Data Theft in the 21st Century

Jay Beale

InGuardians Inc.

Copyright 2016

Talk Sections

- Who Am I?
- Theft and Exposure of PII and PEI
- How do I avoid losing the PII?
- How Do We Detect More Quickly and Mitigate?

Copyright 2016 InGuardians, Inc.

Who Am I?

- Co-Founder at InGuardians
- The first job in my career was as a security guy for University of Maryland - University College.
- Created Bastille Linux, first spearheaded at SANS with UMBC and other universities pushing the effort.
- Teach Linux Lockdown classes at Black Hat, Linux conferences and CanSecWest.
- Led InGuardians' penetration testing efforts at University of Maryland - College Park

Copyright 2016 InGuardians, Inc.

Theft and Exposure of Personally Identifiable Information (PII) and Personally Embarrassing Information (PEI)

Copyright 2016 InGuardians, Inc.

Case Studies

- Sony Online Entertainment: 102 Million Customer Records
- Sony Pictures: Network pillaged and systems destroyed, allegedly in retaliation for the film, “The Interview”
- JP Morgan Chase: 76 million customers + 7 million small businesses
- Anthem: 80 million Costumer Records
- Target: 110 million Costumer Records
- OPM: At least 21.5 million people affected, release of highly confidential and classified information

Copyright 2016 InGuardians, Inc.

Sony Breach - Parts I & II

- 2011 Sony Online Entertainment gets hacked. Playstation 77 Million customer accounts stolen
  - Additional 25 million accounts - credit card and personal information stolen
- November 2014 - Sony Pictures gets warning from hacking group #GOP
- Group demands Sony stop release of the movie "The Interview"
- Attackers exfiltrate large amounts of data - Movies, emails, etc.

Copyright 2016 InGuardians, Inc.

Sony Playstation Breach - 2011

- Sony launches "war on hackers"
  - Sony sues George Hotz (geohot) for jailbreaking its Playstation 3 console
  - Sony sues a second Playstation hacker in Germany
- April 2011 - hackers citing above as "unforgivable" launch attack against Playstation Network
- Release of 77 million personal records + 25 million credit cards
- Sony shut down its network for 24 days, and lost $171 million in the attack

Copyright 2016 InGuardians, Inc.

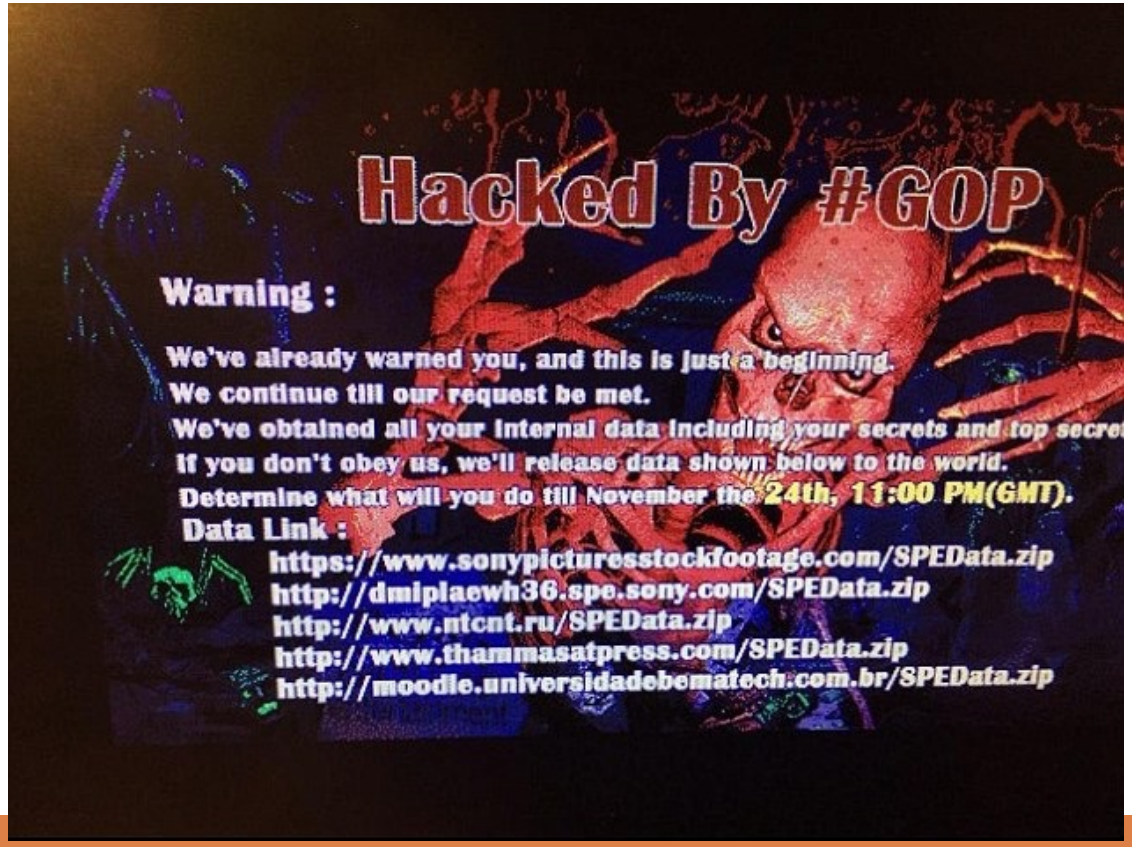
Sony Pictures Breach-Warning Signs

- Norse Security met with Sony Pictures Infosec just before the attack
  - "Their [information security department] was empty, and all their screens were logged in. Basically the janitor can walk straight into their Info Sec department."
- Three days before attack Sony Execs were warned: "The compensation for it, monetary compensation we want. Pay the damage, or Sony Pictures will be bombarded as a whole."

Copyright 2016 InGuardians, Inc.

Sony Pictures Breach - "Detection"

- 7am November 24, 2014 - Sony Pictures employees greeted with sounds of gunfire, threats, & skeleton looming over zombified heads of Sony executives



Copyright 2016 InGuardians, Inc.

Sony Pictures Breach - Effect

- Malware erased everything on:
  - 3,262 of the company's 6,797 PC's
  - 837 of its 1,555 servers.
- Erasure via 7-pass wipe + overwrite MBR
- Damaging emails, including salaries and negotiations
- 48k social security numbers
- 5 Sony films released
- Approximately 450,000 documents published
- Sony reverted back to early 80's. Fax machines, posted messages, and handwritten paper checks.

Copyright 2016 InGuardians, Inc.

Experts Criticizing Defenses

- Ed Skoudis says skill level deployed during Sony Hack: "pretty average"; "It shows the defenses of Sony were not particularly good"; and "I didn't see the bad guys jumping over any extreme hurdles, because there weren't any extreme hurdles in place."
- Fortune article, "based on more than 50 interviews with current and former high-level executives at Sony, cybersecurity experts, and law-enforcement officials. " states:
- Experts say Sony's electronic security probably wasn't worse than that of many others; weak, outmoded practices are the norm at far too many companies. … Sony, which failed to employ several basic safeguards, didn't put up much of a fight.

Copyright 2016 InGuardians, Inc.

Mandiant and the FBI on the Attack

- Kevin Mandia, consultant to Sony, says: “undetectable by industry standard antivirus software.” & “for which neither SPE nor other companies could have been fully prepared”
- FBI: “the malware that was used would have slipped, probably would have gotten past 90% of the net defenses that are out there today in private industry, and I would challenge to even say government”

Copyright 2016 InGuardians, Inc.

Sony Mandiant email

"Dear Michael,

As our team continues to aid Sony Pictures' response to the recent cyber-attack against your employees and operations, I wanted to take a moment to provide you with some initial thoughts on the situation.

This attack is unprecedented in nature. The malware was undetectable by industry standard antivirus software and was damaging and unique enough to cause the FBI to release a flash alert to warn other organizations of this critical threat.

In fact, the scope of this attack differs from any we have responded to in the past, as its purpose was to both destroy property and release confidential information to the public. The bottom line is that this was an unparalleled and well planned crime, carried out by an organized group, for which neither SPE nor other companies could have been fully prepared.

We are aggressively responding to this incident and we will continue to coordinate closely with your staff as new facts emerge from our investigation.

Sincerely,

Kevin Mandia"

Copyright 2016 InGuardians, Inc.

JP Morgan Chase Breach

- 83 million accounts compromised
  - 76 million personal accounts
  - 7 million small business accounts
- Attackers involved in hacking over 12 major financial institutions
- Pump & dump, stock schemes, illegal gambling, and a bitcoin exchange netted the attackers "hundreds of millions of dollars in illicit proceeds"
- 75 shell companies, 30 false passports from 7 different countries

Copyright 2016 InGuardians, Inc.

JP Morgan Chase Breach

- Gery Shalon, Joshua Samuel Aaron, and Zic Orenstein all charged
- Separate charges against Anthony Murgio, for operating unlicensed digital currency exchange
- Attackers used valid login credentials (Aaron's), and the Heartbleed vulnerability to steal the personal data
- Over 100 million customers data stolen - used in pump & dump stock manipulation
  - Emails sent to customers suggesting stocks that the attackers had purchased very cheaply
  - Once stock prices went up, attackers dumped the stock for profit.

Copyright 2016 InGuardians, Inc.

Anthem Breach

- In February 2015, Anthem disclosed it had been the victim of a sophisticated breach
- Fingers pointed to China, Crowdstrike points to Operation DeepPanda
- 80 million health insurance customer Records
  - Names, dates of birth, member ID/ Social Security numbers, addresses, phone numbers, email addresses and employment information.
  - Allegedly no medical information was disclosed

Copyright 2016 InGuardians, Inc.

Anthem Detection

- "On January 27, 2015, an Anthem associate, a database administrator, discovered suspicious activity – a database query running using the associate's logon information."
  - Immediately stopped the query
  - Notified Anthem's Infosec department
  - Additional DBA accounts discovered to have been compromised

Copyright 2016 InGuardians, Inc.

Anthem - DeepPanda - Infoadmin

- Infoadmin (RAT tied to DeepPanda)
  - RAT with malicious payload and dropper
  - Includes DLLs that initiate processes that provide remote access to the attacker
    - Custom protocol over 443/TCP to
      - images.googlewebcache.com
      - smtp.outlookssl.com
  - Use of mimikatz, Htran, pwdump, gsecdump causes FBI and NSA to recommend complete password refresh
    - http://krebsonsecurity.com/wp-content/uploads/2015/02/FBI-Flash-Warning-Deep-Panda.pdf

Copyright 2016 InGuardians, Inc.

Target Breach

- 110 Million Customer Records
- Fazio Mechanical suffers breach via phishing attack.
  - Small HVAC firm in PA worked with Target
  - Attackers stole VPN credentials used to access Target's network
  - Verizon investigation shows: "no controls limiting their access to any system, including devices within stores such as point of sale (POS) registers and servers."
  - Weak and default passwords were used throughout the organization

Copyright 2016 InGuardians, Inc.

OPM Breach

- From Washington Post:
  - "In those files are huge treasure troves of personal data, including "applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and co-workers. Employees log in using their Social Security numbers."

Copyright 2016 InGuardians, Inc.

OPM Breach

- Attackers gained access May 7th 2014 via stolen credentials. They then planted malware that enabled a backdoor for data exfiltration.
- "Discovered" April 15th, 2015 when the agency detected anomalous SSL traffic with a decryption tool. Tool had been implemented in December of 2014
- Approximately 21.5 million current or former Federal Employees, and/or spouses affected
- SF-86 forms obtained - 127 page form detailing background information on individual and family members
- 5.6 million Federal employee fingerprints also stolen

Copyright 2016 InGuardians, Inc.

OPM Timeline

- July of 2014 OPM investigates an intrusion that it traces to China
  - OPM offers free credit monitoring
  - Assures no personal data was stolen
- August 2014 USIS is hacked. USIS offers 27k DHS employees credit monitoring.
  - Attackers got in via exploiting an enterprise management tool from SAP
- December 2014 KeyPoint suffers breach. "no conclusive evidence to confirm sensitive information was removed"
- June 2015 OPM discloses breach affecting up to 4 million Federal employees. Breach grows to over 21.5 million employees
- December 2015 China arrests hackers responsible for OPM breach.

Copyright 2016 InGuardians, Inc.

Ransomware: Big Picture

- We're seeing a significant uptick in the last 4 months in ransomware that encrypts files on a victim's drive.
- The FBI says that ransomware is on track to be a billion dollar business in 2016.
- Delivered by phishing and drive-by ads
- Some droppers are written as Javascript, which downloads exploit kits like Angler.
- Now being deployed with techniques seen only from APT and professional penetration testers/red teams.
- Achieve domain admin rights, then deploy on org. Example: Use GPO to deploy.

Copyright 2016 InGuardians, Inc.

Ransomware Theories

- This has happened at the same time as a downturn in advanced persistent threat (APT) activity.
- Anecdote: ransomware installed on systems in the order they were listed in the help desk password list
- Several theories for this:
  - Money: China cutting contractors loose, who then must monetize previous access.
  - Misdirection: China arresting hackers, giving previous access to organized crime

Copyright 2016 InGuardians, Inc.

How do I avoid losing the PII?

Copyright 2016 InGuardians, Inc.

Challenge: Higher Ed Networks

- You have the hardest type of network to defend.
- Far more diversity of purpose.
- More stakeholders with far more political capability.
- Often: de-centralized IT with different standards.
- Often: default-allow inbound firewalls.

Copyright 2016 InGuardians, Inc.

Mitigations

- Default-deny Firewalls
  - Get as close as you can to default deny
- Segment your network internally
- Use domain administrator privileges sparingly
  - Windows Protected Users group
- Set temp spaces non-executable (ransomware)
- Communication
  - Many of you have federated IT
  - A few beers every week with the other IT/IS departments on campus -> priceless

Copyright 2016 InGuardians, Inc.

How do we detect more quickly and mitigate?

Copyright 2016 InGuardians, Inc.

Sun Tzu says:

To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.

Copyright 2016 InGuardians, Inc.

Detection and Mitigation Axioms

- Got root? You MUST analyze your logs
  - Analyze for performance, operations, and security
- Just because something is configurable, doesn't mean people will configure it
  - Not only are IDS'es tunable and configurable, they MUST be tuned and configured
- If someone attacks your Linux Apache server with a Windows IIS attack, should you care?
  - Focus your deployment on attacks likely to succeed in they environment you are trying to protect
- You MUST segment your network with ACL's.

Copyright 2016 InGuardians, Inc.

Traditional - Bare minimum

- Traditional Network Security
  - Packet Filters & Firewalls - If it doesn't do layer 7, its not a firewall
  - Proxies - forward and reverse
  - IDS - requires analysts to function
  - Network transaction logging (Network flow, netflow, jflow, sflow, etc)
  - System and application logging
  - Encryption protocols used for comms

Copyright 2016 InGuardians, Inc.

Next Steps

- Two factor authentication
  - We have been recommending this since the 90's
- Full time analysis team
  - Either MSSP or in-house
- Hunt teaming
  - InGuardians is doing more and more hunt teaming
  - Assume you are hacked - go find out where and how badly.
- Bro
  - Index of network transactions, sandbox executables, unpronounceable DNS names, SSL analysis
- Deception & Counter Intelligence - Honey technologies
- Network Early Warning Systems

Copyright 2016 InGuardians, Inc.

Network Early Warning Systems

- Centers for Disease Control Model
  - Local hospitals report of outbreaks
  - Centralize monitoring, reporting, and trending
  - Mobilization of resources - local, national and global
  - Goals
    - Contain outbreaks
    - Lessons learned

Copyright 2016 InGuardians, Inc.

What is the value proposition?

- Identify Patient Zero
  - Identify indicators or compromise
  - Identify vector of compromise
  - Search the network for those indicators
- Quickly shut down the vector of compromise
- Isolate infected systems to initiate containment

Copyright 2016 InGuardians, Inc.

Why is this happening?

- Abundant attack vectors – all it takes is one tiny misstep:
  - Company infrastructure security issues
  - Supplier security issues
  - Social engineering
- It isn't that difficult, motivated hackers are persistent, jackpot can be lucrative
- The job of protecting all possible attack vectors is extremely challenging – nearly impossible; it's comparable to defending against guerrilla warfare
- High probability that a compromise will occur with competent motivated hackers, making quick detection and containment urgent before further damage occurs

Copyright 2016 InGuardians, Inc.

But, We Have Detection in Place and We Still Got Pwned!

- Packet loss
  - Hardware insufficient and not powerful enough for the traffic volume
  - Bloated rules or configurations
- Analysis failures
  - Improperly placed sensors
  - Rules not updated frequently enough
  - Untrained analysts
  - Sensors alerting – no one listening
    - Neiman Marcus 350,000 customer records over a 3-month time span with 60,000 alerts unnoticed

Copyright 2016 InGuardians, Inc.

Keys to Early Warning Systems

- Instrumentation
  - System and application logs, packets, network logging
  - Honeypots & tarpits
- Automated Reporting
  - Pull statistical reporting
  - Visualization
- Analysis
  - Axiom: If you retain logs, analyze them!
  - Sysadmin rule: If you "got root", you must review your logs

Copyright 2016 InGuardians, Inc.

Indications & Warnings

- IDS/IPS alert
- Log data correlation
- SIEM correlation of alerts and log records
- Anti-virus/host-based signal
- Unusually high/low network throughput
- Visualization spike
- A call from Brian Krebs

Copyright 2016 InGuardians, Inc.

Readiness: USB thumb drives

- How do we help organizations get ready for inevitable compromise?
- Train help desk to respond to incidents with skill?
  - Side effects: lose help desk to security
- Thumb drives with Volatility / memory capture tools
  - Buy USB thumb drives 2-4x the size of RAM
  - Add Volatility or other copy-RAM tools
  - Instruct help desk to dump RAM before reboots.
  - Throw it in a box.

Copyright 2016 InGuardians, Inc.

Honey Technologies

- Honeypot/net
  - High interaction: Systems and/or applications that give an attacker interactive sessions
  - Low interaction: covered on next slide.
- Honeytoken – Data that serves no other purpose than to lure attackers
- Honeytable – Database tables that have no connection to the code, and are used to identify attackers
- Honeyclient – Great for feeding reverse engineers with targeted malware (primarily research)

Copyright 2016 InGuardians, Inc.

Low-Interaction Honeypots

- In the Honeynet project, we deployed high-interaction honeypots.
  - Very high buck for your bang ratio.
- Low interaction honeypots tip that ratio the other way, getting you more information about where the attackers are.
- If a machine communicates with a honeypot, it is:
  - confused
  - malicious
  - compromised

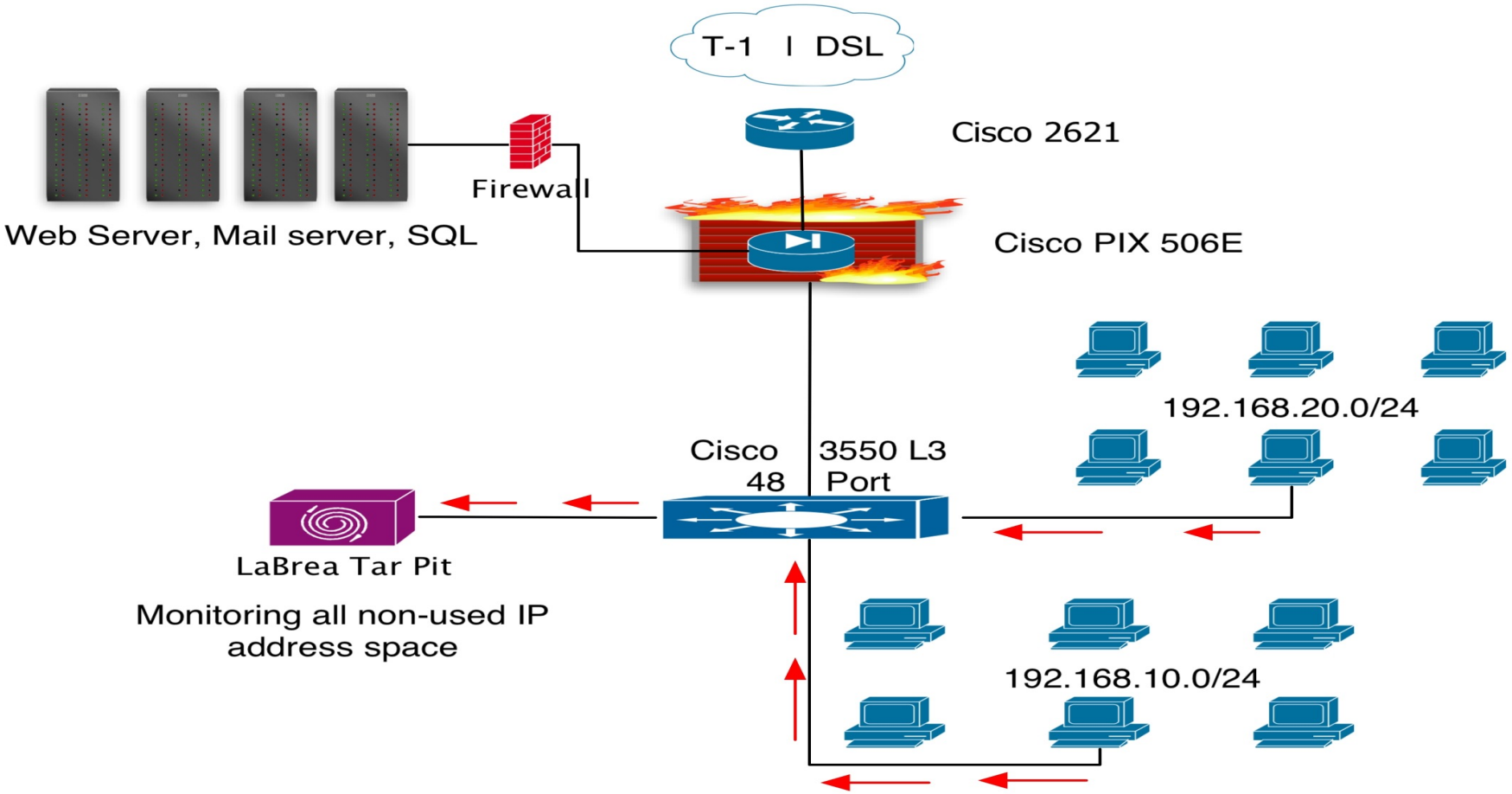
Copyright 2016 InGuardians, Inc.

LaBrea Tar Pit

- Written by Tom Liston originally to “slow down worms”
- Open Source software
- 300,000 Code Red infested machines
  - Each with 100 Scanning threads
  - 8bps per 3 threads
  - 80,000,000 bps required to contain
  - 1000 T-1 sites running La Brea using up to 5.2% of bandwidth

Copyright 2016 InGuardians, Inc.

LaBrea - Internal Patient Zero Detection



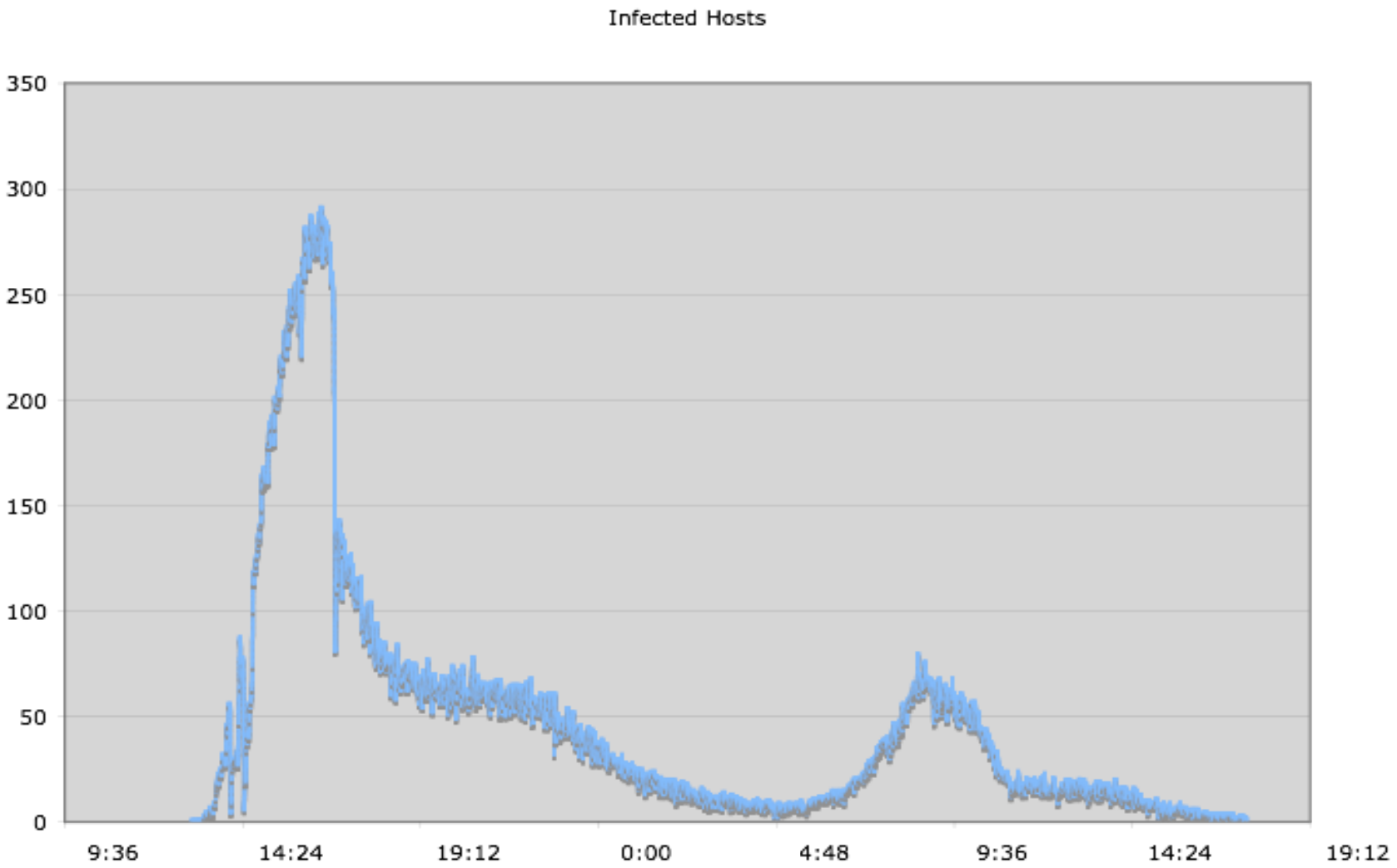
Copyright 2016 InGuardians, Inc.

Real World Example

- Company has LaBrea tarpits installed on one empty class-C network at each site
- LaBrea runs on small embedded Linux boxes
  - $150 USD, http://www.soekris.com
  - Analogous to today's Raspberry PI
- LaBrea sends secure syslog-ng to a central server
- Perl scripts run on the central server analyzing and sending notifications
- Tarpits have been used to identify patient zero **four times this year**
  - Because all detected events on a tarpit are noteworthy, detecting malware requires very little filtering/processing of log data
- Conficker began to propagate on the network
  - Incident Response activated and patient zero identified within 15 minutes of initial infection
  - LaBrea data was used to track worm propagation and remediation efforts

Copyright 2016 InGuardians, Inc.

Conficker on a 30k node network



Copyright 2016 InGuardians, Inc.

Firewall Log Analysis

- Excellent source for intel gathering
- Pareto's law: 80% of your logs are from 20% of your IP's.
- Top 25 IP's and random sample of lowest 10 IP's in your firewall "dropped" logs
- Run each of these IP addresses through:
  - IDS logs - find attacks that get through
  - Critical Web, SMTP, DNS logs - find zero day or lack of signature coverage

Copyright 2016 InGuardians, Inc.

Unique User Agents

- **$ cat access.log | cut -d \" -f 6 | sort | uniq -c | sort -rn**
- 1214 Mozilla/4.75 (Nikto/1.32)
  - 568 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
  - 564 Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/124 (KHTML, like Gecko) Safari/125
  - 363 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
  - 3 </script> HTTP/1.0
  - 2 SurveyBot/2.3 (Whois Source)

Copyright 2016 InGuardians, Inc.

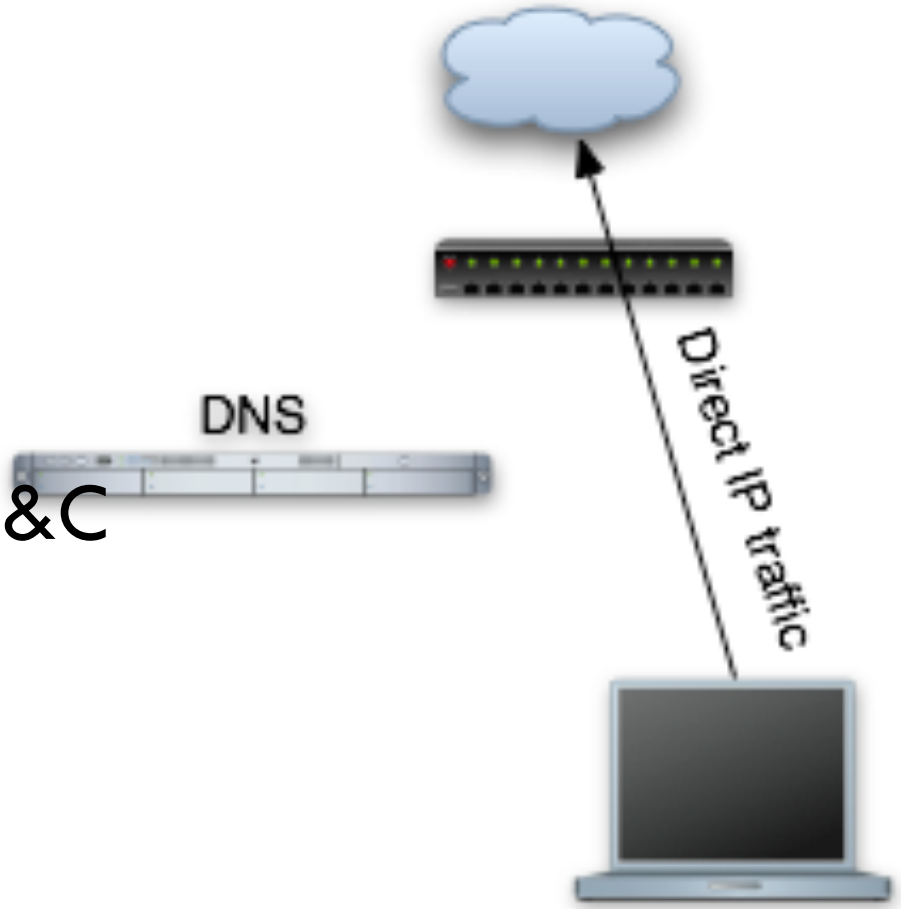
Unique URL's

- Flat file database of unique URI's sent to webservers
- Alert for every new unique one
  - Zero day cgi/web app exploitation detect possible
  - New Nikto / Nessus cgi plugin identification
  - New applications for inventory
  - SQL Injection
  - Blind SQL Injection
  - Database table enumeration

Copyright 2016 InGuardians, Inc.

Unresolved IP Traffic

- Use split-split or split-horizon DNS
- Check for unresolved outbound IP traffic
  - Indicative of preconfigured bot C&C
  - Potential falsing for outliers / official monitoring



Copyright 2016 InGuardians, Inc.

Advanced Persistent Testing™

- Pilot and Test Your Monitoring
  - Controlled environment
  - Known traffic, bandwidth, exploits
  - Pre-defined exploitation
  - Evaluate veracity of story that you can tell with your logs.
  - If you can't tell a story you know, how do you tell a story that you don't know?
- Red Team
  - Professional skilled attackers (yours or another company's)
  - Full emulation of common attack vectors

Copyright 2016 InGuardians, Inc.

Continuous Risk Evaluation

- Continuous vulnerability checking
- Don't just test the box for a vulnerability
  - Test to see if you can leverage exploitation to gain access to the crown jewels – i.e. pivot and pillage the database
  - Can exposure be leveraged to hurt the bottom line
- Provide feedback loop to operations
  - If firewall changed, exposure levels will be different
  - Process & change control used to reduce exposure

Copyright 2016 InGuardians, Inc.

Automated Reporting

- Scripts that pull reports periodically
  - Hourly, daily, weekly, monthly, quarterly and yearly summary reports
  - Statistical and heuristic reporting
    - Session length
    - Session data transfer (inbound and outbound)
    - Top talkers, top firewall and ids offenders
    - NBS: **Never before seen** (by Marcus J. Ranum)

Copyright 2016 InGuardians, Inc.

We check SANS Internet Storm Center every morning - NSA

Copyright 2016 InGuardians, Inc.

Analysis

- Situational awareness
  - Maintain a searchable archive/wiki of incidents
  - Read global N.E.W.S. intelligence sources e.g.:
    - SANS Internet Storm Center http://isc.sans.org
    - ATLAS from Arbor http://atlas.arbor.net/
- Dedicated analysis
  - Large enterprise: full time analysts
  - Medium enterprise: sysadmin log review requirement
  - Small business: Secure and instrument, read auto generated reports

Copyright 2016 InGuardians, Inc.

Wrap-up

- Malware and malicious activity will continue to evolve
- Defenses will have to continue to evolve to counter them
- Preventative maintenance is key!
  - Backups
  - Patches
- Prepare for a deluge of data!

Copyright 2016 InGuardians, Inc.

tcp[13] = 0x01

- Thank you!
  - Jay Beale
    - jay@inguardians.com
    - @jaybeale
    - www.inguardians.com

Copyright 2016 InGuardians, Inc.