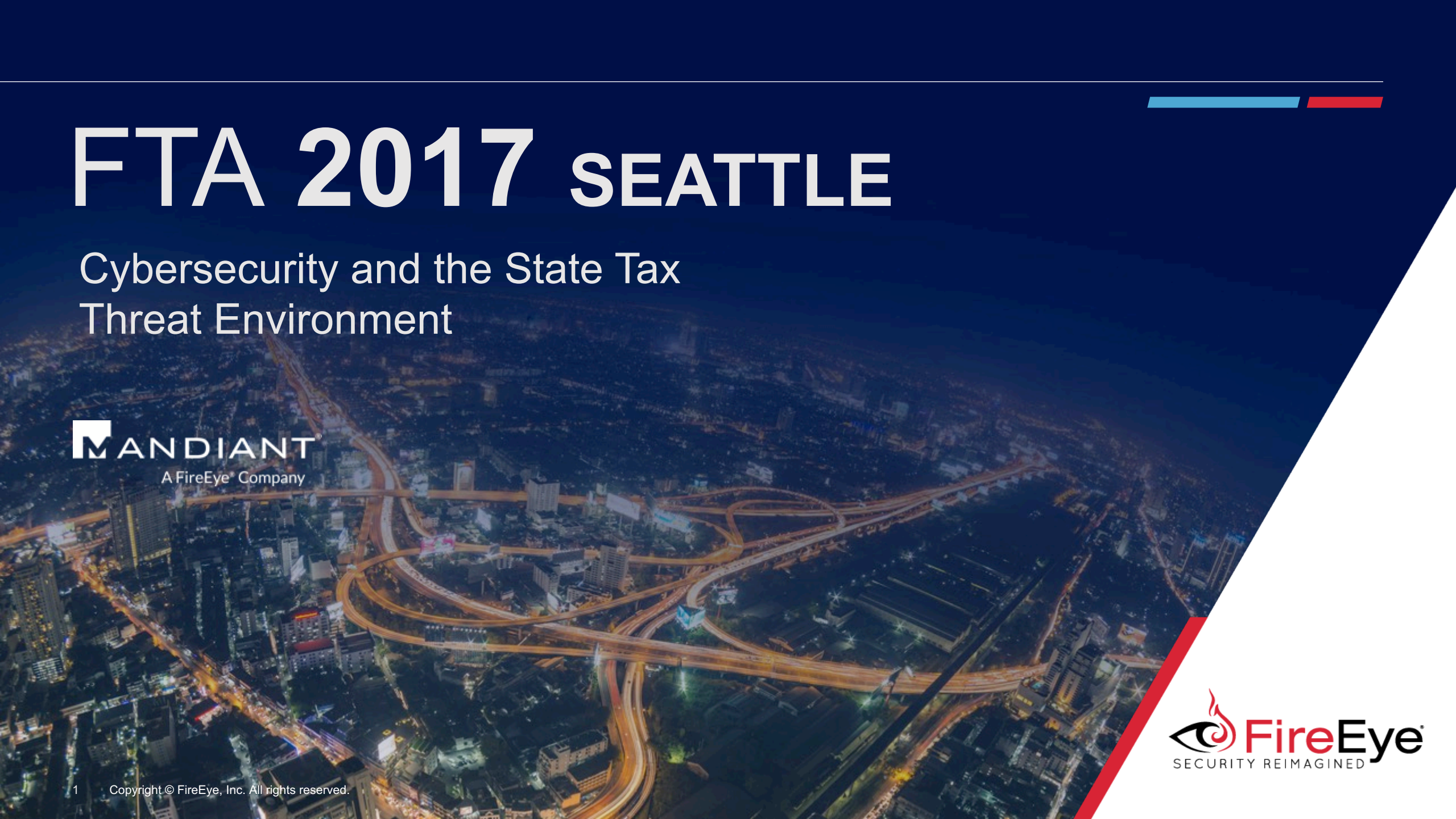
FTA 2017 SEATTLE

Cybersecurity and the State Tax Threat Environment



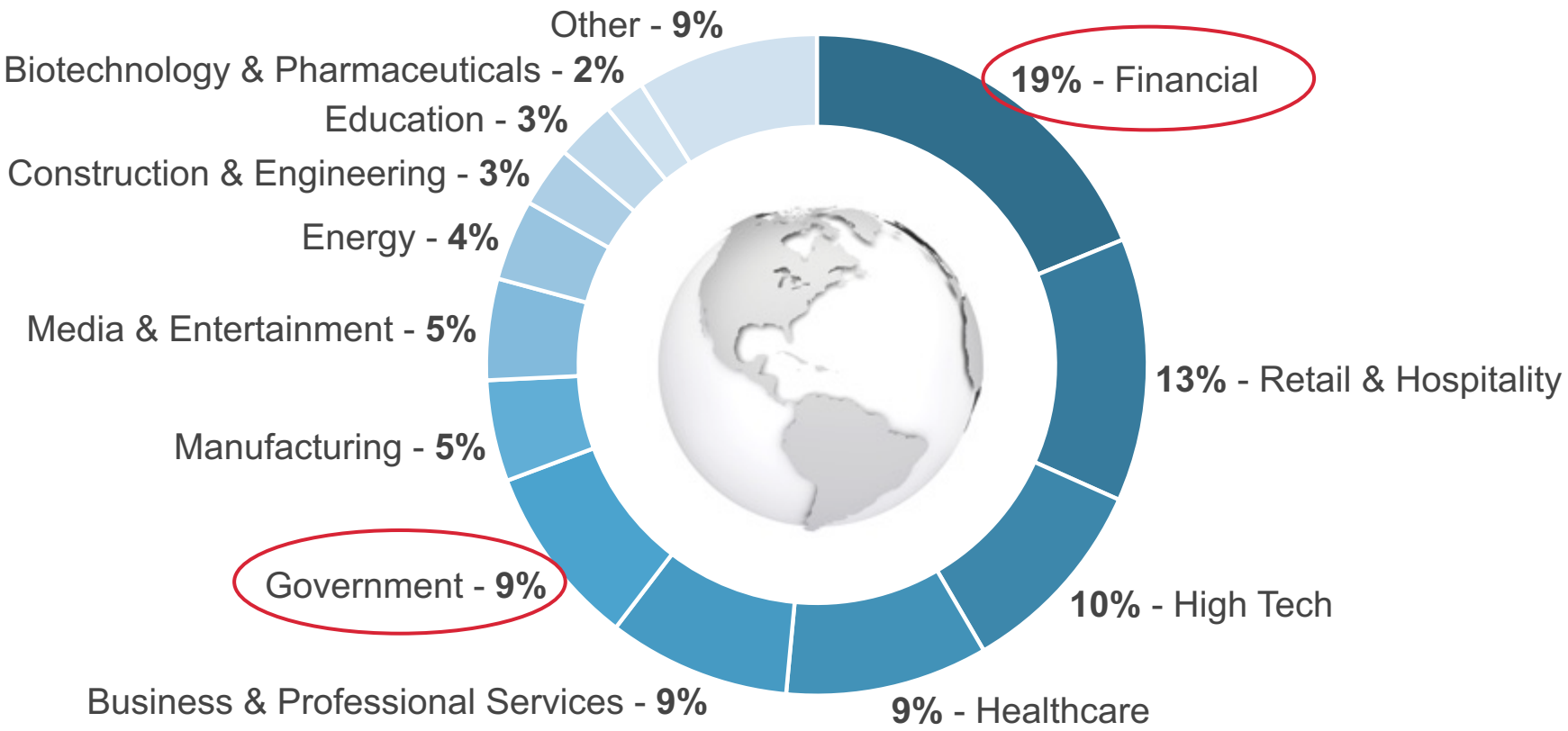
MANDIANT
A FireEye® Company

FireEye
SECURITY REIMAGINED

Agenda

- Cybersecurity Trends
  - By the Numbers
  - Attack Trends
  - Defensive Trends
- State and Local Intelligence
- What Can You Do?

2016: Who's a Target



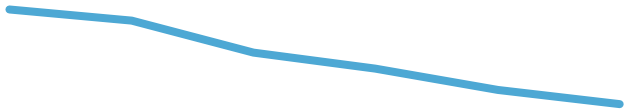
Other: *Telecommunications, Transportation & Logistics, Nonprofit*

2016: Dwell Time

99

DAYS

47



Days Less Than 2015

Detection
vs.
Dwell Time

Internal:	80
External:	107

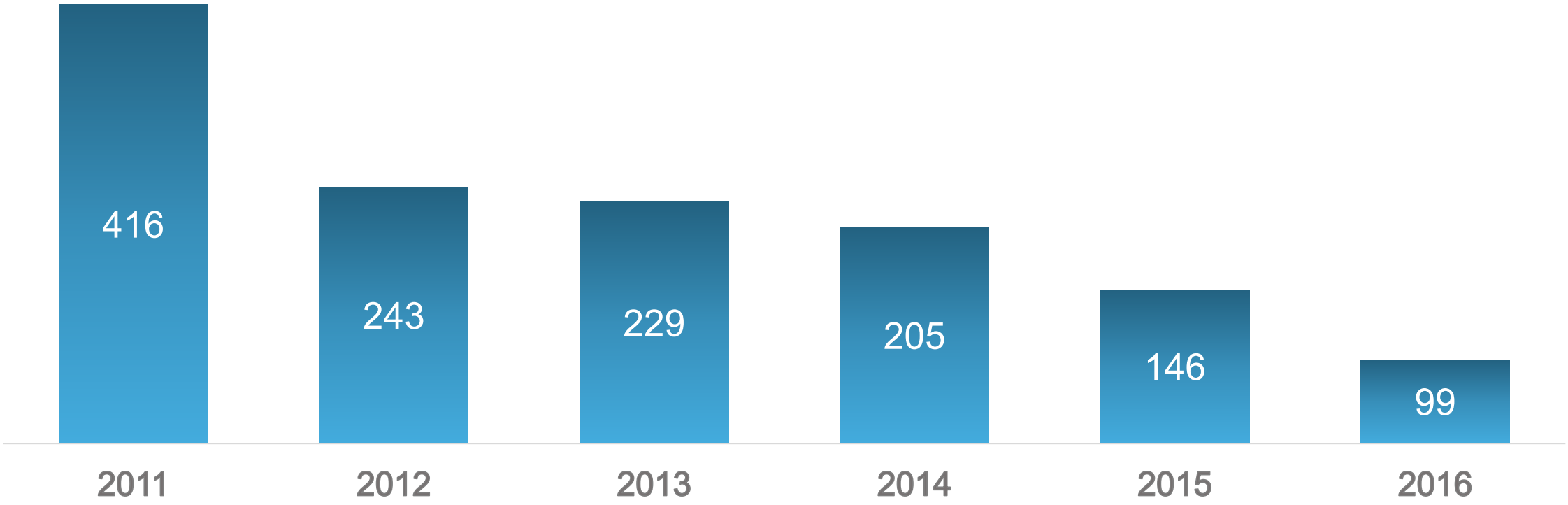
Breach to Discovery

Median time from breach to discovery is getting shorter but still remains too long

MANDIANT
A FireEye® Company

FireEye

M-TRENDS: Median Dwell Time



MANDIANT
A FireEye® Company

FireEye

How Breaches Are Detected

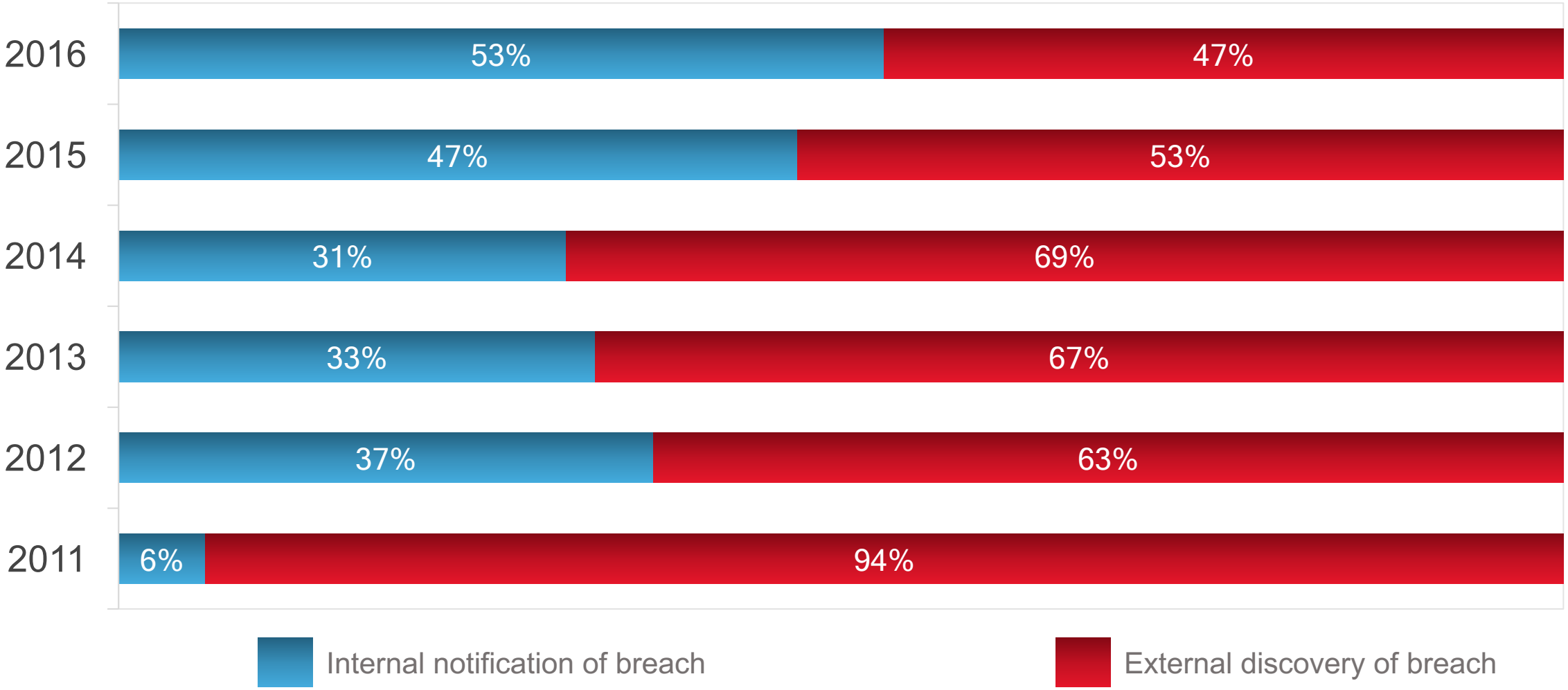
53% INTERNAL DISCOVERY OF BREACH

47% EXTERNAL NOTIFICATION OF BREACH

MANDIANT
A FireEye® Company

FireEye

M-TRENDS: External Notification vs. Internal Detection

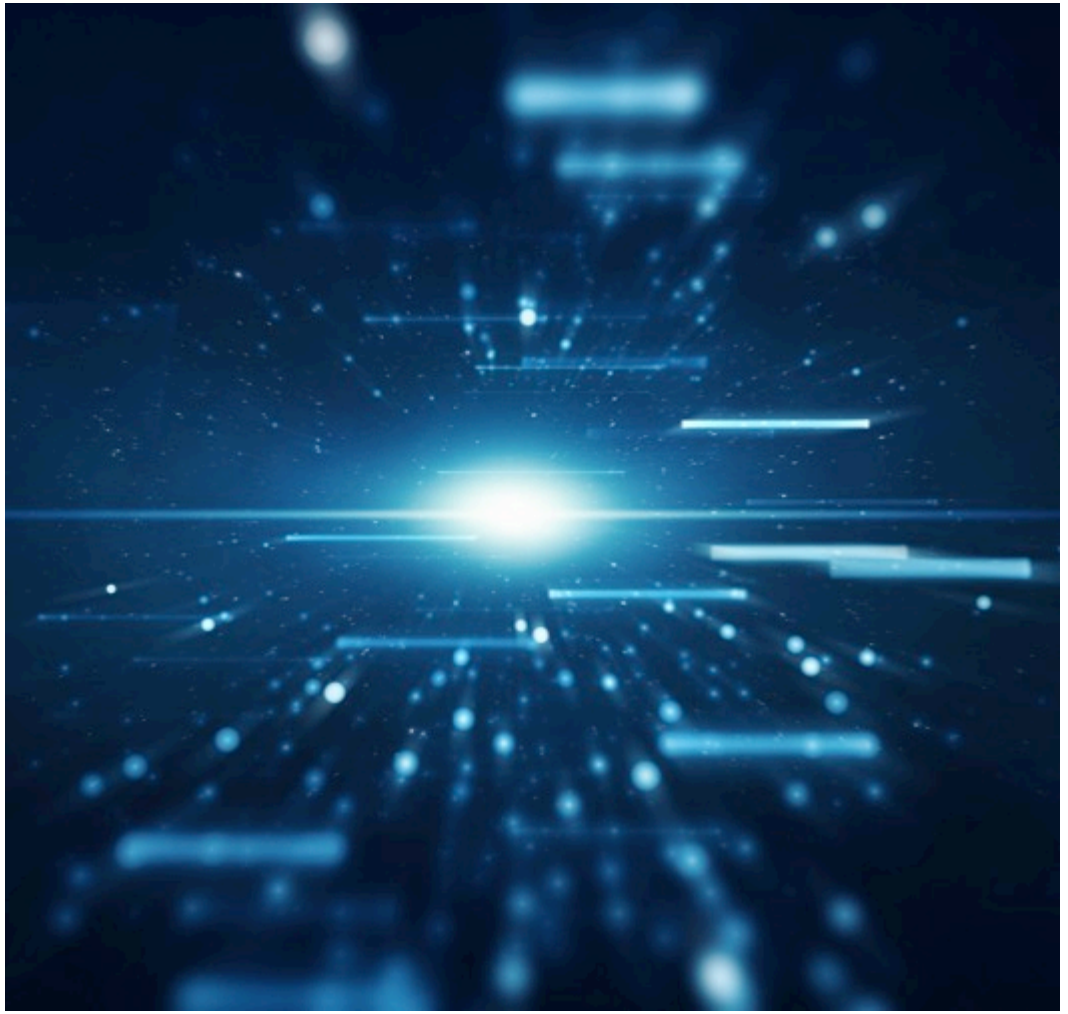


MANDIANT
A FireEye® Company

FireEye

The Problem With Statistics

- Decreasing median dwell time is a good thing … right?
- Time it takes a Mandiant Red Team to gain domain administrator privileges: **~ 3 Days**
- Therefore, median dwell time of 99 days is 96 days too long



Attack Trends

Attack Trends

- Financial Crime - prior to 2013: “Unsophisticated”
  - Loud and straight-forward
  - Opportunistic
  - Rudimentary toolkits
  - (usually) Basic skills
- Since 2013, sophistication has been steadily increasing
  - 2014 M-Trends: “the lines are blurring between run-of-the-mill cyber criminals and advanced state-sponsored attackers”
  - Larger infrastructure, better toolsets, increased focus on persistence

Attack Trends

- 2016: “The line between the level of sophistication of certain financial attackers and advanced state-sponsored attackers no longer exists”
- Custom backdoors with unique, tailored configurations per target
  - Increased infrastructure resiliency
  - Counter-forensic techniques
  - Increased interest in inter-banking networks & infrastructure
  - ATMs

Attack Trends (cont.)

- Email has always been a major target
- 2016 showed an increase in interesting ways to access email
  - Attackers were seen compromising accounts with multi-factor credentials

Attack Trends (cont.)

- Financial attackers tailor phishing email to specific client, location or employee
- Call victims to *help them*

Defensive and Emerging Trends

Adapting Foundational Defenses for the “New Normal”

- Increased focus and interest on “advanced” capabilities (Automation, Cyber Threat Intelligence, Threat Hunting)
- Difficult to apply advanced capabilities if the basics are not addressed
  - Understanding what systems, applications, and data are critical to the business
  - Complete infrastructure visibility. Network, endpoint, events
  - Credential and privilege management / Multi-factor authentication everywhere and always
  - Network segmentation & data segregation
- Foundational fundamentals should be re-evaluated regularly

Adapting Foundational Defenses for the “New Normal”

- Consequences of weak cyber security foundation:
  - Alert overload
  - Difficulty prioritizing threats
  - Inadequate engineering support for new technology deployments
  - Difficulty stopping or slowing attackers once they have a foothold
- These consequences lead to inefficient investments, lack of infrastructure control, and eventually compromise, data loss, and operational outages

Adapting Foundational Defenses for the “New Normal”

- Not everyone is failing at detection and response
  - In 2016 multiple clients were successful at detecting and responding to Mandiant Red Teams
  - The best time so far against a Mandiant Red is 12 minutes
- Common themes
  - Small external threat surface
  - Robust endpoint controls
  - Skilled & empowered detection & response teams
  - Defined and tested detection and response playbooks

Intelligence Led Security

- Threat Intelligence drives operations and decisions
- Mature from reactive defense to proactive threat hunting
- Continuously assessing, training, and integrating enables the Intelligence program to stay aligned and remain ahead of the next threat

Intelligence Led Security

Cyber Threat Intelligence-led security programs have quickly moved from a “bleeding edge” practice embraced by a few to a capability sought by organizations of all sizes

Tips for creating an intelligence led security program

- Design a strategy with threat landscape awareness
- Consider capability level of your program and the individuals charged with executing it
- Expose your resources to the realities they are likely to face in their daily jobs
- Update strategic plans to align with overall realities

By creating such an innovative environment, you can stay ahead of the threat

State and Local Intelligence

MANDIANT
A FireEye® Company

FireEye

State and Local Government Targeting

Nation-state threat groups steal data, abuse assets

- ✓ Track 7 advanced threat groups that target state and local governments
- ✓ Penetrate networks to steal personally identifiable information (PII) or use infrastructure to attack other targets

Criminals access infrastructure or steal data

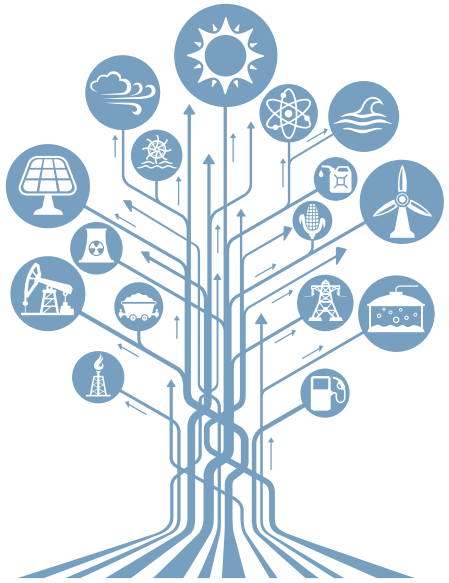
- ✓ Steal tax return and bank account numbers for sale in underground criminal forums

Hacktivists try to gain publicity for their cause

- ✓ Use hacking as a way to protest policy and embarrass governments

Observed Targeting

Targeted Sectors



City and Township Government Organizations
Police Departments
Departments of Transportation
Departments of Finance/Tax/Revenue

Targeted Assets

Payroll
Organization Directories
Legal Documents
Corporate Governance & Standard Operation Procedures
Equipment Maintenance Records and Spec
Financial/Tax Records

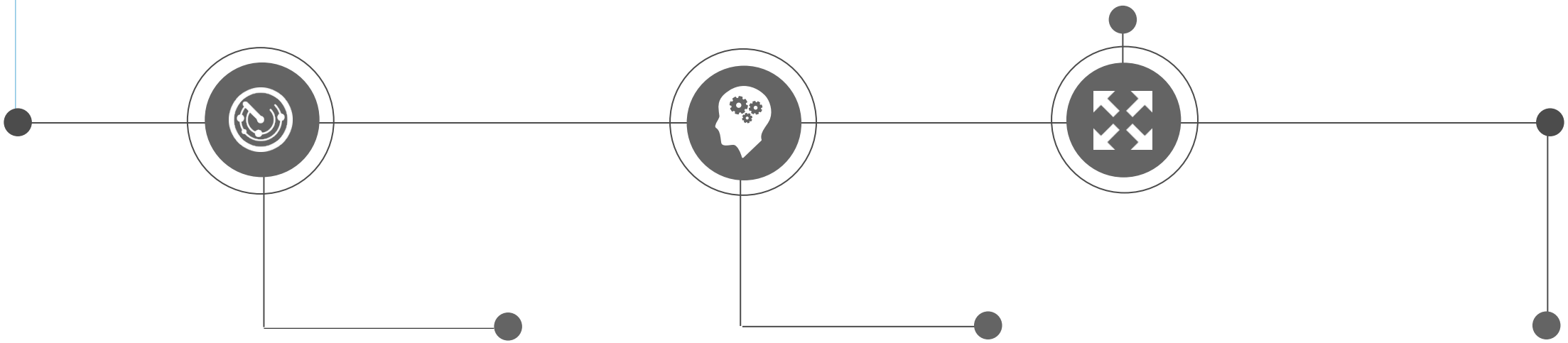
Case Study: Likely FIN1 Targets State and Local Governments

- Targeted a state's **Department of Revenue**
- Enterprise cyber criminal group that we track as **FIN1**
- Group sent targeted **spear-phishing emails** to multiple state employees
- Actors **compromised 44 systems** through password dumping and lateral movement with compromised credentials
- Some of the stolen data included:
  - **~75 GB** of network data
  - **Millions** unencrypted bank account numbers
  - **Millions** tax returns
  - SSNs for Mi**llions** dependents

Case Study: Intelligence in Action on FIN1

WHO ARE THEY? *Financial Motivated Group 1 (FIN1)*

- **Tactic:** *Send targeted emails and password dumping tools*
- **Target:** *Department of Revenue*
- **Impact:** *Attackers accessed 44 systems and stole millions of tax records and bank account information*



HOW DID WE FIND IT?

- State hires Mandiant for IR investigation
- Similar activity, methodology, and malware to previous FIN1 incidents

INFORMS PRODUCT DETECTION

- Deployed IOC across all host-based systems

REPORT PUBLISHED ON FIREEYE INTELLIGENCE CENTER

- Clients warned of operation via the FireEye Intelligence Center

IR INTELLIGENCE

- Gathered intelligence informs log analysis (e.g., terms, IPs, etc.)
- Additional intelligence cycled back into products

MANDIANT
A FireEye® Company

FireEye

State and Local Governments Top 5

TOP 5 MALWARE FAMILIES

FireEye most frequently detected threat actors using the following targeted malware families to compromise state and local governments:

SOGU	(aka Kaba, PlugX) is a backdoor that can upload and download files, execute arbitrary processes, access the filesystem and registry, access service configuration, remote shell access, and implement a custom VNC/RDP-like protocol to provide the command and control (C&C) server with graphical access to the desktop.
MIRAGE	is a backdoor that supports commands for process listing, file listing, retrieving keylogger data, file transfer, remote command execution, and interactive command shell capabilities. The backdoor masks its communications as HTTP traffic using a custom encoding scheme for sending POST data to the C&C server. A configuration file sets the service name and C&C servers used by the backdoor.
EVORA	is proxy-aware backdoor that gives malicious actors the ability to discreetly issue commands on victims' systems. EVORA is typically deployed as a stage-two payload and is part of the Lstudio suite of malware. The main EVORA payload is decoded and loaded into memory, making some aspects of response and analysis more difficult. Additionally, EVORA malware typically comes configured with several C&C domains, making blocking C&C traffic more difficult. EVORA is used by espionage threat actors interested in a variety of industries and regions.
ELISE	(aka Page) is a downloader that attempts to retrieve encoded DLLs from a pre-configured C&C server, with which it communicates using HTTP requests. Once the DLLs are downloaded, the downloader loads them into memory. It also incorporates several source-level anti-reverse engineering functions.
Gh0st	is a remote access Trojan (RAT) derived from publicly available source code. It can perform screen and audio captures; enable a webcam; list and kill processes; open a command shell; wipe event logs; and create, manipulate, delete, launch, and transfer files.

TOP 5 CRIMEWARE FAMILIES

FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in state and local governments:

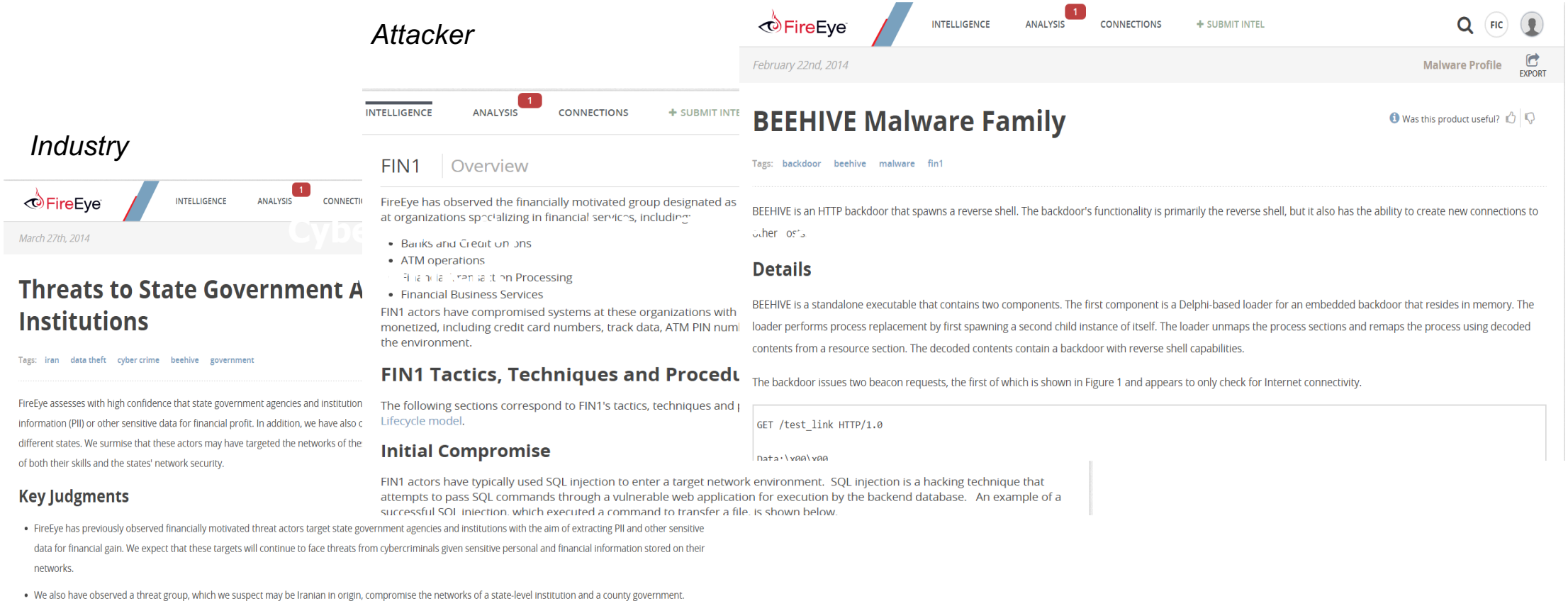
Jenxcus	(aka njw0rm, njworm) is an evolution of the popular tool njRAT that includes additional features such as the ability to spread across removable drives and credential theft. Often delivered via malicious links in email and drive-by downloads on compromised sites, Jenxcus provides the usual functionality of a RAT with additional features such as the ability to spread to new systems through removable drives, such as USB drives, and credential theft. Jenxcus can steal credentials stored in FileZilla and Chrome, and also has the unique ability to capture locally cached credentials for No-IP, a popular dynamic DNS service provider.
Andromeda	(aka Gamarue) is a multipurpose Trojan that can be used as a keylogger, form grabber, or a dropper for other malicious software.
SALITY	is a file-infecting Trojan that can prevent anti-virus software from functioning, send spam, download additional malicious software, and engage in information theft.
Brontok	is a spamming worm that sends copies of itself to everyone in a victim's address book.
Dorkbot	(aka NGRBot) uses Internet Relay Chat (IRC) for its C&C communication and has several robust capabilities, including acting as a user mode rootkit.

Leverage FireEye Threat Intelligence

Tools / Malware

Attacker

Industry



FireEye INTELLIGENCE ANALYSIS 1 CONNECTIONS + SUBMIT INTEL

February 22nd, 2014 Malware Profile EXPORT

BEEHIVE Malware Family

Was this product useful?

Tags: backdoor beehive malware fin1

BEEHIVE is an HTTP backdoor that spawns a reverse shell. The backdoor's functionality is primarily the reverse shell, but it also has the ability to create new connections to other [illegible]

Details

BEEHIVE is a standalone executable that contains two components. The first component is a Delphi-based loader for an embedded backdoor that resides in memory. The loader performs process replacement by first spawning a second child instance of itself. The loader unmaps the process sections and remaps the process using decoded contents from a resource section. The decoded contents contain a backdoor with reverse shell capabilities.

The backdoor issues two beacon requests, the first of which is shown in Figure 1 and appears to only check for Internet connectivity.

```
GET /test_link HTTP/1.0

Data:\x00\x00
```

INTELLIGENCE ANALYSIS 1 CONNECTIONS + SUBMIT INTE

FIN1 | Overview

FireEye has observed the financially motivated group designated as at organizations specializing in financial services, including:

- Banks and Credit Unions
- ATM operations
- Financial Transaction Processing
- Financial Business Services

FIN1 actors have compromised systems at these organizations with monetized, including credit card numbers, track data, ATM PIN numb the environment.

FIN1 Tactics, Techniques and Procedu

The following sections correspond to FIN1's tactics, techniques and p Lifecycle model.

Initial Compromise

FIN1 actors have typically used SQL injection to enter a target network environment. SQL injection is a hacking technique that attempts to pass SQL commands through a vulnerable web application for execution by the backend database. An example of a successful SQL injection, which executed a command to transfer a file, is shown below.

FireEye INTELLIGENCE ANALYSIS 1 CONNECTI

March 27th, 2014

Threats to State Government A Institutions

Tags: iran data theft cyber crime beehive government

FireEye assesses with high confidence that state government agencies and institution information (PII) or other sensitive data for financial profit. In addition, we have also c different states. We surmise that these actors may have targeted the networks of thes of both their skills and the states' network security.

Key Judgments

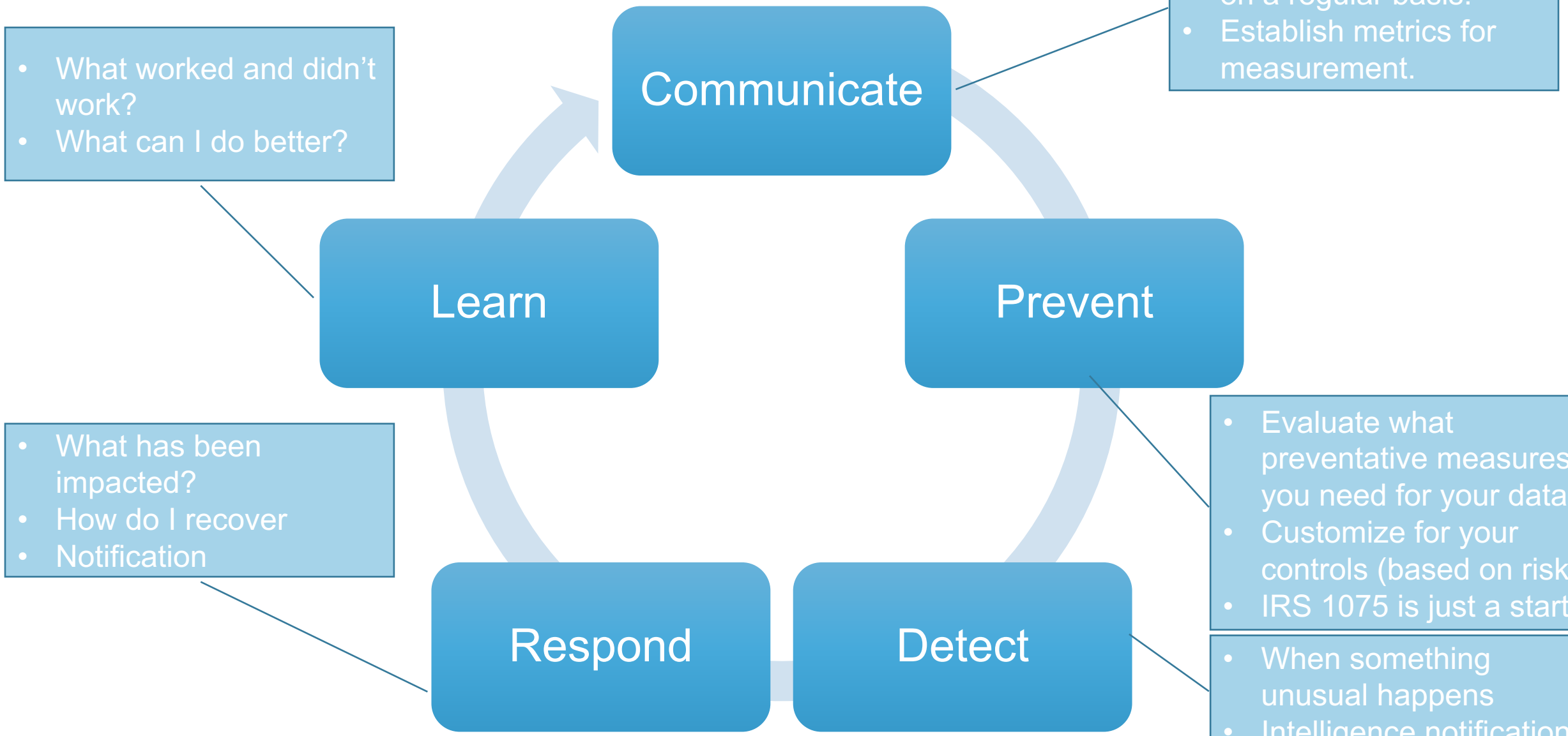
- FireEye has previously observed financially motivated threat actors target state government agencies and institutions with the aim of extracting PII and other sensitive data for financial gain. We expect that these targets will continue to face threats from cybercriminals given sensitive personal and financial information stored on their networks.
- We also have observed a threat group, which we suspect may be Iranian in origin, compromise the networks of a state-level institution and a county government.

What Can You Do?

MANDIANT
A FireEye® Company

FireEye

What you as directors/commissioners can do:



- With you security team on a regular basis.
- Establish metrics for measurement.

- Evaluate what preventative measures you need for your data
- Customize for your controls (based on risk)
- IRS 1075 is just a start

- When something unusual happens
- Intelligence notification

- What has been impacted?
- How do I recover
- Notification

- What worked and didn't work?
- What can I do better?

MANDIANT
A FireEye® Company

FireEye

What you as directors/commissioners can do:

1. Assign security to a team member (CISO or security director)
2. Establish a governance team (technical and business team members) for direction
3. Assess preventative controls
4. Evaluate detection and response capability capability
5. Test everything on a regular basis

Thank You

Tim Hastings
Director, Consulting Services
Mobile: 1 (801) 580.4505
Email: tim.hastings@fireeye.com | Web: http://www.Mandiant.com

MANDIANT
A FireEye® Company

FireEye