RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: EXP-T09R

The Seven Most Dangerous New Attack Techniques, and What's Coming Next

MODERATOR: **Alan Paller**

Director of Research, SANS Institute

PANELISTS:

Ed Skoudis

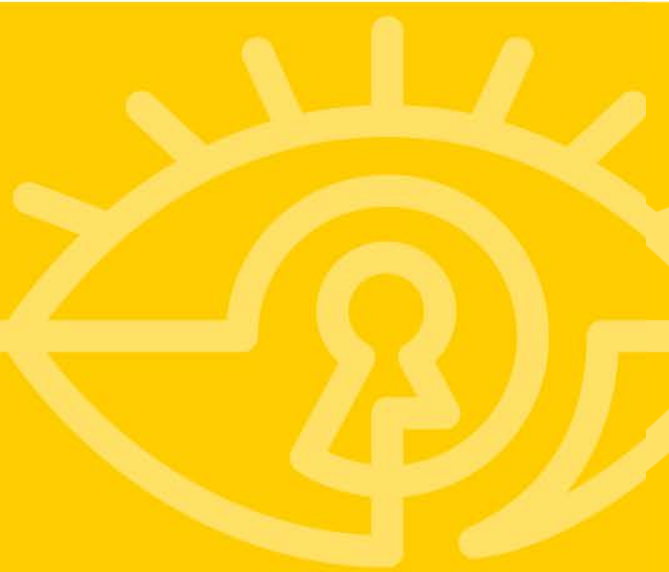
Leads SANS Pen Testing and Hacker Exploits Immersion Training Programs
Created NetWars & CyberCity Simulators
Author of CounterHack Reloaded

Michael Assante

Director of SANS ICS Training Programs
Was VP and CISO of NERC
Directed INL's Electric Power Program
Testified before US House and Senate

Dr. Johannes Ullrich

Dean of Research at STI - SANS' Graduate School
Director of the Internet Storm Center



Ed Skoudis

-- Leads SANS Pen Testing and Hacker Exploits Immersion Training Programs
-- Created NetWars & CyberCity Simulators
-- Author of Counter Hack Reloaded

Top Threats - Skoudis

- Broadening Targets
- Full Weaponization of Windows PowerShell
- What Stagefright Tells Us About Mobile Security Going Forward
- XcodeGhost – How Will You Trust Your Apps Going Forward?

Broadening Targets

- The last 12 months have shown the threat's focus is broadening
  - PII still a target, but much more is in play now
- OPM attack
  - Government background check data and fingerprints
- Ashley Madison attack
  - Sensitive personal information at play
- Extortion malware stealing browser history
- Ukrainian power grid attack

Defenses Against Broadening Threats

- Don’t assume that you are safe just because you lack PII
- Attackers are devising clever uses for all kinds of data with criminal and national security implications
- Vigorously apply robust security standards focused on actual attack techniques used in the wild
- Twenty Critical Controls
- IAD Top 10 Information Assurance Mitigation Strategies
- Australian Signals Directorate Top 4 Mitigation Strategies

Windows PowerShell Weaponization

- PowerShell Empire – Amazing integrated post-exploitation capabilities
  - By Will Schroeder, Justin Warner, and more
- PowerShell Empire features:
  - Powerful agent
  - Pillaging / Privilege escalation
  - Pivoting / Lateral movement
  - Persistence
  - Integrated with attacker operations

- All free and incredibly easy to use, and often works even with application white listing

Weaponized PowerShell Defenses

- Don’t rely on PowerShell’s limited execution policy
  - A safety feature, not a security feature… trivial to bypass
- Enhanced logging in PowerShell 5
  - Pipeline logging, deep script block logging, and more
- Win 10 AntiMalware Scan Interface (AMSI)
  - All script content presented to registered antimalware solution on the box
- PowerShell 5 Constrained Mode and AppLocker integration with “Deny Mode” and “Allow Mode” – behaves like script white listing

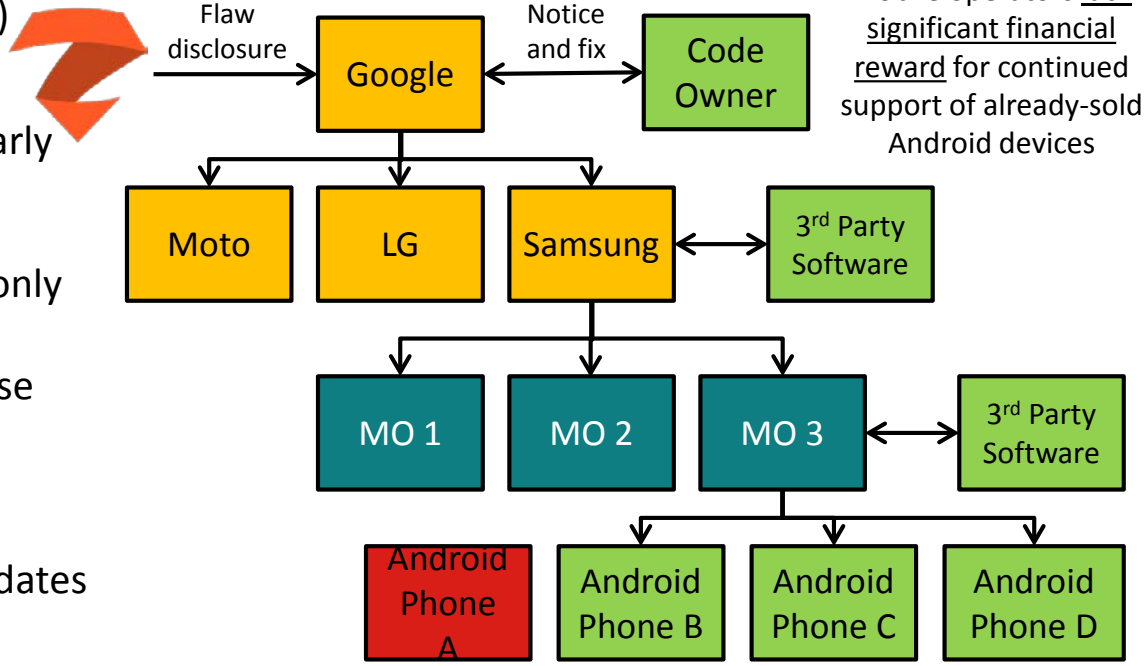
PowerShell ♥ the Blue Team

Stagefright as a Portent of Mobile Vulns

- Stagefright: A series of significant vulnerabilities discovered in Android, all associated with a library that plays multi-media content
  - Discovered by Joshua Drake at Zimperium through exhaustive fuzzing, and then detailed analysis of fuzzing results
- Code execution via text messaging, video viewing in email, browser video watching, and more
- Google patched it quickly…
- ... But there's a problem: For Android devices, the OEMs and Mobile Operators (carriers) sit between the code developer(s) and customers
- Getting patches out in a timely fashion is difficult at best

Stagefright-Style Vuln Defenses

- Upgrade to newer versions of Android (and don't forget iOS!)
  - Implement a corporate strategy for doing so regularly
- Via MDM and network infrastructure, enforce use of only up-to-date versions of mobile operating systems for enterprise apps and data… Deny others
- Give preferential treatment to Android vendors who push updates all the way to devices quickly



Both handset manufacturers and mobile operators lack significant financial reward for continued support of already-sold Android devices

XcodeGhost – Can You Trust Your Apps?

- Historically, attacks against source code and dev tools have proven deeply insidious
- Bad guys can no longer ignore iOS as a malware target
  - With XcodeGhost, they showed innovative ways to undermine iOS
  - Enterprise app store signing is another

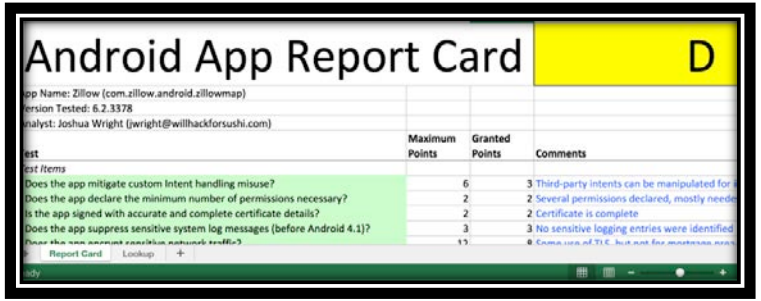
1984
Reflections on Trusting Trust
- Backdoor the compiler

2004-2010
tcpdump, Linux kernel attempt, etc.
- Backdoor the source code

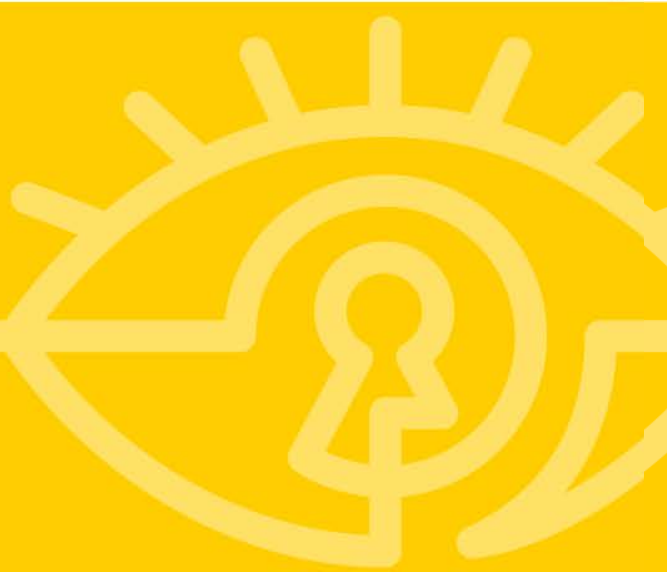
2015
XcodeGhost
- Backdoor the dev environment

XcodeGhost – Implications for Defense

- Analyze the security of permitted apps in your environment
  - Josh Wright's App report card at http:///pen-testing.sans.org/u/64u



- Data isolation from mobile devices
  - Container-based security is waning
  - Virtualized Mobile Infrastructure is rising
- User training can help – don't install untrusted apps… and tell them why
- Look for anomalous activity in the environment
  - New free RITA (Real Intelligence Threat Anslysis) tool from Black Hills Information Security
    - http://bit.ly/BHIS_RITA

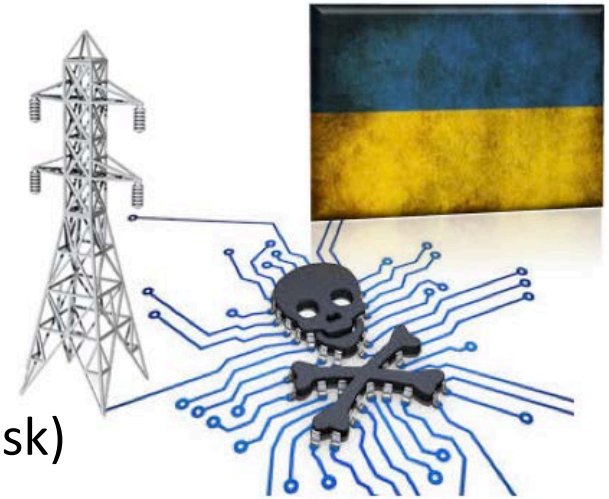


Michael Assante

--Director of SANS ICS Training Programs
--Was VP and CISO of NERC
--Directed INL's Electric Power Program
--Testified before US House and Senate

Lights Out

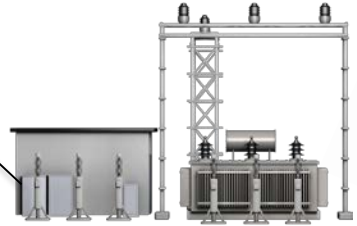
- One, of a hand full: acknowledged ICS attacks with physical effects
- Cyber attacks against 3 Ukrainian power companies on Dec 23
- Successfully cause power outages
- Coordinated & multi-faceted
- Destructive acts
- BlackEnergy 3 Malware plays some role
  - Additional malware (e.g. customized KillDisk)



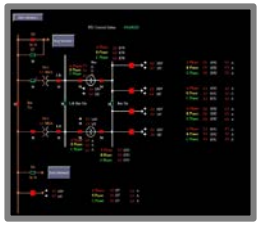
Power System SCADA 101

110 kV Substation

110 kV Substation



35 kV Substation

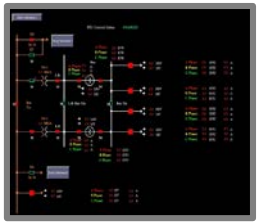


Distribution Control Center

Distribution Utility Systems

Company Network

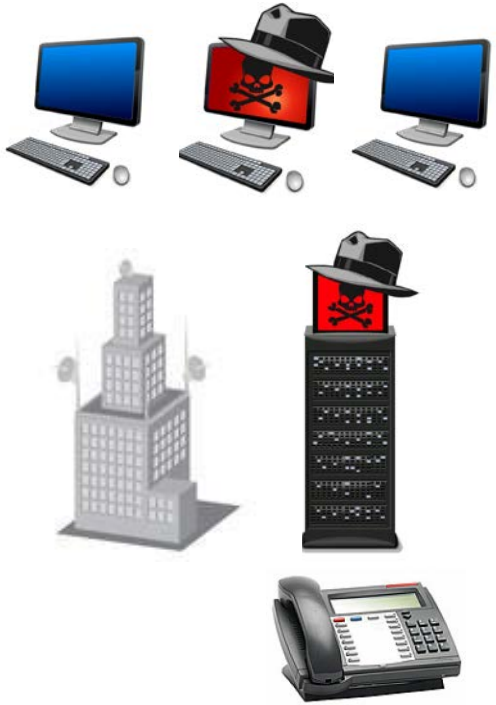
Customer Call Line

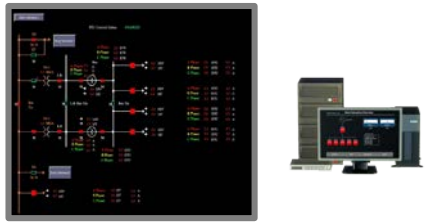


Distribution Control Center
(SCADA DMS)

The Attacks

Malware is simply a tool used for specific actions (e.g. access)





Distribution Control Center

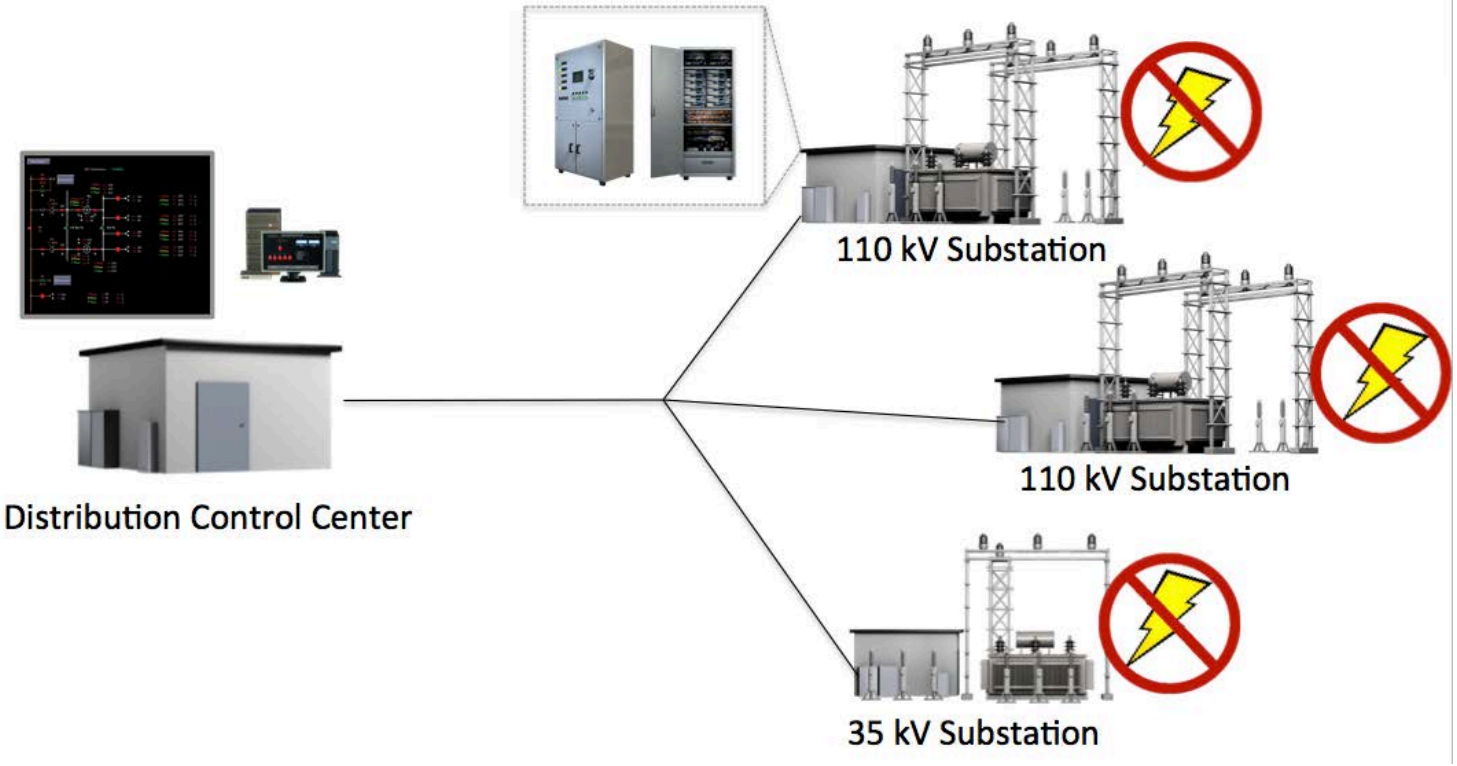
Cyber Attack 1. (ICS Kill Chain)

1. Intrusion (Foothold)
2. Take over credentials & IT
3. Access & remove relevant data
4. Cross-over into SCADA
5. Change the state of power system
6. Damage firmware
7. Wipe SCADA & infrastructure hosts

Cyber Attack 2. (Supporting)

1. Flood Customer Phone Line
2. UPS take over & disconnect

Success…but



Disrupt Power & Anti-restore

Power Grid Cyber Attack

Start

Cyber Intrusion

ICS Intrusion

Attack with Physical Consequence

ICS Kill Chain

Stage 1

- PLANNING: Reconnaissance
- PREPARATION: Weaponization, Targeting
- CYBER INTRUSION – ATTEMPT: Delivery, Exploit
- CYBER INTRUSION – SUCCESS: Install/Modify
- MANAGEMENT & ENABLEMENT: C2
- SUSTAINMENT, ENTRENCHMENT DEVELOPMENT & EXECUTION: Act

Stage 2

- ATTACK DEVELOPMENT & TUNING: Develop
- VALIDATION: Test
- ICS ATTACK: Deliver, Install/Modify, Execute ICS Attack

Cyber Effects

- Host Compromise
- Data Theft
- Persistence & Positioning

"Crossing the Line"

ICS Compromise & Manipulation

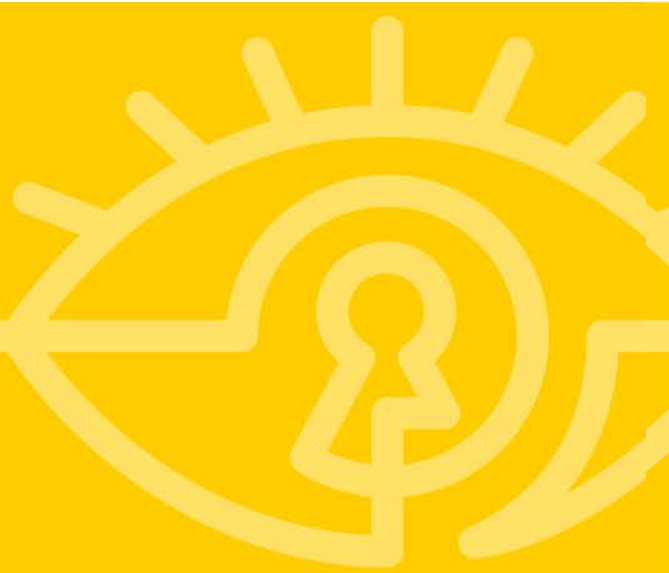
Infrastructure Effects

None

Power Outage Duration

Hours-Day(s) Week(s) Month(s)

- Manipulate-to-Disrupt
- Manipulate-to-Disrupt plus anti-restore
- Manipulate-to-Disrupt (scale & repeated)
- Manipulate-to-Damage



Dr. Johannes Ullrich

-- Dean of Research at STI: SANS' Graduate School

-- Director of the Internet Storm Center

Software Security: Components Matter

- Insecure third party components matter!
- Development environments, software components (libraries) are more and more under attack
- Developer workstations are high on the target list

Apple Xcode Ghost

- Compromised version of Xcode offered for download on Chinese sites
- Compiled software included malicious functionality
- Unnoticed due to trust relationship between Apple and developers

Juniper Backdoor

- Static password added to code.
- Not typical “support password”
- Designed to evade detection
- Who did it?

```
<<< %s(un='%s') = %u
```

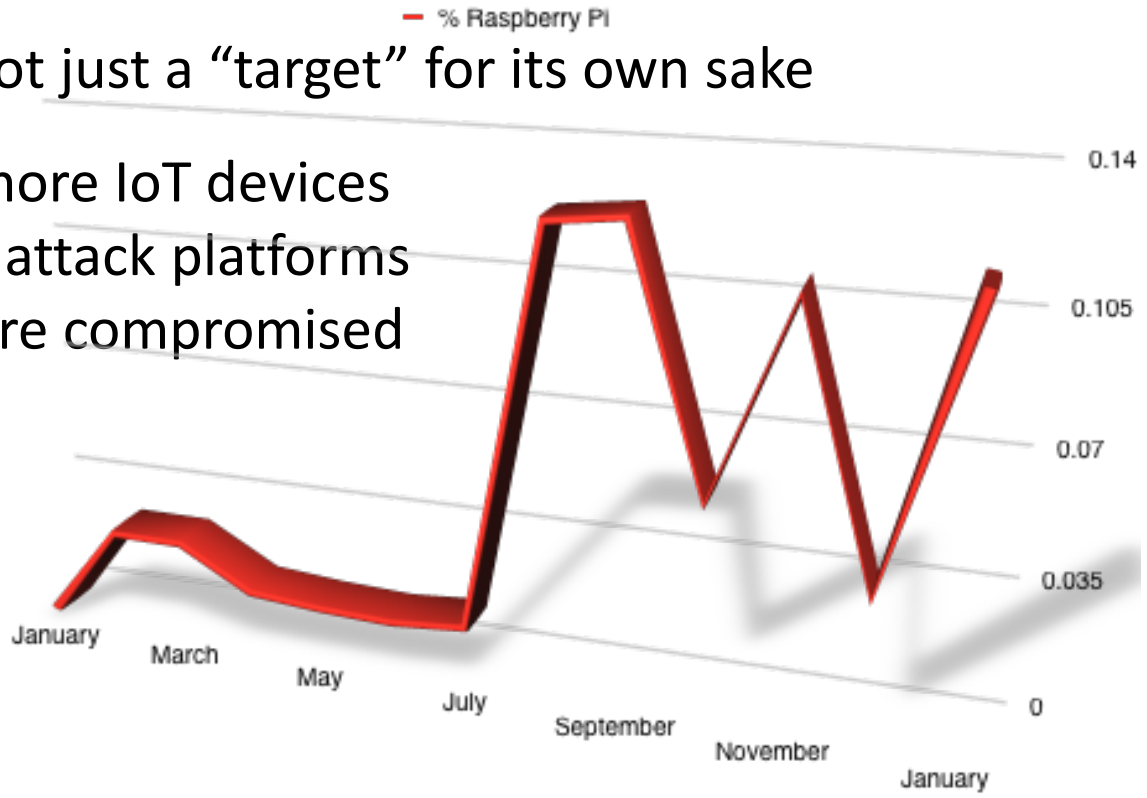
Mitigation

- Accountability: Who did it? Version control systems need to keep a record of which changes were done by whom and why
- Software repositories need regular offline backups
- Traditional code reviews and pentesting will not fix this
- Cryptographic protection against tampering

```
git blame login.html
```

The Internet of Evil Things

- The IoT is not just a “target” for its own sake
- More and more IoT devices are used as attack platforms after they are compromised



Raspberry Pis Attacking!

So it ends up that the devices were Raspberry Pis, default credentials.

Goal:

- Building a proxy or DDoS network
- sometimes: Bitcoins (yes… still!)
- Worst case: Used to attack internal networks

Multi Architecture Malware


```
81896 Jan  1 00:10 10 <- ELF LSB MIPS
82096 Jan  1 00:10 11 <- ELF MSB MIPS
70612 Jan  1 00:10 13 <- ELF LSB x86-64
48996 Jan  1 00:10 14 <- ELF LSB ARM
65960 Jan  1 00:10 15 <- ELF LSB 386
70648 Jan  1 00:10 16 <- ELF LSB PowerPC
65492 Jan  1 00:10 17 <- ELF LSB 386
 2133 Jan  1 00:20 bin2.sh
```

Brute Force Architecture Detection

- All versions are downloaded and execution is attempted for all of them.
- Initial infection usually implement simple bot (IRC/HTTP as C2C)
- Additional components are downloaded later for specific architectures
- “busybox” replaced with trojaned version

Change in Malware Economics

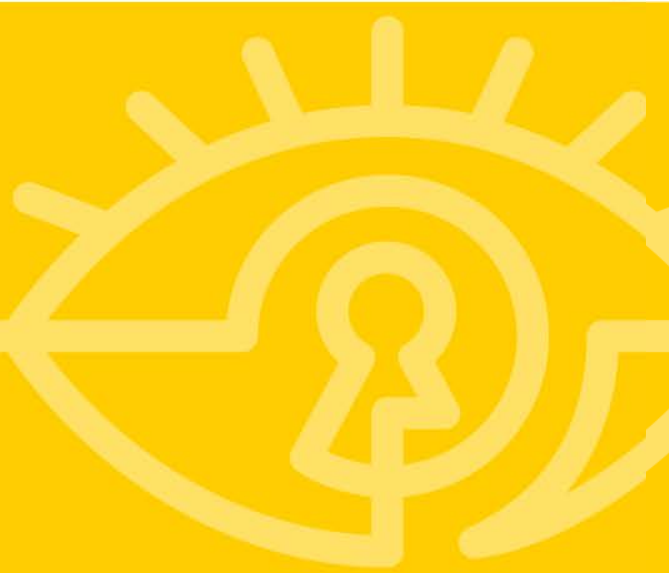
- 170 Million Credit Card Holder vs 61 Million Stolen (2014)
- 450 Million issued SSNs vs 22 Million Stolen (just OPM hack)
- 142 Million registered voters vs. 191 Million records leaked

ALL DATA HAS BEEN STOLEN

little value in stealing the same data over and over.
Reducing scarcity = Reduced Price

Ransom Ware

- Instead of copying data: Encrypt it
  - Ransom ware has been going on for a couple years now
  - Increasing in sophistication (e.g. platform independent Ransom32)
- Instead of stealing data from a web site: Shut it down
  - Used to be more against fringe (e.g. online gambling) sites
  - Or for political motives
  - Now used against any site with insufficient DDoS protection



Your Questions and Discussion