

Keeping pace with emerging threats: Summer 2022 roundup

Get the latest threat intelligence on sextortion phishing, LinkedIn impersonation emails, zero-day exploits, and Ukraine donation crypto scams.

AN EGRESS REPORT

New threats your users should know about

In this report, we've detailed the recent tactics cybercriminals are using and exposed the warning signs your organization needs to stay aware of. Our threat intelligence team offers advice and analysis on the steps you should take to protect your employees, customers, and overall business from sophisticated cyberattacks.

We've shared some of the latest emerging threats they've uncovered through monitoring our B2B platform, including cryptocurrency scams exploiting Ukrainian donation appeals, LinkedIn impersonation emails targeting job hunters, and zero-day exploits circulating on the dark web.

The emerging threats we'll be exploring in this report:

LinkedIn impersonation emails	04
Rise in sextortion phishing	07
Zero-day exploits: Gmail, Facebook and electronic voting	11
Ukraine cryptocurrency donation scams	14

LinkedIn impersonation attempts

THREAT SUMMARY

VECTOR AND TYPE:

Email phishing

TECHNIQUE:

Template spoofing and credential scraping

PAYLOAD:

Obfuscated links to harvest credentials

TARGETS:

Organizations across the US and the UK

PLATFORM:

Microsoft 365

BYPASSED SECURE EMAIL GATEWAY:

Yes (63.7% of emails were not recorded on a blacklist and bypassed SEGs)

What to look out for

In February 2022 we reported a 232% increase in email phishing attacks impersonating LinkedIn. These emails use display name spoofing and stylized HTML templates to socially engineer victims into clicking on phishing links and then entering their credentials into fraudulent websites.

The attack payload is a malicious link that has been obfuscated with URL shorteners. These links were found in up to 10 places within the emails, to increase the chances of it being clicked. A phishing website using LinkedIn branding then scrapes the credentials when the victim believes they are logging in. After doing so, the person is redirected to the real LinkedIn site, so they're not alerted that they've just had their credentials farmed.

Only 36.3% of the emails were caught by Secure Email Gateways (SEGs), with 63.73% getting through. Based on what we've seen, it's likely attackers were able to purchase these email templates and the back-end setup for the phishing website as part of a phishing kit. This suggests SEGs using signatures to detect phishing kits might be behind the curve with updating their blacklists.

We found that the emails are sent from different webmail accounts that have zero correlation to each other. They've been sent from a mixture of compromised accounts as well as spoofed addresses of legitimate email accounts, for example: *notifications-noreply@linkedin.com*.

They use targeted subject lines associated with LinkedIn, including:

- You appeared in 9 searches this week
- You were found by people
- People are looking at your profile
- You have 1 new message
- Your profile matches this job
- We've got a new message for you

As shown in figures 1 and 2, the emails use multiple stylized HTML templates, including the LinkedIn logo, brand colors, and icons. Within the body of the email, the cybercriminal uses other well-known organizations' names (e.g. CVS Caremark, as shown in figure 2) to make the attacks more convincing. The phish features elements from LinkedIn's genuine email footer such as:

- Global HQ address
- Hyperlink to unsubscribe
- Hyperlink to their support section
- Recipient information

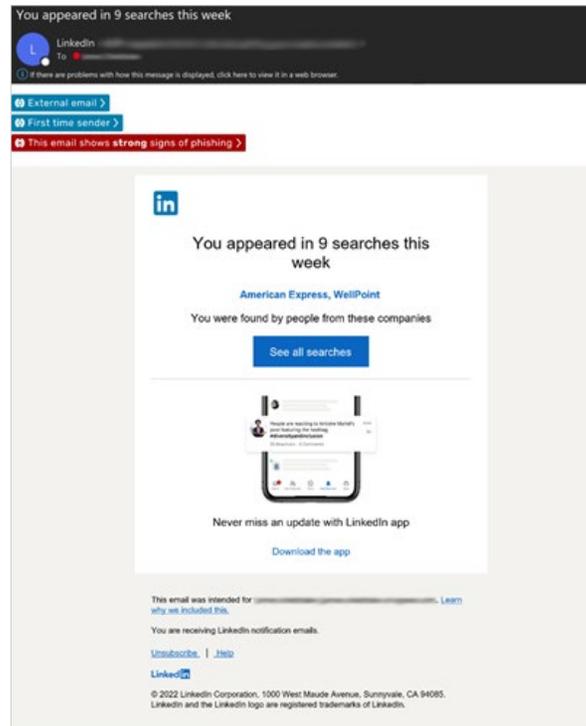


Figure 1: Example of a LinkedIn impersonation email

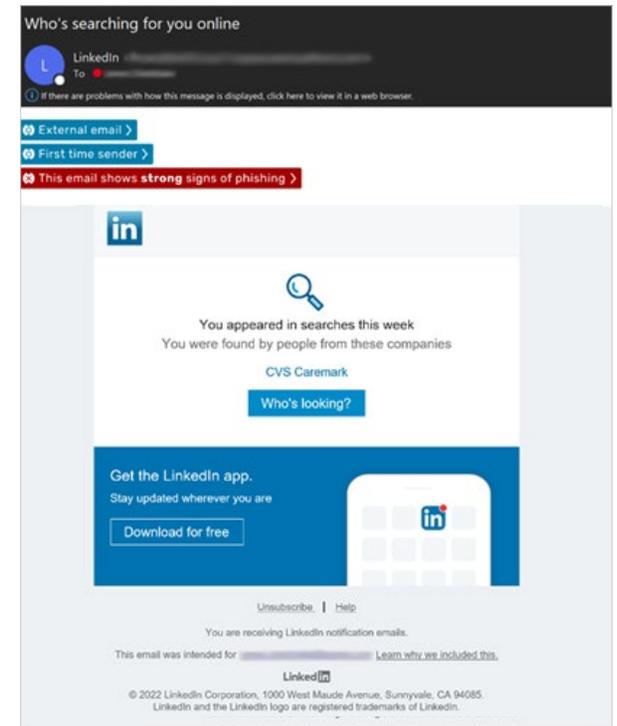


Figure 2: Example of a LinkedIn impersonation attack

The targets vary, covering companies in both the US and the UK, and operating within different industries. LinkedIn states it has over 810 million members in more than 200 countries, which provides an extensive target pool for cybercriminals. Many professionals choose to include their corporate email address within their profile, and many regularly receive update communications from LinkedIn. Consequently, they could be more trusting of a stylized phishing email.



EGRESS ANALYSIS

Jack Chapman, Egress VP of Threat Intelligence

Current employment trends help to make this attack more convincing. ‘The Great Resignation’ saw a record number of Americans search LinkedIn for new opportunities and leave their jobs in 2021. We’ve seen this trend continue, with a 67.4% uptick in resignation emails between the months of February and April 2022. It’s likely these phishing attacks aim to capitalize on jobseekers (plus curious individuals) by flattering them into believing their profile is being viewed and their experience is relevant to household brands.

We advise organizations to examine their current anti-phishing security stack to ensure they have intelligent detection technology in place. We’ve seen these emails bypassing SEGs and arriving into users’ inboxes, only stopping once the payload was added to the SEGs’ blacklist – by which time users may have already clicked through.

Individuals within an organization should be advised to take extreme caution when reading notification emails that request them to click on a hyperlink, particularly on mobile devices. If a user is unsure about a link and cannot verify its destination through hovering over it, we’d recommend they go directly to LinkedIn to check for messages and updates.

Rise in sextortion phishing

THREAT SUMMARY

VECTOR AND TYPE:

Sextortion phishing email

TECHNIQUE:

Social engineering

PAYLOAD:

Cryptocurrency address

TARGETS:

Individuals and organizations across the US and the UK

PLATFORM:

Microsoft 365

BYPASSED SECURE EMAIL GATEWAY:

Yes

What to look out for

We saw a 334% increase in sextortion phishing emails across the UK and the US since March 2022. Across April, we discovered that 53% of these attacks were sent from compromised legitimate email accounts. All of the attacks contained cryptocurrency addresses, rather than traditional phishing payloads such as malicious links or attachments. These tactics were likely the reason they bypassed SEGs, as they're linguistic in nature and harder for traditional solutions to identify.

The attacks feature a variety of subject lines. Some are closely affiliated to the topic of the email in the hope that people panic and click through for more information, such as:

- "All your data has been hacked and copied to my servers. Instructions inside"

- "Here is the last warning! Your entire information has been copied. The entry in system is completed."

We've also seen financial subject lines, for example:

- "You have an unpaid bill."
- "You have to pay a debt."

These might appear bland but they can be more effective. Some people will instantly delete a message with an alarmist subject line like the first examples. Plainer subject lines can catch people off guard and make them click, as well as avoid detection from solutions looking for keywords such as 'HACKED.'

The emails use emotive and threatening language to socially engineer the target to extort payment, such as 'I could ruin your life forever' and 'I don't think this kind of content would be very good for your reputation' (figure 3). The emails we analyzed followed a similar format, stating the problem, the threat, the 'solution', the deadline to comply by, and the futility of reporting the incident.

After analyzing a segment of the recipients of these sextortion emails, we discovered they were all part of either the Apollo and/or the Data Enrichment data breaches. It is possible the cybercriminal(s) used email addresses from these breaches to build their target list(s).

-----Original Message-----
From:
Sent: 11 April 2022 05:29
To:
Subject: All your data has been hacked and copied to my servers. You have 2 days left. Instructions inside

Hi.

This is the last warning.

I hacked your operating system through the Wi-Fi router you were connecting to!

A few months ago, I accessed your devices that you use to access the internet.

All the data from your devices is copied to my servers.

I have access to all your messengers, social networks, emails, chat history and contact list.
And I have access to all your personal data I have already copied to my servers.

My virus constantly updates its signature (driver based), therefore it remains invisible to antivirus software.
I guess now you understand, why I stayed unnoticed until this letter...

In gathering information about you, I discovered that you are a big fan of adult websites and more.
You really like to visit porn sites and watch dirty videos while having an orgasm.

I've already made a screen capture.
A montage of the pornographic video you were watching at the time and your masturbation.
Your face is clearly visible. I don't think this kind of content would be good for your reputation.

I can send this video out to everyone who knows you.

I also have no problem with making all of your private data public on the Internet.
I think you know what I mean.

It would be a real disaster for you.

I could ruin your life forever.

I think you really don't want that to happen.

Figure 3: Ransom demand within a sextortion email

Figure 4: Data breach results from www.haveibeenpwned.com for recipients' email addresses

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

APOLLO **Apollo:** In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. [The Apollo website has a contact form](#) for those looking to get in touch with the organisation.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles

 **Data Enrichment Exposure From PDL Customer:** In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles



EGRESS ANALYSIS

Jack Chapman, Egress VP of Threat Intelligence

Cybercriminals use our psychology against us in phishing attacks. They're designed to make someone act quickly and without rational thought. As the longer we think about it, the more holes we might see in the cybercriminal's story. For example, why has the scammer not included any evidence of what they claim to have?

Shame, panic and fear are very primal feelings. The goal of sextortion is to trigger these feelings and make the recipient act irrationally by using language such as 'dirty videos', 'disaster', and 'ruin your life'. By giving the recipient a deadline to respond by, the cybercriminal puts pressure on the individual to comply quickly, while warning them not to seek help from people who could think more rationally.

However, this is all a psychological threat from the cybercriminals. These sextortion emails we've found are known as 'replay attacks.' The attackers have downloaded a contact list of everyone involved in a previous data breach and sent them their own phishing attack. They're mass-produced attacks that don't require technical sophistication to implement. Searching for the Bitcoin addresses will often turn up examples of the identical scam on cybersecurity forums.

The most important advice is... **Don't pay the ransom!** It's easy for cybersecurity experts to say, and of course it can be alarming for someone to receive an email like this, especially if it's one of the more believable ones. But the scammer is relying on the fact people will be embarrassed and won't ask for help dealing with the issue.

Zero-day exploits: Gmail, Facebook and electronic voting

THREAT SUMMARY

VECTOR AND TYPE:

Zero-day exploits

TARGETS:

Facebook users, Gmail users, and countries using electronic voting

PLATFORM:

Facebook and Gmail

What to look out for

We've recently found three zero-day exploits that have been posted to Empire Market, a DarkWeb forum where exploits, phishing tools, and templates are available to purchase. As you can see in figure 5, it works like any legitimate online marketplace, with categories, filters, and reviews.

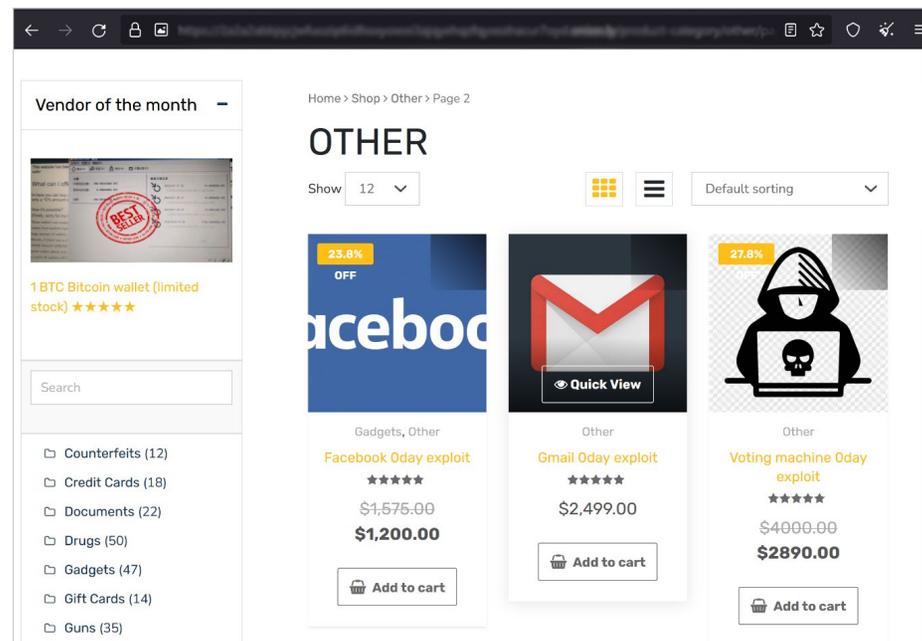


Figure 5: Empire Market dark web forum

At the end of April 2022, our analysts found an electronic voting exploit for sale (figure 6). This exploit claims to allow malicious software to be loaded onto a voting machine via a USB and then cause a score bias per voting machine. For example, it could ensure that every third vote goes to a particular candidate, regardless of what the voter selected. This could have serious impacts on the fairness of an election.

The second involves an exploit to takeover a victim's Gmail account. As you can see in the product description in figure 7, the poster claims the exploit can be deployed remotely via a code injection. It then sends the attacker an authentication code via a burner email (an address which cannot be linked to an attacker's real-world identity).

This exploit allows attackers access to all Gmail accounts, regardless of two-factor authentication (2FA). It goes to show that 2FA is not enough on its own, despite the peace of mind it might give to users. People should be advised that 2FA is not a magic bullet against phishing. They need to make

Voting machine 0day exploit
★★★★★ (3 customer reviews) | Add a review.
~~\$4000.00~~ **\$2890.00**

Our Voting Machine 0day exploit allows you to swing the votes in your favor. This exploit requires access to a voting machine to inject the code and launch this vulnerability.

VIDEO: [https://www.youtube.com/watch?v=XXXXXXXXXX](#)

Quantity:

Categories: [Gadgets](#), [Other](#)

Figure 6: Electronic voting machine zero-day exploit

Gmail 0day exploit
★★★★★ (2 customer reviews) | Add a review.
\$2,499.00

Our Gmail 0day exploit is a fully remote exploit, it exploits a authentication email code input vulnerability via a code injection. You will be able to receive a authentication code via a burner email to takeover the target Gmail account.

VIDEO: [https://www.youtube.com/watch?v=XXXXXXXXXX](#)

Quantity:

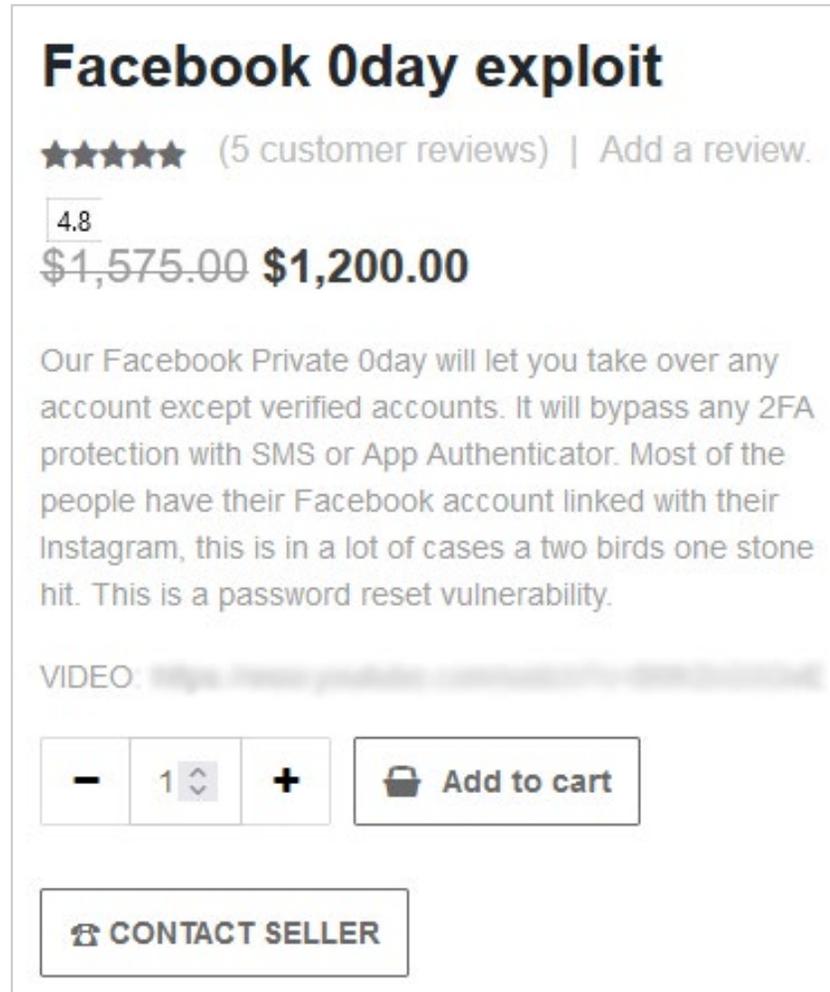
Category: [Other](#)

Figure 7: Gmail zero-day exploit

sure software is updated and stay alert to warnings about suspicious logins.

The final zero-day exploit we've found doing the rounds is a way to takeover a Facebook account through a password reset vulnerability (figure 8). This exploit bypasses any two-factor protection through an SMS or App authenticator. As the product description explains, most people link their Instagram to their Facebook account, so it's a 'two-in-one' exploit.

These accounts can be taken over and then used to harvest even more information about victims to make further phishing attacks more believable. Social media accounts contain a host of information about people, such as date of birth, geographic locations, mother's last name, and plenty more.



Facebook 0day exploit

★★★★★ (5 customer reviews) | Add a review.

4.8

~~\$1,575.00~~ **\$1,200.00**

Our Facebook Private 0day will let you take over any account except verified accounts. It will bypass any 2FA protection with SMS or App Authenticator. Most of the people have their Facebook account linked with their Instagram, this is in a lot of cases a two birds one stone hit. This is a password reset vulnerability.

VIDEO: [https://www.youtube.com/watch?v=9999999999](#)

- 1 + Add to cart

CONTACT SELLER

Figure 8: Facebook zero-day exploit

Ukraine cryptocurrency donation scams

THREAT SUMMARY

VECTOR AND TYPE:

Email phishing

TECHNIQUE:

Display name impersonation and social engineering

PAYLOAD:

Cryptocurrency address

TARGETS:

Organizations across the US and the UK

PLATFORM:

Microsoft 365

BYPASSED SECURE EMAIL GATEWAY:

Yes

What to look out for

We've seen a surge in scammers latching onto communications and appeals regarding the Russia-Ukraine conflict. These come in the form of requesting donations of cryptocurrency or impersonating known bodies in Ukraine and begging for assistance. For example, figure 9 shows

an email impersonating the Ukrainian Government asking for cryptocurrency donations to assist their war effort. Other impersonated organizations and individuals have included:

- Ukrainian Ministry of Defence
- Aid for Ukraine (charity)
- The United Nations
- Ukrainian President Volodymyr Zelenskyy

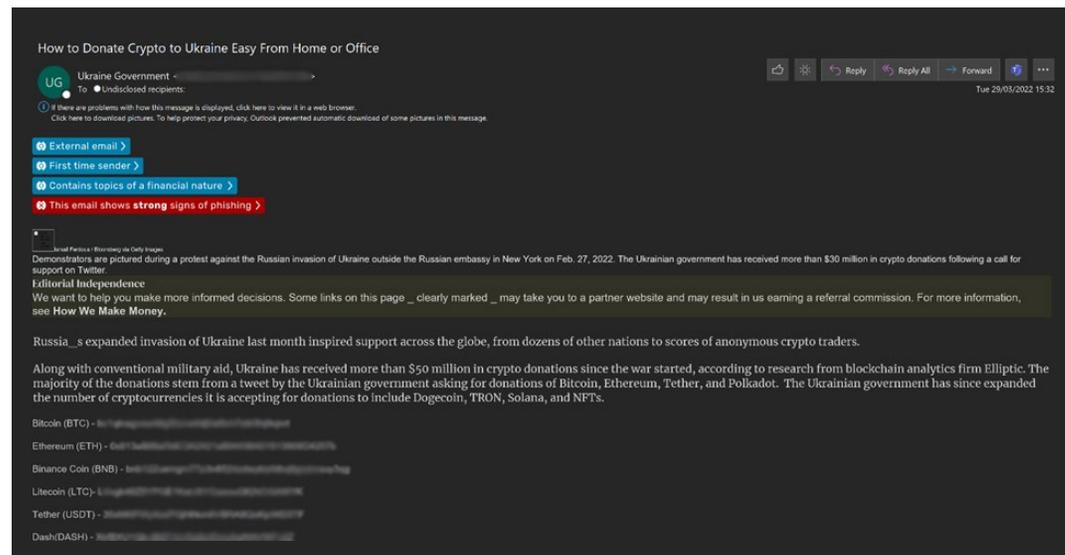


Figure 9: Impersonation attempt of a Ukrainian government appeal

None of the cryptocurrency wallet addresses in these phishing emails match the ones posted publicly by the [Ukrainian government](#). The donation links such as the one shown in figure 10 likely put the proceeds straight into the pockets of cybercriminals.

Of the 962 phishing emails we analyzed, we found 244 separate cryptocurrency addresses (174 Bitcoin and 70 Ethereum). Some requests contained addresses for lesser-known cryptocurrencies such as Litecoin, Tether, Dash, and Tron. These cryptocurrencies are also officially requested by the Ukrainian government – as they can be more secure and offer multiple avenues for donations. Attackers sometimes prefer them as they are less closely monitored by law enforcement than the better-known cryptocurrencies.

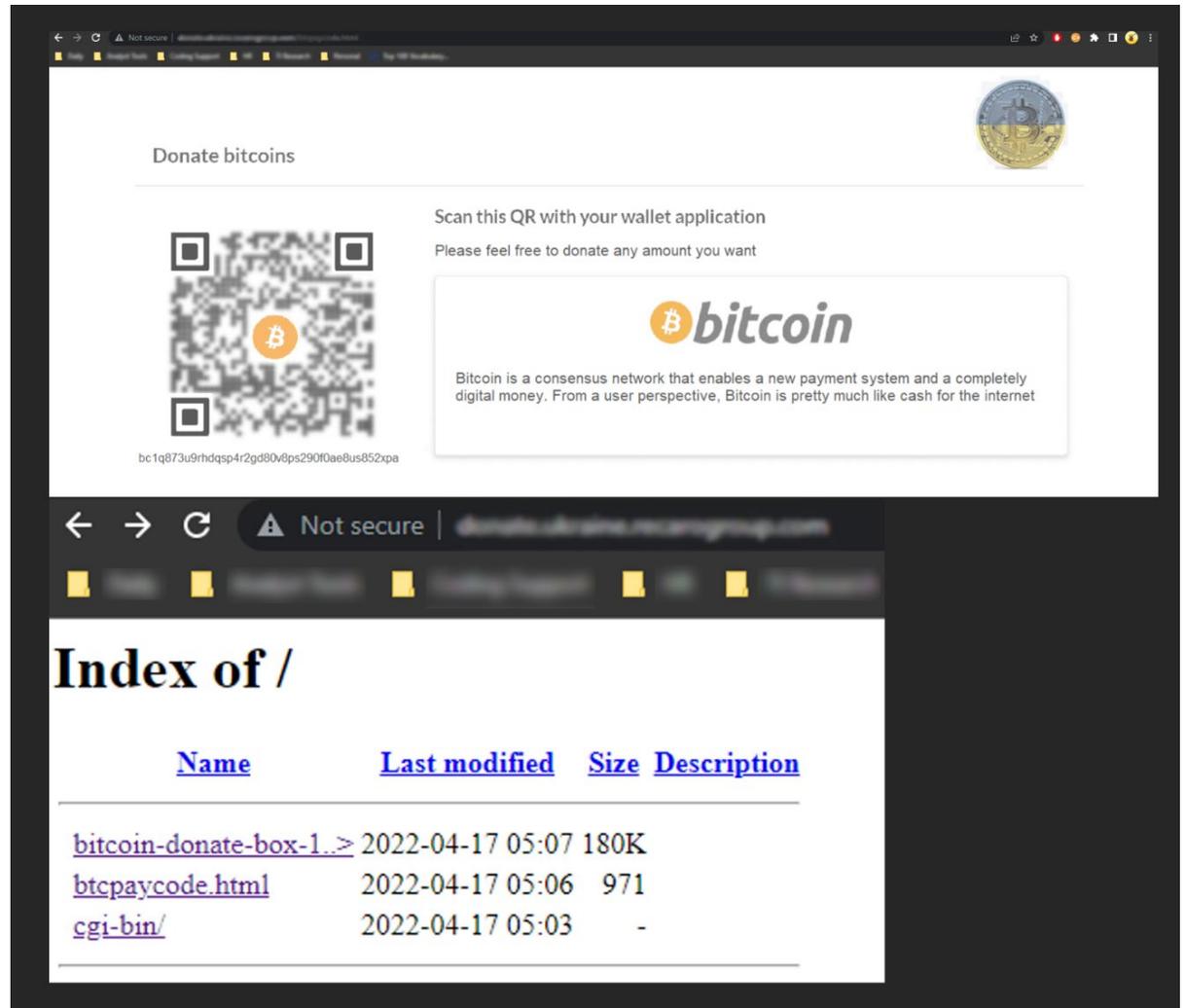


Figure 10: A QR code that would take a victim to the scammer's crypto wallet



EGRESS ANALYSIS

Jack Chapman, Egress VP of Threat Intelligence

These attacks need two things to happen in order to be successful. Firstly, they need to use an obfuscation technique to evade email security. Samples of the emails we discovered have been analyzed and been found to include substitute lookalike Unicode characters to bypass linguistic detection.

Secondly, they need the person to act. The emails we've analyzed all use social engineering to exploit an emotional reaction in people. By asking people to help in the fight against the Russian invasion or for humanitarian help for refugees and children, they hope that people will overlook the warning signs of phishing in their rush to do a good deed.

Communicate to your people to be wary of these scams. If they really want to donate cryptocurrency to a cause but are unsure of the legitimacy of an email, it's best to search for information online from reputable sources and only use publicly available cryptocurrency addresses.

>> Key advice to share with your users

1

Advise people to treat all unsolicited requests for cryptocurrency donations with healthy suspicion – especially those regarding current world events. If they want to donate, advise them to try and find publicly displayed information and wallet addresses from reputable online resources.

2

As the LinkedIn examples in this report showed, spoofed emails can be highly convincing with legitimate subject lines and email templates. Your people should use caution whenever a notification email asks them to follow a link.

3

Sextortion emails tend to be empty threats exploiting previous data breaches. It's important to educate users so they do not fall for psychological tricks. Advise them to simply delete the email – and never pay a ransom.

4

New zero-day exploits are being discovered all the time. Keep your people abreast of the latest threats by staying up to date with advice from your threat intelligence network. They should also be advised to make sure they're always using the latest software versions.

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats. Using patented contextual machine learning we detect and prevent abnormal human behavior such as misdirected emails, data exfiltration and targeted spear-phishing attacks. Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York and Boston.

www.egress.com |  Egress Software

