

NORTHERN UTAH AGA: WHAT EVERY ORGANIZATION SHOULD BE DOING *RIGHT NOW* FOR CYBER SECURITY

Tim Hastings
Director, Consulting Services
Mandiant Consulting
State, Local Government and Education

COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Introduction

- Tim Hastings, Director, Consulting Services - State, Local Government and Education
- Responsible for leading the incident response and strategic services at Mandiant Consulting for SLED
- Former CISO for the State of Utah
- More than 17 years of experience in assessing and developing information technology, security and privacy processes and controls. Tim specializes in security risk and compliance, working with his clients to build security management programs aimed at achieving compliance, reducing risk and providing enterprise value.

2 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



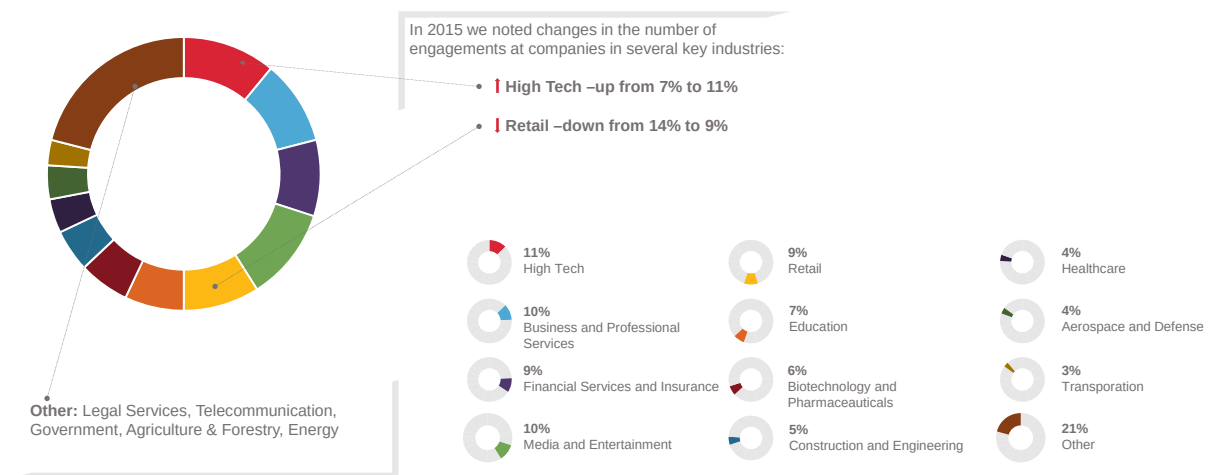
Agenda

- Attack landscape
 - Targets
 - Statistics
 - Trends
- Foundations for a strong security program
- Call to action

COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Who's a Target



4 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Dwell Time

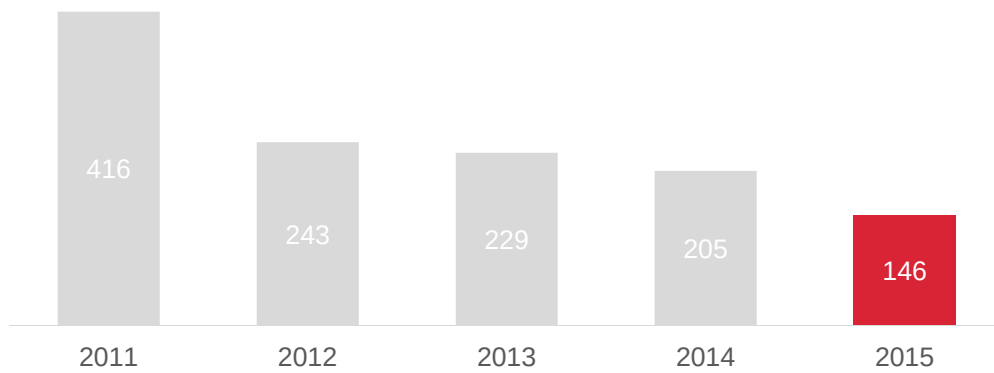


59
DAYS LESS THAN 2014

5 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



M-TRENDS: MEDIAN DAYS BEFORE DISCOVERY



6 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



The Problem With Statistics

- Decreasing median dwell time is a good thing... Right?
- Average of 3 days ← Time it takes my Red Team to achieve domain administrator rights in Windows environments
- Median dwell time of 146 days is therefor 143 days too long
- Lets dispel with a popular myth: Networks are complicated thus an attacker couldn't possibly understand your environment quickly

COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



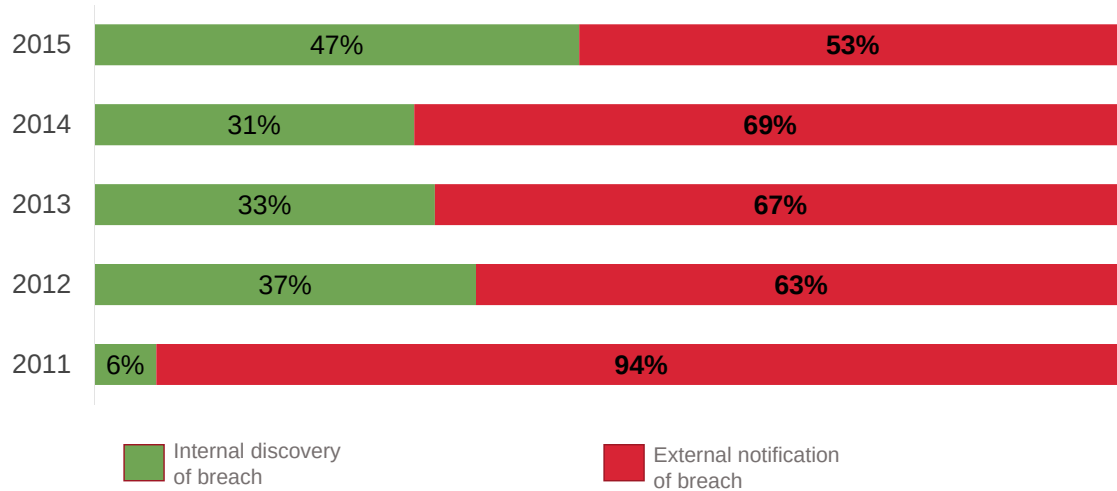
How Compromises Are Being Detected



8 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



M-TRENDS: INTERNAL DETECTION VS EXTERNAL NOTIFICATION

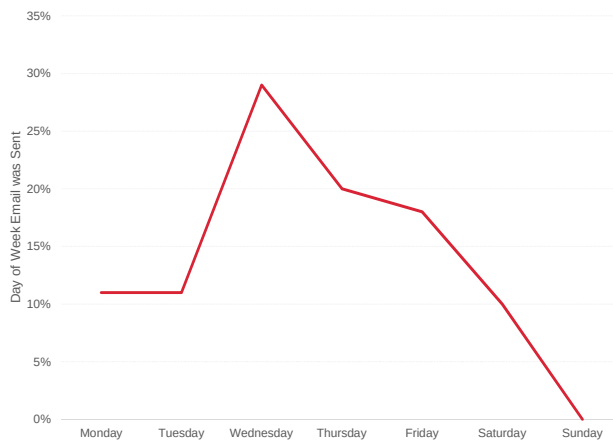


9 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.

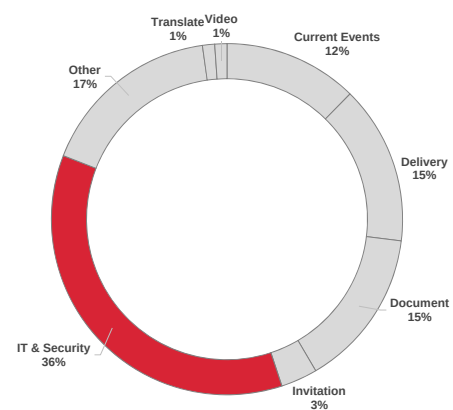


APT Phishing

89% of Phishing Email sent on Weekdays



Majority of phishing emails were IT or security related, often attempting to impersonate the targeted company's IT Department or an anti-virus vendor



10 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



3 Key Observations in 2015



Credentials, in
general



Inability to detect
targeted attacks



Poor egress
controls

11 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Trend 1: David v. Goliath: The rise of business disruption attacks

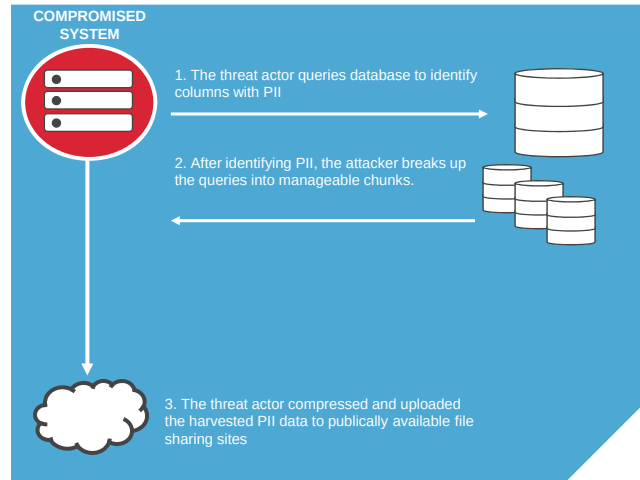


12 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Trend 2: This Time It Is Personal

- Bulk theft of Personally Identifiable Information (PII) by threat actors linked to China.
- The information included Social Security numbers, mothers' maiden names, birthdates, dependents, employment history, and challenge/response questions and answers
- Leveraged the victim's Active Directory information to identify database administrators and their computers
- Demonstrated a thorough understanding of database systems from Microsoft, Teradata, and Oracle, as well as the transaction gateways used to access these systems.



13 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Trend 3: Attacks on Networking Devices

There are numerous reasons why threat actors may target network infrastructure, given the critical role these devices play in a network. Some examples are:



14 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Foundations for a strong security program



15 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Governance and Organization



- Leadership
- Roles and responsibilities
 - *IT*
 - *Security*
 - *Data Owners*
- Policy
- Enforcement

16 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Risk management

Risk Management

- Data ownership
- CIA triangle risk evaluation
- Acceptance
- Monitoring

17 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Visibility

Visibility

- Singular view of network/assets
- Centralized logging
- 3rd party data
- Internal SOC vs. Outsourcing
- Detection capability

18 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Incident response

Incident Response

- Incident response plan
- Teaming
- Outside resources
- Insurance

19 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



Call to action

- All organizations are at risk
- Assign security leadership and establish risk mgmt
- Detection and response capabilities are a must
- Consider what can be outsourced for agility

20 COPYRIGHT © 2016, FIREEYE, INC. ALL RIGHTS RESERVED.



QUESTIONS?

Tim Hastings
Director, Consulting Services
State, Local Government & Education
Mobile: 1 (801) 580.4505
Email: tim.hastings@fireeye.com | Web:
<http://www.Mandiant.com>

