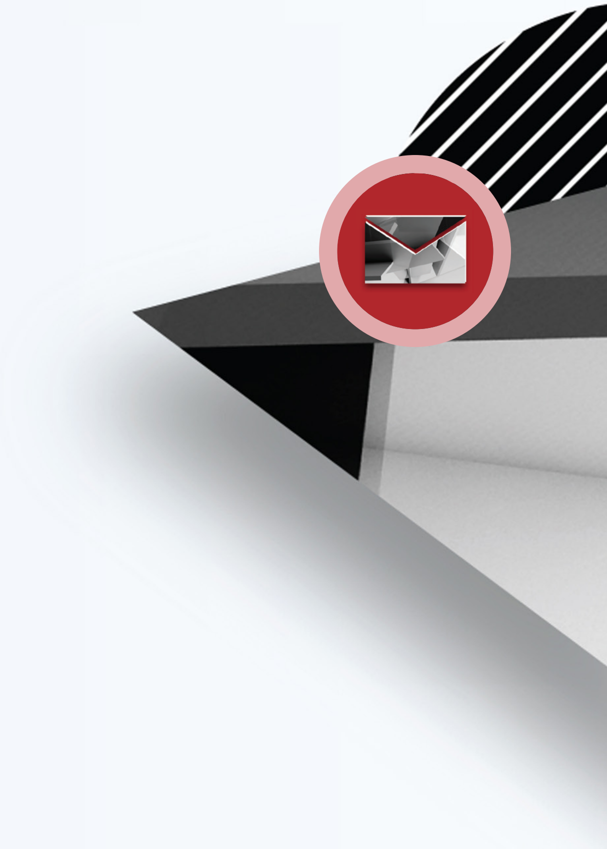
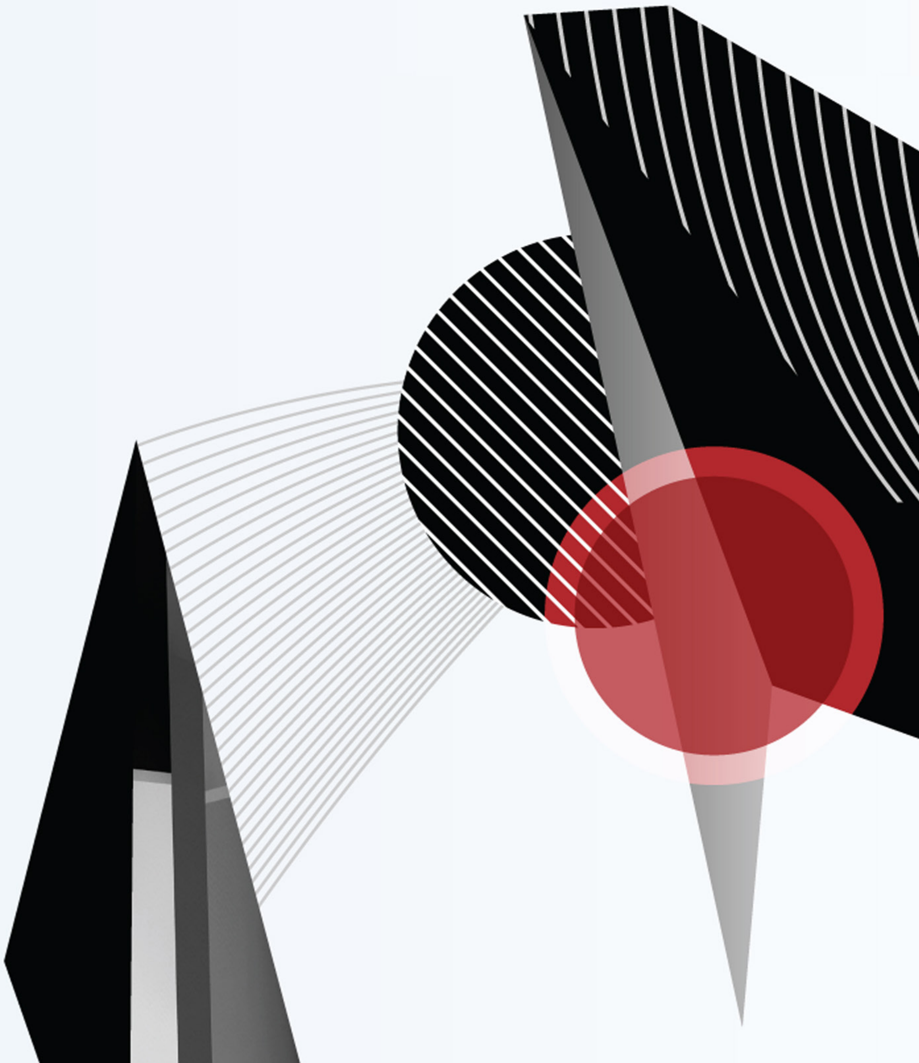
REPORT



FireEye

# Changes in Email Attack Tactics

## Based on data from July to December 2017



# Introduction

Email remains one of the most challenging entry points for organizations to protect as attackers develop new techniques to evade defenses. To identify these new tactics, FireEye analyzed a sample set of six months of email traffic in 2017 to identify potential trends or patterns in techniques used by cyber criminals.

## Data Information

The data in this report consists of a sample set of inbound email traffic from July – December 2017 and analyzes over a half a billion emails processed by FireEye Email Security on both the connection and content level. The focus of this report is on the amount of blocked malware and malware-less attacks during this time.

These include:

- Emails containing URLs from newly existing domains
- Emails originating from a similar domain to the recipient's domain
- Emails originating from a domain that sounds like the recipient's domain
- Emails impersonating a known friendly username or display name
- Emails containing phishing indicators
- Emails containing URLs leading to landing pages containing malware
- Email attachments containing malware or exploits

## Email Attack Types

### Malware Attacks

Malware attacks use email with malware-infected attachments to gain access to a user's computer. These attacks can be hidden within a variety of file types such as PDF and DOCX including password protected PDFs.

#### Common Malware Types

- Ransomware
- Adware
- Viruses
- Spyware
- Trojan horses
- Worms

### Malware-less Attacks

Malware-less attacks rely on user action to gain access to information or company assets. This can be by impersonating a trusted sender, tricking the user to personally send or enter in their credentials or linking to a malware-infected page.

#### Common Malware-less Techniques

- Impersonation attacks – CEO fraud, also known as business email compromises (BECs)
- Whaling
- Spear phishing
- Credential harvesting
- W-2 Scam

**46%** of all ransomware attacks originate from email[1]

On average ransomware attacks cost a business around **$133,000** in corporate losses[2]

CEO Fraud (BECs) have caused over **$5.52 Billion** in corporate losses[3]

Phishing attempts have grown **65%** in the last year[4]

[1] Business Wire (August 3, 2016). International Study Finds Nearly 40 Percent of Enterprises Hit by Ransomware in the Last Year.

[2] Tech Central (January 31, 2018). Ransomware attacks costs $133,000.

[3] Federal Bureau of Investigation (May 2018). 2017 Internet Crime Report.

[4] Phish Me (November 2017). Enterprise Phishing Resiliency and Defense Report 2017.

### Overview

As the most popular vector for attacks, defending against malicious email has become of critical importance for organizations. Of the emails analyzed, 66% were blocked for being spam or high risk.

On average, office workers receive at least 200 messages a day and spend about two and a half hours reading and replying to emails.[5]

### Levels of Filtering

#### Connection Blocking

Emails are blocked on the connection level for factors such as not having a good IP or domain reputation or not having a SPF record or domain created in DNS.

The connection level accounts for 56% of the email analyzed that is blocked by FireEye Email Security.

**295,387,491**
amount of email blocked on the connection level

#### Content Blocking

The content level looks at message headers and the content of the email to determine if the email should be blocked, quarantined or considered clean and sent through to the receiver. Emails blocked at this level have suspicious content or header information, contain attachments or links infected with malware or are considered spam.

After the connection level, there were 228,132,745 emails to hit the content level, where an additional 22% of overall traffic were blocked.

Email on the content level is blocked and classified under three main categories: malware and viruses, malware-less with phishing or impersonation indicators, and spam. For the purpose of this report only attacks (malware or malware-less) will be examined. Below is a graph displaying the amount of blocked and clean email:

**49,528,754**
amount of email blocked on the content level

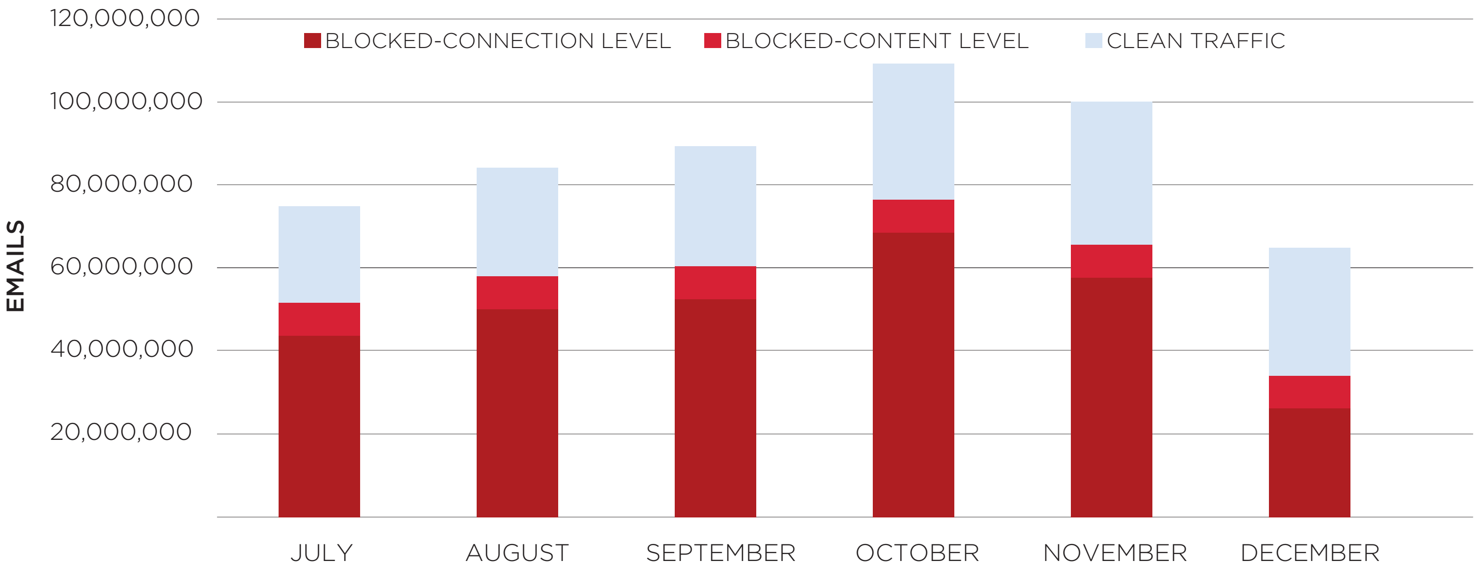
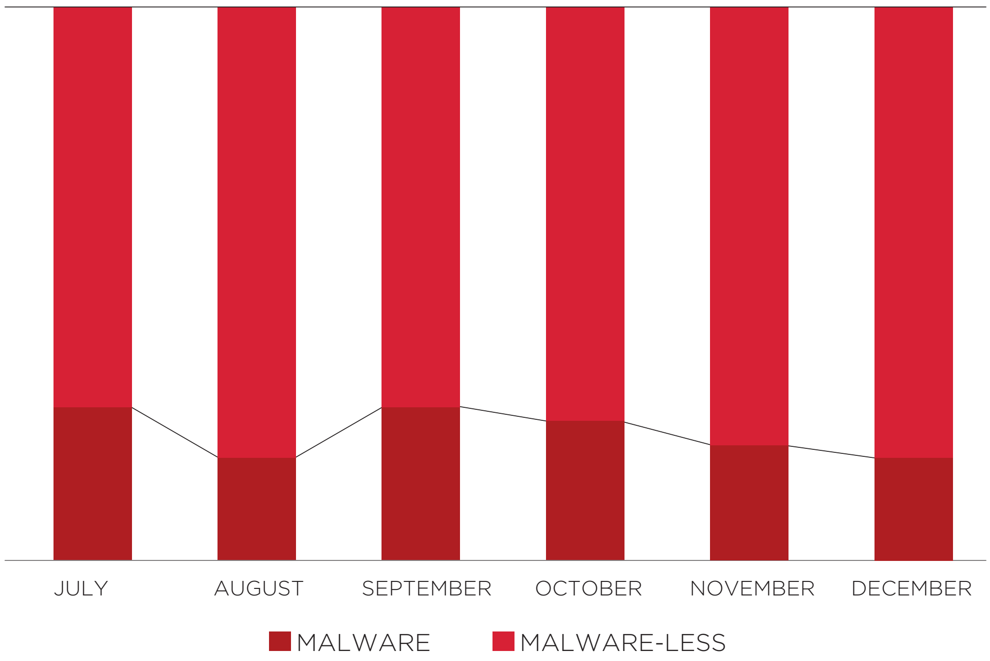


Figure 1. Monthly blocked and clean email 2017.

[5] Business Wire (August 3, 2016). International Study Finds Nearly 40 Percent of Enterprises Hit by Ransomware in the Last Year.

### Monthly Trends

Figure 2 shows the percentages of malware and malware-less attacks blocked on the content level.



**86%**
of attacks blocked were classified as malware-less

**14%**
of attacks blocked were classified as malware

Figure 2. Attacks blocked at the content level 2017.

The content level of each month shows a clear shift in tactics employed by cyber criminals. Malware attacks peaked in September at 15% but dropped consistently throughout the remainder of the year. This decrease and the supplementary increase of malware-less attacks show a clear trend of cyber criminals using more malware-less techniques as the year went on. This corresponds to an increase in impersonation indicators toward the end of the year, such as using a spoofed friendly username and similar sender domains to the receiver domain. The increase in malware-less attacks in August may be attributed to the fact that a large number of employees take vacation during that month. Before an impersonation attack, social media and out-of-office responses are used to identify when a key employee is away from the office to create credibility.

**150,704**
Average amount of malware attacks per month

**1,045,581**
Average amount of malware-less attacks per month

**60%**
of malware-less attacks blocked in August were due to the Newly Existing Domain (NED) lookup

**Phishing**
attacks increased during the holiday season (30% between October and December)

### Day of Week Trends

Cyber attacks happen every day, however, more attacks tend to be sent on weekdays rather than weekends. The following graph shows the percentage of total malware and malware-less attacks per day of the week over the last three months of 2017.

More emails are opened on Tuesdays than any other day of the week. It is also the weekday that the most malware and malware-less attacks are sent.[6]

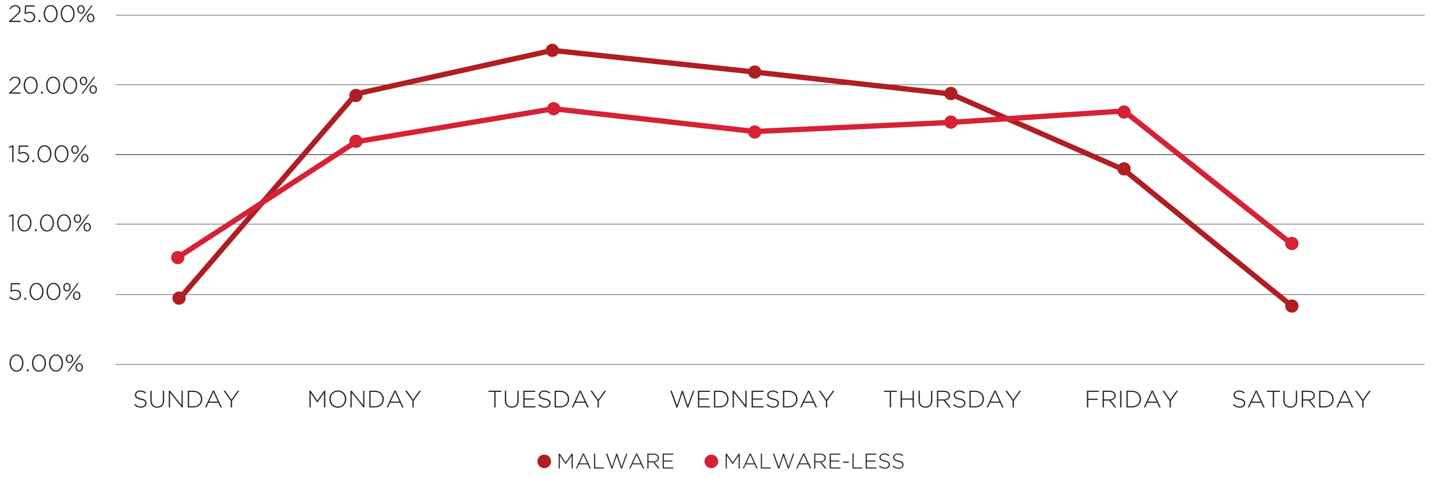


**Figure 3.** Percentage of attacks per day of the week 2017.

The data highlights that the amount of malware-less attacks remained relatively consistent throughout the week, while malware attacks dropped significantly towards the end of the week. Weekends accounted for almost double the amount of malware-less attacks than malware attacks, showcasing the fact that malware-less attacks are a threat every day of the week.

The large percentage of malware-less attacks compared to malware attacks on the weekend is also indicative of cyber criminals inferring that most people who are out of the office on Saturday and Sunday are likely checking their email on their phones. Mobile email clients tend to only show the display name instead of the email address. Cyber criminals take advantage of this fact and will often just spoof the display name, a fast and easy task. This will trick users into thinking they are corresponding with someone they know and trust, making it easier for the attack to succeed.

**1%**
of malware-less attacks blocked on the content level were phishing attacks

**99%**
of malware-less attacks blocked on the content level were impersonation attacks

Amount of total clean email
**178,604,000**

**78%**
of traffic seen on the content level was blocked for being spam or malicious

[6] Life Wire (April 20, 2018). The Number of Emails Sent Per Day (and 20 Crazy Email Statistics).

### Conclusion

The last six months of 2017 showed that the majority of email traffic in the sample set was blocked because it was malicious or spam. While the news last year may have focused heavily on malware and malware-related attacks such as WannaCry and Petya, the data shows that malware-less attacks are more of an increasing threat.

With the majority of email security services focusing heavily on detecting malware, organizations are being potentially exposed to malware-less attacks such as CEO fraud (BECs). This report highlights how cyber criminals evolve and change their tactics, emphasizing the importance of an agile and innovative email security service, one which comprehensively protects organizations from all variations of email-borne attacks.

Learn how FireEye incorporates research findings like these into solution improvements with its Innovation Cycle. Visit **www.fireeye.com/solutions**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

**About FireEye, Inc.**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.