SEXTORTION 101

WHAT TO KNOW & WHAT TO DO

COFENSE™

COFENSE.COM

"WAIT! THEY HAVE ***WHAT?!***"

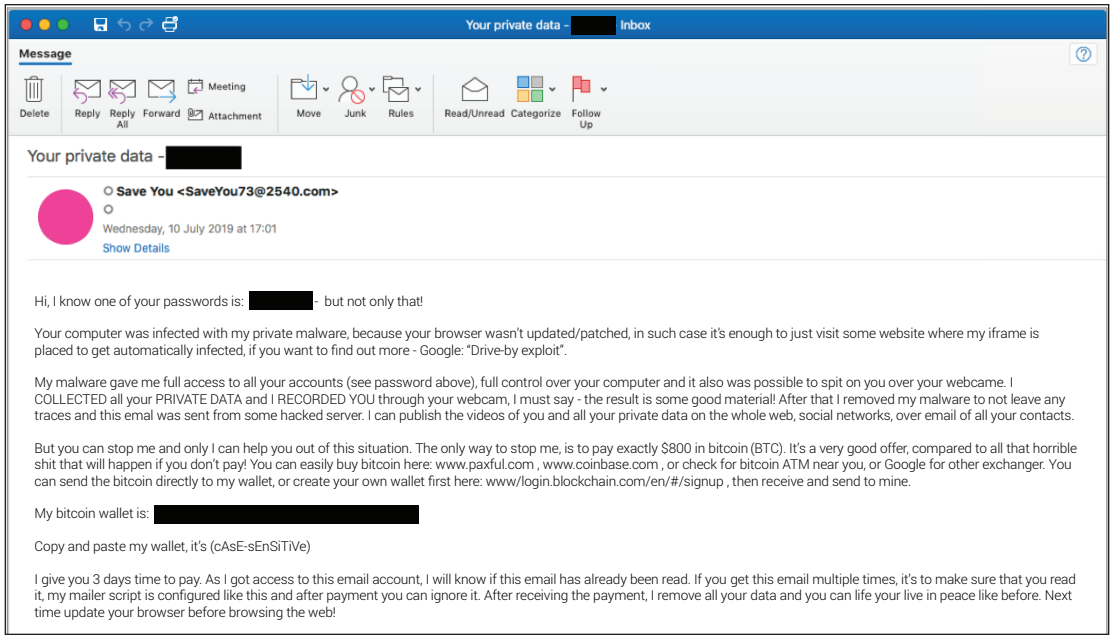
If you receive a sextortion email at work, how did the criminals find you? Do they really have embarrassing videos, your browsing history, or password?

Cofense™ can shed some light on this dark corner of the web. After all, we've been monitoring the largest confirmed dump of email addresses used for sextortion to date. But first, ***what is sextortion?***

According to the Cambridge Dictionary, sextortion is:

"The practice of forcing someone to do something by threatening to publish sexual information about them."

A sextortionist is a scammer who uses these threats to pressure victims into paying a ransom. It's just another type of extortion or blackmail. An example can be seen to the right.



Your private data - [redacted] Inbox

Message

Delete | Reply | Reply All | Forward | Meeting | Attachment | Move | Junk | Rules | Read/Unread | Categorize | Follow Up

Your private data - [redacted]

Save You <SaveYou73@2540.com>

Wednesday, 10 July 2019 at 17:01

Show Details

Hi, I know one of your passwords is: [redacted] - but not only that!

Your computer was infected with my private malware, because your browser wasn't updated/patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: "Drive-by exploit".

My malware gave me full access to all your accounts (see password above), full control over your computer and it also was possible to spit on you over your webcame. I COLLECTED all your PRIVATE DATA and I RECORDED YOU through your webcam, I must say - the result is some good material! After that I removed my malware to not leave any traces and this emal was sent from some hacked server. I can publish the videos of you and all your private data on the whole web, social networks, over email of all your contacts.

But you can stop me and only I can help you out of this situation. The only way to stop me, is to pay exactly $800 in bitcoin (BTC). It's a very good offer, compared to all that horrible shit that will happen if you don't pay! You can easily buy bitcoin here: www.paxful.com , www.coinbase.com , or check for bitcoin ATM near you, or Google for other exchanger. You can send the bitcoin directly to my wallet, or create your own wallet first here: www/login.blockchain.com/en/#/signup , then receive and send to mine.

My bitcoin wallet is: [redacted]

Copy and paste my wallet, it's (cAsE-sEnSiTiVe)

I give you 3 days time to pay. As I got access to this email account, I will know if this email has already been read. If you get this email multiple times, it's to make sure that you read it, my mailer script is configured like this and after payment you can ignore it. After receiving the payment, I remove all your data and you can life your live in peace like before. Next time update your browser before browsing the web!

EZ PASSWORD = EZ THEFT

Typically, here's how sextortionists find you.

When a major breach occurs--for instance, the LinkedIn breach in 2012 resulting in 117M stolen passwords—threat actors take the dump of email addresses, user names (if different than email), and passwords and sell the list on the black market. The purchaser then takes one of two paths—resell the full list "as is" or validate account info and sell validated accounts for a higher price.

Why is the threat actor able to validate the account information? It's common for people to reuse the same password across multiple sites. It's just easier. Many organizations have defaulted to using your email address as your username—again, it's simple to remember. But convenience comes at a price. Easy credentials make it too easy to compromise accounts.

In the past few years, breaches have exposed millions of email addresses and passwords. With this information so readily available, threat actors look for ways to leverage this data to score their next big win. That's when some creep sends you an email.

"PAY UP OR I'LL SHARE!"

Sextortionists often demand payment via Bitcoin. The cryptocurrency lets people exchange money through virtual wallets instead of bank accounts. There are exchanges that enable anonymous trades, making it easier for criminals to cover their tracks.

Another reason sextortionists like Bitcoin: they can get their money quickly and then move it to another wallet, passing the buck, so to speak. It becomes harder for law enforcement or research teams to know who's behind the crime.

Sextortionists will even provide instructions on getting started with Bitcoin. How thoughtful.

17,090	321	1,265	155.908	$1.8M
Unique Bitcoin wallets identified	Bitcoin wallets with transactions	Transactions (victims)	Total Bitcoin paid	Approx. total Bitcoin value

The sextortion botnet Cofense Labs is monitoring is massive. To date, we've identified over 330 million unique compromised accounts (a number that could rise significantly) and analyzed 7,854,099 sextortion emails. The above is how all of that translates to Bitcoin activity.

WHAT YOU SHOULD (AND SHOULDN'T) DO

If you receive a sextortion email, the following steps can help protect you.

We Recommend You **DON'T** Pay!

Sextortionists are counting on fear and panic to trigger an instant payment. But experts agree that it's highly unlikely sextortionists have been watching you on a webcam or keeping tabs on your browsing. Like most forms of fraud, sextortion is a volume business. There's little chance a sextortionist has the time to spy on you or thousands of other targets, though attackers include personal details culled from data dumps, then use automated scripts to send convincing emails en masse.

We Recommend You **DON'T** Respond!

At a minimum, the threat actor wants to engage with you, to start a conversation and ratchet up the pressure. These fraudsters are masters of manipulation, playing on fear, shame, and urgency. The best way not to get played is to stay out of the game. Do, however, notify your IT team so they can investigate.

And We Recommend that You **DON'T** Assume the Worst!

If a sextortionist dangles an old password or user name as "proof", we recommend you think twice. Stolen credentials do not equal blackmail materials. Remember how these criminals find you. The sextortionist likely purchased your credentials on the black market, from a source like the data dump Cofense Labs is monitoring, and is looking to turn them into a quick payday.

If a sextortion email comes to your corporate email and shows a related password, the attacker could potentially reuse the credentials on other corporate apps. There's also the risk of other phishing attacks beyond sextortion—and the risk rises if you pay a sextortion ransom.

IF YOUR EMAIL IS ON THE SEXTORTION LIST...

- If your email address shows up on the list but you haven't received a sextortion email, be on the lookout! The sextortionist may well contact you.
- Don't be alarmed by the threat in the email. Again, alarm is precisely the reaction the attacker is trying to trigger with threats of account compromise and public shaming if you don't respond.

- Sextortion emails normally don't have common phishing elements like a malicious link or attachment. However, if you see either, don't click. Instead...
- If received to a personal account, just delete the message. If received at work, report the email to your security team.

HOW TO AVOID BEING SEXTORTED

If you receive a sextortion email, the following steps can help protect you.

Practice Safe Passwording

Lock 'em up. With so many breaches of email addresses and password combinations, you really should use a password vault. Chances are your IT department has one they recommend.

- Setting up a password vault is a bit time consuming, but it's well worth it.
- Maintain updated account information—once your vault is set up, this is quick and easy.

Enable multi-factor authentication. More and more websites and applications are offering the option to authenticate your identity with two or more factors. When this option is provided, use it!

Create a unique login for each website whenever possible. Use a unique password and, if you're stuck using your email address, it's critical to create a new password for every website login.

- If you're notified your account is affected by a breach, login directly to the website and navigate to the account settings to update password. Be sure to update your password vault at the same time.

Get sophisticated. Create a few email accounts to use for different groupings, for instance, social media or online shopping. Keep your main email for use in banking and other financial transactions.

Cover Your Webcam

Get a webcam cover and use it! If they can't see you, they can't threaten you with personal photos or videos.

Update Your Machine

Keep your device's operating system and applications current. This minimizes your vulnerability to malicious activity. Turn on auto-update. Make it a no-brainer.

IF YOU'RE IN SECURITY OPERATIONS...

Here are some ways you can help users avoid sextortion scams:

- Monitor your domains via the cofense.com/sextortion website. If the database currently displays no results, you should continue to check back periodically. These attacks are ongoing and dynamic, so the results are subject to change. Cofense will continue to add more domains and accounts as the threat evolves.
- Create gateway filters to block key terms used in sextortion emails. Stay current on messages being used, since attackers will regularly use new messages. It's the typical cat and mouse chase.
- Write YARA rules to scan your mail servers, looking for IOCs related to these campaigns.
- Keep in mind that many sextortion emails don't even include a link or attachment, similar to Business Email Compromise (BEC) campaigns. They're just looking for a response they can exploit.

IF YOU'RE IN IT: HAVE "THE TALK" WITH USERS

Like parents broaching the birds and the bees with their appalled children, IT teams sometimes need to have 'The Talk' with users. If employees' email addresses are on the list Cofense is tracking, they need to know they're vulnerable—and that sextortionists sometimes target victims at work, which makes it your business.

A few tips before diving in:

- Brief your senior leadership teams on the threat and potential risk.
- When you talk with exposed users, be calm but direct. After all, it's a business conversation.
- Tell users where their email address showed up, whether on the botnet Cofense is watching or somewhere else.
- Stress that an email address or password doesn't mean that users are known to visit certain sites or that a sextortionist really possesses blackmail material. It simply means that someone purchased stolen credentials and is trying to profit.
- Remind users that they should use their corporate email address for business only, including social media accounts like LinkedIn. You may well have a corporate policy to which you can point employees.
- Give users a link to this e-book or any other helpful source on handling and preventing sextortion.

OTHER WAYS COFENSE CAN HELP

The Cofense Phishing Defense Center™ is seeing increased reports of sextortion and other ransom scams. Condition users to be resilient to evolving phishing attacks with Cofense PhishMe™ and remove the blind spot with Cofense Reporter™.

Quickly turn user reported emails into actionable intelligence with Cofense Triage™. Reduce exposure time by rapidly quarantining threats with Cofense Vision™.

Attackers do their research. Every SaaS platform you use is an opportunity for attackers to exploit it. Understand what SaaS applications are configured for your domains—do YOUR research with Cofense CloudSeeker.

Thanks to our unique perspective, no one knows more about the current REAL phishing threat than Cofense. Understand the current phishing threat—read the 2019 Phishing Threat & Malware Review.

ABOUT COFENSE

Cofense™, formerly PhishMe®, is the leading provider of human-driven phishing defense solutions world-wide. Cofense delivers a collaborative approach to cybersecurity by enabling organization-wide engagement to active email threats. Our collective defense suite combines timely attack intelligence sourced from employees with best-in-class incident response technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global 1000 organizations in defense, energy, financial services, healthcare and manufacturing sectors that understand how changing user behavior will improve security, aid incident response and reduce the risk of compromise. To learn more, visit https://cofense.com/