

zix | *appriver*

Global Threat Report

Mid-Year 2021



Introduction

Threat actors are constantly adding to their repertoire by exploring new tactics and techniques to help bolster their efficacy against both technological blockers and humans. So far, this year has been no different as they have continued to add new methods to their toolchest.

Thus far in 2021, we have observed several new techniques in the realm of customization as well as obfuscation. We will cover several examples in this report. We will also examine several consistent attack trends that continue to plague organizations across the globe.

We are halfway through 2021 and one thing remains unchanged - email is still the number one attack vector for infecting organizations globally. Through the first half of 2021, phishing attacks continued their evolution with greater levels of sophistication. For the first time we observed attackers leveraging real web certificate data to add credibility to their attacks through customization. We also observed greater levels of obfuscation as some attacks threat actors went to great lengths to disguise the nature of their attacks. We observed phishing attacks leveraging CAPTCHA technology to avoid detection.

Threat actors also continued the cycle of abuse by leveraging legitimate services to hide their intent. Job seekers and hiring functions within organizations were also targeted with phishing emails designed to mimic legitimate job sites.

IC3 recently reported Business Email Compromise as the costliest of cybercrimes in 2020 with adjusted losses totaling \$1.8 billion. It is not surprising we observed a large and growing volume of BEC attacks throughout Q1('21) and Q2('21) which show no signs of abating.

In late January, the world learned of the coordinated law enforcement effort that had resulted in the takedown of the Emotet malware group in what is unfortunately all too rare of an event. Prior to the takedown, Emotet had been one of the most advanced, professional, and sustained malware services in operation. Emotet began operating as a banking trojan but over time had expended its scope to act as a loader for other distributors of other malware types to leverage thus Emotet became widely relied upon as MaaS (Malware-as-a-Service).

Many of the “Banking Trojans” we cover below were already following a similar trajectory though some appear to have further embraced the MaaS model given the demand left in the wake of the Emotet takedown.

We also look at some RAT (Remote Access Trojan) activity as RAT’s have been quite active throughout the first half of 2021.



Personalized Attacks – Site Certificate Data

We predicted in our [2020 Global Security Report](#) that we would see attackers further personalizing and customizing their attacks this year and the following attack was one of many that lived up to this prediction. This phishing attempt was posing as certificate errors for the recipient's website. What made it unique was it pulled their real certificate data and DNS (Domain Name System) A-record to tailor the phishing message to their domain. The payload URL also led to a credential harvesting site customized for their specific web platform admin page. While testing, we observed the generic WordPress admin login page and Shopify login pages (depending on the target).

EXAMPLE 1: CERTIFICATE ERRORS

Certificate Error on [example-domain.com](#)

Let's Encrypt <tlsreport@securemailer.net>
To: [example-domain.com](#) Thu 4/15/2021 9:02 AM

Let's Encrypt Error Prevention

Conflict in SSL/TLS Certificate Signature Algorithm

Your e-mail address is registered as the owner of [example-domain.com](#). This domain address is using a **R3** certificate, and our systems automatically detect any errors related to your certificates.

As a matter of quality and security, we intensively upgrade our error prevention and reporting services. Currently we're fully integrated to **Shopify Support Team**. You're able to resolve this issue by logging to your Shopify Panel.

example-domain.com Certificate Data
Let's Encrypt / R3
Issuance Date: 2/5/2021 1:10:54 AM / Expiry Date: 5/6/2021 1:10:54 AM
Serial Number: 04:E3:70:DC:26:51:F4:BB:7F:EB:6A:3B:F6:4E:82:6F:EB:E4
DNS A Record: ns1.uniregistry-dns.com

What can happen to [example-domain.com](#)?
Your website can show certificate errors to your customers and in critical cases suffer attacks such as POODLE-TLS.

We highly recommend you to fix the issue described in <https://error-prevention-sys.com/?u=example-domain.com>
Click or tap to follow link.

[Start the update process](#)

By clicking on the link you agree with Let's Encrypt Terms and Conditions.

If you're not the owner of [example-domain.com](#): please ignore this message.
All data you submit during update process is your responsibility.

Do not reply to this message. This is an automatic message.

Obfuscation – Morse Code Scripting

Attackers are always evolving with innovative methods attempting to avoid email security gateways via obfuscating code. One of the more unique methods we have run across this year so far utilizes Morse Code within an .html attachment that, when opened, appears as a blurred-out Excel file with a fake login screen containing the recipients company logo. It was designed to harvest user credentials and post them back to the attacker's infrastructure.

EXAMPLE 1: MORSE CODE FUNCTION

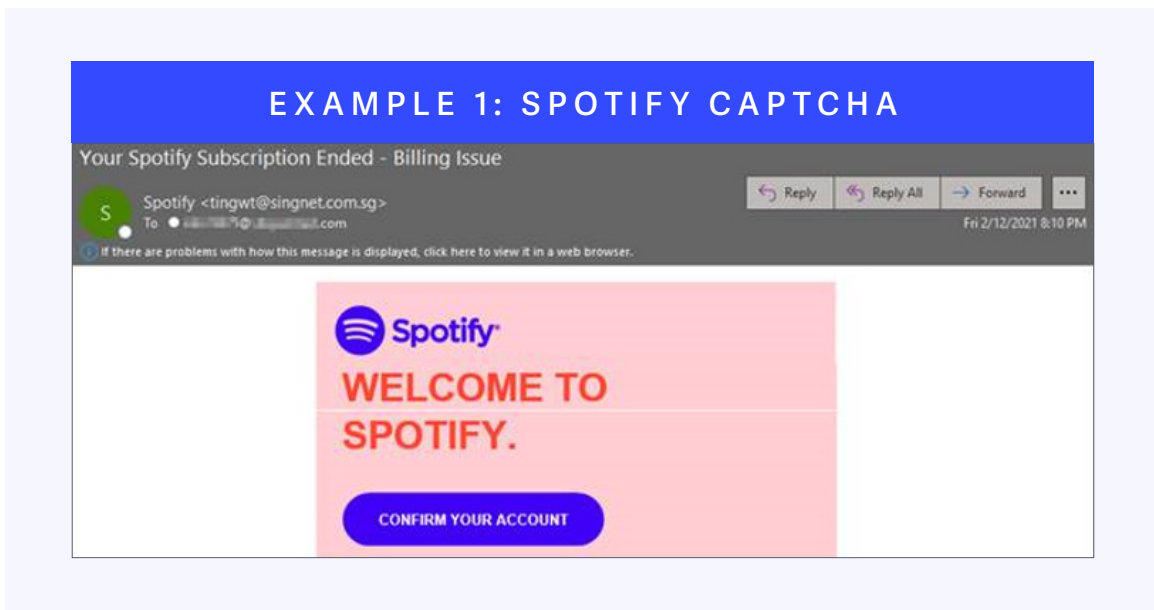
The screenshot shows an email interface with a subject line "Approved Message for [redacted] 2343k2" and a recipient "Receiverpayska | 8267 -k.iwasawa@ai-service.co.jp". An attachment named "Report-272222_xls.HTML" (9 KB) is highlighted with a red arrow pointing to the text "Morse Code Function". Below the email, a hex editor window displays the raw HTML code. The code defines a JavaScript function named `decodeMorse` that takes a Morse code string as input and returns the decoded text. The function uses a mapping of Morse code characters to their corresponding letters and digits. The decoded text is then concatenated into a single string and returned.

```
Offset(h) 29 2A 2B 2C 2D 2E 2F Decoded text
00000000 27 6D 65 73 73 61 67 <!doctype html>...<html>...<body>...<p id='messag
00000030 25 6D 6F 72 73 65 43 e'></p>...<script>...function decodeMorse(morseC
00000060 2C 27 2D 2E 2E 2E 27 ode) {... var ref = {... '-': 'a', '-...
00000090 3A 20 20 20 20 20 20 : 'b', '-.-': 'c', '-..': 'd', '-.-.-
000000C0 3A 20 20 20 27 68 27 : 'e', '-.-.-': 'f', '-.-.-': 'g', '-.-.-': 'h'
000000F0 6B 27 2C 27 2E 2D 2E : 'i', '-.-.-': 'j', '-.-.-': 'k', '-.-.-
00000120 2D 27 3A 20 20 20 20 : 'l', '-.-.-': 'm', '-.-.-': 'n', '-.-.-
00000150 20 27 72 27 2C 20 27 : 'o', '-.-.-': 'p', '-.-.-': 'q', '-.-.-': 'r'
00000180 2C 20 27 2E 2E 2E 2D : '-.-.-': 's', '-.-.-': 't', '-.-.-': 'u', '-.-.-
000001B0 2D 27 3A 20 20 20 27 : 'v', '-.-.-': 'w', '-.-.-': 'x', '-.-.-': 'y'
000001E0 20 20 27 32 27 2C 27 y', '-.-.-': 'z', '-.-.-': '1', '-.-.-': '2',
00000210 27 2D 2E 2E 2E 2E 27 : '-.-.-': '3', '-.-.-': '4', '-.-.-': '5', '-.-.-
00000240 27 3A 20 20 27 39 27 : '6', '-.-.-': '7', '-.-.-': '8', '-.-.-': '9'
00000270 64 65 0D 0A 20 20 20 : '-.-.-': '0',... }... return morseCode..
000002A0 20 20 20 20 20 20 20 : .split(' ')... .map(... a => a..
000002D0 3D 3E 20 72 65 66 5B : .split(' ')... .map(... b => ref[
00000300 0A 7D 0D 0A 0D 0A 76 b]... ).join('').... ).join(' ')?...v
00000330 2E 20 2E 2E 2E 2D 2D ar decoded = decodeMorse("...).join(' ')?...v
00000360 2E 20 2D 2D 2D 2D 2D : .....
00000390 2E 20 2D 2D 2D 2D 2E : .....
000003C0 2E 2E 2D 2D 2D 2D 2D : .....
000003F0 2E 2E 2E 2E 2D 20 2E : .....
00000420 2E 20 2D 2E 2E 2E 2E : .....
00000450 2D 20 2D 2E 2E 2F 2E : .....
```

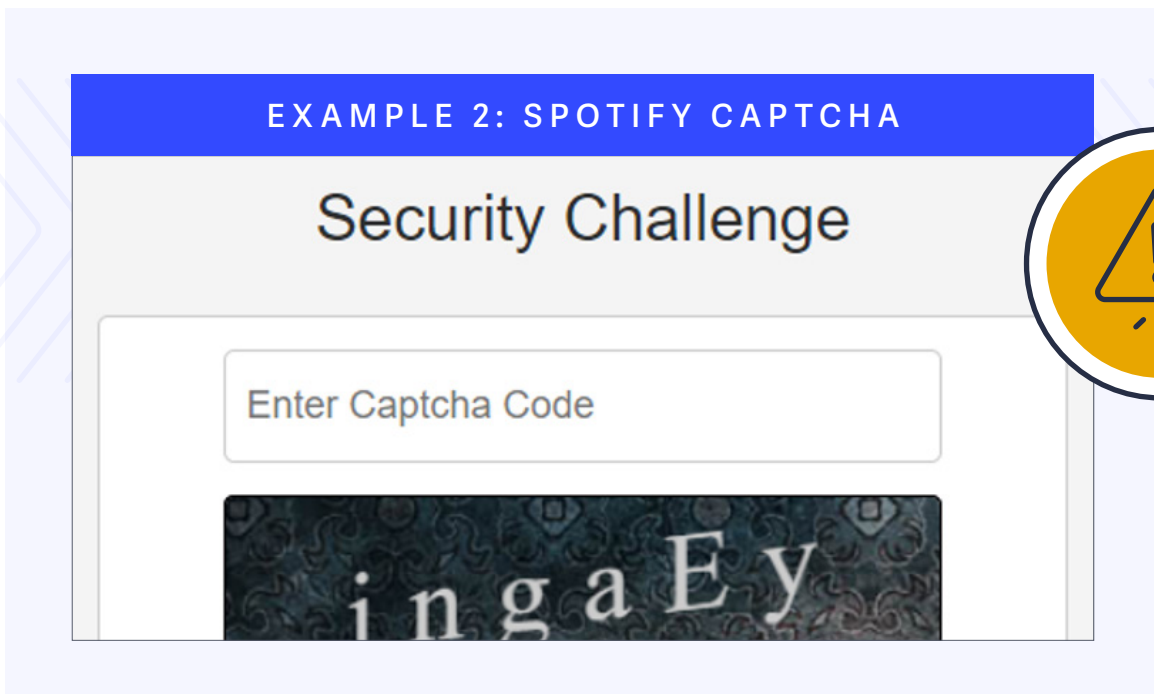


More Obfuscation- Captcha Phishing

Thus far in 2021, we are seeing more captcha technology incorporated into phishing attempts. In February we observed a Spotify phishing campaign using captchas. We anticipate seeing this used more often as the presence of the captcha helps attackers hide the content of their landing pages from web scanning services that might otherwise identify it as suspicious.




Clicking on the "CONFIRM YOUR ACCOUNT" link leads to this captcha security challenge which must be entered correctly to proceed.



Once the captcha is completed you are brought to a convincing Spotify branded credential harvesting page.

EXAMPLE 3: SPOTIFY CAPTCHA



To continue, log in to Spotify.

Remember me

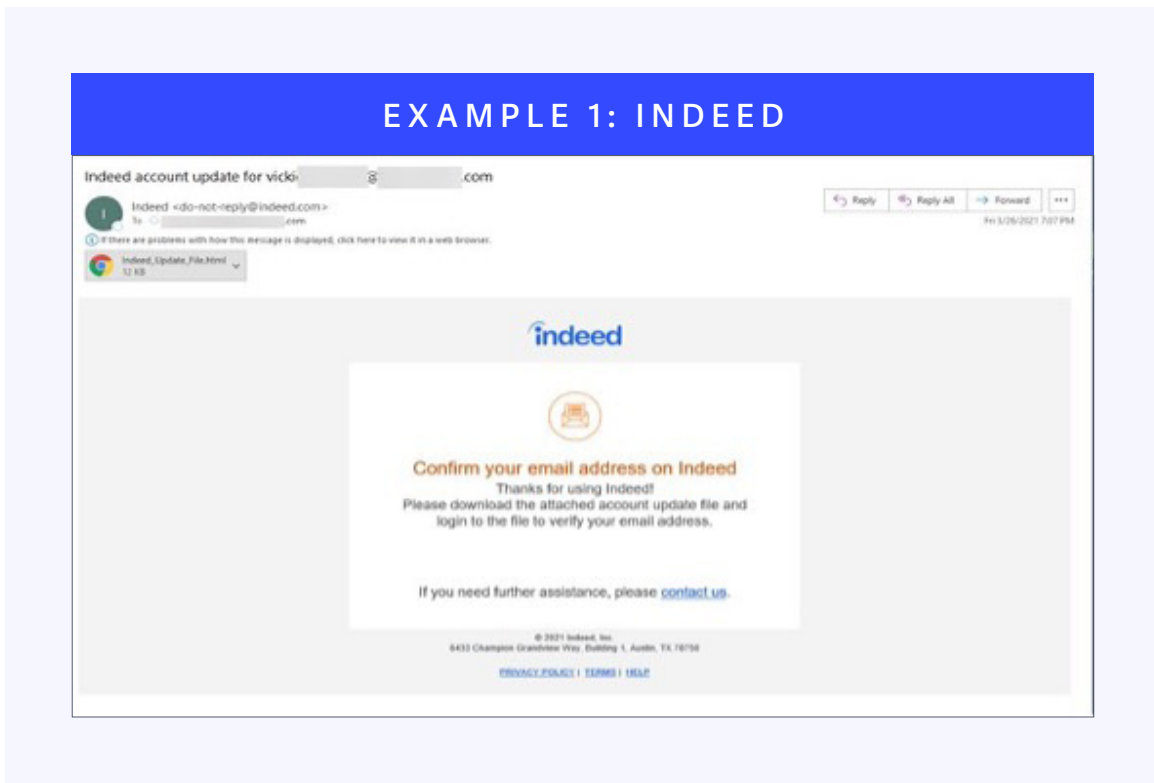
[Forgot your password?](#)

[Terms, Conditions and Privacy Policy.](#)



Targeting Workers/Hiring Organizations

In late March, as millions of workers were re-entering the workforce post pandemic, we observed phishing attacks targeting Indeed users. This poses a risk not only to job seekers but to employers as well, particularly HR functions. As you can see in the example below the attackers are utilizing an HTML attachment to deliver the phishing page used to gather personal credentials.



Living off the Land (LOtL) Phishing Attacks

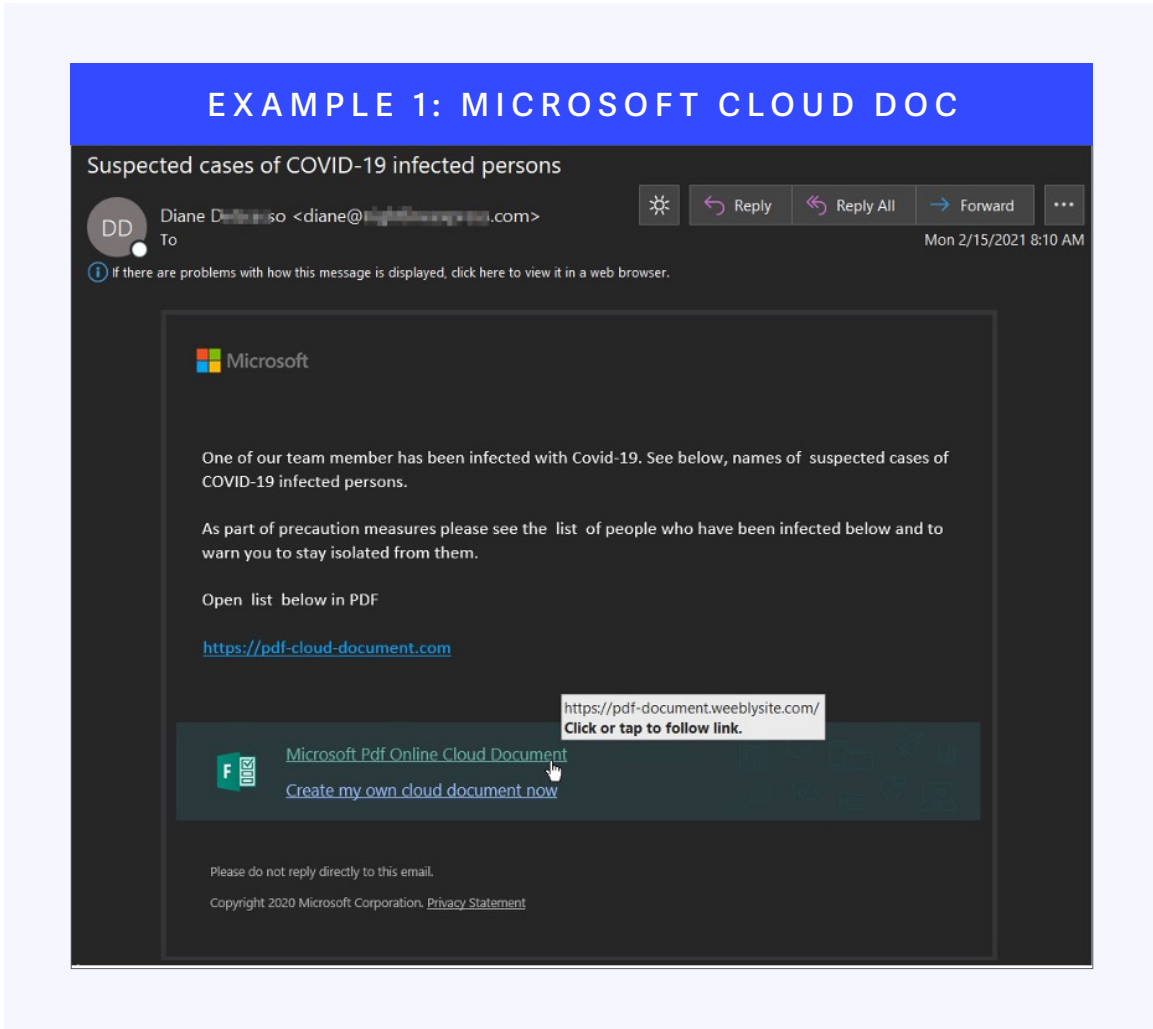
LOtL phishing attacks continue to proliferate as they offer threat actors the benefits of using legitimate services for illegitimate purposes. In addition, it is much easier to conduct attacks from the legitimate platform as little to no extra infrastructure is needed. We see some of the best attackers rotate through different platforms over time to keep defenders on our toes.

Top 20 services abused in LOtL Phishing attacks (by email volume).

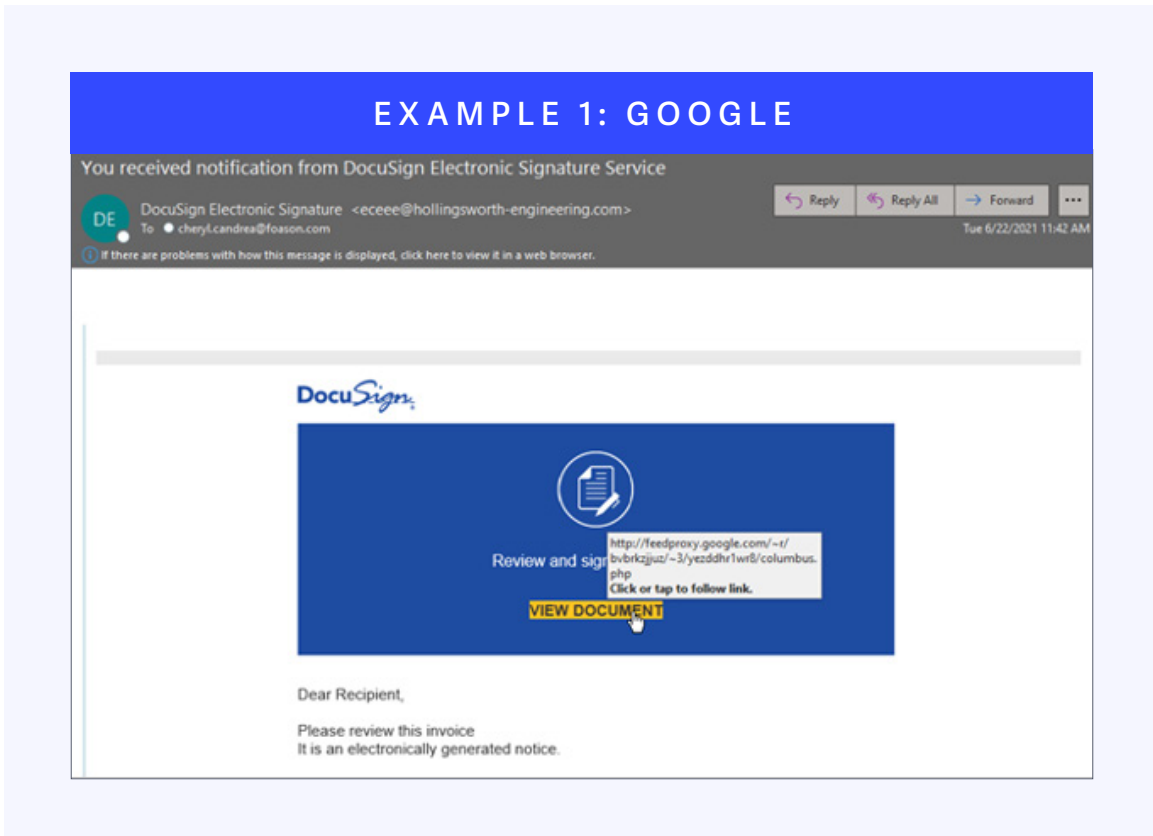
Google APIs	OracleCloud
GoogleDocs	AzureWebsites
AppSpot	WeTransfer
Amazon AWS	FireBaseApp
WebApp (Google)	MySharepoint
PageLink	ReBrandly
FeedProxy	BlogSpot
SendGrid	SurveyMonkey
WindowsNET	AzureEdge
ListManage	GoogleSites



A COVID-19 themed LOTL attack we captured stated that “a team member has been infected with Covid-19” and to see the below names of suspected cases and stay isolated from them. The message contained a payload link to a “Microsoft PDF Online Cloud Document.” The link led to an Adobe PDF Online Cloud Document themed phishing page. Weebly is an abused website and form builder that we have seen an uptick of LOTL attackers utilizing this year.



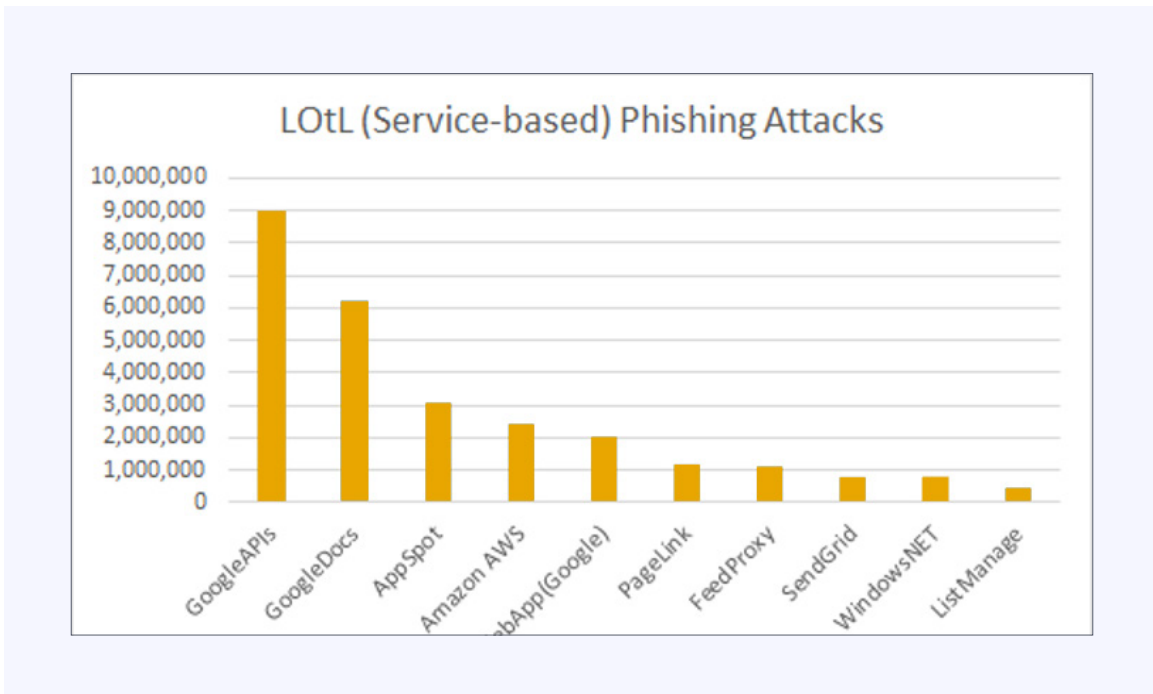
Attackers utilizing LOTL phishing tactics are always looking to add additional services to their toolkit for abuse. In June, we observed a major surge in abuse of Google's Feedproxy/ Feedburner service. Attackers have been observed repeatedly abusing Google's Sites, Docs, and APIs (Application programming interfaces) service with malicious links as they are always looking for legitimate services to help blend in and fly under the radar of security solutions. Though the Feedburner service has been around for quite a while, attackers discovered a method for abuse and began launching phishing attacks utilizing feedproxy.google.com links to host redirects to phishing pages.



LOtL by the numbers...

These attacks are becoming more frequent as senders attempt to remain below radar with perimeter defenses and to confuse their targets regarding the message's legitimacy. Through the first six months of 2021 we saw an 11% increase in phishing attacks relying on this technique. In total we recorded 29.7 million phishing emails utilizing this tactic, among the 43 services we are actively tracking.

Below is a look at the top ten by volume of email-based attacks:

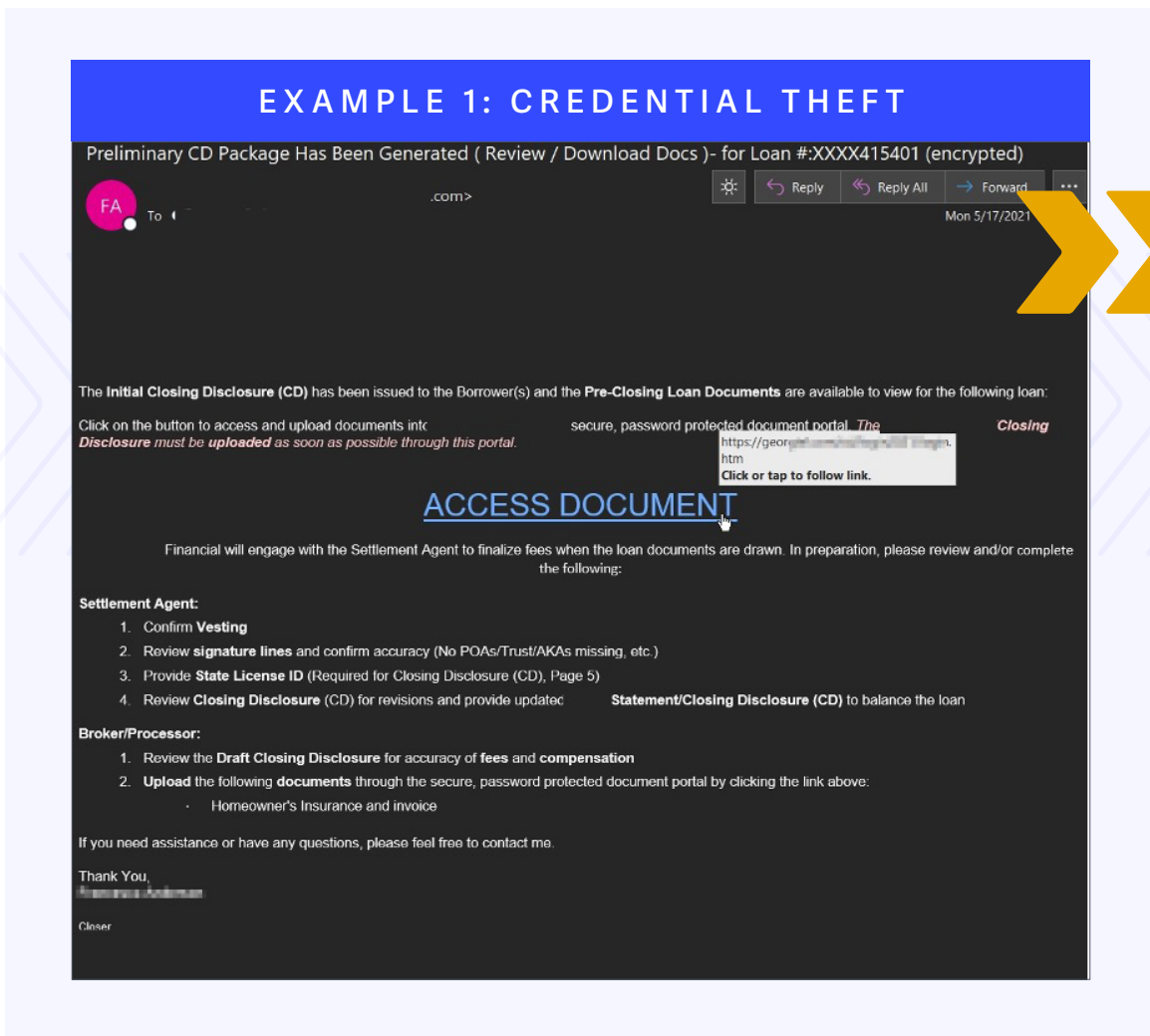


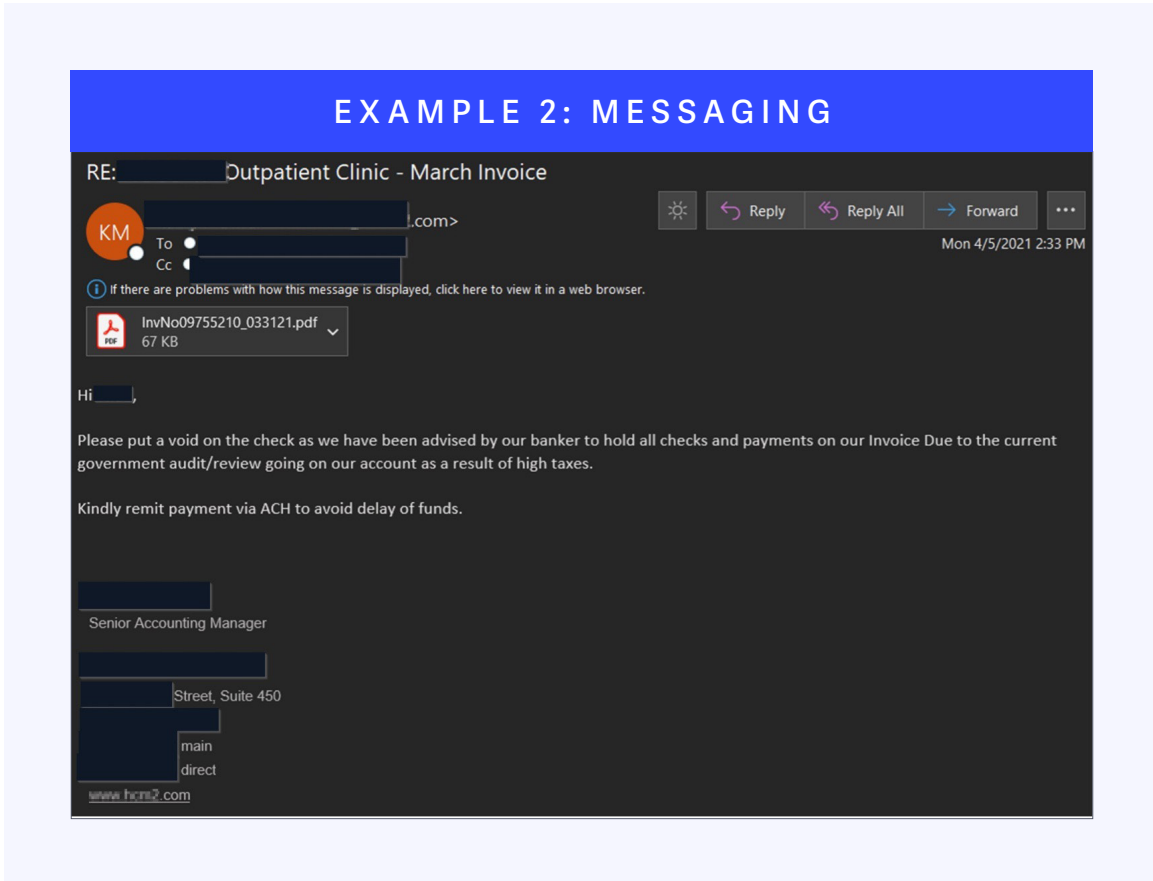
Business Email Compromise (BEC)

Business email compromise attacks continue to be a favorite avenue of threat actors as one of the most profitable cybercrime endeavors in 2021. The attacks require minimal time or money investment and can yield huge windfalls for the attacker. BEC attacks have also proven easier to get past layers of security solutions when compared to malware attacks. While also avoiding the complex infrastructure (i.e., command and control) and testing that goes along with malware operations. Attackers utilize a variety of different methods to achieve their goal, financial fraud. The most common version we see begins with spear phishing emails designed to grant the attacker access to an account.

Once inside an account, the attacker will monitor legitimate conversations and look for an opportunity to insert themselves at just the right time. They will do this to redirect financial transfers and payments into their own account. If they are unable to do this in the account that they have compromised, they will pivot to another account by sending more phishing messages to the contact list of the account they are in currently. Using this method, the attacker can gain access to someone else's account that does handle monetary transfers.

BEC Credential Theft Message Example (Redacted)





Banking Trojan – Trickbot

Trickbot helped fill in the banking trojan void left behind early this year after the Emotet botnet take-down. Campaign themes have varied per Trickbot affiliates and range anywhere from fake traffic violations to purchase order ruses. Follow-up payloads observed from Trickbot infections include crypto-mining software but are often more severe with ransomware deployments throughout the victim's network using Ryuk or Conti. The largest Trickbot campaign we have attributed to this trojan so far this year comprised of ~11,300 messages targeting customers using a generic Purchase Order theme.

EXAMPLE 1: PURCHASE ORDER

Re:New PO#87534

Howard [redacted] <info@[redacted].gr>
To: k@[redacted].com

Reply Reply All Forward

Wed 3/31/2021 3:40 PM

P O#87534.7z
10 KB

Good day,


Please find attached our new PO and kindly confirm back if everything looks good on the PO.

Also, please advise on ETA for the shipment.

Thank you.

Best regards,

Howard [redacted]
採購及資源部-採購員
PNR – Purchaser
Purchasing and Resources
[redacted] Group Ltd.



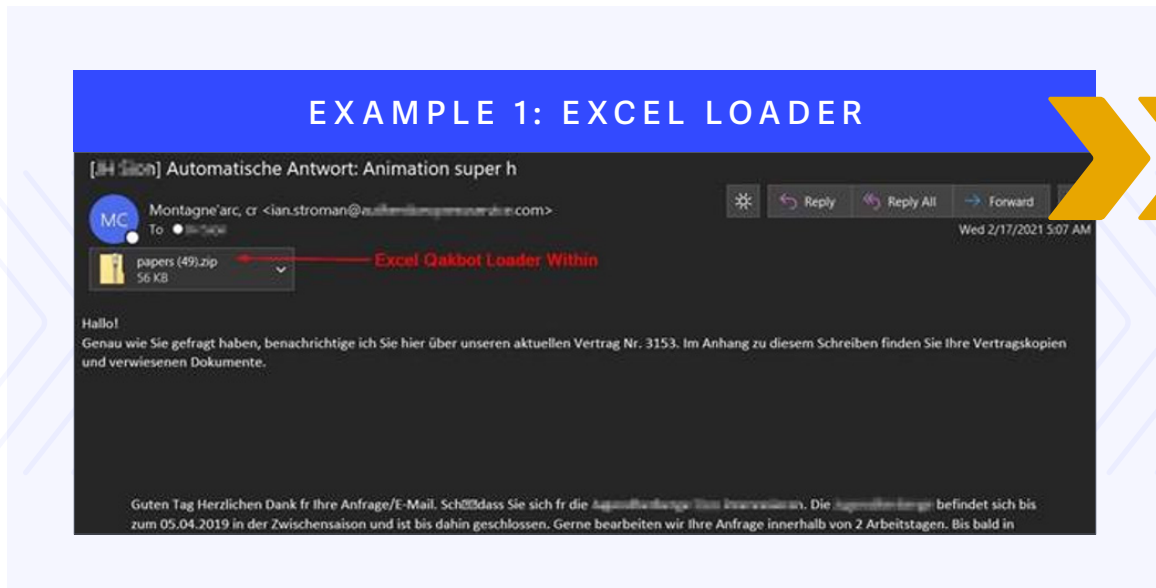
Banking Trojan – Dridex

Dridex has been the leading malware threat by email volume with directly attached malware this year. We have captured over 4.8 million Dridex laden messages in the first two quarters with most originating out of the Cutwail Botnet. Dridex campaigns have varied but most use an Excel attachment as the dropper to deliver the Dridex banking trojan. Outstanding invoices or purchase receipts are popular message lures that are utilized with some of the more recent examples spoofing NetSuite, QuickBooks, and Office Depot.

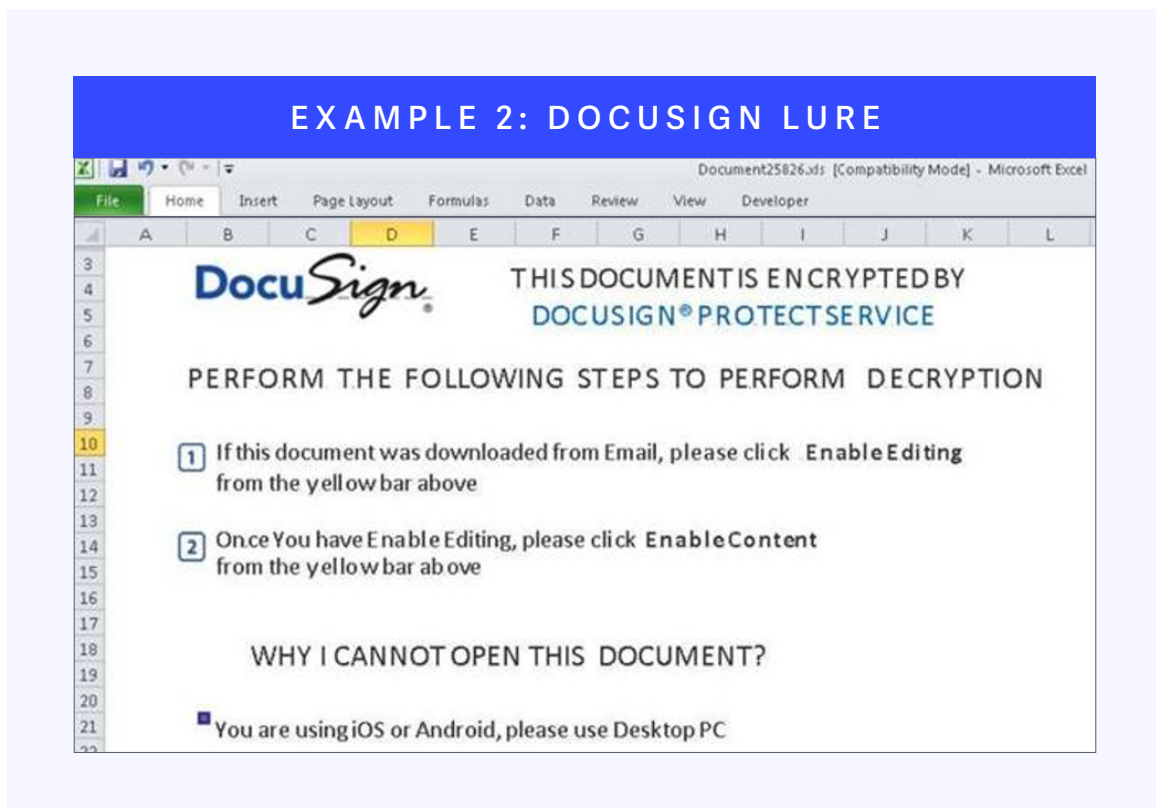


Banking Trojan – Qakbot

Qakbot is another banking trojan that appears to be attempting to fill in the void resulting from the Emotet botnet takedown. Thus far in 2021, we have captured email lure variants in many languages and themes attempting to distribute this threat. A German-based example is pictured below that contains a Qakbot Excel loader within the attached zip file.

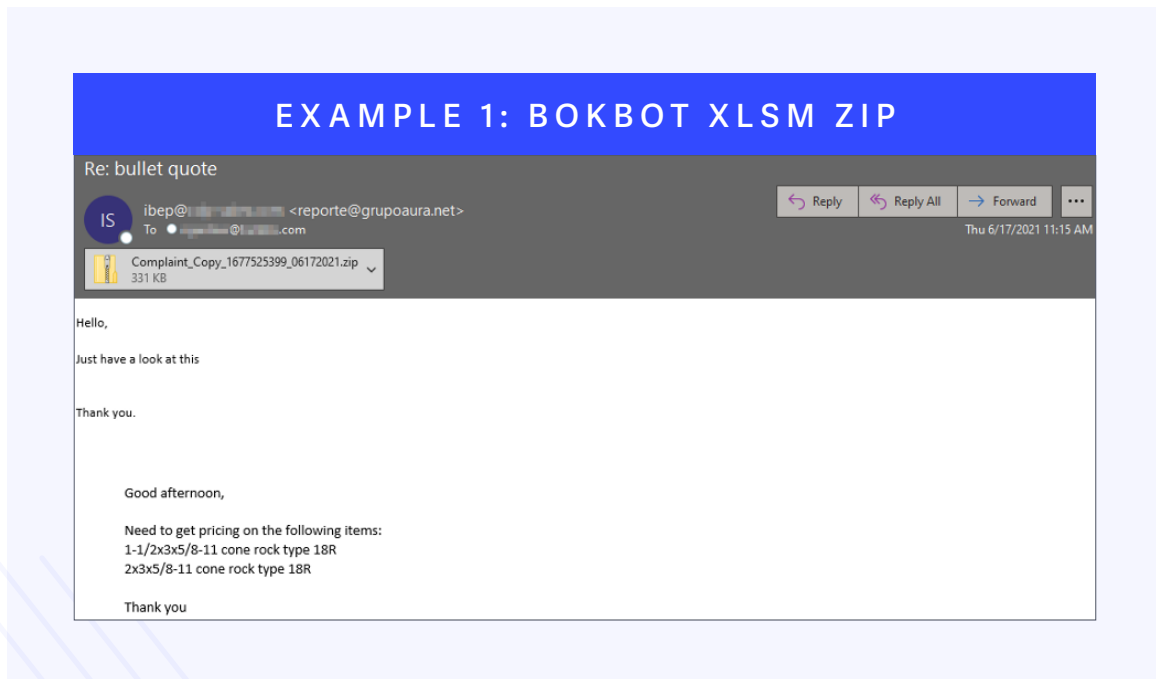


Once the recipient extracts the Excel attachment and runs it, they will see a DocuSign lure that urges the user to Enable Editing and Content to circumvent MS default disabled macros and the protected view, which will launch the infection chain.



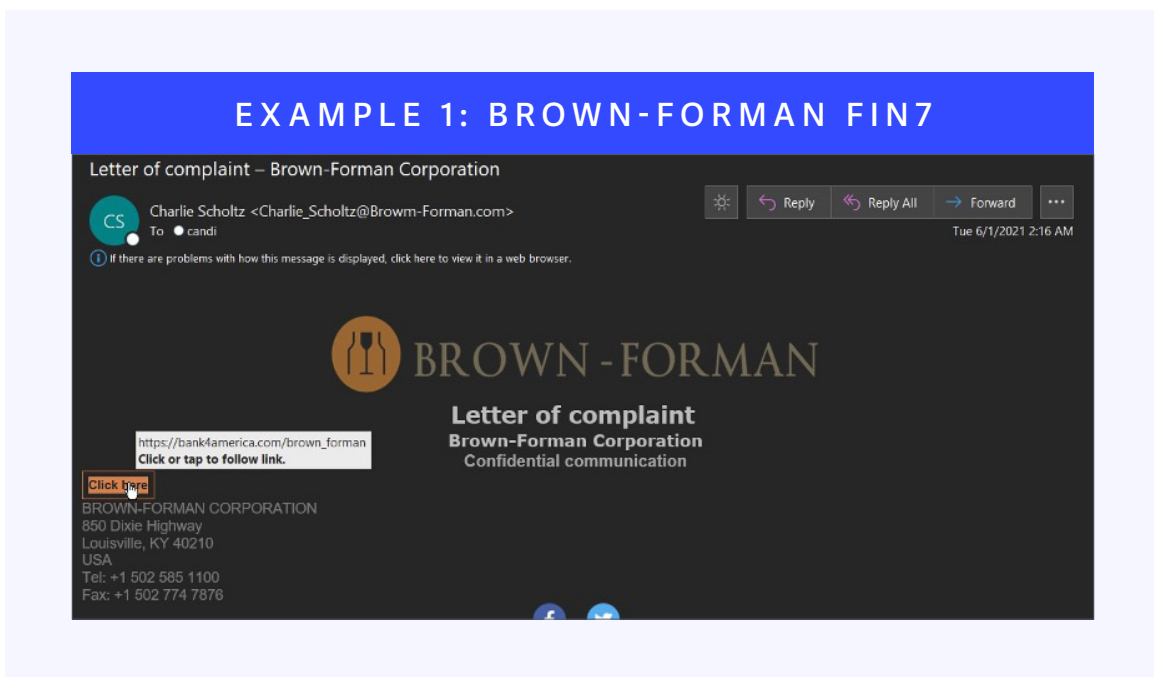
Banking Trojan – IcedID (BokBot)

IcedID continued its evolution from its primary use as a Banking Trojan to a dropper for other malware and that evolution has been accelerated in the wake of the Emotet takedown. IcedID is a modular malware which historically targets user financial information and credentials but is increasingly being used as a dropper for other malware. In this campaign the bad actors used a ZIP file containing an XLSM (macro-enabled excel) file and macros to deliver the malware payload as XLS files have been its primary method for delivery.



APT (Advanced Persistent Threat) Spotlight - FIN7 / JSSLoader RAT

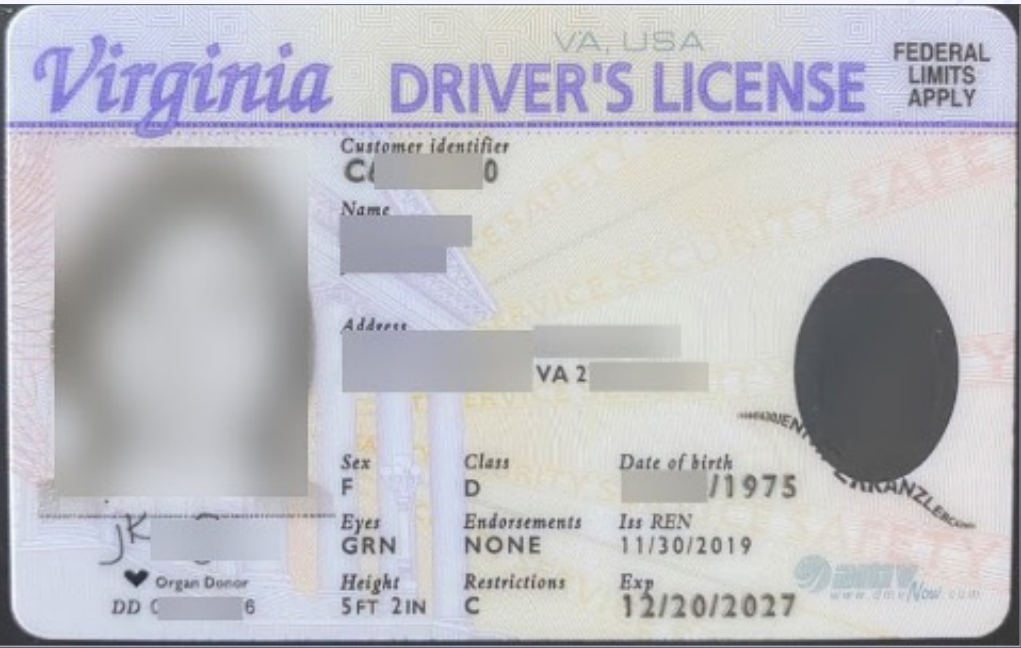
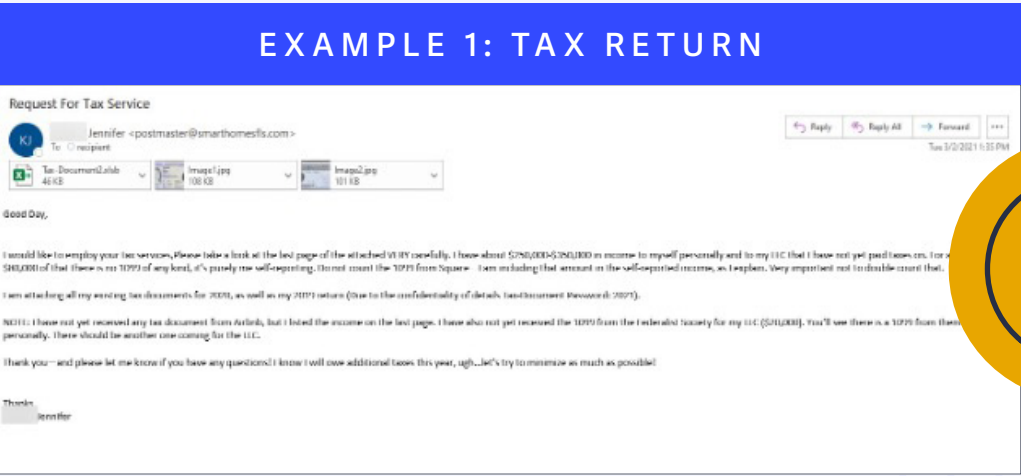
FIN7 is one of the leading financially motivated APT actors who have been reported to be a [billion dollar hacking group](#) by Wired with a [long history](#) of high-profile attacks. A recent campaign attributed to the group was messages masquerading as a Brown-Forman Corporation Letter of Complaint. The message enticed the recipient to click a link to retrieve the “confidential communication.” If the user proceeds, they were redirected from the original payload link to a site that was typo-squatting Brown-Forman (Browm-Forman[.]com). This site contained a page with a “show complaint” button linked to a .xlsb file (Excel with binary workbook) which dropped the FIN7 [JSSLoader remote access trojan](#).



Remcos RAT -Tax Scam

This week we also saw malware distributors getting in on the tax theme. Below is a very intriguing tax return malware campaign delivering the Remcos RAT. These actors exclusively targeted CPA offices and like a campaign we observed around the same time last year. Attached to the email are front and back images of a driver's license which correspond with the senders' display name and email signature. The password protected XLSB (Excel Binary File) unleashes the Remcos RAT after the password is used to open the file and the malicious macros embedded within are run.

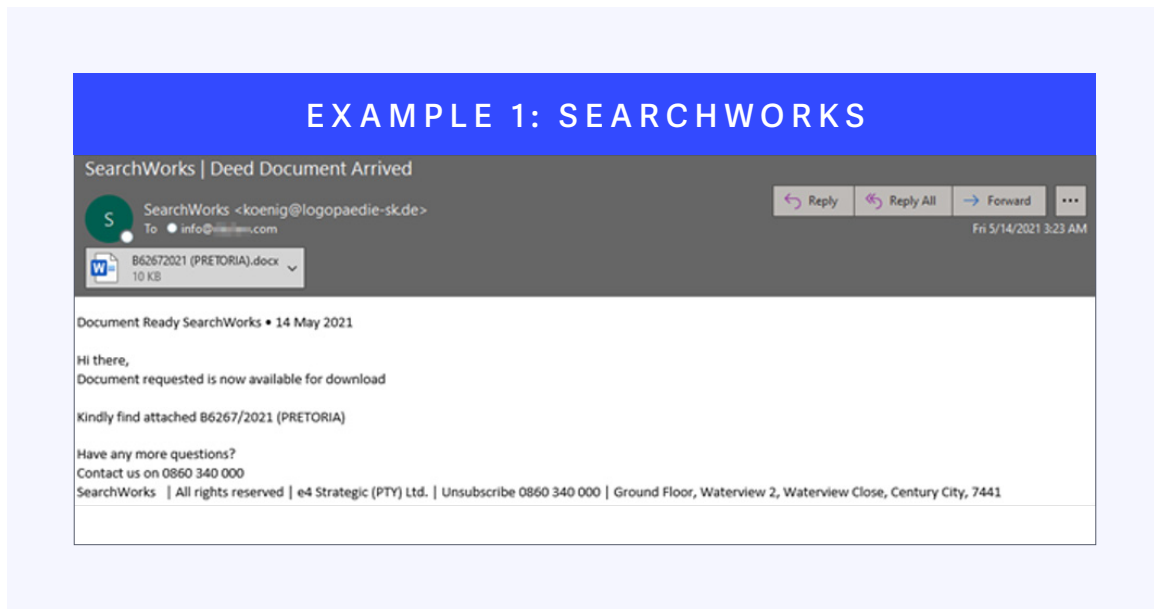
Upon investigation, it appears some if not all the DL data is accurate, and this is indeed a real person whose information was compromised. The images are high resolution, but we were not able to come to a determination one way or another on the legitimacy of the driver's license.



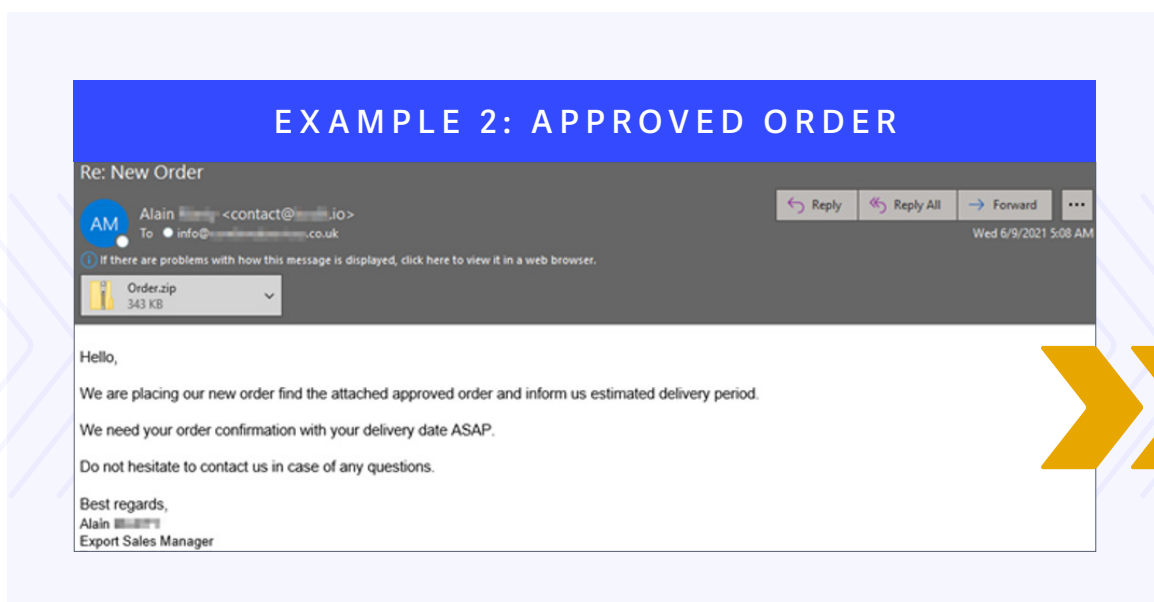
RAT – Formbook

The info-stealing Formbook malware actors continue to proliferate this year. They remain relevant because Formbook is sold as “malware as a service” (MaaS) since 2016 and is easily accessible. The threats offered via malware as a service model are particularly concerning since they offer thorough support, tiered packages, and allow the average person with little to no technical expertise the capability to cause significant harm.

In this campaign the executive recruiting company Search Works is being spoofed and Formbook is delivered via macros embedded inside the DOCX file which is disguised as a deed document.



Another Formbook campaign originated from an exploited mailbox peddling a malicious “approved order” ZIP file. The ZIP contains an executable file which initiates the infection process.



Snake Keylogger (404 Keylogger)

The Snake info-stealer has been on the scene since around 2012 and has a few dangerous capabilities to include stealing the victim's sensitive information by logging keystrokes, taking screenshots, and extracting information from the clipboard. Earlier this year we observed a "Payment Instruction" malware campaign using an executable file to deliver this keylogger.



EXAMPLE 1: PAYMENT INSTRUCTION

RE: PAYMENT INSTRUCTIONS

Administration <administracion@...co.uk>
To: sales@...co.uk

Reply Reply All Forward ...

Wed 3/17/2021 10:22 AM

Outlook blocked access to the following potentially unsafe attachments: PAYMENT_INSTRUCTIONS_COPY.exe.

Dear Sir,

Pls Find Attached and confirm payment instruction copy.

We have wired the payment to your account twice and it returned to us.

Please confirm from the attached instruction if there are missing figures in account details and make corrections were necessary so

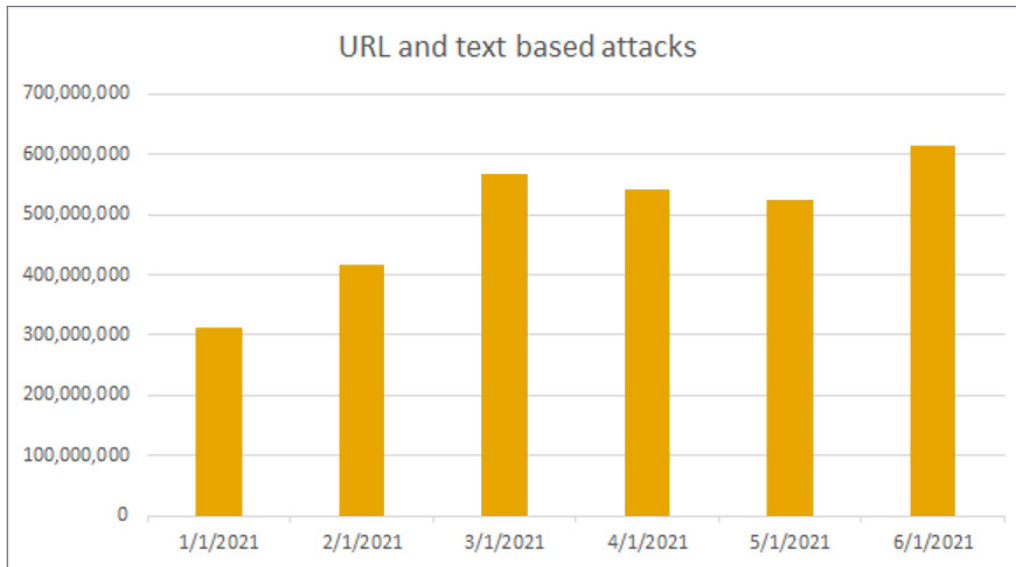
Below you can see that these malicious actors packed what we suspect is Google chrome's offline dinosaur game into this executable file. There are references in the executable file to "TRexUI," "RunGameLogic," and "JumpPressed" which leads us to this assumption. This is a common tactic to pack legitimate programs like games into malicious executables trying to evade detection.

EXAMPLE 2: LEGITIMATE PROGRAM PACKING

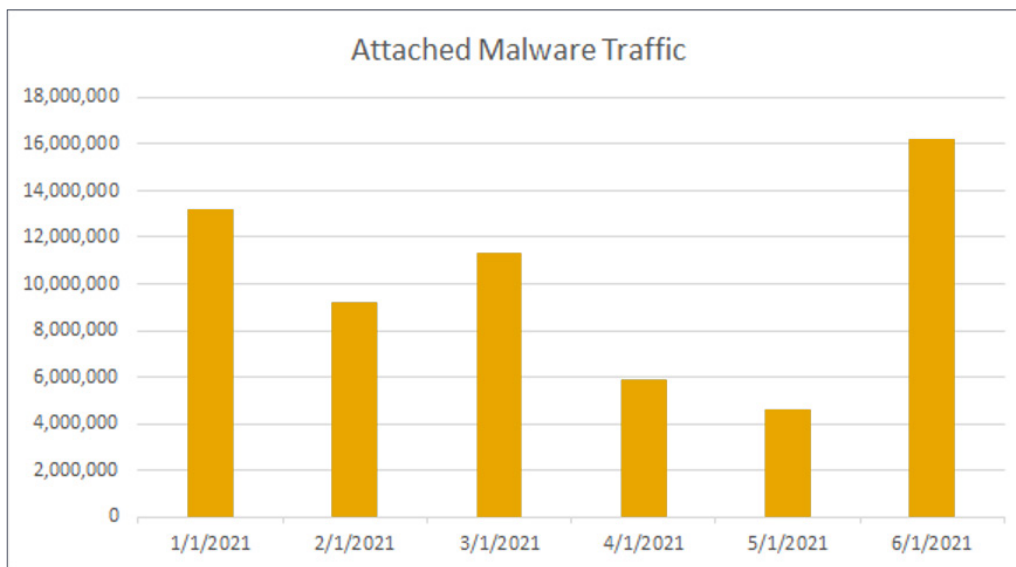
```
ateListOfTrackedObjects>b_4_0 <>c__DisplayClass4_0 <>c__Di
splayClass4_1 <UpdateListOfTrackedObjects>b_1 IEnumerable`
l Predicate`1 Stack`1 Comparison`1 List`1 obj1 CS?<>8__loca
ls1 v1 Int32 obj2 Vector2 v2 <>9 <Module> B CreateCompatibl
eDC ReleaseDC DeleteDC GetWindowDC TRexAI VK_ARROW_DOWN Sys
tem.IO KEYEVENTF_KEYUP VK_ARROW_UP CAPTUREBLT positionX KEY
EVENTF_EXTENDEDKEY SRCCOPY positionY value_ screenshotArea
mscorlib <>c hDc hdc PerSec RunGameLogic System.Collectio
n.Generic nXSrc nYSrc hdcSrc currentId Thread Load Add spee
d dinosaurGroundedButNotCrouched speedFramesTracked CrouchP
ressed JumpPressed id yJumpingThreshold hWnd Find isTouchin
gGround CreateInstance keyCode set_Mode CipherMode get_BigE
ndianUnicode rawBGRAImage DetectObjectsInImage rawImage ima
ge BGRAImageToGrayscale IDisposable CheckAndMarkObstacle Is
PointObstacle Idle RuntimeTypeHandle GetTypeFromHandle Rect
angle Console WriteLine Adope ValueType ObjectType objectTy
pe System.Core get_Culture set_Culture resourceCulture GetG
rayscaleScreenCapture ScreenShotCapture Dispose RunUpdate c
```


Trend Data

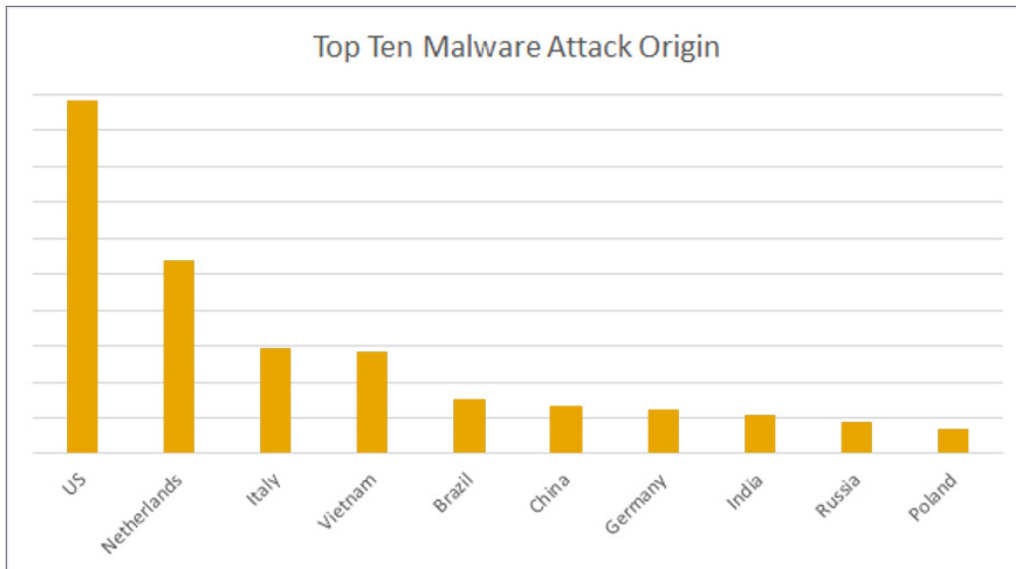
Overall email threats were on an upward trend throughout the first half of 2021. We quarantined over 2.9 billion email threats throughout the first half of 2021, which was a 13.5% increase over the trailing 6-month period.



Email with malware as an attachment trended down throughout the first five months of 2021 before rebounding in June. In all, we quarantined over 60 million messages with a malicious attachment through the first half of the year.



The US was the most common point of origin for emails with malicious attachments. Below are the top ten origination points for attached malware thus far in 2021.



Below is a list of the most common malware attachment file type as observed by our filters through the first half of 2021. Many of the archive formats listed below would include another file type.

