The Hacker Factor Blog

Not mad, just a scientist

Hello my perverted friend

Saturday, 3 May 2025

Rated 5, 4 votes ↓◆◆◆◆◆↑

At conferences and when first meeting customers, I'm often asked how I got started developing forensic tools. I've been involved in computer security since before "computer security" became a term of art. (People didn't really think about 'computer security' until the Morris Worm in 1988. I was in college when *that* happened. It was exciting!) However, I didn't start developing forensic tools until a decade later, when I started tracking down spammers. It's been nearly 30 years and I still read, classify, and archive every spam message that I receive.

Sometimes I wonder why spammers still do it, and the answer isn't always obvious. Back in 2003/2004, I gave a presentations on covert channels in spam. I had identified over a dozen groups that were hiding messages in spam. The basic gist:

- Back then, anyone could forge the email sender. This meant that the sender was anonymous. (Newer technologies, like SPF (2014) and DKIM (2011), put a stop to completely forged headers.)
- The emails were sent to a large mailing list. Most of the recipients were chaff; only a few addresses in the list were intentional. Unfortunately, nobody (except the sender) had the entire list, so no external observer could identify the intended recipients. This made the intended recipient anonymous.
- The covert message would be hidden somewhere in the email -- in the header, subject, or buried in the content. If you didn't know to look for it, you wouldn't see it.
- Any email message would work, but spam was ideal. The sender could re-use any spam message as camouflage. The unintended recipients (regular people) had already been trained to see and delete spam, so nobody (well, except me) would look closely enough to see the covert message.

I had been categorizing spam based on the sending tool signatures (email headers) and spam contents. The re-used spam messages really stood out. "Hey, that content is from the guy in Detroit, but that's not his tool signature!" The first time I had a mismatch, it was a covert channel and I could see the hidden message plain as day. At the time, I had been hanging out in hacker forums, where people write in "leet speak" (replacing letters with similar shaped characters, phonetic spelling, and horrific abbreviations). The message was in leet:

```
[gvjrFov-ka1AsHb3-oOGIgZSseoUJF]
```

It translates as:

```
[gvjr Fov - ka1AsH b3 - oO G I gZSseo UJF]
[Governor of - class B - oh gee I guess UJF]
```

A few days later, I saw this message:

```
[whQZsFOtOcY-AWw9fYuTUvLS-EBdh4gbj2Py5H]
```

About

Dr. Neal Krawetz writes The Hacker Factor Blog. Follow him on Mastodon.

Tools

• FotoForensics: Test your own photos.
• Hintfo: View metadata.
• Gender Guesser: Use your words.

Links

Security
Internet Storm Center
Krebs on Security
Bruce Schneier

Images
Photo Stealers
Awkward Family Photos
Unsplash

Debunking News
iMediaEthics
Poynter

Debunking Politics
FactCheck
PolitiFact

Debunking Other
Snopes
Math with Bad Drawings

Calendar

Archives

Feeds

Categories

> It translates as:
> ```
> [whQZs FOtO cY - AW w9f Yu TUvLS - EBdh4gbj2 Py5H]
> [Who's photo Cy? I love your tools - *something in Tagalog*
> ```

Long story short, this series of messages came from a group of Filipino elementary school k covert messages in spam. (They called themselves "The Hangouters" because they would h "Cy" was short for Cybersad. She was the collector and distributor of tools for the group.) Wl these kids showed me how to spot covert messages. As soon as you can see it, you start se is the Baader-Meinhof Phenomenon or "red car theory"; when you learn to see it, you notice quickly identified a few other 'covert channels in spam' groups, including organized crime, na and other organizations. It wasn't just kids.

Covert channels in spam dried up when spam filters got better. I mean, there's no point in se messages in spam if some upstream filter silently blocks the spam and prevents the intende seeing the message.

The volume of spam today is nothing like it was a few decades ago. A lot of the obvious scar or significantly reduced in volume. For the ones that are left, I have to wonder if there is an u

Extortion(?)

The other day I received a fun spam message:

> Date: Tue, 29 Apr 2025 10:36:41 +0300
> From: Dawson Monroe <[REDACTED]@piplslovers.ru>
> To: [REDACTED]@[REDACTED].com
> Subject: New Message
>
> Well, hello there, my perverted friend.
> I'll get right to the point.
> We've actually known each other for a while now, at least I've known you.
> You can call me Big Brother or the All-Seeing Eye.
> I'm a hacker who a few months ago gained access to your device, including your brov
> and webcam.
> And I recorded some videos of you jerking off to highly controversial "adult" videos.
> I doubt very much you'd want your family, coworkers, and your entire contact list to se
> of you pleasuring yourself, especially given the specifics of your favorite genre.
> I'll also put these videos on porn sites, and they'll go viral, so much so that it will be ph
> impossible to remove them from everywhere.
>
> How did I do that?
> Because of your disregard for Internet security, I was able to easily install a Trojan hor
> device.
> which accessed all the data on your device and allowed me to control it remotely.
> Once I infected one device, I had no problem accessing all the other devices.
> My spyware is embedded in the drivers and updates its signature every few hours, so
> or firewall can even detect it.
> So now I'm just gonna give you a condition. A small sum in exchange for your former
> Transfer 1200 USD to my bitcoin wallet:
>
> bc2de3y7z[REDACTED BITCOIN ADDRESS]
>
> As soon as I receive confirmation of the transfer, I will delete all the videos that compr
> remotely erase the virus on your devices and you will never hear from me again.
> Agree, it's a very small price to pay for not destroying your reputation in the eyes of ot

> judging by your correspondence in messengers,
> has an opinion of you as a decent human being.
> You can think of me as a kind of mentor who wants you to start appreciating what you
> You have 48 hours - I'll be notified as soon as you open this letter, and from then on it
> countdown.
> If you've never dealt with cryptocurrency before, it's super easy - type "crypto exchang
> search engine, and the next thing to do.
> Here's what you shouldn't do:
> Don't reply to my email. It was sent from a disposable e-mail account.
> Don't call law enforcement. Remember, I have access to all of your devices, and as s
> notice such activity, it will automatically lead to the release of all of your data.
> Do not attempt to reinstall your system or factory reset your device.
> First of all, I already have the video and all your data, and secondly, as I already said,
> remote access to all your devices and as soon as I notice such an attempt, it will lead
> irreversible consequences.
> Remember that crypto-addresses are anonymous, so you won't be able to figure me
> wallet.
> Anyway, let's make this a win-win situation.
> I always keep my word, unless I'm being tricked.
> Advice for the future: take more seriously your security on the Internet. Also regularly
> passwords and set up multi-factor authorization on all your accounts.

This specific email came from a newly-created domain (registered 2024-08-20) that appears
for sending spam and scams. It came from a cloud provider in the Netherlands. This is comr
these days: register a burnable domain at a cloud provider, then send as much spam as you
account gets shut down.

With minor variations, this type of spam message has been going around for years. When th
it was as a blind extortion attempt:

- The extortion letter claims to have compromised the recipient's account. Originally, the
  included your LinkedIn password from a 2012 data breach. This latest instance exclud

- The scam plays an odds game. It makes a wild-guess accusation that you have been
  must pay an extortion. A small percent of the population might think it is a real threat a
  I mean, *if* you view porn *and* are ashamed of it *and* think your computer might be com
  might consider paying the ransom.

As scams go, this one is pretty weak. My various email addresses have received dozens of
the years. They all include blockchain identifiers. I've looked up the blockchain addresses; *n*
ever received payments. This is an ineffective scam.

The biggest flaw in this approach is that they want payment by bitcoin. When the scam first
receive the occasional contact from friends or friends of friends (part of my PTSD -- People
Duties). A few of those contacts were embarrassed and didn't know how to pay in bitcoin. S
and wanted to know how to stop the false allegations. They were all relieved to hear that it w
extortion attempt. The scammer was spraying everyone and hoping someone would fall for i

Frankly, if you're technical enough to use bitcoin, then you're probably not going to fall for it.
it, you probably don't know how to pay it.

Opportunity?

This most recent email went to one of my honeypot email addresses. (Yes, the scammer is
honeypot account isn't a real person, it never goes out and watches porn.

But this got me thinking. Let's pretend this is true. Let's assume that the sender compromise and has incriminating evidence that I look at porn. Would this surprise *anyone*? I run a photo service. *Of course* I see porn. Daily. (And it's not even the good stuff. It's usually creepy ugly who really should be wearing clothing.) I see it and I immediately ban the user. I even send to NCMEC (if it involves child pornography). I often write about this in my blog; this shouldn't

The email clearly shows that he doesn't know his victim (me). I mean, which would be more he claims I watch porn and am embarrassed about it, or (B) that he claims my computer was the most he could get is a few bitcoin for porn extortion? I develop computer forensic softwa services. I'm sitting on tons of viable zero-day exploits (things I've stumbled across while doi the most he can extort me for is $1200? I feel insulted!

At FotoForensics, we've found that some people upload porn because they get their kicks by As far as he knows, I might find that to be a turn-on. If he has videos of me watching porn, w to release it?

Then again, "videos of Neal watching porn" seems like it's own sick genre. I could probably selling it online! (Hey, who wants to join me on a money making venture?) I'm envisioning ar account that is just me making disgusted faces as I look at poor-quality porn online.

Ulterior Motives

Since this scam is so ineffective, I have to wonder if there is some ulterior motive. It's word-f other spam that I've received over the years; there's no subtle encoding in the content. I don indications of a covert message.

Maybe there is something else going on, such as:

- **Testing mailing lists**. Maybe he's looking for email bounces or delivery problems.

- **Testing the mail server**. Does my server exist? What server version am I running? Do that is missing SPF or DKIM headers? (This is my honeypot, so "Yes, it accepts everyt servers won't accept email that lacks any kind of sender validation.

- **Testing the hosting provider**. How many emails, and over what duration, can he abu hosting provider before he gets shut down? This could just be a 'sending volume' chec while the domain was registered 9 months ago, it doesn't appear to have been used fo recently.

- **Creating chaff**. Maybe the purpose is to just generate a lot of network traffic. While th focus on the spam, they may not notice some other subtle, nefarious activity on their n

With each of these options, the email's content means nothing. Maybe he'll get lucky if some
that's not the main goal. The primary goal may be to validate the spam mailing list, check the
the reaction time of the hosting provider, and/or divert attention away from some other activi
maybe he has some other motive.

Some spam messages are simple advertisements or obvious grifting opportunities. But othe
phishing or other attacks. When it comes to spam, it's often not what you think.

Read more about Forensics, Network, Security | Comments (2) | Direct Link

COMMENTS

#1 Dodo on 2025-05-04 05:47 (Reply)

"I've looked up the blockchain addresses; none of them have ever received payments. This
scam."

I think you might be wrong about this.
Everyone in the spam list probably gets the email with a **different** bitcoin address.
This makes it possible for the attacker to know who fell for it and who didn't, which is valuat
(If they fall for this, they may fall for other scams too.)

Also, i don't know what, but there's something off about that email.
Almost as if it isn't from a real scammer?

> #1.1 Dr. Neal Krawetz (Homepage) on 2025-05-04 06:55 (Reply)
>
> Hello Dodo,
>
> With prior instances of this email, I can search Google for the bitcoin address and find ot
> received the same email with the same bitcoin address.
>
> You're right: in theory they could give everyone a unique address. In practice, they are n
> to change the bitcoin address between mailing campaigns, not between each mailing.
>
> Then again, if they are mailing millions of people, then it takes time to generate a million
> addresses. That will delay their ability to send spam quickly.
>
> I can't speak for this latest email since it's too new to have been indexed by Google.

ADD COMMENT

Code of conduct

- Name calling and anti-social comments will not be posted.
- Comments must be related to the topic. Unrelated comments will not be posted. Make
submitting your comment to the correct blog entry; Yes, people have submitted great co
wrong blog entries.
- Comments should be rational and logical, citing findings as appropriate.
- Opinions and speculations are desired and welcome, but if they are represented as fac
moderated or censored.
- The moderator reserves the right to end tangential discussions and censor offensive or
content.

Name

Email

Homepage

In reply to [Top level]

Comment

Enclosing asterisks marks text as bold (*word*), underscore are made via _wo
Standard emoticons like :-) and ;-) are converted to images.
E-Mail addresses will not be displayed and will only be used for E-Mail notifica

□ Remember Information?

Submitted comments will be reviewed by moderators before being displayed.

Submit Comment | Preview

Copyright 2002-2025 Hacker Factor. All rights reserved.