WELCOME

Thank you for joining us!
Wi-Fi and Webcast

- Network: FireEyeRSA
- Password: 2019SPUR_guest
- Webcast: investors.fireeye.com
Participate in the Discussion

Use Kahoot! to participate in this interactive discussion:

- Open a browser on your mobile phone
- Type kahoot.it in the browse field
- Enter the game pin for this event → 177889
Today’s Goals

- **Engage** in an interactive presentation
- **Illustrate** the complexity and challenges of today’s security operations
- **Demonstrate** how FireEye is building a platform, differentiated by our threat intelligence and expertise, that address these challenges
- **Encourage** you to learn more about FireEye and our vision for the future of cybersecurity
FireEye @ RSA 2019 – Booth #5959, North Hall

Keynote: A View from the Front Lines of Cybersecurity
Kevin Mandia & Sandra Joyce—Wednesday, March 6, 4:00 – 4:25 pm

Special Topic: Playing with Fire: How Cyber-Physical Attacks Threaten Our Connected World
Sandra Joyce—Tuesday, March 5, 1:00 – 1:50 pm

Panel: Tales from the Front Lines
Stuart McKenzie—Wednesday, March 6, 9:20 – 10:10 am

Classroom: Reverse Engineering Attribution: The Man Behind the Man Behind the Curtain
John Miller & Jayce Nichols—Thursday, March 7, 1:30 – 2:20 pm
Today’s Agenda

8:30 – 8:45  **FireEye Today:** Uniquely positioned to lead in cybersecurity

8:45 – 9:45  **Interactive Case Studies**
The Power of Threat Intelligence
The Attack Lifecycle and FireEye Helix
The Managed Defense Partnership

9:45 – 10:00  **Q&A**
Kevin Mandia
FireEye CEO
RSA 2019 Announcements

**Expertise on Demand**
Access to a full range of industry-leading cybersecurity experts

A full solution of technology, intelligence and expertise working together

**M-Trends 2019 Release**
10th anniversary edition
Median dwell times
New name APT groups
Regional case studies

**Email Security Upgrade**
Now provides full secure email gateway (SEG) functionality

Email detection and protection with one singular solution
M-Trends 2019 – 10th Anniversary

Median Dwell Time by Detection Source

New APT Groups

Retargeted Incident Response Client, by region

<table>
<thead>
<tr>
<th>Region</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>56%</td>
<td>64%</td>
</tr>
<tr>
<td>Americas</td>
<td>44%</td>
<td>63%</td>
</tr>
<tr>
<td>APAC</td>
<td>91%</td>
<td>78%</td>
</tr>
<tr>
<td>EMEA</td>
<td>47%</td>
<td>57%</td>
</tr>
</tbody>
</table>
Recent Accolades

**Endpoint Security MITRE Att&ck**
FireEye ranked #1 reaching highest efficacy and highest number of behavior detections among all participating solutions
Based on Forrester scoring

**2019 Fast Company Innovator**
FireEye earns #6 spot on Fast Company’s global list of 410 companies
Recognized for innovation in cyber security

**Microsoft Intelligent Security Association**
FireEye joins Microsoft association
Shared intelligence with Microsoft products and alliance partners
Breaches are inevitable...
Impactful breaches don’t have to be.
Intelligence for Decisions
The power of threat intelligence in cybersecurity

Grady Summers
CTO
Tool or Weapon?

Is this a weapon?

- YES
- NO
- MAYBE
- IT DEPENDS

Answer at kahoot.it
PIN 177889
Forensic Intelligence

Is this actionable?

YES
NO
MAYBE
IT DEPENDS

Answer at kahoot.it
PIN 177889
Contextual Intelligence

The hammer is found next to a boot print. Local police present intel of a similar boot print found at recent crime scenes in the area within the past 12 months.

Is this actionable?

Answer at kahoot.it
PIN 177889
INTELLIGENCE: THE FOUNDATION FOR EVERY DECISION

MILITARY  SPORTS  BUSINESS
FireEye Ecosystem

FireEye Expertise
- Mandiant Services
- Threat Intelligence
- Managed Defense

FireEye and Third Party Apps

Expertise On-Demand

FireEye Market

FireEye Helix Security Operations Platform
- Next Generation SIEM
- Orchestration & Automation
- Contextual Intelligence
- Compliance Reporting
- Alerts / Case Management

FireEye Network Security and Forensics
FireEye Email Security
FireEye Endpoint Security
Third Party Solutions
This innovation cycle cannot exist without our experts embracing the technology we build as their own, and our product teams embracing the world-class expertise provided by our frontline teams.
Security Incident

Steve Booth
FireEye Chief Security Officer
ACME Co. Security Profile

$3B in revenue, 2,500 employees

- $15M annual IT budget, 3M for security
- 4 dedicated security professionals; average industry experience of 1.6 years
- Implemented O365 for email and collaboration
- Standard security tech stack from various vendors
- No documented and tested incident response plan
- No reverse engineering or threat intelligence capability
You (A/P Manager at ACME) receive an urgent email from Shelly Smith, CFO of ACME. The email includes an attachment that she says is a past-due invoice. She requests the vendor be paid immediately to avoid disruption in the delivery of key manufacturing components.

Which of the following emails look legitimate?

- shelly.smith@acme0.com
- SHELLY.SMITH@ACME0.COM
- Shelly.smith@acmet.com.com
- Shelly.sm1th@acmeco.com

Go to kahoot.it
PIN 177889
Day 1 – 8:35 am

You double-click the attachment to open it, and the Duo sign-in screen pops up. You check “Remember me for 8 hours” so you remain authenticated for the day and enter a passcode. Word begins to load the file.

Word takes forever to load, so you close and try it again. After three tries, you:

- Decide to wait until later and move on to something else.
- Check the “From” address, see it’s fake and delete the email.
- Open a email helpdesk ticket about problem opening Word.
- Call helpdesk about the problem opening Word.
- Go to kahoot.it PIN: 177889
Day 1 – 8:35 am

- The Duo authentication screen is fake and links back to the attackers.
- The .DOCX file was loading from a remote server and established a connection.

Critical Unknowns:

- When the passcode was entered, they gained the ability to log into the corporate VPN.
- While the DOCX was loading, it captured credentials for the local network.

In the meantime:

- Helpdesk scans your machine for malware and, finding none, suggests you reboot. You check outgoing wires and see the vendor was paid recently.
A second employee receives a similar email from the CEO, also with a suspicious attachment and forwards the message to ACME’s abuse inbox without opening the attachment.

Established security process is to check the abuse inbox first thing every morning.

Comments:
- Sophisticated phishing attacks often target a small number of people within an organization.
- It is not uncommon to impersonate executives.
Day 2 – 8:00 am

The first SOC analyst to arrive checks the Abuse inbox for new emails and sees the email forwarded by Employee #2 at 9:00 am the previous day.

What should the security team do with this notification?

- Open the attachment that was in the email in the Abuse Inbox
- Call the CFO to ask if he sent the email
- Open a ticket to launch an investigation
- Upload the attachment to a free sandbox for analysis

Go to kahoot.it
PIN: 177889
After reviewing the email in the Abuse inbox, the Analyst thinks the email *might* warrant further investigation. He notifies the SOC manager.

**Day 2 – 10:30 am**

**What is the next step in the investigation?**

- Search for similar emails across the enterprise
- Re-image the affected system, just in case.
- Conduct open source research
- Further analyze the attachment

**Go to** kahoot.it  
**PIN:** 177889
Google search results return no direct hits, but results for similar scenarios suggest a common criminal campaign designed to trick companies into wiring funds. The SOC analyst and manager conclude the incident was isolated and contained.

They congratulate themselves that security processes worked, and no funds were lost. As a pre-caution, they re-image Employee #2’s laptop and create a new rule to block emails from the sender.

Critical Unknowns:
- With VPN access and local network credentials, attackers were able to escalate privileges and access detailed customer data, including payments due, taxpayer IDs, correspondence and other information.
Security Analysts’ Day

- The average company spends $2.4M per year on cyber security defense
- >90% of attacks begin with email
- >50% of organizations receive more than 10,000 threat alerts a day, and 27% receive more than 1M threat alerts a day
  - >50% of IT pros admitted to ignoring alerts worthy of investigation based on prior false positive behavior or because they don’t have the staff or expertise to handle
  - 2/3 of alerts go uninvestigated every day
- >90% of security professionals report high stress levels over inability to manage alerts

29% of threat events investigated via online sources
- Staying current on security news bulletins (5%)
- Investigating potential incidents via online sources (25%)
- Manually correlating data from multiple systems (35%)
- Investigating and responding to critical alerts (35%)
No further emails impersonating the CEO or CFO are reported and the new rule does not generate any alerts.

Believing the risks are minimal and current security processes are solid, the team moves on to other tasks.

The average “dwell time” of attackers in Mandiant 2018 incident response engagements was 78 days.

31% had dwell times of less than 30 days, attributed to an uptick in financially motivated compromises such as ransomware and business email compromise.

64% of breached organizations were retargeted within 12 months.
the CFO, stops by the A/P desk to ask if updated bank account and wiring instructions for two of your key vendors has been received.

When you respond that you didn’t know the information had changed, she tells you that the CFOs of both firms said ACME had requested the information in an email. You both realize you did not send an email requesting new information.

Concerned, she sends an email to the security ops alias about possible malicious insider activity or cyber crime.

What should the security team do next?

- Escalate to leadership team
- Notify third-parties of suspected malicious activity
- Search outbound emails
- Phone a friend

Go to kahoot.it
PIN: 177889
ACME Situation Recap

Emails with malicious attachment sent to a targeted number of employees from altered email address

Event deemed contained; new detection/block rules created

Two suppliers ask the CFO if the updated banking information she requested was received.
The CISO asks you, the SOC manager, for a full debrief and recommended next steps.

He reminds you he is supposed to leave for a planned vacation with his wife and children in the morning.

What is your first recommended action?

- Immediately search for and remediate all compromised systems
- Call FireEye Mandiant
- Continue scoping incident to ensure full containment
- Go to kahoot.it

PIN: 177889
The CISO has cancelled his vacation and begins process of engaging an outside incident response firm.

Several more vendors call to confirm updated banking information requested by the CFO was received.

Evaluating the problem:

- How widespread is the problem? How many emails were sent, and from how many mailboxes?
- How did the sender access the CFO’s email account without her knowledge?
- Is this an inside job, or a targeted attack?
- What else was compromised?
ACME Incident Timeline

Emails with malicious attachment sent to a targeted number of employees from altered email address

Event deemed contained; new detection/block rules created

Two suppliers ask the CFO if the updated banking information she requested was received.

Forensic investigation begins

Day 1
SEG fails to block initial impersonation attack

Day 2
Investigation reveals no compromise, impacted laptop re-imaged

Day 13
Investigation into suspicious outbound opened (still no linkage to initial compromise)

Day 14
Outside consultants engaged

Day 30
Engagement concludes; security transformation project launched
Same security incident …with the FireEye solution

Grady Summers
CTO
Email ostensibly from Shelly Smith blocked at email gateway for further analysis.

**Action Taken**

**Helix** displays a malicious object alert from **Email Security** to the security team.

**Threat Intelligence** from FireEye displayed within Helix immediately indicates this is credential stealing malware associated with a specific APT threat group.

- Organization now has FireEye Helix platform, Email Security & Expertise on Demand
- Average staff industry experience is 1.6 yrs.
- No reverse engineer on staff
- Does not have a documented and tested incident response plan
Day 1 – 8:30 am

Email from Shelly Smith, CFO of ACME, is **blocked** as potentially malicious. The email includes an attachment she says is a past-due invoice. She requests the vendor be paid immediately to avoid disruption in the delivery of key manufacturing components.

- **Targeted Executive Impersonation email blocked by FireEye Email Security**
- **Alert flagged in Helix**
Alert flagged as critical

IOC identified, with an overview of behavior

All available resources a single click away
Double Click on Contextual Intelligence

We now know:

- The identified malware was used to steal credentials to gain a foothold in the customer environment
- It is associated with a specific APT group (APT3)
- With a FireEye Intelligence subscription, we can deep-dive to learn about associated tactics, techniques, and procedures used by this group
A second employee receives a similar email with a suspicious attachment and forwards the message to SmartCo’s abuse inbox.

**Action Taken**

With **Helix**, the security team was notified from the first alert. Next steps:

- Use **Investigative Tips** tab for recommended next actions
- **Automations tab** to quickly triage systems and find additional impacted systems

With **Expertise on Demand**:

- Security team researches the threat with Analysis Tools
- Security team submits request for analyst support, included in their subscription package.

---

- Organization now has FireEye Helix platform, Email Security & Expertise on Demand
- Average staff industry experience is 1.6 yrs
- No reverse engineer on staff
- Does not have a documented and tested incident response plan
Helix Investigative Tips Tab

Investigative Tips provide a series of "next steps" for things they would look for to determine...
A security analyst deems this a critical alert and escalates the event to the SOC manager.

**Action Taken**

With **Helix**, the security team already assigned this to an analyst.

With **Expertise on Demand**, they assess this is an active attacker threat.

The SOC manager has full visibility into this investigation.

- Organization now has FireEye Helix platform, Email Security & Expertise on Demand
- Average staff industry experience is 1.6 yrs
- No reverse engineer on staff
- Does not have a documented and tested incident response plan
Engage directly with experts – from the Helix console
As the SOC manager, you review an email from the CFO with a (presumed) malicious email attachment.

**Action Taken**

With Helix and Email Security, the security team sees all the email alerts, and effectively block the threat from proliferating within the environment.

With Expertise on Demand, the security team accesses their Incident Response Retainer and Threat Intelligence support to help them determine whether this is part of a known campaign or new targeted activity.

- Organization now has FireEye Helix platform, Email Security & Expertise on Demand
- Average staff industry experience is 1.6 yrs
- No reverse engineer on staff
- Does not have a documented and tested incident response plan
Search results show emails from same sender
Current “Known” Situation… with Helix, Email Security & Expertise on Demand

- 50 legitimate employees received the email
- 25 employees opened the attachment
- 37 devices affected
- This was a targeted industry attack
- Attacker TTPs similar to that of a recently named APT Group
The CISO asks you, the SOC manager, for a full debrief and recommended next steps.

**Action Taken**

Turn to **Expertise on Demand** for a **Custom Threat Briefing** and **Incident Response**.

Your first recommendation is ....

- Organization now has Helix platform, Email Security & Expertise on Demand
- Average staff industry experience is 1.6 years
- No reverse engineer on staff
- Do not have documented and tested incident response plan
- No threat intelligence capability
Cobalt Strikeout

**PROBLEM:**
Alert disguised as legitimate testing activity.

**HOW WE DID IT:**
Leveraged internal FireEye resources to investigate and confirm true attacker activity.

**HOW WE DID IT BETTER:**
Frontline experience enabled FireEye team to connect attacker activity to a previous client intrusion within the same industry.

**RESULT:**
In under 4 hours, FireEye was able to discover, attribute and contain an aggressive threat actor that disguised itself to deeply infiltrate the customers environment.

Diagram:
- Initial Detection: 0 Hours
- Investigation: 3.5 Hours
- Managed Defense: Alert to Containment
- Attacker lost access to victim environment: 3.5 Hours

©2019 FireEye
Winning with FireEye
Managed Defense in Action

9:03 UTC
WEBSHELL CREATED
Attacker exploited popular web UI development framework

10:57 UTC
ENDPOINT SECURITY ALERT
Endpoint Security alerted on a publicly available penetration testing tool

12:21 UTC
ACTIVE ATTACKER
Managed Defense performed additional research and proved that this was an active attacker – and not pentesting activity

13:40 UTC
MANDIANT ENGAGED
Managed Defense activated Mandiant to help contain the incident

14:33 UTC
ATTACKER ERADICATED
Last evidence of attacker activity

Scoped & Contained

Total Time 3:36
Intelligence-Led Detection

Identify intrusions that have evaded other controls to avoid security incidents

Mitigate the risk of an attacker going undetected for an extended period of time, exposing intellectual property, sensitive customer data, or financial resources.

Leverage FireEye’s unique vantage point to identify emerging threats and campaigns which may impact customers broadly, or in a particular industry or region.

Cut through the noise of the “alert-cannon” to focus on the most impactful threats, saving your team time and effort.
Proof Points: Attacker Lifecycle

- Managed Defense is proven to help identify malicious activity early in the attacker lifecycle to help minimize the impact of a breach

<table>
<thead>
<tr>
<th>Stage</th>
<th>Managed Defense Analysts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Compromise</td>
<td>43%</td>
</tr>
<tr>
<td>Establish Foothold</td>
<td>29%</td>
</tr>
<tr>
<td>Escalate Privileges</td>
<td>9%</td>
</tr>
<tr>
<td>Internal Recon</td>
<td>2%</td>
</tr>
</tbody>
</table>

Threats found by Managed Defense Analysts at Each Stage
Our Mission

To relentlessly protect security-conscious organizations and critical infrastructure from cyber threats with innovative technology and expertise learned on the front lines of cyber attacks.
Did you have fun?

(as much as you can at 8am on a Tuesday?)
Thank you for joining us
Cyber Simulation Event