On the Front Line with FireEye Email Security

Joshua Bass
Product Management – Email, FireEye

Fredrik Berntsson
Head of IT Security Operations, Ericsson
Email Security Overview
Key Differentiator

Example APT29 Phishing Campaign

- FireEye Threat Intelligence identifies campaign
- Campaign analyzed, tested by threat researchers
- FireEye Email Security detections in place
- Campaign reported to FireEye Labs
Hi Helen,

I'm tied up in a meeting but need you to make a payment to one of
Can you take care of this for me?
I cannot take calls right now, only contact me through email.
Thanks,
Mike
Hi Helen,

I'm tied up in a meeting but need you to make a payment to one of our suppliers. Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike
$12.5B
Global loss to CEO fraud

Source: Federal Bureau of Investigation, Public Service Announcement, July 12, 2018.
91% of attacks begin with email

Hi Helen,

I'm tied up in a meeting but need you to make a payment to one of our clients. Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike

91% of attacks begin with email

281B emails sent daily

Email Security is the first line of defense
78 Days
Avg. time to discover breach

Hi Helen,

I'm tied up in a meeting but need you to make a payment to one of our vendors. Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike

78 Days
Avg. time to discover breach

$3.9\text{M}$
avg. per breach

Ponemon: 2018 Cost of a Data Breach Study: Global Overview
Email Security

Secure Email Gateway*

<table>
<thead>
<tr>
<th>FireEye Email Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>√ File Detonation</td>
</tr>
<tr>
<td>√ URL Analysis</td>
</tr>
<tr>
<td>√ AV/AS filtering</td>
</tr>
<tr>
<td>√ Impersonation Detection</td>
</tr>
</tbody>
</table>

*FireEye Email Security Cloud Edition with AV/AS only.
BEC on the Rise Globally

Source: Beazley (March 2019), 2019 Breach Briefing.

133%
2017-2018 Increase in BEC

BEC Most Targeted Industries in 2018

- Financial Institutions: 27%
- Healthcare: 22%
- Education: 12%
- Professional Services: 11%
IMPERSONATION ATTACKS

✓ CEO Fraud  
✓ BEC (Business Email Compromise)  
✓ SUPPLY CHAIN

Go-to-tactic for Cyber criminals.
Accounts Payable Fraud

Legitimate CEO Name (Impersonated)

Friendly Display Name Analysis (VIP List)

Illegitimate external email address

Action to be taken with discretion

Smart DNS - Deep Relationship Analysis

Content Analysis – Machine Learning
Accounts Payable Fraud

Purchase

Clarence DeCEOzar
To Steve Jenkins

Hi Steve,

I need you to make a purchase for me.

Kindly keep this between us and let me know when you are available.

Regards,

Clarence
Post delivery and weaponized URL protection.
O365 Auto Remediate

**Auto Remediate**
Policy action quarantines, moves or deletes malicious message from inbox

**Move**
Moves malicious email from the inbox to any administrator-defined folder

**Quarantine**
Removes malicious email from the inbox and quarantines email for review

**Delete**
Permanently deletes malicious email from the inbox
Post Email Delivery Weaponized URL Example

- RECEIVE
- DETECT
- ANALYZE
- ALERT
- AUTO REMEDIATE
Post Email Delivery Weaponized URL Example

7:55 am email received by inbound mail server
Post Email Delivery Weaponized URL Example

RECEIVE

7:55 am email received by inbound mail server

DETECT

AV / AS

ANALYZE

ALERT

AUTO REMEDIATE
Post Email Delivery Weaponized URL Example

7:56 am email is analyzed as benign

7:55 am email received by inbound mail server

RECEIVE

DETECT

AV / AS

ANALYZE

MVX and Advanced URL Defense

AUTO REMEDIATE

ALERT
Post Email Delivery Weaponized URL Example

7:55 am email received by inbound mail server

1. RECEIVE

7:56 am email is analyzed as benign

2. DETECT

AV / AS

3. ANALYZE

MVX and Advanced URL Defense

7:56 am email is clean and delivered to recipient's inbox

4. ALERT

5. AUTO REMEDIATE
Post Email Delivery Weaponized URL Example

7:55 am email received by inbound mail server

8:15 am URL in email turns malicious post delivery

MVX and Advanced URL Defense

RECEIVE

DETECT

AV / AS

ANALYZE

Retroactive Analysis

8:15 am URL is weaponized post email delivery
Post Email Delivery Weaponized URL Example

7:55 am email received by inbound mail server

1. RECEIVE

8:15 am URL turns malicious post delivery

2. DETECT

X

3. ANALYZE

MVX and Advanced URL Defense

RETROACTIVE ANALYSIS

8:15 am URL in email turns malicious post delivery

4. ANALYZE

5. ALERT

Admin receives an alert of malicious message after delivery

RECEIVE DETECT ANALYZE ALERT AUTO REMEDIATE
Post Email Delivery Weaponized URL Example

7:55 am email received by inbound mail server

8:15 am URL is weaponized post email delivery

1. RECEIVE
2. DETECT
   AV / AS
3. ANALYZE
   MVX and Advanced URL Defense
4. RETROACTIVE ANALYSIS
5. ALERT
   Admin receives an alert of malicious message after delivery
6. AUTO REMEDIATE
   - Quarantine
   - Move
   - Delete
FireEye Email Security Resources

1. Product Tour


2. Email Threat Analysis

Analyze of up to 10M emails that already got through their security.

Receive results with help from FireEye Security Experts.
1989

Song of the Year

Don't Worry Be Happy

BOBBY McFERRIN

Best Picture

RAIN MAN

4 ACADEMY AWARDS INCLUDING BEST PICTURE
2019 Ericsson Connected Vehicles
First with 5G Networks in Four Continents
Fredrik Berntsson
Head of IT Security Operations
ERICSSON

Founded: 1876
Employees: 94,756
Number of patents: 49,000
R&D employees: 24,800
Describe the security challenges Ericsson faces and the potential impacts of a breach.
What were some of the specific pain points you experienced before choosing FireEye Email?
Which other vendors did you consider to help solve your challenge?
How are you measuring value with FireEye Email Security?
How do you think security vendors and cloud services can integrate to improve the customer experience?
Thank You.