Email: Click with Caution

Contents

Introduction

Last year, spam turned 40. Yes, it was clear back in 1978 that Gary Thuerk, a marketing manager with Digital Equipment Corporation, sent the first spam message to 393 people on the original ARPANET to market a new product. It'll come as no surprise that this message was about as well-received as much of today's spam. Thuerk was given a stiff reprimand and told not to do it again.

If only it were that simple today. Forty years on, spam has grown exponentially in prevalence, inundating our inboxes with unwanted offers for pharmaceuticals, diet products, and job opportunities. Not only that, but it's been joined by its far more dangerous cousins, phishing and malware. Phishing was first conceived more than 30 years ago, and malware also has a decades-long history of email distribution.

Today, the sad fact is a lot of emails are unwanted spam and worse. The volume is staggering—85 percent of all email in April 2019 was spam, according to Talos Intelligence. The volume of unwanted email is on the rise too; spam hit a 15-month high in April.

Sender vs. recipient

You could argue that email is structured in an almost ideal format for scammers. Email forces the user to read and make assessments about what they receive and then make decisions as to what they open or click as a result. Just the right amount of social engineering, exploiting the individual's good nature, can push the user to action.

It's this social engineering that not only makes it an enticing delivery vector, but also so challenging to systematically defend. Rarely, if ever, does an email-borne attack bypass the user. While things like URLs leading to compromised or malicious web sites utilizing exploit kits are common, they still rely on coercing the user into clicking on a link in an email first.

What this means for business

No wonder email is one of the primary challenges that keep CISOs up at night. In our most recent CISO Benchmark Study, we learned that 56 percent of CISOs surveyed felt that defending against user behaviors, such as clicking a malicious link in an email, is very or extremely challenging. This ranks higher than any other security concern surveyed—higher than data in the public cloud, and higher than mobile device use.

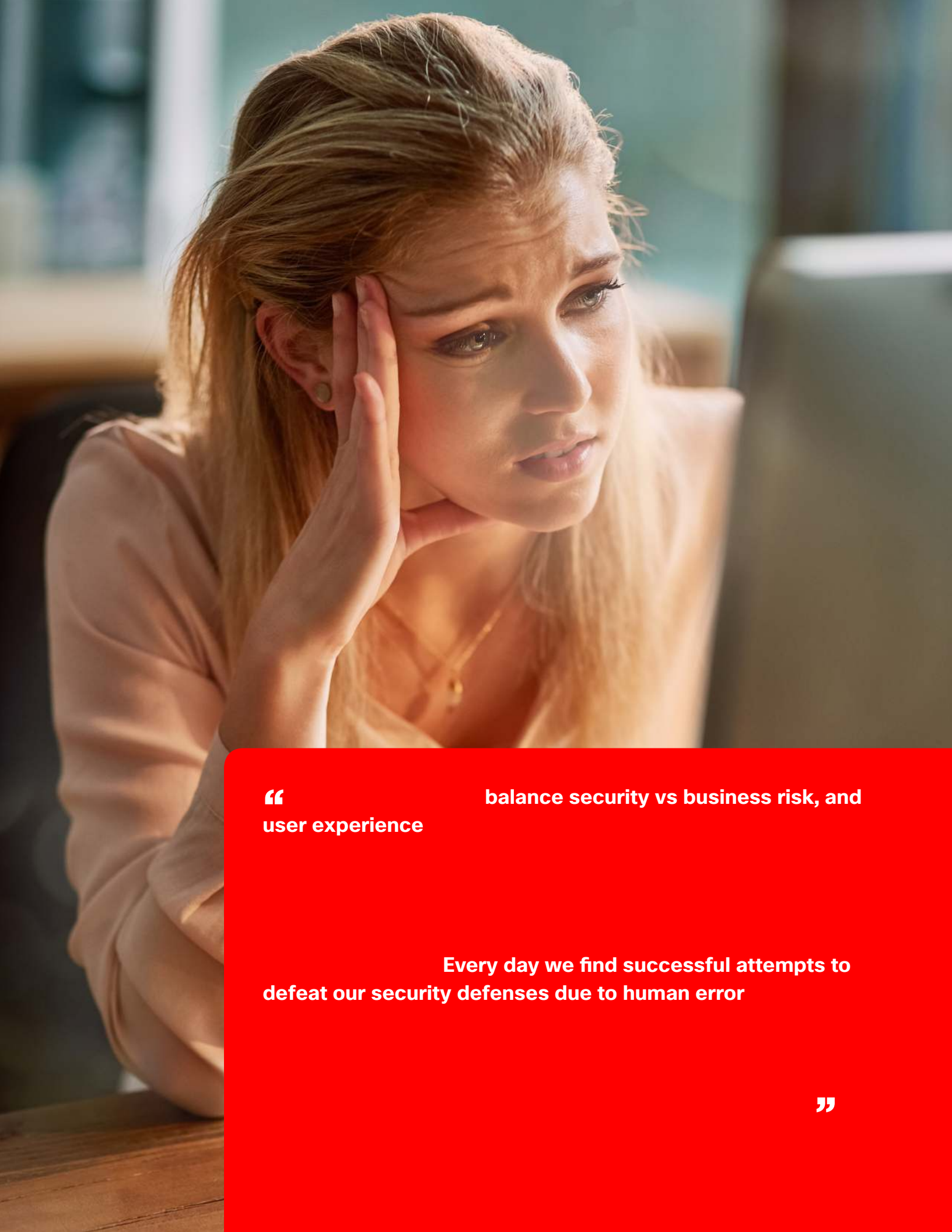
It's also the frequency of such attack attempts that draw the attention of CISOs. For instance, 42 percent of CISOs surveyed dealt with a security incident that manifested as the result of a malicious spam email being opened within their organization. Thirty-six percent dealt with a similar incident as the result of details stolen from a phishing attack. According to our CISO Benchmark data, CISOs consider email threats to be the number one security risk to their organizations.

In a separate study, commissioned by Cisco and carried out by ESG in 2018, 70 percent of respondents reported that protecting against email threats is becoming more difficult. In terms of the consequences of email-borne attacks, 75 percent of respondents said they experienced significant operational impacts and 47 percent reported significant financial impacts.

Response required

How do you secure something that's both a necessity and a risk at the same time? For many organizations, the move to the cloud has been viewed as a solution. However, the cloud is no silver bullet against the dangers of email. In more cases than not, it's simply kicking the can down the road. The security issues don't go away, but rather persist.

There are several ways you can minimize the impact email threats have overall. In this paper, we'll discuss the current threat landscape, providing an overview of the most common email attack types today. We'll break down how they play out, their goals, and the infrastructure behind them. We'll discuss what you can do to keep your business safe, as well as how to identify email-borne threats when your users encounter them.



“ balance security vs business risk, and user experience

Every day we find successful attempts to defeat our security defenses due to human error

”

The Current Email and Phishing Landscape

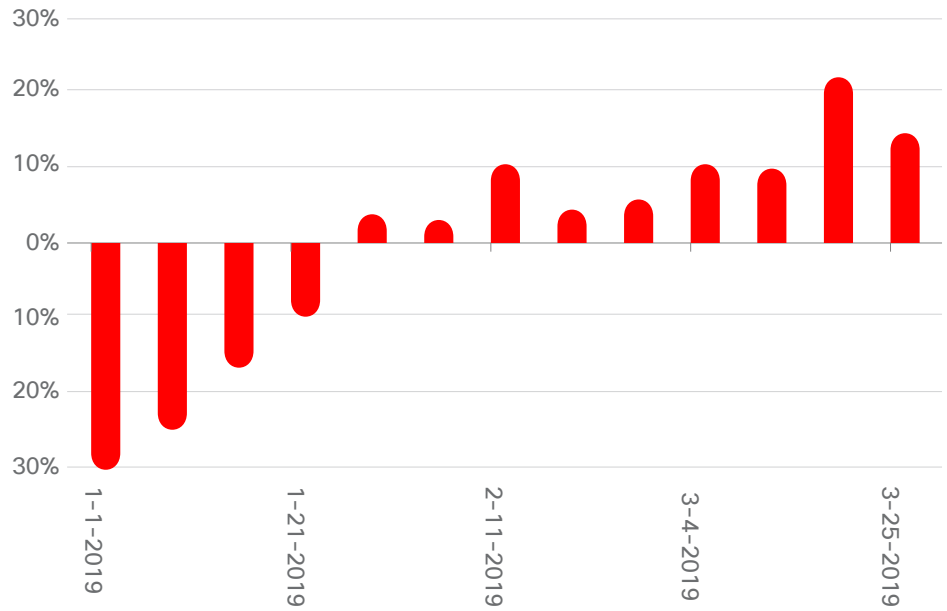
The hazards presented by email are numerous. According to Verizon's 2018 Data Breach Investigations Report, for which Cisco is a contributor, email is the number one vector for both malware distribution (92.4 percent) and phishing (96 percent). Act upon the wrong email and you could find yourself the victim of cryptomining, your credentials stolen, or, if you fall for the wrong socially engineered scam, out of large sums of money. Scale this to the enterprise level, and the wrong email can wreak havoc.

How regularly do users fall for email scams? Just ask the folks in Duo Security. The team created the free Duo Insight tool a few years ago, which allows users to craft their own fake phishing campaigns and test them out within their own organizations to see who falls for them and who doesn't.

Unfortunately, many people do fall for the ruses. According to The 2018 Duo Trusted Access Report, 62 percent of the phishing simulation campaigns that ran captured at least one set of user credentials. Of all the recipients, almost a quarter of them clicked the phishing link in the email. And half of those entered credentials into the fake website.

With this level of success, it's no wonder that email is such a popular choice for launching phishing campaigns. In fact, it seems that phishing activity could be ramping up, if the number of new phishing domains identified by Cisco Umbrella is any indication. We took a weekly average for the first quarter of 2019, and then compared each week against this average. The results in Figure 1 show that, while the year began slow, the number of new domains being produced accelerated, seeing a 64 percent increase from the first week of the quarter to the last.

Figure 1 Weekly new phishing domains compared to first quarter weekly average.



Source: Cisco Umbrella

Common Email Attack Types

The following is a run down of the most common email-based scams of today. Grab your laptop, open your inbox, and imagine the following unread messages are waiting for you.

Office 365 phishing

The email appears to come from Microsoft. It says that your Office 365 email address will be disconnected due to errors or policy violations. The only way to prevent this from happening is by verifying the address at the provided link.

Similar phishing attacks have been observed against other cloud-based email services such as Gmail and G Suite.

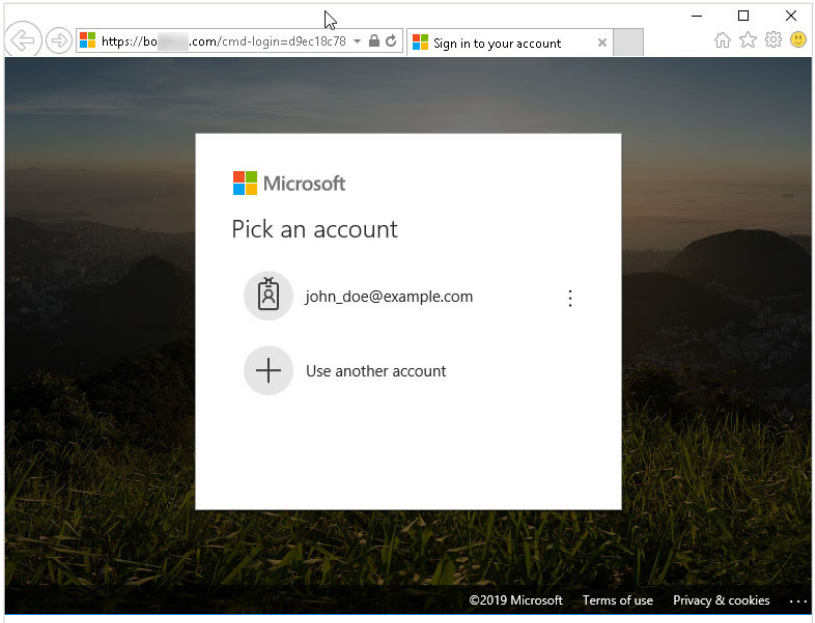
This is an attempt to phish your Office 365 credentials. The emails and URLs used may even look like something you'd expect to find surrounding Office 365, for example: micros0ftsupport@hotmail.com. If you click the link, it will take you to an official-looking login page, requesting your email address and password.

However, the site is fake. Once the scammers have your credentials, they may try to log into other Microsoft related services, as well as harvest your contacts. One common technique is to log into your email account and send your contacts an informal email (e.g., Subject: FYI) that includes another phishing URL.

This style of attack is on the rise. According to data published by our partners at Agari in their Q2 2019 Email Fraud and Identity Deception Trends report, 27 percent of advanced email attacks are being launched from compromised email accounts. This is up seven percentage points from the last quarter of 2018, when 20 percent of phishing attacks came from compromised email.

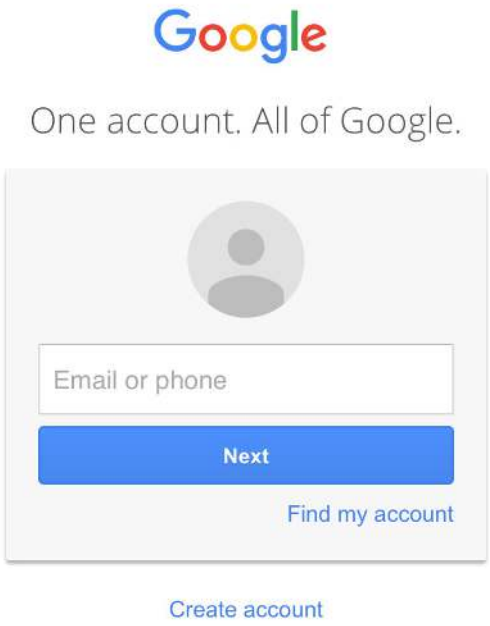
It's not just Office 365 that is being targeted either. Similar phishing attacks have been observed against other cloud-based email services such as Gmail and G Suite, Google's cloud email offering. Given the prevalence of Google accounts, and how they are leveraged across the Internet to log into various websites, it's no surprise that attackers have created phishing sites in this arena as well.

Figure 2 Phishing site deliberately designed to look like Microsoft's sign-in page.



Note: This visual representation of a Microsoft screen is a false representation as a cyber threat actor would create and use to trick the viewer into believing it is a legitimate logo and communication from Microsoft.

Figure 3 Google account login example. Can you tell a real from a fake?



Note: This visual representation of a Google screen is a false representation as a cyber threat actor would create and use to trick the viewer into believing it is a legitimate logo and communication from Google.

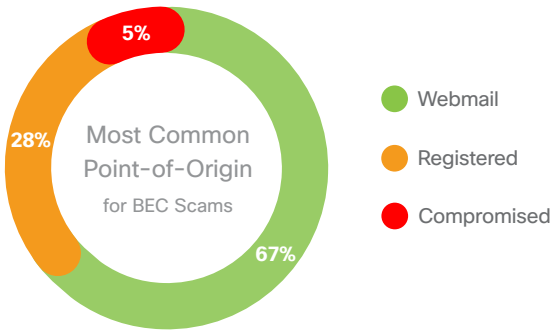
Business email compromise

It's the week of the big company summit and everyone is out of the office, save for a small number of folks maintaining critical functions. You're a member of the finance team and part of the skeleton crew still on site. Suddenly, an email arrives in your inbox that appears to come from the CFO with the subject "Missed Payment." The email explains that a payment that was supposed to go out last week was missed and could result in disruption to the company's supply chain. Attached are wire transfer instructions. The sender ends by saying they will call you within the hour regarding this.

This is business email compromise (BEC) at its core. BEC scams are a form of email fraud where the attacker masquerades as a C-level or above executive and attempts to trick the recipient into performing their business function, for an illegitimate purpose, such as wiring them money. Sometimes they do indeed go as far as calling the individual and impersonating the executive. And it seems to work. According to the Internet Crime Complaint Center (IC3), there were U.S. $1.3 billion in losses in 2018 due to BEC scams.

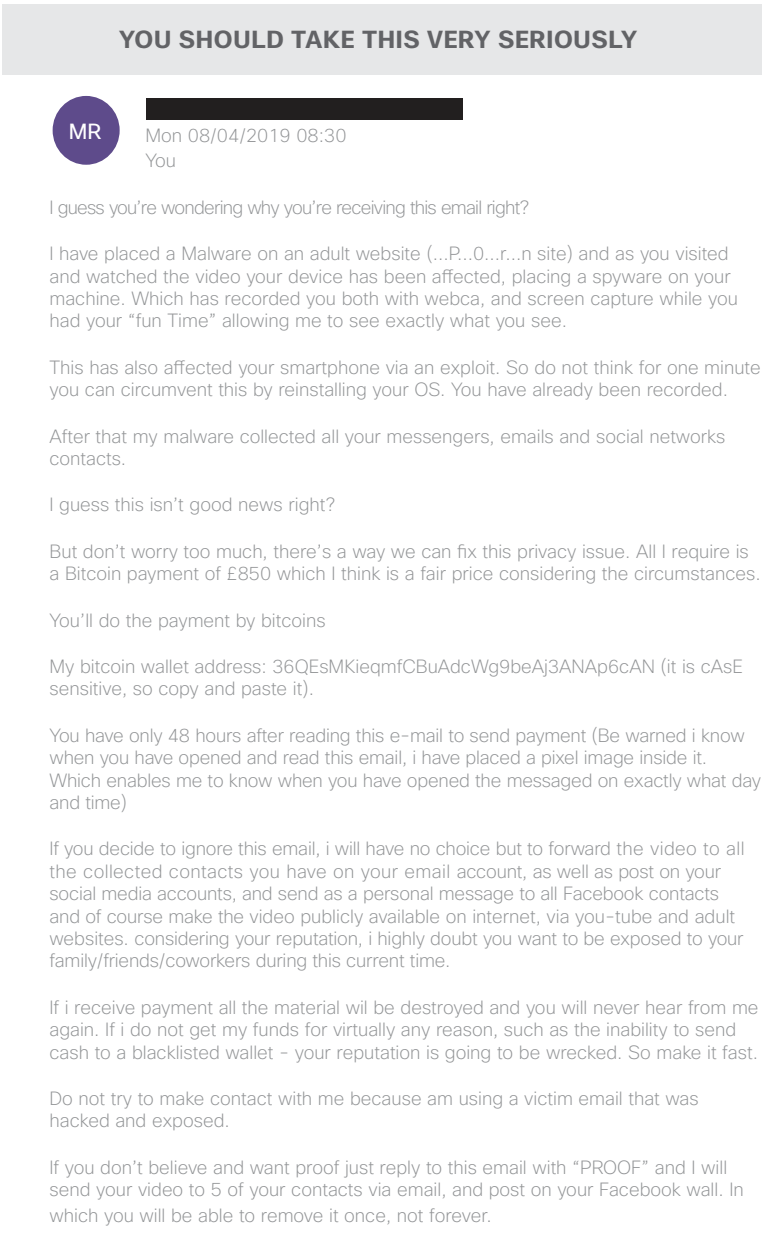
You would think that attackers would leverage compromised accounts in BEC scams, like they do with Office 365 phishing scams. Surprisingly, according to the Agari Q2 2019 Email Fraud and Identity Deception Trends report, only about five percent of these scams do. Two thirds of such attacks still use free webmail accounts to launch the attacks, while the remaining 28 percent craft tailored attacks using registered domains. The latter level of personalization extends into the body of the email, where according to Agari, one out of every five BEC emails includes the name of the targeted recipient.

Figure 4 BEC email point-of-origin.



Source: Agari Data, Inc.

Figure 5 A recent digital extortion example.



YOU SHOULD TAKE THIS VERY SERIOUSLY

MR [redacted]
Mon 08/04/2019 08:30
You

I guess you're wondering why you're receiving this email right?

I have placed a Malware on an adult website (...P...0...r...n site) and as you visited and watched the video your device has been affected, placing a spyware on your machine. Which has recorded you both with webca, and screen capture while you had your "fun Time" allowing me to see exactly what you see.

This has also affected your smartphone via an exploit. So do not think for one minute you can circumvent this by reinstalling your OS. You have already been recorded.

After that my malware collected all your messengers, emails and social networks contacts.

I guess this isn't good news right?

But don't worry too much, there's a way we can fix this privacy issue. All I require is a Bitcoin payment of £850 which I think is a fair price considering the circumstances.

You'll do the payment by bitcoins

My bitcoin wallet address: 36QEsMKieqmfCBuAdcWg9beAj3ANAp6cAN (it is cAsE sensitive, so copy and paste it).

You have only 48 hours after reading this e-mail to send payment (Be warned i know when you have opened and read this email, i have placed a pixel image inside it. Which enables me to know when you have opened the messaged on exactly what day and time)

If you decide to ignore this email, i will have no choice but to forward the video to all the collected contacts you have on your email account, as well as post on your social media accounts, and send as a personal message to all Facebook contacts and of course make the video publicly available on internet, via you-tube and adult websites. considering your reputation, i highly doubt you want to be exposed to your family/friends/coworkers during this current time.

If i receive payment all the material wil be destroyed and you will never hear from me again. If i do not get my funds for virtually any reason, such as the inability to send cash to a blacklisted wallet - your reputation is going to be wrecked. So make it fast.

Do not try to make contact with me because am using a victim email that was hacked and exposed.

If you don't believe and want proof just reply to this email with "PROOF" and I will send your video to 5 of your contacts via email, and post on your Facebook wall. In which you will be able to remove it once, not forever.

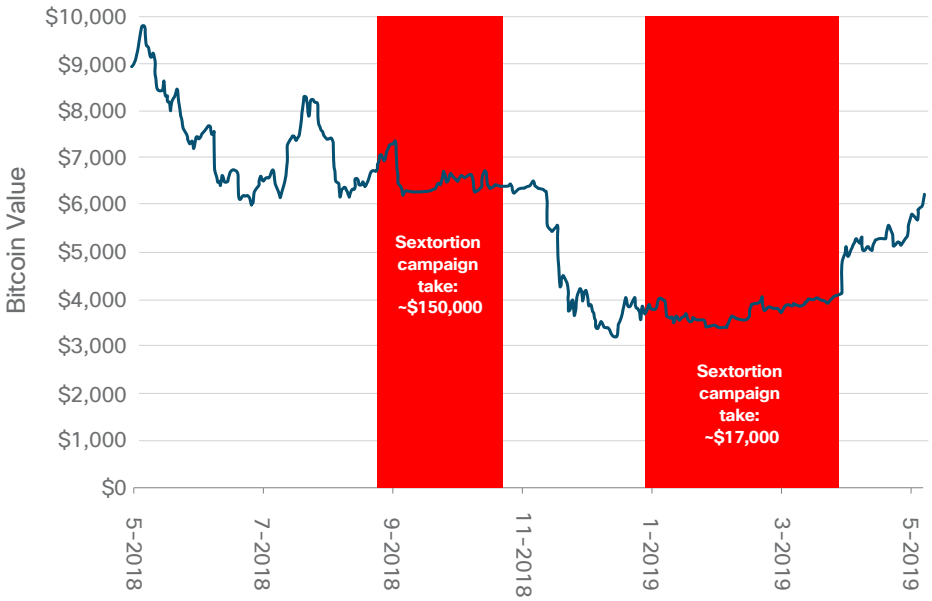
Digital extortion

An email arrives in your inbox with the subject **"YOU SHOULD TAKE THIS VERY SERIOUSLY."** The sender of the email claims to have compromised an adult video web site and that you visited the site. He or she also claims to have recorded you over your webcam, alongside the videos they assert you have watched. Besides that, the sender claims to have gained access to your contacts and will send them all the footage, unless you pay them hundreds, if not thousands, of dollars in Bitcoins.

This is digital extortion. The only thing that separates this from more traditional extortion scenarios is that the claims are completely fabricated. The scammers haven't compromised a web site, they haven't recorded you, and they don't have your contact list. They're simply hoping to trick you into believing that they do.

We cover the many forms of this type of email scam in our Threat of the Month blog post,

Figure 6 Comparison of Bitcoin's value (USD) to the take of sextortion campaigns.



Source: Cisco Talos

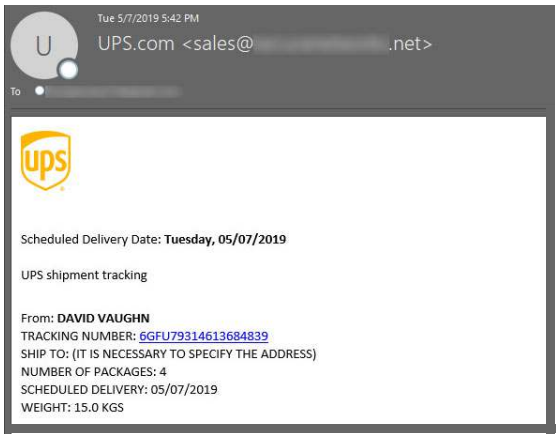
It's an interesting trick and it's lucrative for the attackers, where profits gathered from a digital extortion campaign reached into the six-figure range near the end of 2018. However, according to the latest analysis conducted by Cisco Talos, covering January through March 2019, profits have declined. Still, the rise and fall of these profits loosely track with the value of Bitcoin, albeit with larger declines. As the value of Bitcoin appears on the rise at present, it will be interesting to see if the same thing happens with digital extortion payouts.

Packaging and invoice spam

"I don't remember buying a subscription to this mobile app," you say to yourself. That's at least what the email implies: a lifetime subscription to, say, a movie club. Hold on, the location listed in the invoice says it was purchased in Sri Lanka. And you don't even live in Sri Lanka. "There must be some mistake," you say to yourself as you quickly open the attached PDF to investigate.

Unfortunately, that PDF contained an exploit, which ultimately downloaded Emotet onto your device. The scam varies but usually centers around a package you didn't order, an invoice for something you didn't purchase, or a monthly payment for a subscription or service you didn't enroll in. This can lead to any number of malicious results, from stolen banking credentials to cryptomining.

Figure 7 Emotet scam email, pretending to come from UPS.



Note: *This visual representation of a UPS screen is a false representation as a cyber threat actor would create and use to trick the viewer into believing it is a legitimate logo and communication from UPS.*

Figure 8 Recent advance fee fraud example.

Mr. Christoper A. Wray

CW

Director of the Federal Bureau of Investigation (FBI)
To: [redacted]
Reply-To: [redacted]

ATTN: Beneficiary.

According to the ethics of an office, introduction is always very important on a first contact like this. I am Mr. Christopher A. Wray, Director of the Federal Bureau of Investigation (FBI). This Official Memorandum is to inform you that we discovered that some officials whom work under the United States government have attempted to divert your Funds through a back-door channel. We actually discovered this today, through our Secret Agents under the Disciplinary Unit of the Federal Bureau of Investigation (FBI) after we apprehended a suspect.

The mentioned suspect was apprehended at the Dulles International Airport early this morning, as he attempted to carry the enormous cash outside the shores of USA. In respect to the money laundering decree of United States, such amount of money cannot be moved in cash outside United States because such attempt is a crimincal offense and is punishable under the money laundering act of 1982 of United States of America. This decree is a globalize law applicable in most developed countries in order to check-mate terrorism and money laundering.

From our gathered information here in this Unit, we discovered that the said Funds in question actually belongs to you, but it had been purposly delayed because the officials in charge of your Payment are into some sort of irregularities which is totally against the ethics of any Payment institution. Presently, this said Funds is under the custody of the Paying Bank and I can assure you that your Funds will be released to you without a hitch provided that you are sincere to us in this matter. Also, we require your positive cooperation at every level because we are closely monitoring this very transaction in order to avert the bad eggs in out society of today.

Today dated 9th May 2019, we have instructed the Executive management of the Paying Bank to Release the said Funds to you as the certified Beneficiary in question, because we have valuable information's/records to authenticity that the said Funds truly belongs to you. Be that as it may, you are required to provide us with below listed information's (for official verification).

1. First Name, Middle Name and Last Name.
2. Age.
3. Occupation.
4. Marital Status.
5. Direct Telephone/Fax Number.
6. Residential address.

We await your immediate compliance to this official obligation, so that you can be paid by authorized Paying Bank.

Officially Sealed.

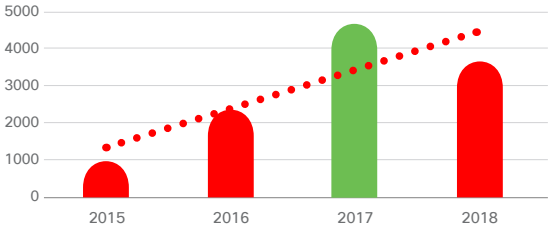
Mr. Christopher A. Wray
Director of the Federal Bureau of Investigation (FBI)

Advance fee fraud

It's not every day you receive an email from the FBI. It's even less common to receive one informing you of a pending transfer of $10.5 million! All you need to do is reply to the email, and they will instruct you on what you need to do to receive the payment.

This is a classic advance fee fraud scam. As the name implies, the scammers will ask for a fee before they'll send you the promised money—money that never appears. It's also one of the older email scams, having taken different forms over the years, from a foreign prince wishing to share his wealth to loan approvals for people with bad credit. Still, the scams persist, with thousands of such email scams reported to the U.S. Better Business Bureau (BBB) each year.

Figure 9 Advance fee fraud scams as reported to the BBB by year.
(Total of Advance Fee Loan, Nigerian/Foreign Money Exchange, Romance, Credit Repair/Debt Relief, Investment, and Travel/Vacations scam type categories.)



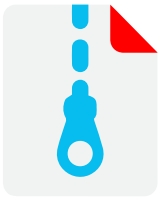
Source: Better Business Bureau

Malware in Email

A good portion of malware is still delivered through email. It used to be more prominent, with .exe files attached directly to emails. But as users got wise to the idea that opening an executable wasn't a safe decision, malicious actors changed their tactics.

Nowadays, malware is much more likely to be served indirectly, either through less suspicious attachments like commonly used business documents or by URLs contained within the message body–all of which are items regularly sent in regular, valid email communication. The idea here is to get past traditional email scans that would catch and quarantine a binary file or other infrequently distributed attachments.

This is most evident when looking at flagged email attachments seen so far this year (January-April 2019). Binary files make up less than two percent of all malicious attachments–that's not just .exe files, but all binaries. This is quite a change from years past, when executable, Java, and Flash files were regularly encountered. In fact, Java and Flash have fallen so far out of favor that if you add them to binaries, you're still only looking at 1.99 percent of attachments.



Archives, such as .zip files, make up almost a third of malicious attachments, and four of the top ten types of files used by attackers.

two in every five

So what sorts of attachments have attackers gravitated towards? Archives, such as .zip files, make up almost a third of attachments, and four of the top ten types of files. Scripts like .js files make up 14.1 percent. These scripts have shown a dramatic increase since the last time we looked at attachment types in the 2018 Annual Cybersecurity Report (ACR), when .js files, combined with XML and HTML, only made up one percent of malicious file extensions.

Their frequency as malicious attachments has continued to grow, going up almost five percentage points since the 2018 ACR. Throw PDF documents into the mix, and more than half of all malicious attachments are regularly used document types, ubiquitous within the modern workplace.

Table 1 Malicious attachment types.

Type	Percentage
Office	42.8%
Archive	31.2%
Script	14.1%
PDF	9.9%
Binary	1.77%
Java	0.22%
Flash	0.0003%

Source: Talos Intelligence

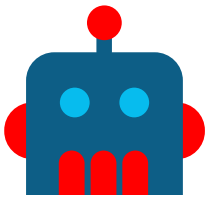
Table 2 Top 10 malicious extensions in email.

Extension	Percentage
.doc	41.8%
.zip	26.3%
.js	14.0%
.pdf	9.9%
.rar	3.9%
.exe	1.7%
.docx	0.8%
.ace	0.5%
.gz	0.5%
.xlsx	0.2%

Source: Talos Intelligence

Email Delivery Infrastructure

Let's step behind the curtain now, away from the types of emails or the payloads, and take a look at the way malicious emails are distributed. There are two primary methods that scammers use to launch spam campaigns: botnets and bulk email toolkits.



Botnets

Spam botnets are by far being used as the main culprits for the majority of spam being sent today. The following are some of the key players in the spam botnet landscape.

Necurs

The Necurs botnet first emerged in 2012 and has spread a variety of threats, ranging from Zeus to ransomware. While its activity has received far more attention in the past, Necurs appears to have faded into the background, at least in terms of press coverage. However, this botnet is still very much active. In fact, the Necurs botnet is the primary distribution vehicle for a variety of scams, including digital extortion.

For more on Necurs, check out the analysis, The Many Tentacles of the Necurs Botnet, carried out by Cisco Talos.

Emotet

Much of the spam sent by Emotet falls into the packaging and invoice category. Emotet is modular malware and includes a spambot plugin. Given how the actors behind Emotet make money by using it as a distribution channel for other threats, the goal of most spam sent by the spambot module is to infect more systems with Emotet, further extending the reach of the malicious distribution channel.

Because Emotet steals content from victims' mailboxes, it is often able to craft malicious, yet realistic-looking threaded messages that appear to recipients to be part of established conversations. Emotet is also known to steal SMTP credentials, commandeering victims' own outbound email servers as a vehicle for outbound spam.

For more on Emotet, read our previous threat report in the Cybersecurity Report Series, Defending against today's critical threats.

"

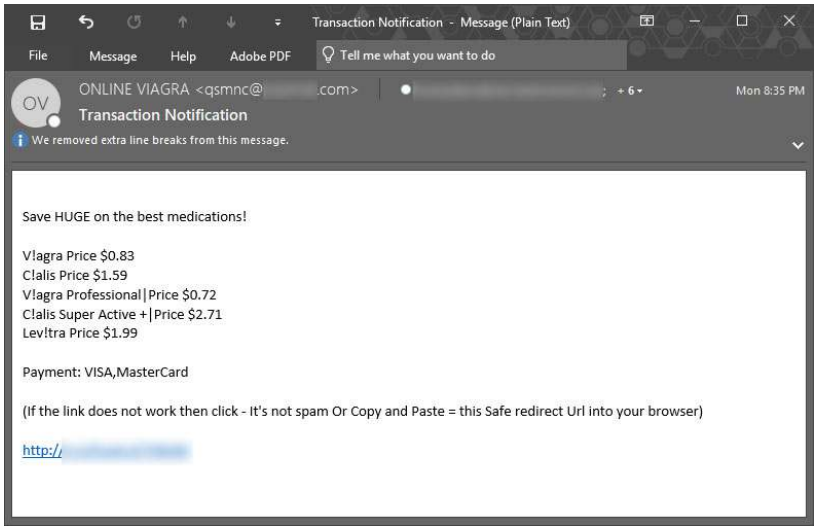
"

Gamut

The Gamut botnet has been busy sending out dating and intimate relations spam, primarily around the premise of meeting people in your area. In other campaigns, the actors behind the botnet send out messages hawking pharmaceuticals or job opportunities (see Figure 10).

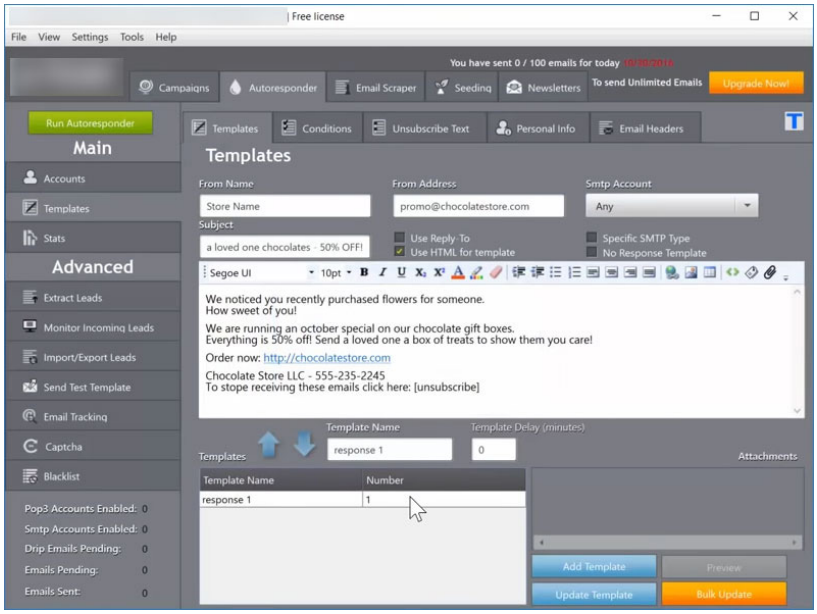
They have registered a variety of domains, though the infrastructure itself seems fairly simple, with multiple subdomains under one domain, and often pointing to one IP address. While Cisco has not confirmed if the services offered are legitimate, the registration process does appear to attempt to phish personal information.

Figure 10 Spam email sent by Gamut botnet.



Note: This visual representation of a screen is a false representation as a cyber threat actor would create and use to trick the viewer into believing it is a legitimate communication.

Figure 11 Example of a spam toolkit.



Note: This visual representation of a screen is a false representation as a cyber threat actor would create and use to trick the viewer into believing it is a legitimate communication.

Bulk email toolkits

An alternative approach that many spammers take is purchasing toolkits to send out a large number of emails. Many of these tools are semi-legitimate, meaning that if you were selling your own hand made, bespoke shower curtains, you could technically use one of these toolkits to raise brand awareness via bulk email to your own opt-in mailing list. However, some of the features included in such toolkits, such as those that allow the rotation of sending IP addresses and customized rebuilding of attachments in order to generate unique hash values, are far less likely to be used in such scenarios.

Recently, Cisco Talos engineers uncovered Facebook groups where malicious actors were selling bulk email tools along with extensive email address lists, likely taken from data breaches. In these cases, the purchasers of such tools were clearly using them for nefarious purposes.

Fraud as the Method

If email is the most common vector, fraud is the most common method – especially for organized crime.

If email is the most common vector, fraud is the most common method – especially for organized crime. Malicious actors behind BEC scams are attempting to defraud companies out of thousands of dollars. Digital extortionists are fraudulently tricking users into paying them in Bitcoins. And when it comes to advance fee fraud, well, it's right there in the name.

None of this is new. Email is just one of the latest tools criminals have used to commit fraud. Historically speaking, criminals strive to grasp the opportunities to maximize illicit takings presented by each generation of technology.

Looking at the losses recorded by the German Federal Police (Bundeskriminalamt BKA) and the FBI, more than 80 percent of all recorded cybercrime losses can be attributed to the pursuit of fraud. The emphasis here is on 'recorded,' since there may be intangible losses that are hard to quantify and record accurately. This does mean that the statistics that are recorded are fairly reliable.

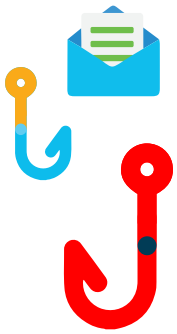
Therefore, stating that fraud is the driving force behind cybercrime losses is accurate. In fact, in examining two fraud methods called out by the FBI statistics—namely Business Email Compromise (BEC) and Email Account Compromise (EAC)—we see that losses in 2018 were $1.3 billion. As a comparison, the equivalent losses recorded for ransomware, an oft mentioned and analyzed form of cybercrime, was $3.6 million. And the fact remains: every indication is that losses associated with undetected fraud will continue to grow, as losses associated with BEC/EAC increased 78 percent alone between 2016 and 2017.

“

”

For more on fraud and cybercrime losses, check out our blog series on

“It’s about looking at people, processes, and the technology across all of the business.”



How to Protect Against Email Attacks

Telltale signs of a phishing email

The silver lining when it comes to threats delivered by email is that there are usually discrepancies that identify them as such, if you just know what to look for. The following are some examples. See the following page for details on each.

To: you@youremail.com

1 From: Amazon Shipping <amz@123fnord.com>

Subject: You're recent order

Dear,

2

Thanks you for your order. Details are as follow:

Purchase: Monthly delivery subscription for Puppy Food™ brand puppy food

Monthly cost: $121 USD

Date and Time : Mei 03, 2019 10:21

IP Address : 254.189.234.159.01

Country of purchase: Guatemala

3

If you no longer wish to subscribe please cancel immediately by following the instructions in the attached or entering your credit card details here:

4

5 http://badphishingsite.com/dontgothere.html

Sincerely,

Amazon Shipping

FILE

6 **dontopenthisis.bad**

Note: This visual representation of an Amazon screen is a false representation as a cyber threat actor would create and use to trick the viewer into believing it is a legitimate logo and communication from Amazon.

Figure 12 Microsoft Office warning about macros in the opened document.

1. **The From: address.** Does the name in the From: address not align with the email address?
2. **Numerous spelling and grammatical errors or blurry logos.** If the email appears to have been carelessly crafted, it may not be legitimate.
3. **Sense of urgency.** If an email asks you to take immediate action, if it has a sense of urgency, or piques your curiosity – be very suspicious.
4. **Request for personal or sensitive information.** Never reply to an unsolicited email asking you for personal, financial, or sensitive information.
5. **Illegitimate looking URL.** Many phishing email URLs look unusual, if scrutinized, and shouldn't be clicked on. If the URL is hidden within a text link, hover over it and look at the bottom of your browser to examine it. When in doubt, don't click it.
6. **Unrecognized file type.** In most professional capacities, only a few file types should ever be sent by email. If the file type looks strange, don't open it.

In addition:

- **Slow down.** The average person spends 8–10 seconds scanning an email before they take action. Slow down and look for the clues that could indicate a phishing attempt.
- **If it sounds too good to be true, it probably is.** Is the email offering you millions of dollars? Threatening to embarrass or hurt you? It's likely that it is entirely fabricated.
- **Pay close attention to warnings.** If you do recognize the sender and open an attachment, pay close attention to banner warnings about extensions or macros needing to be enabled (Figure 12). Rarely, if ever, are these necessary.

Attack prevention strategies

There are several approaches that can be taken to reduce the risk that email threats pose.

Run regular phishing exercises. Your employees are your greatest defense against phishing, especially the most tailored phishing attempts. Employees that can learn to recognize a phishing attempt outright can stop the #1 source of endpoint compromise.

To raise awareness, run regular corporate phishing exercises to test and educate users. Emulate the latest real-world techniques to keep people abreast of what they may encounter. Cisco suggests running these exercises monthly, starting with easy-to-spot test phishing campaigns and gradually raising the complexity. For users that fall for emulated phishing attacks, provide education immediately (e.g. send a test "malicious" URL that leads to further information about phishing). For high-risk users in your organization, where significant damage could occur if they fall for a ruse, practice tailored phishing campaign exercises.

Use multi-factor authentication. In the event that a corporate email account's credentials are successfully stolen, multi-factor authentication can prevent an attacker from gaining access to the account and wreaking havoc.

The beauty of multi-factor authentication lies in its simplicity. Let's say that someone does manage to get a hold of your, or someone on your network's, login credentials and attempts to log in. With multi-factor authentication, a message is automatically sent to the individual who owns the credential to check if they just attempted to log in. The user, in this scenario, realizing that they did not just attempt to log in, denies the request outright. This successfully thwarts the attack.

Keep software up-to-date. In some cases, emails that include malicious URLs may point users to pages with exploits. Keeping browsers and software updated, as well as any plugins, helps to alleviate the risks posed by such attacks.

Never wire money to a stranger. This applies to advance fee fraud and BEC scams. If you're at all suspicious about a request, don't respond. For BEC in particular, set up strict policies that require the wire transfer authorization of a high-ranking individual within the company, and have a designated secondary signatory.

Be careful with requests to log in. Malicious actors, intent on stealing login credentials, go to great lengths to make their pages look like the login pages you would be familiar with. If encountering such a login prompt, be sure to check the URL to ensure it's coming from the legitimate owner's site. If encountering a pop-up style window, expand the window out to make sure that the full URL, or at least the full domain, is visible.

Make sure the email sounds plausible. In the case of scams like digital extortion and advance fee fraud, the senders often craft elaborate stories to try to convince you that the email is legitimate. Does the scenario as laid out make sense? Are there any holes in their stories, from a technical side, financial process perspective, or other? If so, approach with an eye of skepticism.

Be Prepared

There are a lot of different ways that email threats attempt to trick or entice you into replying, clicking URLs, or opening attachments. This justifies the use of email security software that can capture and quarantine malicious emails and filter spam.

Unfortunately, we've discovered a concerning trend: the percentage of organizations using email security is declining. According to our latest CISO Benchmark Study, only 41 percent of those surveyed currently use email security as part of their threat defenses, even while reporting it as the #1 threat vector putting their organizations at risk. This is down from 2014, when 56 percent of organizations used email security.

There are several possible reasons for this decline. One cause could be the move to the cloud. In a recent study conducted by ESG on behalf of Cisco, more than 80 percent of respondents reported that their organization is using cloud-based email services. As more and more organizations opt to have their email services hosted in the cloud, on-site, dedicated email appliances appear less necessary, with some IT teams assuming they can go without.

However, while many cloud email services provide basic security features, the need for layered protection can't be stressed enough. In fact, in the same survey conducted by ESG, 43 percent of respondents discovered that they required supplementary security to defend their email after the move. At the end of the day, there are still valid needs for IT teams to set policies, gain visibility and control, utilize sandboxes, and leverage external blocking capabilities.

Another issue that security teams currently face is an increased attack surface, which naturally results in more areas where protection is needed. If security budgets haven't kept up with this increase, then teams may find themselves scaling some resources back to cover the larger attack surface.

Given that email is the most common threat vector, the importance of protecting it cannot be understated. When performing any cyber risk assessment, it's important to prioritize your most critical entry points with thorough defense and risk management systems and work down in order of probability of attack and risk to the organization if a breach occurs. Then allocate resources that are commensurate with the criticality of potential losses.

In addition, Gartner suggests that security and risk managers (SRMs) take a three-pronged approach to improving their defenses against phishing attacks:

1. Upgrade secure email gateway and other controls to improve protection for phishing.
2. Integrate employees into the solution and build capabilities to detect and respond to suspect attacks.
3. Work with business managers to develop standard operating procedures for handling sensitive data and financial transactions.

How to Protect Your Email

We've looked at the telltale signs of a phishing email, and attack prevention strategies. Now, we'll look at the expectations for email security technology in 2019.

Like in the past, a layered approach to security is critical in defending your organization from email-based attacks. There are several tried and tested email security capabilities that still matter today.

For instance:

- Spam defense must still be in place to keep unwanted email and malicious spam out of inboxes.
- Email threat defense like malware and URL blocking capabilities are vital to block malware, spear phishing, ransomware, and cryptoming in attachments, along with URL intelligence to combat malicious links in emails.
- Integrated sandboxing should happen automatically in the background for new files arriving in email to quickly understand if they are malicious.

However, it can't be stressed enough that the threat landscape is constantly evolving, and malicious actors are always looking for new avenues to launch attacks.

In addition to the tried and tested, the following security technologies can help combat this ever-shifting landscape:

- More advanced phishing protections have emerged using machine learning to understand and authenticate email identities and behavioral relationships to block advanced phishing attacks.
- DMARC domain protections can now be activated to protect a company's brand by preventing attackers from using a legitimate corporate domain in phishing campaigns.
- Message quarantine functionality is useful to hold a message while a file attachment is analyzed prior to either releasing a message to the recipient, removing the malicious attachment, or removing the message completely.
- Email remediation helps if a file is detected as malicious after delivery to the recipient, allowing you to go back and quarantine the message with a malicious attachment from within a mailbox.
- External email threat feeds in STIX are now commonly consumed by email security products, which is helpful should an organization want to consume a vertical-focused threat feed beyond the native threat intelligence in the product.
- Email security integration with broader security portfolios is also becoming common to understand if advanced malware or messages in an environment may have been delivered to particular users or inboxes.

“

”

About the Cisco Cybersecurity Series

Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impacts of data breaches.

In our new approach to our thought leadership, Cisco Security is publishing a series of research-based, data-driven publications under the banner: Cisco Cybersecurity Series. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise in threat researchers and innovators in the security industry, the previous collection of reports in the 2019 series include the Data Privacy Benchmark Study, the Threat Report, and the CISO Benchmark Study, with others to come throughout the year.

For more information, and to access all the reports and archived copies, visit www.cisco.com/go/securityreports.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published June 2019 THRT_02_0519_r1