Internet Security Threat Report

ISTR

Email Threats 2017

An ISTR Special Report

Analyst: Ben Nahorney

October 2017

Contents

Symantec

Contents

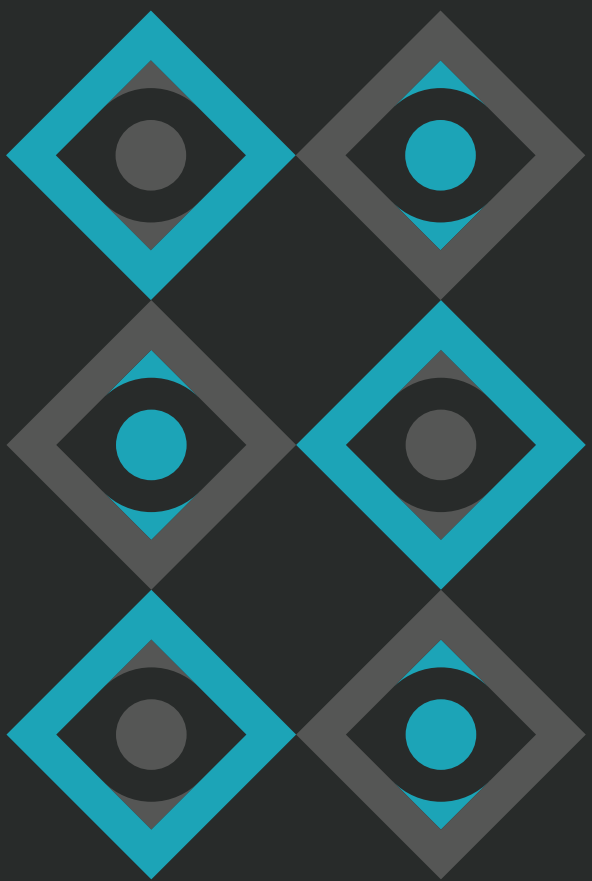
Figures and Tables

Symantec

Executive summary and key findings

Section

00



Symantec

Executive summary

Email is everywhere. In its 40-plus-year history, email has become one of the most ubiquitous electronic technologies to date, with billions of messages sent each day.

With that level of popularity comes its share of risks. Email is by far the most popular method for attackers to spread malicious code. At present, a user is almost twice as likely to encounter malicious code through email than being impacted by an exploit kit. They are many more times as likely to encounter a malicious email than see their devices fall prey to a worm or encounter a malicious banner ad. On average, one out of every nine email users has encountered email malware in the first half of 2017.

Malicious code is not the only threat utilizing email. With their heavy reliance on social engineering, and their urgent nature, business email compromise BEC scams are one of the more potent email attacks making the rounds. No longer do such attacks appear to be a rarity either, with approximately 8,000 businesses reporting attacks in a given month. On average a targeted organization has 5.2 BEC emails sent to them each month.

Spam continues to represent a vast proportion of email traffic, increasing to 54 percent of email in the first half of 2017, after the rate had appeared to bottom out over the last two years. The importance of filtering spam has never been more important, where not doing so can cost businesses the equivalent of employing multiple people just to manage that spam.

The risks found in email are not evenly distributed either. Attackers appear to be targeting certain businesses at higher rates than others. Some industries are particularly targeted, often seeing threat rates twice as high as the overall average.

While most of these threats come from outside an organization, it's equally important to protect outgoing email. Our findings indicate that more could be done on this front in order to ensure sensitive data sent by email is protected, thus avoiding the exposure of private information.

Email continues to play a vital role in our electronic lives, but so too does it play a vital role in the distribution of threats. It's as important as ever to understand email's part in the threat landscape and what can be done to protect yourself and your business from them.

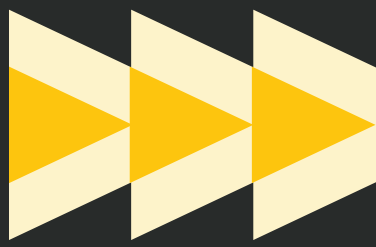
Key findings

- An email user is almost twice as likely to encounter malware through email than they are through the next-most common infection method, exploit kits.
- One out of every nine email users encountered email malware in the first half of 2017.
- Approximately 8,000 businesses each month are targeted by BEC scams.
- A targeted organization has 5.2 BEC emails sent to them in a given month.
- The spam rate for the first half of 2017 reached 54 percent, and is expected to continue to climb as the year progresses.
- Without spam filters, a business effectively employs two people to manage spam for every 100 employees.

Big numbers

352

Section 01



Symantec

Email Threats 2017

The Big Numbers

Malware

One out of **nine** email users encountered email malware in the first half of 2017.

2x

A user is almost **twice as likely** to encounter malware through email than they are through exploit kits.

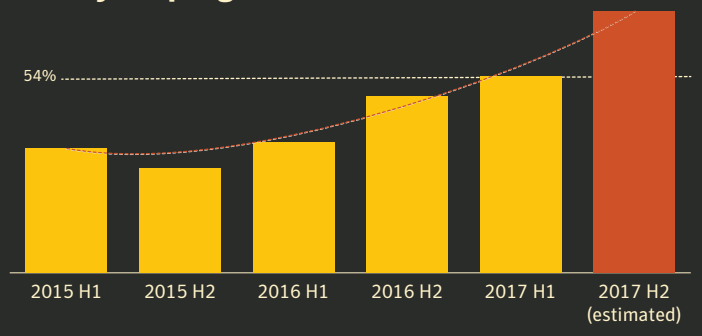
BEC scams

Approximately **8,000 businesses** each month are targeted by BEC scams.

A targeted organization is sent **5 BEC emails** in a given month.

Spam

The spam rate reached **54 percent**, and is expected to **continue to climb** as the year progresses.



Without spam filters, a business effectively employs **two people** to manage spam for every **100 employees**.

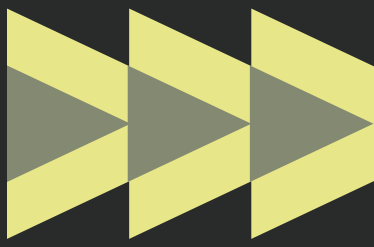
Symantec™

Internet Security Threat Report

Malware

Section

02



Symantec

Email is the most frequently used delivery mechanism for malware. According to research we conducted across different threat vectors, no other distribution channel comes close: not compromised websites containing exploit kits, not network file sharing technologies like SMB, not malicious advertising campaigns that entice users to click on banner ads. In fact, a user is almost twice as likely to encounter malware through email than come across a malicious website.

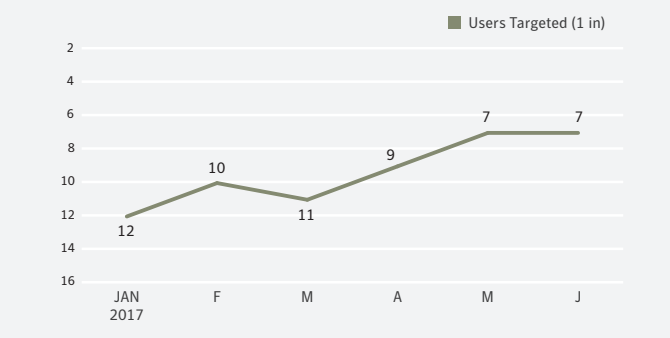
The strengths that have made email such a popular communication tool are the same reasons cyber criminals use it to spread their wares. The attackers just fire off a spam message to a target, or group of targets, and that's it—no need to rely on indirect methods where the target might or might not visit a compromised site or click a malicious banner ad. It is a direct channel to an end user who, if they can be convinced to open an attachment or click a link in the email, can cut a large swath through a variety of network security layers, gaining an attacker access to their intended target.

Impact

This direct access to the intended target is reason alone to get businesses to take malicious email seriously. Businesses are regularly targeted by malicious emails. In fact, in the first half of 2017, more than 11 percent of users had at least one malicious email sent to them. That's one out of every nine email users.

This figure trended upward as the year progressed. In January, only one out of every 12 users (8.6 percent) had a malicious email sent to them. By May this number had climbed to more than one in seven (15 percent) and remained at that level through June. Yet regardless of the level, it only takes one user to fall victim to an attack, and the business has been compromised.

Email users targeted by malware per month



Depending on the industry that a given user works within, this number could rise even higher. The percentage of users that will have a malicious email sent to them climbs as high as 23.8 percent in industries such as Wholesale Trade and 22.6 percent in Mining. It's 18.4 percent in Agriculture, Forestry, & Fishing and more than 18.2 percent in Manufacturing.

Percent of email users targeted by malware by industry

Industry	Users that had malicious emails sent to them (%)
Wholesale Trade	23.8
Mining	22.6
Nonclassifiable Establishments	20.3
Agriculture, Forestry, & Fishing	18.4
Manufacturing	18.2
Public Administration	16.9
Retail Trade	14.4
Construction	12.9
Services	9.5
Transportation & Public Utilities	7.2
Finance, Insurance, & Real Estate	6.8

Malware distribution

The vast majority of malicious emails attempt to entice the user through socially engineered subject lines and message bodies in order to trick the user into opening a malicious attachment. While the subject matter varied, the top three themes centered around billing, package delivery, and scanned documents—all topics where an email attachment wouldn't appear out of the ordinary.

Top three malicious email themes

Topic	Percentage of malicious emails
Bill or Invoice	9.2
Package Delivery	9.1
Scanned Documents	8.4

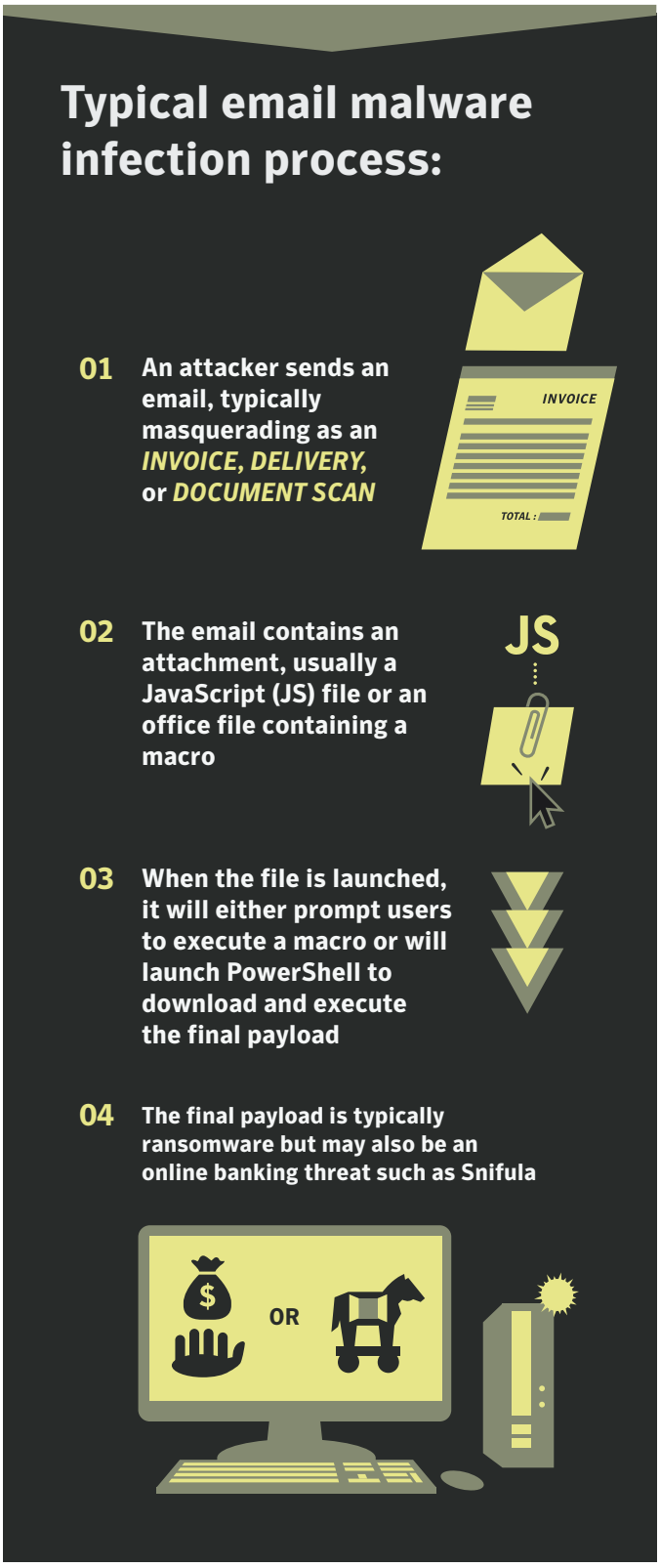
There are generally two ways malicious code is distributed by email—either by a URL in the message body or an email attachment. Email attachments continue to be the most popular way to deliver malicious code. In the first half of 2017, 74 percent of malicious emails distributed their payload through email attachments, though at times during that period the rate was closer to 85 percent.

Now the payload in-and-of-itself wasn't necessarily attached to the email directly. Only about one-third of attachments were executables in the first half of 2017. Overall, executable payloads are not the easiest way to distribute a threat because organizations can easily block them outright, and with good reason—very few users have a justifiable need for distributing or opening programs via email attachments.

Over the years, to improve their chances of delivering their malware, attackers have moved from distributing their payloads outright and come to rely on downloaders. Generally speaking, downloaders are small programs or scripts that, when run, can download further files. In the first half of 2017, 53.3 percent of malicious attachments were scripts or macro-loaded office files, designed to download further malicious software once they are run by the user.

The popularity of downloaders is due to a few simple reasons:

- Downloading a payload separately divorces the process of obtaining and executing a malicious payload from email. Once the script is launched all the network traffic for getting the payload is completely separated from email protocols, and thus email-based protections. The email may deliver the downloader, but the downloader does the heavy lifting on its own.

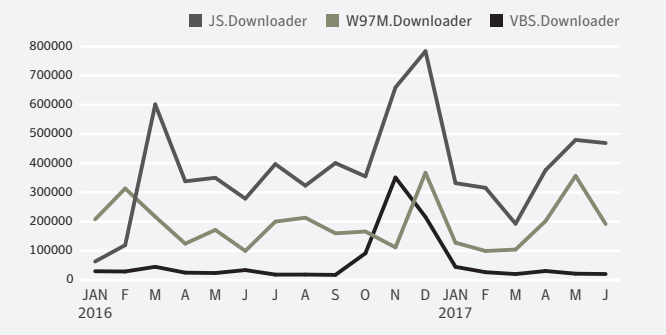


- The server can check the IP of the downloader and send localized payloads, or no payload if the compromised computer doesn't meet certain criteria.
- The attacker can quickly change the final payload should it get detected. New users compromised by the downloader will get a fresh, undetected payload, increasing the number of infections.

Overall, downloaders are split into three primary camps: JavaScript, Office macros, and VBScript (VBS). JavaScript downloaders were twice as common as Office macro downloaders in the first half of 2017—a ratio that has remained in line with what was observed throughout 2016. For the most part VBS has come in a distant third, though it did pass Office macros briefly in late 2016.

However, all three types of downloaders saw declines coming into the new year and throughout the first quarter, with JavaScript and Office macros only picking back up again in April, around the time the Necurs botnet resumed its activity, after a three-month hiatus. VBS downloader numbers appeared to stay low through the first half of 2017, though there are indications they may pick up again in the later part of the year.

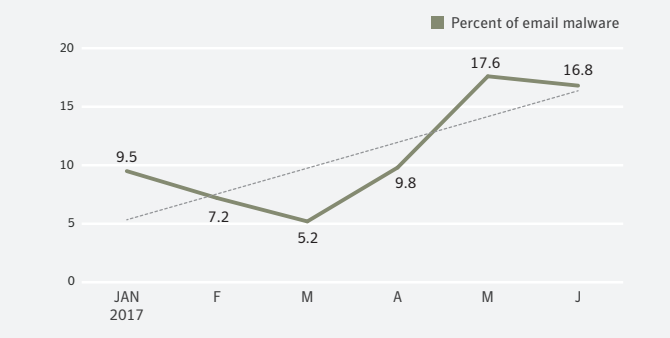
Downloader detections by month



Another tactic used by attackers is to forego attachments entirely and include a link to a malicious website instead. This is not a new technique, but the proportion of malicious email containing a URL has been in decline since 2011.

However, in the first half of 2017 we saw a reversal of this trend, where the proportion of URL-laden malicious email has trended up. By the end of this period, one in six malicious emails contained a URL instead of an attachment. This is the highest rate seen since November 2014, when the now-defunct Asprox botnet sent out a large volume of holiday-purchase-themed, URL spam—and that was a once-off occurrence.

URL malware rate



Spambots

Section

03

The primary method that malicious email is distributed is by way of spambots. Spambots often take the form of a module within a larger botnet, being one of many tasks that the particular botnet carries out.

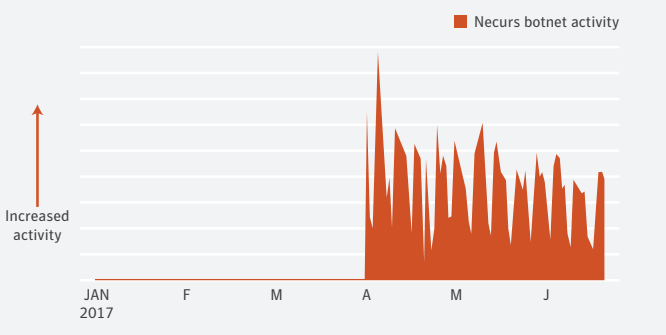
In other cases a spambot is a self-contained threat installed on a compromised computer through a number of different means and exclusively focused on sending spam.

Others still are groups of attackers responsible for varied campaigns, using a variety of tools, as opposed to maintaining a signature family of threats. While these cases don't fall neatly into a particular spambot family, their activity is worth mentioning.

Necurs

As far as botnets go in 2017, Necurs is responsible for the largest amount of malicious email activity. This is despite the folks behind the botnet having taken the first three months of the year off. However, the botnet's activity is far lower than what was seen in the lead-up to Christmas 2016.

Necurs botnet activity



It's hard to underestimate the impact that this botnet has made on the threat landscape. During the three-month period that Necurs was offline there was a dramatic decline in a variety of malicious activity. Email malware rates plummeted, the number of downloaders blocked per month dropped, and the number of infections from certain payloads, known to be distributed by Necurs, also declined. When the botnet returned in late March, the rates for all of these threats also rose once again.

The reason for the disappearance of this botnet remains a mystery. It's possible to speculate that the disappearance was indirectly related to the disappearance of other botnets during 2016. Popular botnets, such as those run by the Avalanche crimeware group, were shut down last year and in some cases the botnet administrators were arrested. It's possible that the folks behind Necurs were spooked by this activity and decided to close up shop. Alternatively, the three-month hiatus could have been time spent shoring up measures to remain anonymous or the original administrators could have sold the botnet on to a new group of attackers. Regardless, while the botnet has returned, it has yet to reach the same level of activity that was seen prior to its disappearance in late 2016.

Some campaigns of note include invoice-themed spam with a malicious PDF attachment that drops a macro and downloads Jaff, emails purporting to be cancelled banking transactions with .rar and .7z files containing Locky, and pump-and-dump spam intended to bump up stock prices.

- **Downloader types:** JavaScript, Macro, VBS
- **Payloads:** Locky, Globelmposter, Jaff, Trickybot

BlankSlate

Following Necurs is a malicious spam campaign group known more for the structure of the email messages they send than the tools they use to spread them. BlankSlate got its name due to the email subject and message bodies being empty. The fact that the email only includes an attachment with no context could be a deliberate ploy to entice users to open them in order to find out why the blank email has been sent. Alternatively, it could simply be a way to cut down on overhead. If the attackers behind it don't have to concern themselves with crafting new socially engineered text to include in a spam email then it's less work. It's also possible that attackers wanted to minimize the footprint of the spambot, making it more difficult to detect.

In one campaign in particular, BlankSlate sent .zip files that contained the Cerber ranomware threat.

- **Downloader types:** JavaScript, Macro
- **Payloads:** Cerber, Locky, BTCware

Fioesrat

Fioesrat is a spambot that is usually installed by attackers who hack into legitimate PHP web servers and install a PHP-based email client for sending out spam. In some cases they simply implement the built-in mail function in PHP, while in others they utilize their own custom scripts to send email over SMTP. The hacked web servers that we've observed tend to be used

in the distribution of the Nemucod family of threats—a downloader that leads to a ransomware payload. In other situations, ad-clicking threats such as Kovter are delivered as the payload, where its intended purpose is to boost ad-clicking revenue for the attackers.

- **Downloader types:** JS.Nemucod
- **Payloads:** Locky, Kovter, Ransom.Nemucod

Silentbrute

This is one of the smaller botnets out there, but nonetheless Silentbrute has been active in 2017. Threats usually arrive as an attached Office document. If the user opens the document, a macro inside prompts the user to enter a password that is contained in the message body of the email in order to launch the downloader and download the payload.

- **Downloader types:** Macro
- **Payloads:** Various banking Trojans

Pandex

The longest-active botnet in our list, Pandex has been around for more than 10 years. It has evolved and morphed over the years, assisting in the distribution of a variety of malware families, such as W32.Cridex and the Dyre infostealer. A recent campaign of note distributed the Snifula banking Trojan in Japan, though the author of this threat has since been arrested. In other recent activity, Pandex has been observed distributing the Sage 2.0 ransomware (Ransom.Cry) using sexually explicit spam emails.

- **Downloader types:** Macro, JavaScript
- **Payloads:** Snifula, Ransom.Cry

Oliner

The Oliner botnet (a.k.a. Onliner) has been active for a while, but grabbed headlines when it inadvertently exposed its own email spamming list that included 711 million addresses.

Downloader types: JavaScript

Payloads: Reports of Snifula

Sarvdap

A smaller spambot distributed by the Dromedan botnet (a.k.a. Andromeda). What is interesting with the Sarvdap spambot is that, before it begins sending spam, it checks the IP of the compromised computer against a Realtime Blackhole List (RBL). If it finds the IP on the list, it terminates its malicious processes. This ensures that the systems that send spam in this spambot aren't prevented from doing so by being on the blacklist.

- **Downloader types:** JavaScript, Macro
- **Payloads:** Dromedan

Emotet

A Trojan with botnet capabilities, Emotet is known for distributing spam that appears as an update to Adobe Reader. When the user launches the downloader, it gives the impression that the installation failed, leaving the user none the wiser. In other cases the botnet sends spam that simply contains a malicious URL. The threat adds compromised computers to the botnet and implements a banking Trojan module to steal information.

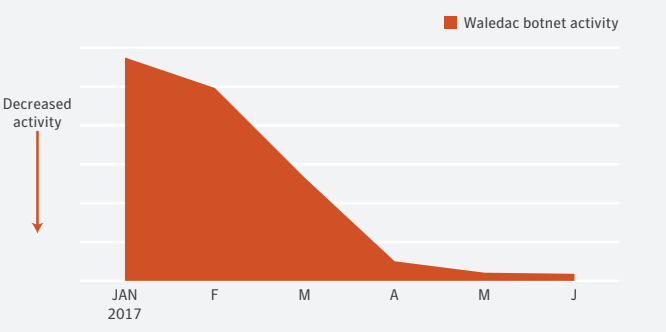
- **Downloader types:** Macro, JavaScript
- **Payloads:** Various banking Trojans

Waledac

One major spambot that has been active in recent years is the notorious Waledac (a.k.a. Kelihos) botnet. While the botnet was certainly active at the beginning of the year, the latest takedown attempt by the FBI in April largely knocked the bot offline and resulted in the arrest of the botnet's alleged owner. Over the years there have been a number of attempts to bring Waledac down, only to see it return at a later date. Time will tell how successful this latest attempt to dismantle the botnet has been.

- **Downloader types:** JavaScript
- **Payloads:** Ransom.Troldesh

Waledac (Kelihos) botnet activity



BEC scams

Section

04

Imagine that you are a junior-level accountant in a medium-sized enterprise. It's almost 5:00 p.m. on a Friday, before a three-day weekend, and you're the last one in your department to wrap up. Just then an email arrives from an executive from within the company with a subject line that reads "URGENT". There isn't much to the email, she's just asking if you are at your desk. Naturally, you reply that you are and ask what you can do to help.

The follow-up email itself appears hastily written, with spelling and formatting errors, but it seems as though the executive is in a hurry. Apparently an invoice for major supplier has not been paid and they are threatening to withhold much-needed supplies. If it isn't resolved immediately this could have a knock-on effect to your company's own production and distribution plans.

The executive includes details on the outstanding amount, the supplier's banking details for payment, and asks if you can initiate a wire transfer immediately, before the banks close for the weekend.

The question is: What do you do?

The threat of business email compromise (BEC) scams continues to grow, as does the financial impact of the scam. According to recent analysis by the FBI, over US$5 billion in losses have occurred between late 2013 and the end of 2016. It's not just large enterprises that are being targeted either, as businesses of all sizes have reported attempted attacks.

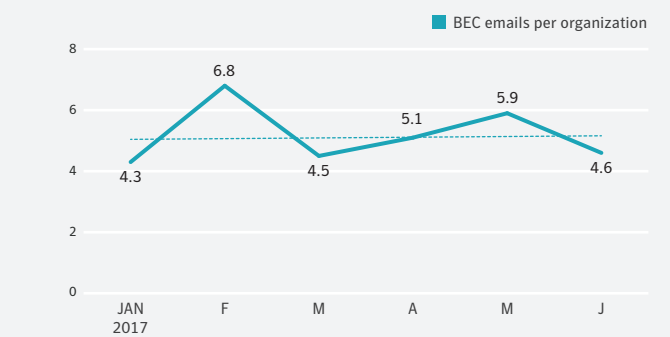
BEC scams have evolved to take on many forms. Most commonly the scammer impersonates an executive within the company requesting an urgent wire transfer. The executive in question may have had his or her email account compromised, but oftentimes the executive's email address has been spoofed. This email is often sent to an employee within the company or, in some cases, directly to a bank that holds the accounts of the targeted company.

In other cases the scammer masquerades as an attorney working on a time-sensitive matter, attempting to pressure the target into transferring funds near the end of a business day or workweek. The scammer can also play the part of a supplier with a relationship with the targeted company, claiming that a bill has not been paid and requesting the money be sent to a bank account that they provide the details for.

Latest trends

In 2017, we have seen approximately 8,000 businesses targeted by BEC scams in a given month. On average there were 5.2 BEC scam emails sent to an organization each month. However, not all organizations are targeted equally and some receive far more attempts per month than the average.

BEC emails received per organization



Looking at the content of BEC scam emails, the dominant motif seen in the subject lines tends to carry a sense of urgency, requiring immediate action, in the hopes that the recipient will be coerced into acting quickly without thinking too much about what it is he or she is being asked to do. In fact, when looking at the top email subject lines seen in emails we have identified as BEC scams, this trend becomes all the more clear.

Top subject lines in BEC scam emails

Subject	Percent of BEC emails
payment	18.9
urgent	10.3
request	8.6
attention	7.3
transfer	2.4
today	2.1
update	2.0
51hr	1.8
attn	1.4
w2	1.4

The emails tend to be short and to the point, often containing spelling errors that would normally raise a red flag when dealing with other phishing scams. However, when paired with this sense of urgency, and the apparent direct message from someone in power, such errors are often overlooked or explained away as the sender simply being busy and in a rush.

Beyond wire transfers

One of the more interesting developments in the BEC sphere are attacks where the scammers are attempting to obtain other assets, as opposed to directly stealing money.

In one BEC campaign early in 2017 the scammers appeared to be focused on obtaining the employee's American tax form, the W2, from the targeted organizations. For example:

Subject:

```
Urgent W2 Request
```

Message body:

```
Hi [TARGET],

How are you today? I need you to send me the W2 of
all the Company's Employees,I need it for a Quick
Review

thanks
[IMPERSONATED EXECUTIVE]
```

The scammers in this case could be looking to gather a large cache of sensitive information across the organization, either as reconnaissance for further attacks or in order to carry out identity theft with the information contained in the tax records.

In another case, attackers targeted two small record labels involved in the production of music for pop singer Lady Gaga. The attackers, impersonating an executive at Interscope Records, sent an email message to executives at both labels asking them to send on stem files—files commonly used in the production of music. These executives, falling for the ruse, complied with the request, resulting in the exposure of new, unreleased songs. This instance highlights just how easily a supply chain can be manipulated with BEC scams.

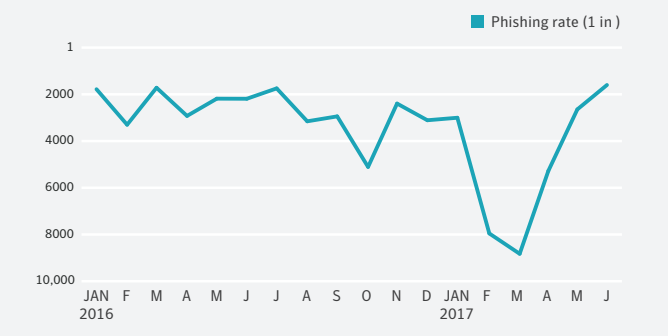
Typosquatting

One trend that has become more prominent in the BEC landscape is typosquatting. Attackers are frequently registering domains that look similar to the official email addresses of the organizations they intend to target. The domains may have a character or two misplaced, for instance "amce_inc.com" for the legitimate business, "acme_inc.com." (In other, less common instances, attackers may use a different domain, or simply add words to masquerade as a particular department, such as "acme_inc_sales.com.") These typosquatted domains have become common enough that, when looking at 100 customers over one 90-day period, we identified more than 4,000 typosquatted domains.

Phishing

While traditional phishing scams have steadily declined over the last few years, it appears that they may have begun to creep up slightly. There is no question that the phishing rate continues to trend downward, but in the second quarter of 2017, the rates have returned to similar levels seen one year prior. Whether this is an indication that simple phishing scams are making a comeback remains to be seen.

Phishing rate



Phishing scams of note

In a rather peculiar incident in May, a phishing scam was discovered that could provide an attacker access to a user's Gmail account and Google Contacts. The attack worked by providing a legitimate Google sign-in screen, leading to a "continue to Google Docs" link. However, this link points to a non-Google-associated, third-party app simply named "Google Docs."

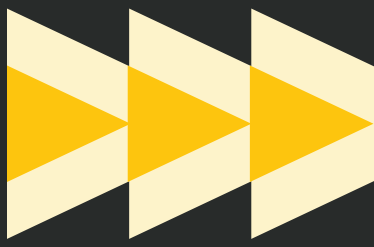
While a clever attack on the surface, what followed was even more bizarre. The following day a Twitter account named @EugenePupov appeared, claiming that this wasn't a phishing scam but simply a Coventry University project gone awry. However, Coventry University stated that no one by that name was enrolled at, or had ever attended, their institution. All told, Google stated that 0.1 percent of their users were impacted by this scam; some estimates put this at close to one million accounts.

Internet Security Threat Report

Spam

Section

05



Symantec

"Two years from now, spam will be solved."
–Bill Gates, January 24, 2004

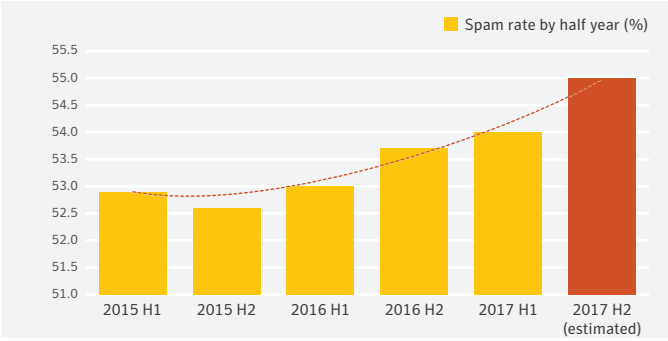
The most predictable of annoyances in the email landscape is spam. While it has declined since this infamous quote from Bill Gates, often blocked or relegated to a folder that most users ignore entirely, it still sticks around.

While seemingly in decline, the spam rate continues to comprise more than half of all email traffic. In the last decade, only once has it dipped below half—back in June, 2015.

Year on year, we've watched the spam rate decline. Beginning in 2011, back when the spam rate was 75 percent, the rate has dropped on an annual basis to the point where it appeared to bottom out at 53 percent for both 2015 and 2016.

However, dig a little deeper and a slightly different trend emerges. While the calendar years for 2015 and 2016 average out to be the same, it appears the spam rate may have actually hit rock bottom in the latter half of 2015. Breaking the spam rate into six-month intervals shows that it has been slowly, but steadily, increasing since that point. For the first half of 2017, this rate has reached 54 percent and all signs point to a continuation of this upward trajectory.

Spam rate by half year



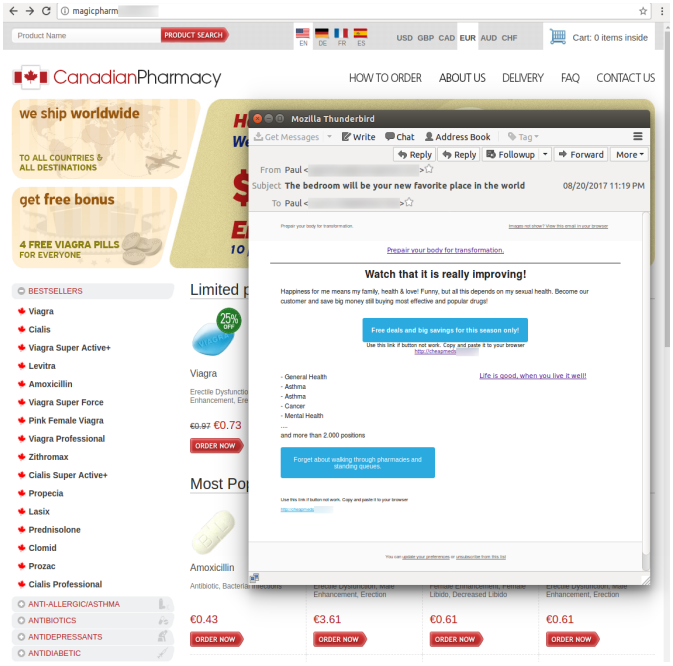
As of the end of the first half of 2017, this upturn translates into an increase of 11 more spam emails in your inbox each month than a year prior. However, some industries see far more than that. Users who work in the manufacturing, retail trade, construction, and mining sectors all saw around 1.5 times more spam emails per month on average in the first six months of 2017. Users in the wholesale trade industry—establishments that sell goods to retailers, industrial and commercial contractors, etc.—potentially see twice as much spam as the average user would.

Advertising spam

It comes as no surprise that the primary culprits in the distribution of spam are spambots. Many of the usual suspects, which receive plenty of attention for distributing malware, are also involved in spreading non-malicious varieties of spam. For instance, Necurs was observed sending out pump-and-dump spam when it returned in early April.

However, there are other spambots that appear to focus almost exclusively on advertising spam. The Gamut botnet is one such instance. In fact, when looking strictly at advertising spam estimates gathered from Symantec honeypots, there are times Gamut appears to have sent more of this type of spam than the Necurs botnet. A sample of the emails sent show campaigns hawking pharmaceuticals and diet pills in multiple languages.

Spam campaign advertising pharmaceuticals



In other cases, it appears as though the scammers are attempting to recruit unsuspecting users looking to make a fast buck with work-from-home opportunities. However, these opportunities are likely money mule scams, where the participants are asked to launder money for the scammers. These scams generally operate by getting the mule to convert bitcoins into another currency, or vice versa, using bitcoin ATMs or bank accounts of their own, keeping a small portion for themselves. However, these activities are highly illegal and put users who participate in real, legal danger.

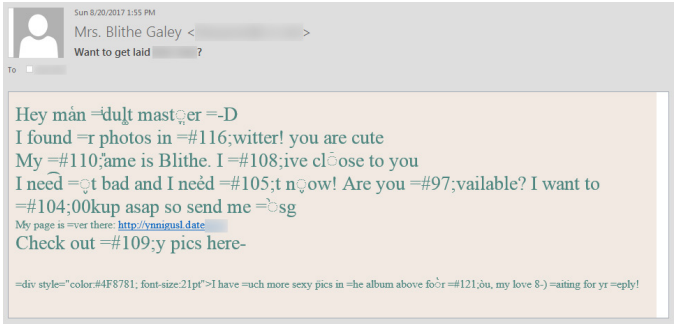
Bitcoin scam email

English translation:

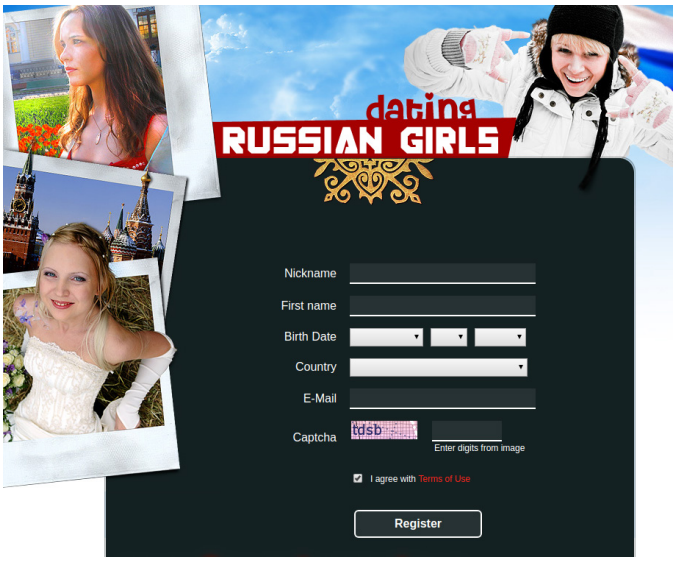
> I just joined Bitcoin Code.
>
> Let me explain to you...
> No, I'm not a millionaire yet.
>
> But I earned a solid $ 13,150.26 using this brand new system.
>
> And that was only within 24 hours.
>
> You have heard well:
> By this time tomorrow, you could also have more than $ 13,000 in your checking accounts.

The Tofsee spambot, another botnet sending out advertising spam, has recently been involved in dating spam. The messages tend to include obfuscation, such as the inclusion of equal signs through the message body, in the hope that the email messages can make it past spam filters. The links within the emails lead to phishing sites, where any personal details entered are likely used for identity theft or further romance scams.

Example Tofsee email



The website Tofsee email links to



Other distribution methods

While responsible for most spam, spambots aren't the only method of distribution. Another way that spam often ends up in your inbox is actually from things you signed up for.

There are plenty of legitimate organizations that use email as a method to advertise their wares. However, problems arise when organizations do not offer a way for you to unsubscribe from their mailing list. These bulk email senders gone rogue sometimes even share your email address with other other bulk senders, further increasing the amount of unwanted spam in your inbox.

There are select cases of ISPs gone rogue as well. For instance one European-based ISP has garnered a reputation for sending spam, phishing scams, and even malware. The abuse from this ISP has been severe enough that wide swaths of IPs belonging to the ISP have been blocked and emails coming from their domains have automatically been sent to spam folders.

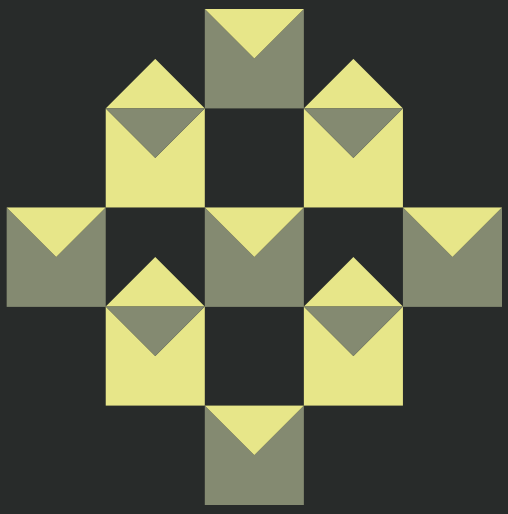
The cost of spam

When looking at spam on an email-by-email basis, its impact seems trivial at best. As an individual user in a corporate environment, you may spend no more than 5-10 minutes a day clearing out spam (assuming your company has no spam filters in place). Simply identifying and dismissing spam is a small footprint in overall email usage.

However these costs add up when looking at the organization as a whole. Based on median salary data from the U.S. Census Bureau, spending 10 minutes managing spam adds up to $4.51 per employee each day. That's $1,177.42 spent annually for one employee to filter spam.

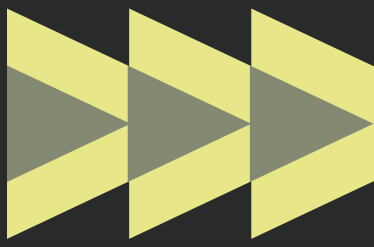
For every 100 employees a business has, this comes out to $117,741.67 per year. That's the equivalent of having two full-time employees dedicated to simply managing spam—a far less trivial figure.

User email behavior



Section

06



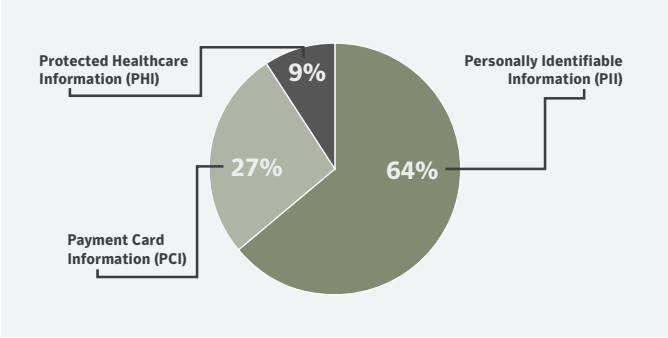
Symantec

Quite often the way email is used can lead to security-related issues. For instance, if a user is careless when opening unsolicited attachments it can lead to a malware infection. In other cases, a user that inadvertently shares sensitive data to a large email distribution list runs the risk of a data breach.

According to the latest data presented in the Symantec Shadow Data Report, 29 percent of all emails within an organization are widely distributed throughout that organization, shared externally with external contractors and partners, or shared with the public. This in-and-of-itself isn't a huge issue, and is often a necessity when doing business.

The risk associated with such emails comes into play when sensitive data is involved. Of these broadly shared emails, nine percent of them contain sensitive data, such as personally identifiable information (PII), payment card information (PCI), and protected health information (PHI). In fact, almost two-thirds of broadly shared documents with sensitive information contained PII, while almost a third contained PCI.

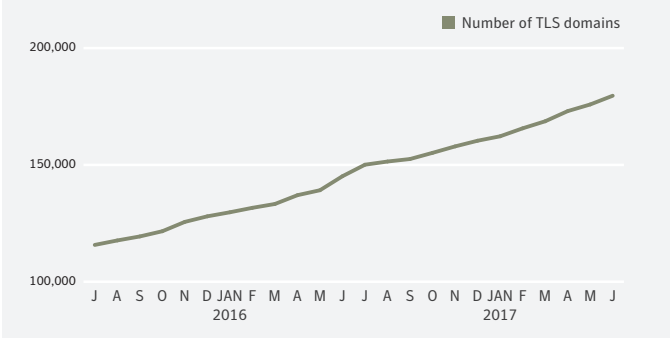
Broadly shared emails with sensitive information



Beyond sensitive information of this nature, there are also instances where other company data is broadly shared, such as distributing source code thorugh email. In fact, one out of every 18 emails that contain code is broadly shared.

Sometimes it is necessary to share these various types of data widely, and email can be a good way to distribute it quickly. This is generally fine, so long as the sender implements encryption. The good news is that overall there does appear to be a definitive move towards the adoption of encryption when it comes to transmitting email. Over the past two years, Symantec has seen a steady increase in the rate of transport layer security (TLS) adoption when businesses send email to their partners and clients. TLS is an encryption protocol that can secure the communication channel over which email traffic is sent to the server.

Number of registered TLS email domains



The adoption of TLS improves the security of email messages, at least while they are in transit. However, it does not encrypt the emails themselves, which could still feasibly be intercepted at either end of the transmission.

Fortunately it appears that in most cases users are encrypting the email they send, using standards like S/MIME or PGP. However, there are cases where encryption isn't present and one out of every nine emails that lack encryption contains sensitive information. Clearly more could be done to ensure that the emails themselves are encrypted.

Protection and best practices

Section

07

Symantec

Adopting a multilayered approach to security minimizes the chances of infection. Symantec has a strategy that protects against malware in three stages:

01 **Prevent:** Block the incursion or infection and prevent the damage from occurring

02 **Contain:** Limit the spread of an attack in the event of a successful infection

03 **Respond:** Have an incident response process, learn from the attack and improve the defenses

Preventing infection is by far the best outcome, so it pays to pay attention to how infection can be prevented. Email is the most common infection vector for malware. Adopting a robust defense against this infection vector will help reduce the risk of infection.

Ensuring there is adequate incident response handling also helps to reduce the risk and impact of an incident if and/or when one occurs.

Email security

Email-filtering services such as Symantec Email Security.cloud can help to stop malicious emails before they reach users. Symantec Messaging Gateway's Disarm technology can also protect computers from email-based threats by removing malicious content from attached documents before they even reach the user. Email.cloud technology includes Real Time Link Following (RTLF) which processes URLs present in attachments, not just in the body of emails.

In addition to this, Email.cloud has advanced capabilities to detect and block malicious scripts contained within emails through code analysis and emulation. It removes all active content from attachments such as Microsoft Office documents and PDFs, including macros and JavaScript. A digital carbon copy of the active content is created and attached to the email instead, meaning the endpoint is never exposed to the original malicious content.

Email.cloud can also track and identify emails sent by spambots proactively at an early stage. This means that more bandwidth is given to legitimate emails and that spam is filtered as quickly as possible, preserving resources and ensuring that unwanted email is not delivered to the company's clients.

CloudSOC

An industry-leading Cloud Access Security Broker (CASB) solution, CloudSOC is designed to secure email provided through cloud apps, such as Office365 and Google applications. Enabling the security features present in CloudSOC meets a variety of regulatory compliance requirements and can be integrated with a variety of enterprise security tools.

Download Insight

Symantec Download Insight technology examines files that are downloaded through or launched by web browsers, messaging clients, and other portals. Download Insight determines whether a file is a risk based on reputation.

Download Insight automatically computes reputation and rating of files, URLs, and websites using the "wisdom of crowds" (analytics). It classifies every program that it encounters as either good or bad.

Advanced antivirus engine

Symantec uses an array of detection engines including an advanced antivirus engine with heuristics, just-in-time (JIT) memory scanning, machine-learning engines, and emulator. The emulator enables the engine to heuristically detect encryption behavior without needing a signature. Together with Auto Protect, it will detect malicious files when they hit the disk, bypassing the packers and encryptors employed to evade static detection technologies.

SONAR behavior engine

SONAR is Symantec's real-time behavior-based protection that blocks potentially malicious applications from running on the computer. It detects malware without requiring any specific detection signatures. SONAR uses heuristics, reputation data, and behavioral policies to detect emerging and unknown threats. SONAR can detect malicious behaviors common to lateral movement and block them. It also employs machine learning to block programs that exhibit combinations of thousands of different suspicious behaviors.

Ongoing development

Symantec has a 24/7 Security Technology and Response (STAR) team responsible for ongoing development and improvement of generic signatures for email threats. The team carries out continuous monitoring of email threats and their delivery chain in order to harvest new samples and ensure robust detection.

STAR also cooperates with various law enforcement agencies, sharing details about active botnets and assisting in shutting them down.

Best practices

In addition, users and administrators should adhere to the following advice to reduce the risk of email-based attacks:

- Periodically perform a full network audit to identify any computers sending spam. Compromised computers should be isolated from the network until they have been fully cleaned and restored.
- Immediately delete any suspicious emails received, especially those containing links and/or attachments.
- Be wary of Microsoft Office attachments that prompt users to enable macros. While macros can be used for legitimate purposes, such as automating tasks, attackers often use malicious macros to deliver malware through Office documents. Microsoft has disabled macros from loading in Office documents by default. Attackers may use social-engineering techniques to convince users to enable macros to run. As a result, Symantec recommends that users avoid enabling macros in Microsoft Office unless it comes from a well-known, trusted source.
- Maintain standards through continual monitoring and ensure the right balance of internal education and awareness-raising has been implemented—it's not only the IT team responsible for security—but everyone in the organization. Having the right technology in place not only to prevent attacks and to reduce the risk of an attack from causing more damage, but also the right technology to monitor and manage the policies that the organization needs to implement to maintain the right level of security going forward. Being secure and meeting strict standards of compliance and regulations enables businesses to become more competitive.
- Adopt and enforce industry standards on security, such as ISO 27002 in order to avoid becoming the weakest link in your supply chain.
- In the event of a payload arriving on a computer, a critical step is to limit the spread of the attack. Symantec's file-based technologies ensure that any payload downloaded on the computer will not be able to execute its routines.
- In the case of individuals with private email accounts, it is advisable to have separate emails for personal communication, with friends and family, and online shopping.
- In a corporate environment, it may be advisable to limit or block the access of personal email accounts on company networks in order to reduce the risks threats from these channels pose.

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

Symantec Worldwide: http://www.symantec.com

ISTR and Symantec Intelligence Resources: https://www.symantec.com/security-center/threat-report

Symantec Security Center: https://www.symantec.com/security-center

Norton Security Center: https://us.norton.com/security-center

Symantec

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

Symantec.com

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

10/17