

Security Brief: Threat Actors Pair Tax-Themed Lures With COVID-19, Healthcare Themes

 proofpoint.com/us/blog/security-briefs/threat-actors-pair-tax-themed-lures-covid-19-healthcare-themes

April 14, 2021





[Blog](#)

[Threat Insight](#)

Security Brief: Threat Actors Pair Tax-Themed Lures With COVID-19, Healthcare Themes



April 15, 2021 Selena Larson

On 30 March 2021, the United States Internal Revenue Service (IRS) issued a security alert detailing an ongoing email-based IRS impersonation campaign primarily targeting educational institutions. Impacted people included university and college students and staffers using “.edu” email addresses.

Educational institutions are not the only organizations that financially motivated threat actors have set their sights on using tax-themed lures. Proofpoint observed similar threats impacting dozens of verticals from manufacturing to healthcare to energy. But this year is a bit different. Threat actors take advantage of every tax season by mounting tax-themed campaigns that aim to steal money and sensitive information. What makes 2021 unique are the continuing and unprecedented pandemic, healthcare, and financial crises that these threat actors are combining with typical tax lures in the ongoing campaigns Proofpoint observed.

These findings demonstrate threat actors are agile and flexible and take current events into account in their campaign development to maximize their advantage and encourage victims to fall for their tactics.

Proofpoint observed over 30 tax-themed malicious email campaigns totaling over 800,000 email messages so far in 2021. These include attempts to compromise personal email accounts or steal sensitive personal data for likely financial gain. Proofpoint also observed multiple campaigns aligned with business email compromise activities. Such attacks can be used to facilitate payroll fraud, costing victim organizations millions of dollars.

Campaign Trends

So far in 2021, Proofpoint identified over 30 discrete campaigns targeting thousands of people from multiple threat actors that leveraged malicious email lures associated with taxes, tax and refund support, and government revenue entities. At least four threat actor groups tracked by Proofpoint have leveraged tax-themed malicious email campaigns.

Credential theft phishing attempts – which can be used to target individuals or leveraged for email account takeovers – accounted for 40% of the tax-themed email campaigns, followed by remote access trojan (RAT) campaigns at 17%. However, despite RATs featuring in fewer campaigns, they were far more popular in total message volume. Half of identified tax-themed and related messages containing malware were used to distribute the Remcos RAT, a commodity malware with extensive data theft and surveillance capabilities. Other broad tax-themed malware distribution campaigns included Dridex, TrickBot, and ZLoader.

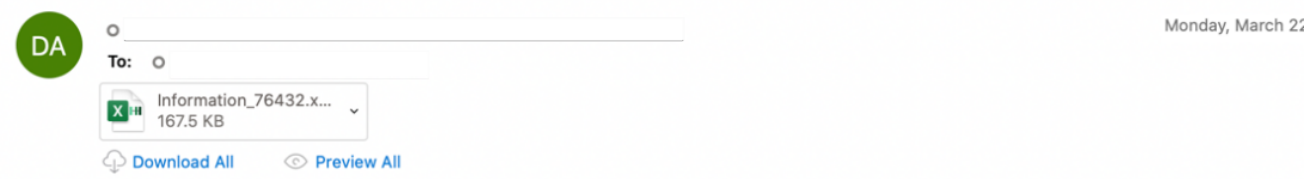
Over the course of 2020, threat actors began increasingly leveraging Excel 4.0 (XL4) macros to distribute malware, and this trend has continued in 2021. Proofpoint observed a 500% increase in tax-themed email threat campaigns delivering weaponized XL4 Macros in the first three months of 2021. Proofpoint assesses this is due to limited detection coverage in modern security systems. (Although Microsoft still supports XL4 macros, the company suggests migrating them to the latest version of Microsoft Visual Basic Application.)

Campaign Samples

TrickBot

One of the most prolific IRS-themed malware campaigns leveraged IRS tax credit distribution for employee retention lures benefiting employers impacted by COVID-19. This campaign identified in March 2021 contained over 18,000 messages to over 2,000 target entities. It distributed the TrickBot banking trojan. TrickBot is designed to steal banking information and acts as an initial payload for additional malware, gaining notoriety in 2018 for distributing Ryuk ransomware which reportedly accounted for a third of ransomware distributed by many actors across the threat landscape in 2020.

IRS Documentation Policies Modifications



Hello!

The Employee Retention Credit

This is a automatic message from Internal Revenue Services (IRS).

New taxation policies for all types of business as a result of the Covid-19 situation Form1859-2021
*kindly get in touch with the IRS for any issues, details in attached document. IRS

* Because of new security measures, document can be opened on the PC ONLY (any browser except Edge and IE).

Sincerely, Alan S. Houle Administrative Assistant Employee ID 3-81534 IRS Head Department

Figure 1: IRS Themed Lure offering an Employ Retention Credit

Unlike typically observed activity, this TrickBot campaign distributed malicious Excel files leveraging the XLSB filetype, a lightweight file format that can only be opened in Excel. Proofpoint assesses with moderate confidence the threat actor leveraged this document format as it is less likely to be detected by anti-virus systems. Researchers previously observed the multipurpose trojan QBot distributed via XLSB files in October 2020.

Dridex

The threat actor Proofpoint tracks as TA575 distributed emails purporting to be from IRS representatives associated with the American Rescue Plan. The emails contained links to download Microsoft Excel documents containing macros that, when enabled, downloaded the Dridex malware designed to steal banking and other personal information.

Also known as the COVID-19 Stimulus Package, the American Rescue Plan, was signed into law on 11 March 2021. The \$1.9 trillion economic stimulus package aimed to provide financial relief to people and businesses in the U.S.

IRS Rescue Plan Act




o IRS American Rescue Plan Dept <rescue_plan@federa1.gov.lrs>

To: c

n

Today at 5:



Greetings!

IN ACCORDING TO AMERICAN RESCUE PLAN ACT OF 2021*:

If you're United States Citizen
or have any legal status,
it is **possible to get aid** from the federal government of
your choice.

Quotes for AMERICAN RESCUE PLAN aid:

Aid	Qutoes
\$4000 Stimulus Check	2 678 988
Skip queue for vaccination	254 567
Increase Minimum Wage Federal Warranties	346 744
Free Meals	1 232 144

[Get apply form](#)

Approve your confirmation **using form** as soon as possible.

Figure 2: IRS Rescue Plan Lure

The TA575 campaign, which began in early March, included almost 16,000 messages and impacted over 1,800 organizations across dozens of verticals.

Consumer Credential Phishing

Tax-themed phishing attacks also occur globally, and one campaign Proofpoint identified posed as the United Kingdom's tax and customs authority, HM Revenue and Customs (HMRC). As part of the country's COVID-19 response, HMRC introduced multiple Self-Employment Income Support Schemes allowing people financially impacted by the pandemic to claim financial aid.

The malicious email campaign that began in mid-February 2021 distributed messages with links that led to a fake Self-Employment HMRC tax themed authentication page designed to harvest user credentials.

Your HMRC Fourth SEISS Tax Refund Notification



GOV.UK <support@access.service.gov.uk>
To

Reply Reply All Forward

Tue 2/16/2021 1:58 AM

If there are problems with how this message is displayed, click here to view it in a web browser.



GOV.UK

HMRC Fourth SEISS Tax Refund Notification

Claims for the Fourth SEISS grant have now opened for Application.

The date for submitting application for the Fourth SEISS grant start 9 February 2021.

Please "Sign in to HMRC online services" reference below and follow step 1 of 3 to have your tax refund credit to your bank account, also note you might need your Passport number details

Sign in to HMRC online services self assessment.

Note : For Security reason we will record (IP Address, Time and Date) Delibrate Wrong input or flooding with be criminally pursued.

Best regards,
HM Revenue & Customs

This is an automatic email - please don't reply.

Figure 3: Her Majesty's Revenue and Customs Tax Refund Notification Lure

TA574

Typical IRS-themed lures remain popular. The cybercrime actor TA574 sent almost 40,000 messages in one campaign using lures posing as the IRS and financial representatives. TA574 is an actor operating at a large scale that indiscriminately targets multiple industries and attempts to deliver and install malware like banking trojans. The IRS-themed emails contained malicious Microsoft Excel documents that requested victims enable macros to view content, thereby downloading and executing the ZLoader malware on a victim machine. ZLoader is a typical banking malware that steals credentials and other private information from users of targeted financial institutions.

INTERNAL REVENUE SERVICE needs your instant focus document case NO: GI3952024792

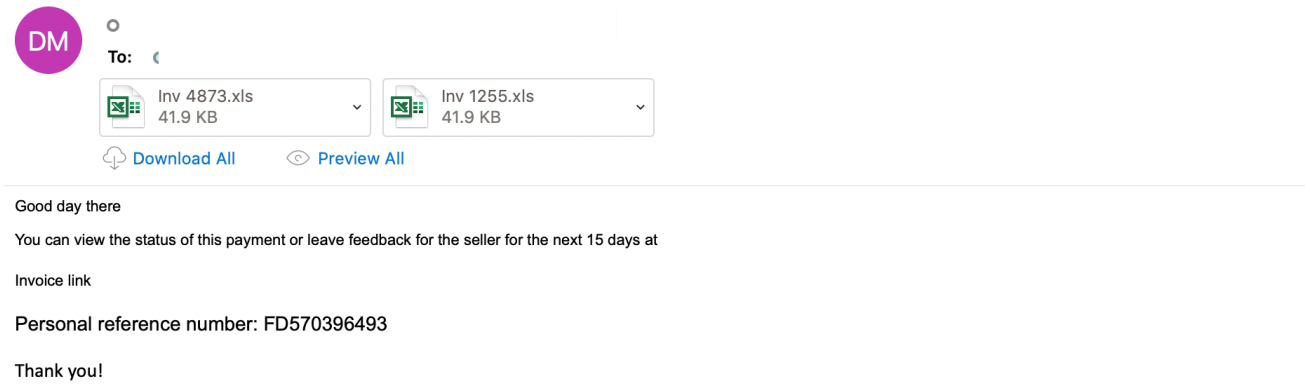
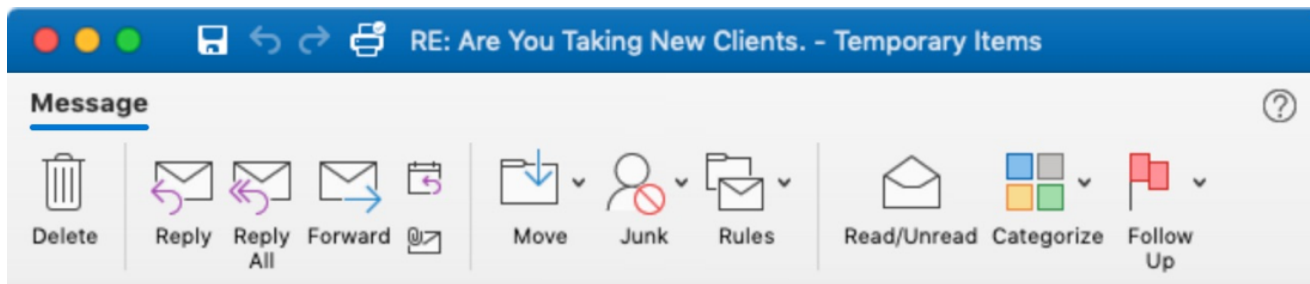


Figure 4: Internal Revenue Service Fake Case

New Client Tax Lures

One small campaign identified in March 2021 leverages subjects purporting to be requests from new clients or tax filing assistance. The emails begin with a benign request for tax preparation assistance from "John Stevens" and his wife. The emails target financial and accounting organizations in North America. If the recipient replies, they then receive a follow up email with a URL linking to a document that uses macros to drop a downloader that pulls in NetWire RAT. NetWire is typically used by criminal threat actors targeting a wide range of organizations including financial services, businesses, medical companies, and educational institutions.



RE: Are You Taking New Clients.



John Stevens <john.stevens@bitruc.com>

Yesterday at 2:52 PM

To: [Redacted]

From: John Stevens [<mailto:john.stevens@bitruc.com>]

Sent: Thursday, March 25, 2021 11:55 AM

To: [Redacted]

Subject: Are You Taking New Clients.

Hello

Please confirm if you are available at this time as i and my wife are in need of a Tax Preparer for our 2020 personal taxes.

Please give me a good time to ring you so that we can further discuss our previous tax situations and documents at hand.

My name is John Stevens and I look forward to having you help us with this.

Best Regards,

John Stevens

Figure 5: Phishing themes matching previous tax-themes campaigns distributing malware.

Proofpoint researchers observed similar campaigns since 2018. Proofpoint assesses with high confidence the same threat actor is responsible for these campaigns. This actor targets accounting, financial, and related industries typically around tax season.

Conclusion

Tax season is a popular time for threat actors to conduct email-based attack campaigns designed to steal sensitive information for financial gain. In 2021, threat actors are often combining current events such as COVID-19 or healthcare themes alongside typical tax lures to further entice victims.

To reduce the risk of successful exploitation, Proofpoint recommends the following:

Train users to spot and report malicious email. Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into real-world attack trends and the latest threat intelligence.

At the same time, assume that users will eventually click some threats. Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting employees before they reach the inbox. Invest in a solution that can manage the entire spectrum of email threats, not just malware-based threats. Some threats—including business email compromise (BEC) and other forms of email fraud—can be hard to detect with conventional security tools. Your solution should analyze both external and internal email—attackers may use compromised accounts to trick users within the same organization. Web isolation can be a critical safeguard for unknowns and risky URLs.

Manage access to sensitive data and insider threats. A cloud access security broker can help secure cloud accounts and help you grant the right levels of access to users and third-party add-on apps based on the risk factors that matter to you. Insider risk management platforms can help protect against insider threats, including users compromised by external attacks.

Partner with a threat intelligence vendor. Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques at scale to detect new attack tools, tactics, and targets—and then learns from them.

Subscribe to the Proofpoint Blog