Understanding the Data Breaches of 2014: Did it have to be this way?

Josef Meier
Manager Pre Sales Engineering Fortinet Germany
The year?

I'M THE CREEPER. CATCH ME IF YOU CAN!
The Creeper – “Catch me if you can”...

- Experimental self-replicating program
- Written in 1971 by Bob Thomas of BBN
- Infected DEC PDP-10 computers
- Just one year after unix epoch began
- ‘Reaper’ worm created in 1972 to delete it
Crimeware and Crime Services

CRIME SERVICES

ENABLERS

Victims

Criminal Organizations

Affiliates

Partnerships

Sales, Licensing, Maintenance

CRIMEWARE PRODUCERS

Exploits

Special Platforms

Senior Developers

Source Code

Junior Developers

CRIMWARE

PRODUCERS

Packers

Mobile

Bank Accounts

Credentials & Data

Digital Real Estate

Quality Assurance
Crypters / Packers
Scanners

Hosting
Infections / Drop Zones
Management

Botnet Rentals
Installs / Spam / SEO / DDoS

Money Mules
Accounts Receivable

Consulting

Exploits

Special Platforms

Source Code

Copy & paste

Affiliate Programs
FakeAV
Ransomware
Botnets
Anyone Want To Add Anything?

- **eBay**: 145,000,000
- **JP Morgan/Chase**: 76,000,000
- **Target**: 70,000,000
- **Home Depot**: 56,000,000
- **Michaels**: 2,600,000
- **Goodwill**: 868,000
- **SuperValue**: 500,000
- **Aaron Brothers**: 400,000

*Milton Security*
Point of Sale

- 2013 was the “year of the megabreach”
- Target and Home Depot made the headlines
- Between them details of 90 million credit cards stolen
- POS attacks still very prevalent — small targets, large scale
- PCI 3.0 released in 2013 to reinforce protection
Finding the Common Thread

Target - Outside contractor clicks on phishing email

JP Morgan/Chase – Stolen employee credentials

Home Depot Stolen login credentials from Third party vendor
Industrial Malware

- Havex – the sequel to Stuxnet
- RAT (remote administration tool)
- Harvests information on hardware control systems (SCADA)
- OPC – OLE for Process Control
- Communication between Windows and control hardware
- OPC servers control machines via PLC

Stuxnet-like 'Havex' Malware Strikes European SCADA Systems

Thursday, June 26, 2014
Swati Khandelwal
Server-side Attacks

HeartBleed

ShellShock

500,000 Web Servers Affected

Time to Protect Critical
Surge in attacks while fresh

Millions of Internet Connected Devices Affected
Advanced Persistent Threat Structure

- Commodity Threats
- Advanced Persistent Threat
- "Hactivism"

HOW?
- Initial intrusion
- Deployment
- Outbound connection initiated
- Expand access and obtain credentials
- Strengthen foothold
- Exfiltrate data
- Cover tracks and remain undetected

Define Target
- Find and organize accomplices
- Build or acquire tools
- Test for detection

Social Engineering
- Research target infrastructure/employees
Exploiting the Weak Link
The Technology Side of Things

Prevent
Two Factor Authentication
Anti-Virus
Intrusion Prevention
Secure Email Gateway
Web Application Firewall
End Point Protection

Detect
Botnet Detection
IP & Client Reputation
Sandboxing

Mitigate
People
Process
Technology

Threat Intelligence
Zero Day Research
Continuous updates
Advanced Threat Protection

- FortiGuard Lab
- FortiGuard Services
- FortiMail
- FortiSandbox
- FortiGate
- FortiWeb
- FortiClient
The FortiGuard Minute

- 25,000 Spam e-mails intercepted
- 390,000 Network intrusion attempts resisted
- 83,000 Malware programs neutralized

- 160,000 Attempts to access malicious websites blocked
- 59,000 Botnet command and control attempts thwarted

- 39 Million Website categorization requests

- 5,800 Application control rules
- 170 Terabytes of threat samples
- 17,500 Intrusion prevention rules
- 250 Million rated websites in 78 categories
- 173 Zero-Days discovered

- 100 Intrusion prevention rules
- 2 Million New and updated antivirus definitions
- 8,000 Hours of research in labs around the globe
- 47 Million New and updated antispam rules
- 1.3 Million New URL ratings
So What Do We Do With Dave?

Date: Thu, 15 Jan 2016 15:07:19 +0100
From: "Internal Revenue Service" <complaints@irs.gov>
To: <pastore@cxo.com>
Subject: Complaint against your company

Dear business owner,

A criminal complaint has been filed against your company.

Your company is being accused of trying to commit tax evasion schemes.

The full text of the complaint file (PDF type) can be viewed on the IRS website, by visiting the following link:


An official response from your part is required, in order to take further action.

Please review the charges brought forward in the complaint file, and contact us as soon as possible by:

Telephone Assistance for Businesses:
Toll Free, 1-800-829-4933

Email: complaints@irs.gov

Thank you,
Internal Revenue Service
Fraud Prevention Department
Training To Raise Awareness

http://krebsonsecurity.com/2012/01/phishing-your-employees-101/

- Policy
- Procedure
- Process

You're Being Phished
Don't take the bait
And At the Opposite End of the Spectrum...
Looking Forward

✓ Technology is only part of the solution
✓ Single vendor solutions may provide an advantage
  ✓ But only if elements actually work together
✓ Remember your network extends beyond you
  ✓ Remote employees, third party suppliers and contractors
✓ Your employees are the first line of defense
  ✓ Equip and use them
✓ Never assume
  ✓ You’re fully protected
  ✓ The network hasn’t already been breached
Understanding the Data Breaches of 2014:
Did it have to be this way?

Vielen Dank!