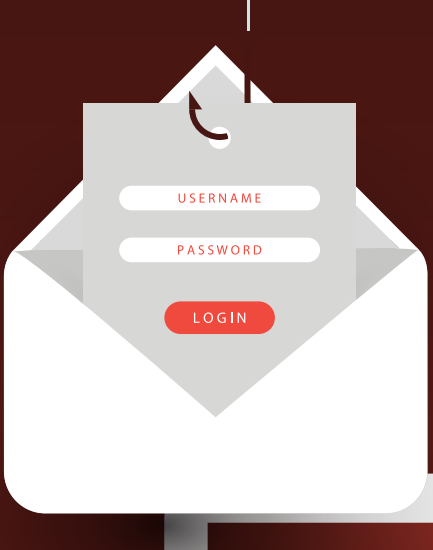


HOW THREAT ACTORS TRY TO TRICK YOU WITH

PHISHING EMAILS

Diving into Phishing Trends by Categorizing Phony Emails

To learn more about trends in the phishing and spam email landscape, our analysts created accounts for fake email addresses that were posted on the darknet. These addresses were mainly sourced from combolists, which are large batches of credentials that typically came from a variety of different breaches or otherwise illicitly obtained methods.

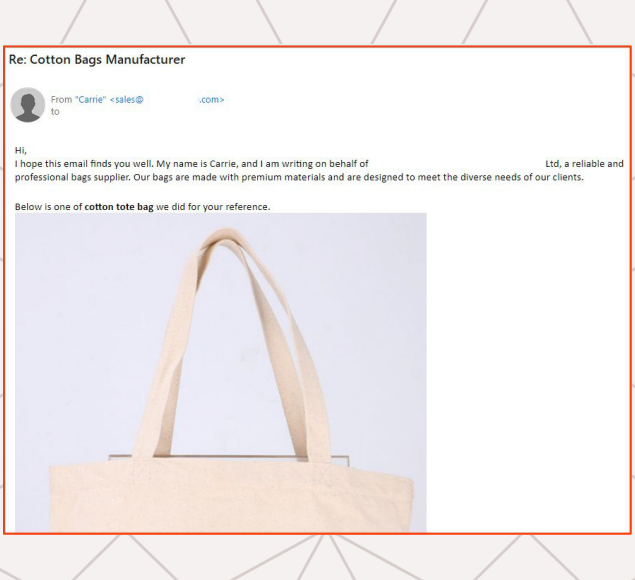
To demonstrate examples of the kinds of dubious emails our analysts received (all 1,407 of them), we ranked them by most popular to least popular and assigned them with the following categories: Personally Identifiable Information (PII) Stealers, Fraud, Malware, and Spam.

- Sales Spam (26%)
- Survey Scams (17.5%)
- "I hacked you" Scams (16.8%)
- "You've won free stuff" Scams (7%)
- Phone Scams (6.8%)
- "Generic" Scams (4.8%)
- Counterfeit Spam (4.1%)
- Junk Car Scams (3.7%)
- Fake Lawsuit Scams (3%)
- Elder Abuse Scams (2%)
- Other (8.3%)

1. SALES SPAM

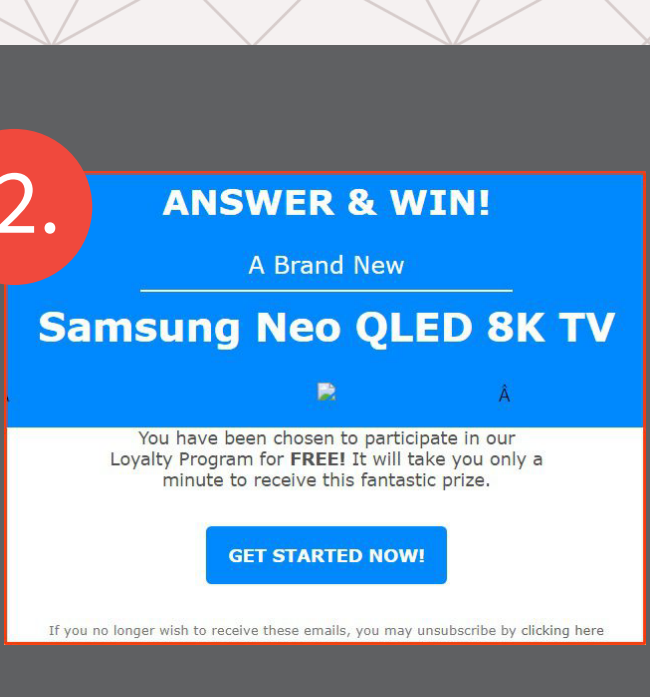
26%

Of the 1,407 emails, a whopping 365 of them were generic sales spam with no clear motive suggesting the reason for sending them was to commit fraud.



TYPE: SPAM

2. SURVEY SCAMS



TYPE: PII STEALER, FRAUD

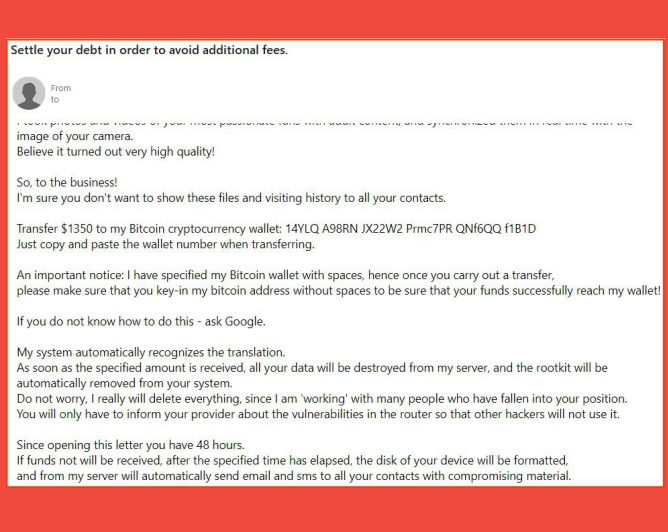
17.5%

Most of these emails invited the recipient to take a survey to win a gift card to popular stores like Walmart and Ace Hardware. This can be used to gather personal information from the target to execute more refined spearphishing in the future, or leveraged for account takeover.

3. "I HACKED YOU" SCAMS

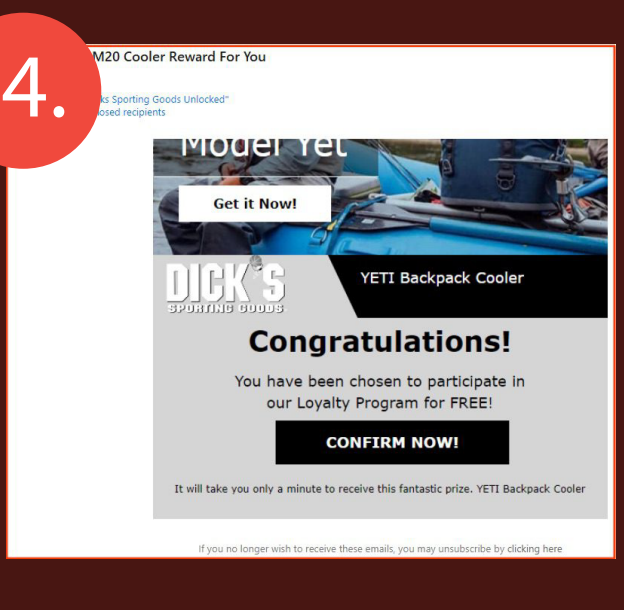
16.8%

"I hacked you" scams typically contained some sort of variation of threat such as "I caught you on webcam" – with the sender threatening to release "footage" or encrypt the recipients computer unless they pay a Bitcoin ransom. There were a significantly higher number of emails in this category than observed in previous years.



TYPE: FRAUD

4. "YOU'VE WON FREE STUFF" SCAMS



TYPE: MALWARE

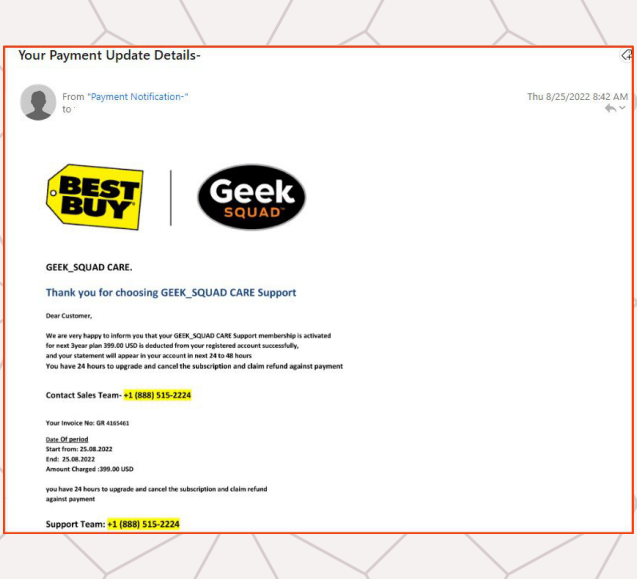
7%

97 of the emails claimed that the recipient had won some type of reward, including reward points, commercial goods, rebates, and so on. Once the target clicks the link or opens the attachment to claim their "free stuff", they end up installing ransomware instead.

5. PHONE SCAMS

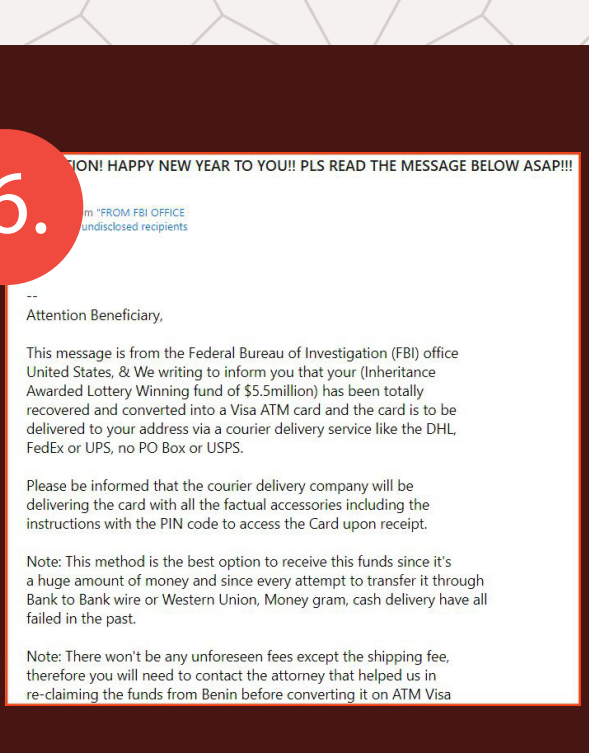
6.8%

Designed to get around endpoint security, fake invoice for software subscriptions with a real toll-free "customer assistance" number. Once the victim calls, the operator usually attempts to social engineer them into revealing PII, or trick them into installing ransomware. Overall, we saw a big uptick in these compared to previous years – with many leveraging big names such as Geek Squad, McAfee, and Norton.



TYPE: MALWARE, PII STEALER

6. "GENERIC" SCAMS



TYPE: PII STEALER, FRAUD

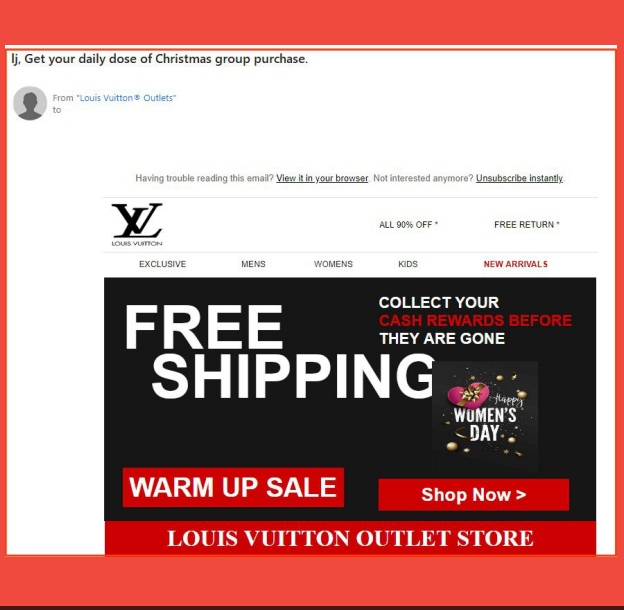
4.8%

A significant portion of the email data set fell into the category of "generic" – including 419 scams and "advanced fee" schemes. These are mainly weaponized to steal personal information and commit financial fraud or identity theft.

7. COUNTERFEIT SPAM

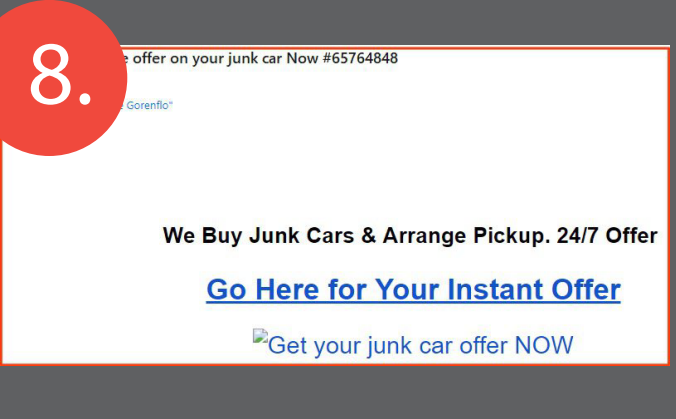
4.1%

These emails advertise below-market rates for high-end brands that are ultimately for counterfeit goods. Of the 58 sent to our analysts, most advertised for well-known luxury brands such as Louis Vuitton and Ray Ban.



TYPE: SPAM, FRAUD

8. JUNK CAR SCAMS



TYPE: FRAUD

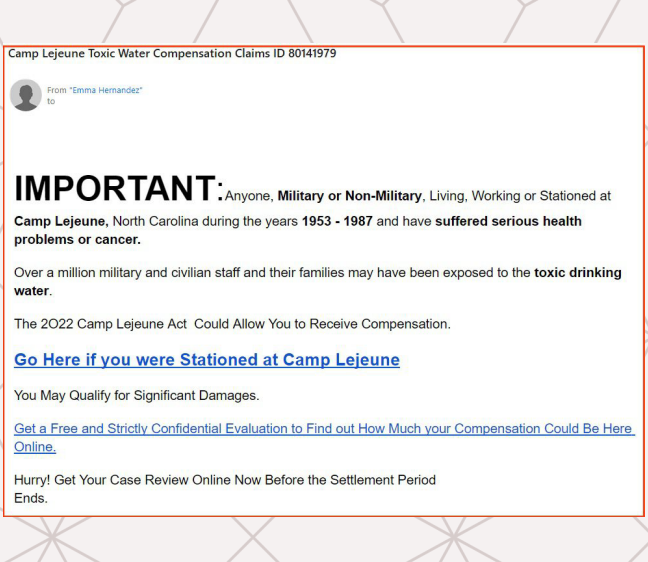
3.7%

"We'll buy your car" scams continue to be pretty consistent in popularity – though they may not be reported about as often as some of the other categories on this list.

9. FAKE LAWSUIT SCAMS

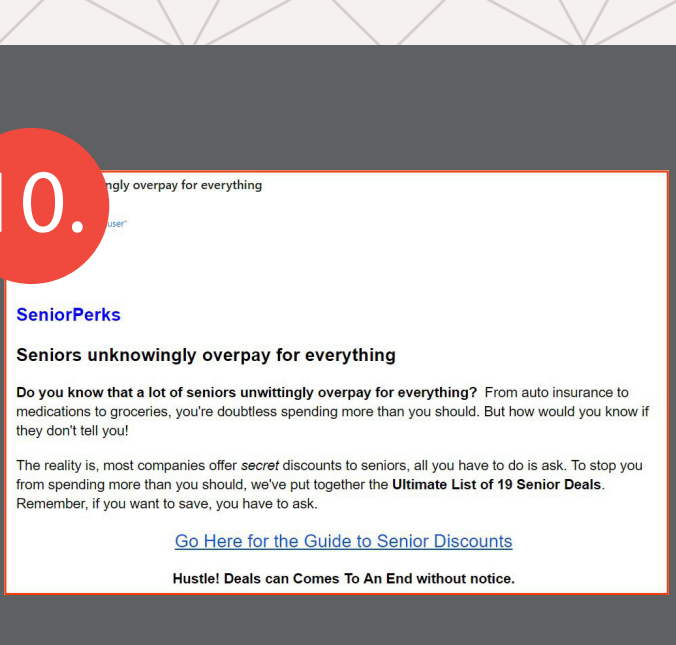
3%

"You could be eligible for compensation" - these types of infostealers usually falsely claim the victim could be eligible for compensation if they participate in a phony lawsuit.



TYPE: PII STEALER

10. ELDER ABUSE SCAMS



TYPE: PII STEALER, FRAUD

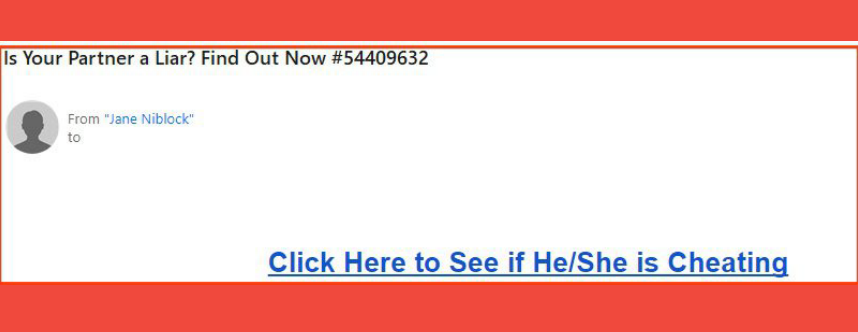
2%

Our analysts identified 28 emails that were directly targeting seniors. Most of these could be identified by keywords such as "senior", "55+", "timeshare", "retirement", and "over 60". This suggests that not only is this attack vector still as popular as ever, but that actors are being quite blatant in their marketing towards this demographic.

11. "CHEATING" SCAMS

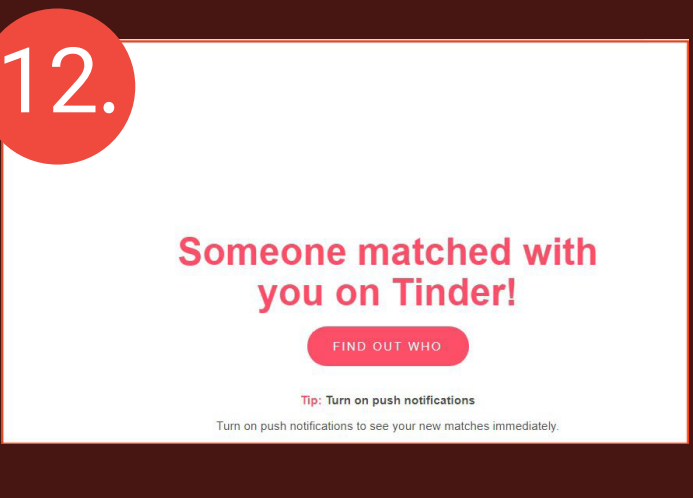
2%

Many of these emails touted a tool that claimed it could enable the recipient could see or verify the (likely) phony claim that their spouse or partner is cheating on them by installing spyware on their computer.



TYPE: MALWARE

12. FAKE NOTIFICATIONS SCAMS



TYPE: MALWARE

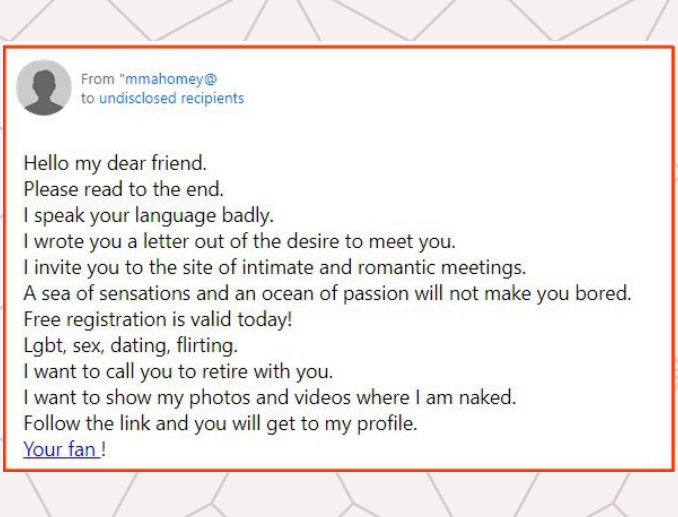
1.6%

The 23 emails that fell in this category included phony alert emails claiming that the recipient had unread notifications from popular services such as Tinder, Reddit, Whatsapp, and LinkedIn. Popular subject lines contained some variation of "12 unread messages" or "You've matched with someone", etc.

13. ROMANCE SCAMS

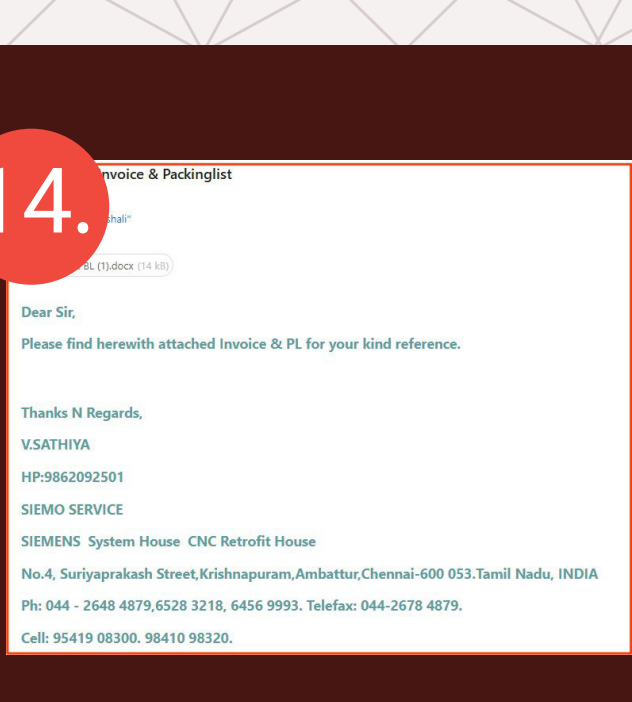
1.4%

Seeing as how romance scams have tripled in popularity in the past few years, our analyst expected to see more of this type of phishing scheme.



TYPE: FRAUD

14. FAKE INVOICE SCAMS



TYPE: FRAUD, MALWARE

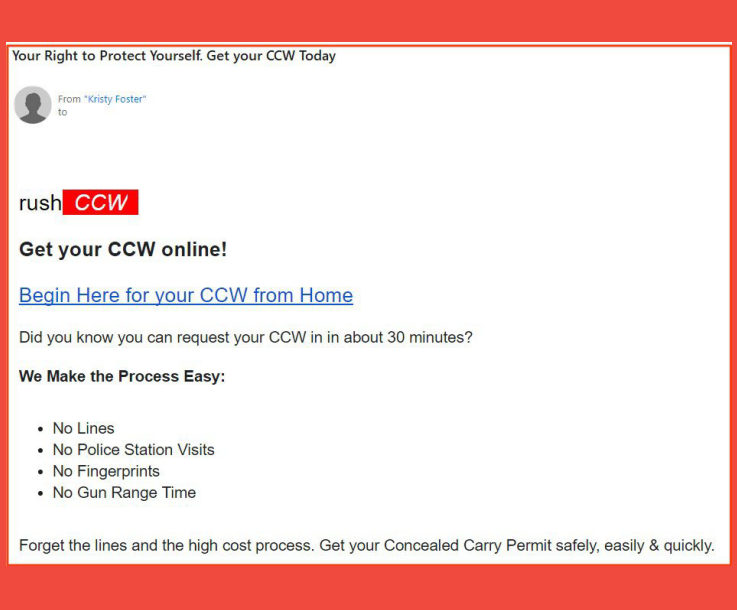
1.3%

These emails were consistent with the typical invoice scams that have been popular in past years. They are typically blasted out to businesses or email addresses that look like the might be accounts payable, office managers, or other administrative invoices and include a "real" invoice for nonexistent goods or services.

15. CCW/2A SPAM

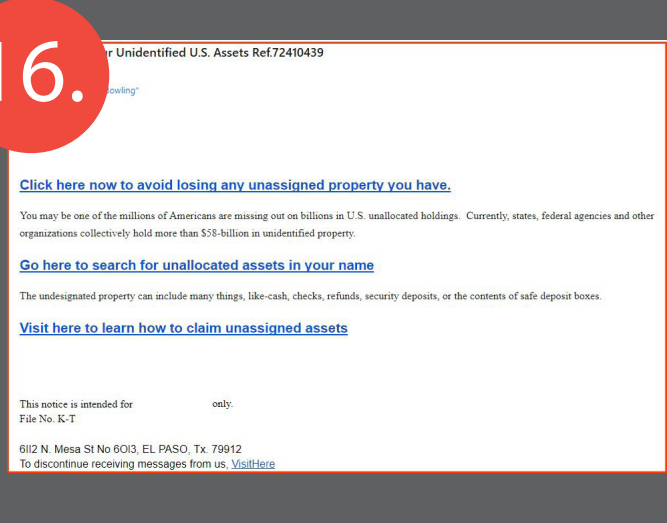
.7%

This type of scam is not one that our analysts have observed very often, if at all, before this analyses. These phishing emails mainly offered assistance in obtaining concealed carry permits. Most likely, this is a PII stealer scheme.



TYPE: PII STEALER

16. UNCLAIMED ASSETS SCAMS



TYPE: PII STEALER, FRAUD

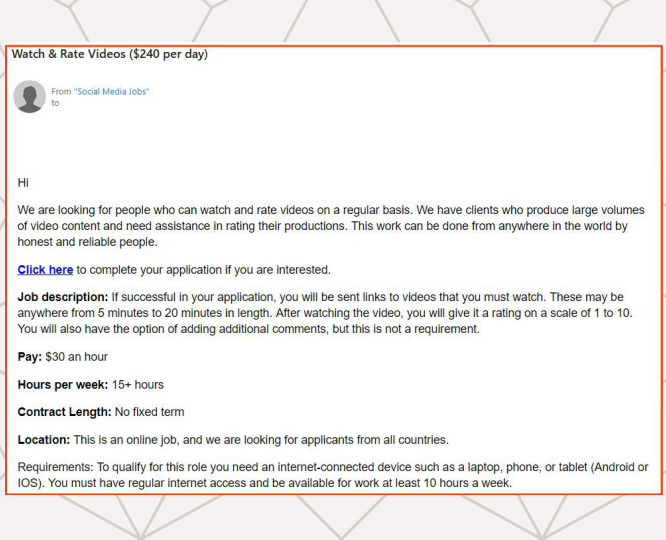
.5%

Many of the unclaimed asset scam emails claimed that the recipient was entitled to property from either inheritances, or from unallocated government holdings. In the example below the sender broadens the asset to "unidentified property" – making the chances that a target might think it could apply to them more likely.

17. SCAM JOB OFFERS

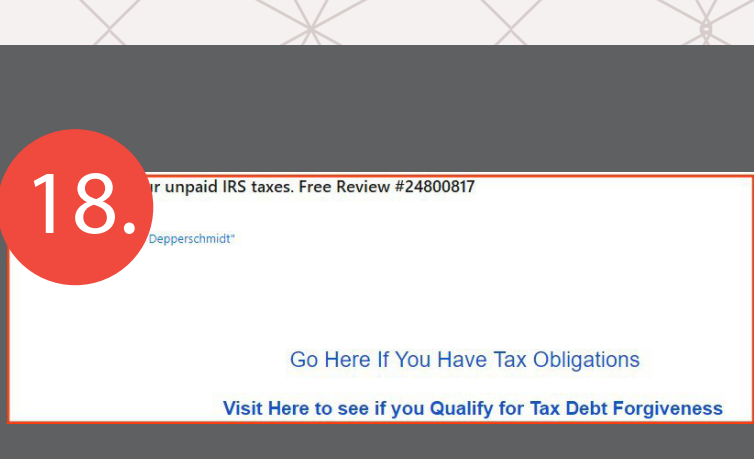
.3%

Only four emails consisted of fake job postings. Given the overall uptick in scams of this nature, this was fewer than our analysts expected.



TYPE: PII STEALER, FRAUD

18. IRS SCAMS

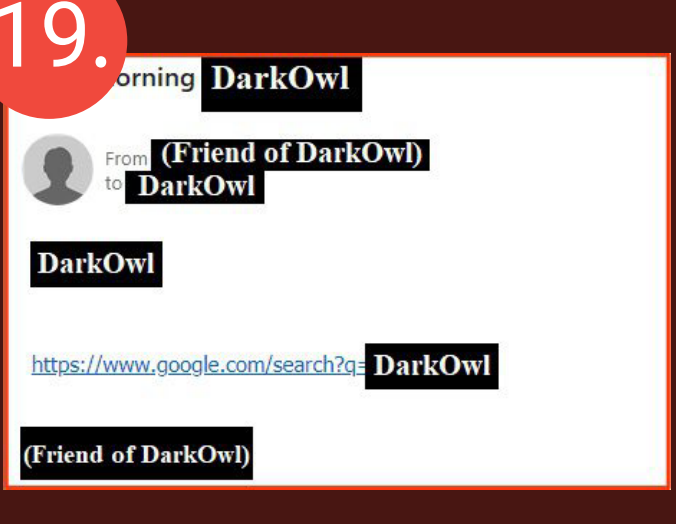


TYPE: PII STEALER, FRAUD

.2%

Given that this data set included two tax seasons, it was surprising to see how few IRS scams there were. Specifically, our analysts found the lack of specific "IRS" and "tax/taxes" keywords in emails' subject lines to be significant.

19. OTHER MALWARE



TYPE: MALWARE

.2%

These emails contained malicious links that were likely ransomware. Their phishing pretexts didn't fit into any of the other categories.

DarkOwl is the industry's leading provider of darknet data. We offer the world's largest commercially available database of information collected from the darknet. Using machine learning and human analysts, we automatically, continuously, and anonymously collect and index darknet, deep web, and high-risk surface net data. Our platform collects and stores data in near real-time, allowing darknet sites that frequently change location and availability to be queried in a safe and secure manner without having to access the darknet itself. Customers are able to turn this data into a powerful tool to identify risk at scale and drive better decision making.

DarkOwl is unique not only in the depth and breadth of its darknet data, but also in the relevance and searchability of its data, its investigation tools, and its passionate customer service. As importantly, DarkOwl data is ethically and safely collected from the darknet, allowing users secure and anonymous access to information and threats relevant to their mission. Our passion, our focus, and our expertise is the darknet.