – Begin testing, applying as quickly as possible
• Subscribe to and read vendor advisories
  – follow vendor’s prescriptive advice
• Budget for network infrastructure should cover
  – post-warranty security updates
  – replacement if no longer securable
• Keep up with reputable security news sources
  – stay current with “early warnings,” etc.
2014: The Year of the Data Breach

To view this slide, please see the original presentation at https://www.brighttalk.com/webcast/1718/125051
2014: The Year of the Data Breach

- PCI DSS audits are a good thing, but...
  - remember, they represent **minimum** requirements
- look into business data breach insurance
- your bank may offer some security options:
  - SMS notifications for transactions
  - 2FA for banking accounts
  - ask to flag/confirm int’l transactions
- check bank account activity at a regular interval *(decide based on your risk factors... daily? weekly?)*
Survey No. 3

Have you/your business been affected by a data breach?

- yes, once
- yes, multiple times
- no
- not sure / don’t know
Security beyond anti-malware

In 2014, greater interest in privacy means formerly esoteric security technologies become popularized:

– encryption
– multi-factor authentication

Some quick predictions for 2015:
• we’ll see both technologies talked about more
  – often with bad advice given (around capabilities, etc.)
• we’ll see both technologies used more frequently
  • often incorrectly (bad implementation, used incorrectly, etc.)
Kudos!

Special thanks to my colleagues

Bruce P. Burrell
Stephen Cobb
Amelia Hew
David Harley

for their assistance with the IT Security Lessons Learned in 2014 report.
Polling question:

I would like to request one of the following:

- Contact from ESET Sales
- Business Edition Trial
- PassMark® Competitive Analysis Report
- Monthly Global Threat Report
Q&A Discussion
Better security through knowledge