HOW HACKERS ARE LEVERAGING GOOGLE TOOLS FOR BEC ATTACKS

Business Email Compromise is the most financially damaging form of attack. It's a bit of misnomer, as it's a phishing attack at its heart, but it uses classic business communication to steal information and money from end-users.

Business Email Compromise has undergone a long evolution over the years. It has its roots in the classic Nigerian Prince Scam—the same principles apply to the more modern version, whereby someone is asking for something in return.

What made Business Email Compromise (BEC) so successful is that it started by spoofing CEOs or other executives. These attacks took off during COVID, when everyone was working from home and seeing an email from an executive made a lot of sense.

But these emails shared something that could tip off eagle-eyed users. They did not come from the company address.

Instead of CEO@company.com, the email would be CEO@gmail.com

This is easy to for end-users to fall for. Most end-users aren't actually looking at the email address, instead looking at the name associated with it. Seeing the CEO's name on an email with an urgent ask—usually a quick phone call or purchase of a gift card.

There's no compromise of the CEO's account involved here, just a spoof of the account.

Hackers then evolved into compromising accounts—often of a partner or even an internal employee-and using those accounts to do what's called thread hijacking. Hackers often hop into a thread that has to do with invoices or other bank details and redirect a routing number to their account.

Email security tools have evolved to identify and stop these on a consistent basis. So what do hackers do? They evolve into something new. We call these new attacks BEC 3.0.

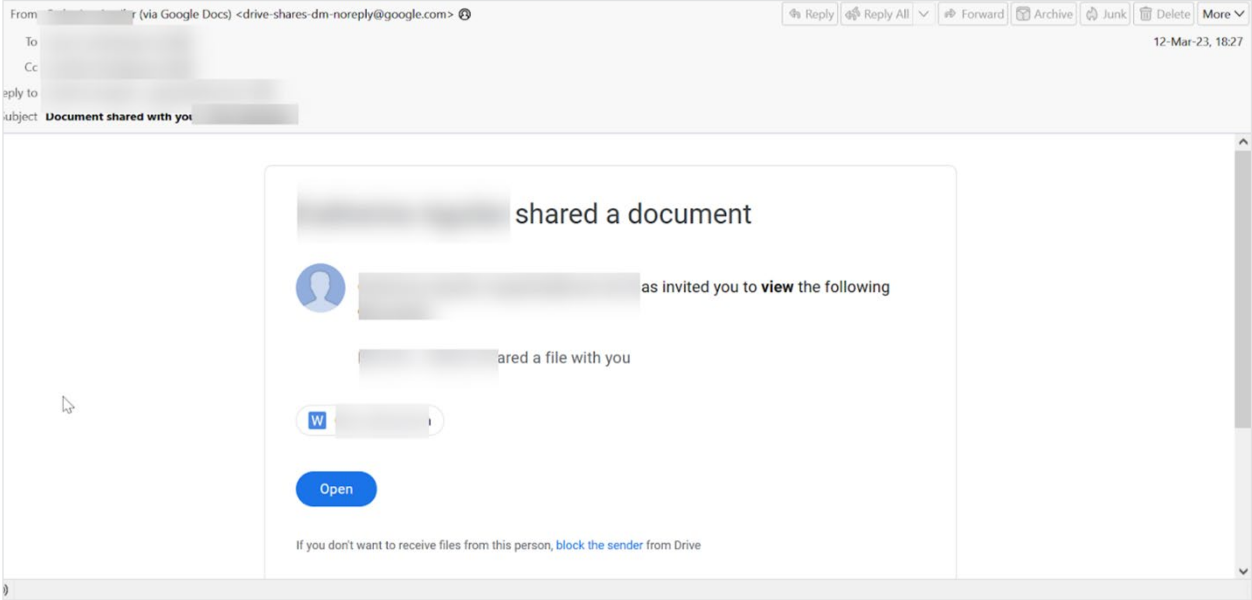
BEC 3.0 involves the usage of legitimate sites, like Google, PayPal, Dropbox and more. By leveraging the trust of these sites, the emails always get into the inbox, and even advanced tools won't detect them as illegitimate—because they are not!

By leveraging legitimate tools for illegitimate means, hackers can bypass security tools and get more end-users to click and respond.

In this whitepaper, we'll take a deep dive into how hackers are specifically using Google to launch these attacks. By leveraging Google tools, hackers can send out these attacks at scale, with limited chance for detection.

Attack 1: The Google Docs Comment Feature

This attack starts like many others we've written about. All the hacker has to do is create a Google document. From there, the hacker shares the document with the end-user. Like sharing all Google docs, it's done via email. Google sends the email directly; it comes from a no-reply@google.com address.



From [redacted]r (via Google Docs) <drive-shares-dm-noreply@google.com>
To [redacted]
Cc [redacted]
eply to [redacted]
ubject **Document shared with yo**[redacted]

12-Mar-23, 18:27

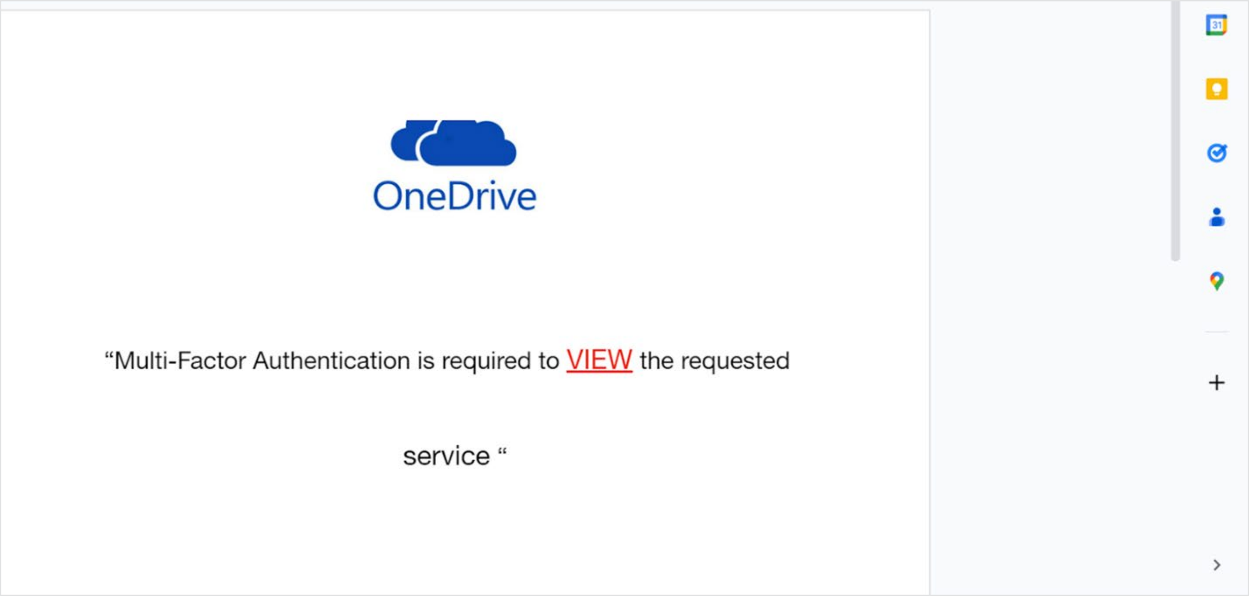
[redacted] shared a document

[redacted]as invited you to **view** the following

[redacted]ared a file with you

If you don't want to receive files from this person, block the sender from Drive

When the user clicks on the link, they will be redirected to the below Google doc.



"Multi-Factor Authentication is required to VIEW the requested

service "

This is a legitimate Google doc page. It's supposed to be a OneDrive knockoff page, although having it built on Google sort of defeats the purpose.

Regardless, the link that is put on the Google page is where the attack gets you.

That link once again is redirected to a fake crypto currency page, which has been taken down.

A perfect example of BEC 3.0 is illustrated above. It takes away a lot of the uncertainty that BEC gives to hackers. A successful BEC is not as simple as the attacks of yesterday. With no link or malicious download, you are hoping that an end-user replies, engages and eventually hands over money. It's not one-and-one. It requires a lot of time and energy. The payoff can be big. But you have to get to the payoff.

BEC 3.0 takes away some of that uncertainty. It requires the best of standard link or attachment-based phishing, with the social engineering and detection-evasion that can make BEC so successful.
It leverages something we all trust–Google— and processes we all trust–getting a shared document from Google Docs. There is nothing inherently wrong with this. And, as a reminder, there's nothing wrong with Google here. It's taking advantage of how email protocols work.

Security professionals have a dilemma. You can't block Google. Workers will revolt. What you can do is change how you evaluate all webpages, not just Google. That requires looking past NLP and actually emulating webpages behind the link. Integrating with browser security can be helpful here, too.

But as hackers shift, so must security professionals, and this shift is starting to happen right now.

Attack 2: Google Ads

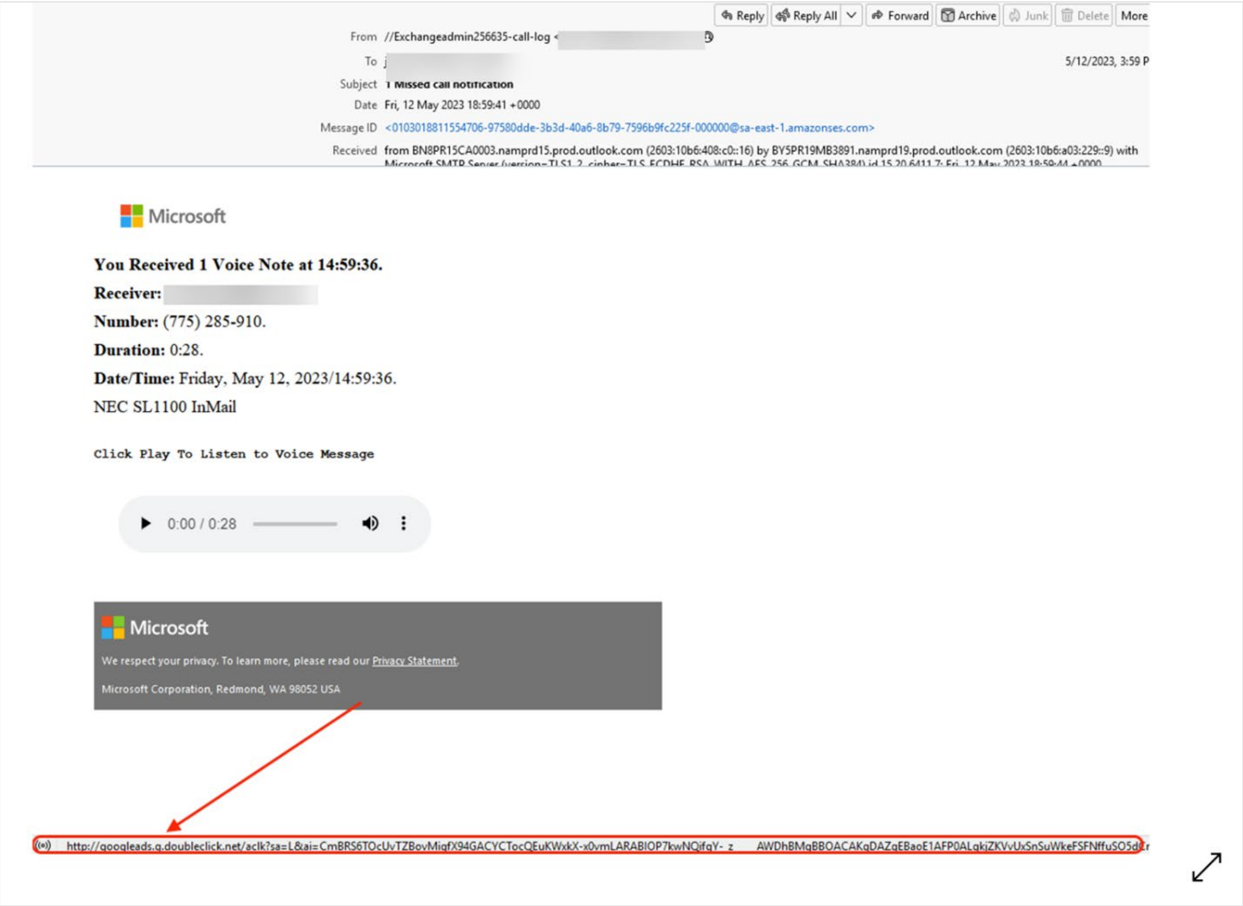
Ads make the internet go round. And nobody does more with online ads than Google.

Google is the leading ads provider on the Internet, and companies large and small–including this one–use their services.

It's simple and straightforward, and a great way to get the word out about your company or product.

Hackers are also utilizing it as a way to re-direct users to malicious sites of interest.

This email actually starts as an impersonation of a Microsoft voicemail. The hope is that by seeing a missed voicemail, the user will click. Eagle-eyed end-users, however, will see that the URL has nothing related to Microsoft. It has a Google ads URL. This is where the re-direct begins.



From //Exchangeadmin256635-call-log <[redacted]

To j[redacted]

5/12/2023, 3:59 P

Subject 1 Missed call notification

Date Fri, 12 May 2023 18:59:41 +0000

Message ID <0103018811554706-97580dde-3b3d-40a6-8b79-7596b9fc225f-000000@sa-east-1.amazonses.com>

Received from BN8PR15CA0003.namprd15.prod.outlook.com (2603:10b6:408:c0::16) by BY5PR19MB3891.namprd19.prod.outlook.com (2603:10b6:a03:229::9) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6411.7; Fri, 12 May 2023 18:59:44 +0000

Microsoft

You Received 1 Voice Note at 14:59:36.

Receiver: [redacted]

Number: (775) 285-910.

Duration: 0:28.

Date/Time: Friday, May 12, 2023/14:59:36.

NEC SL1100 InMail

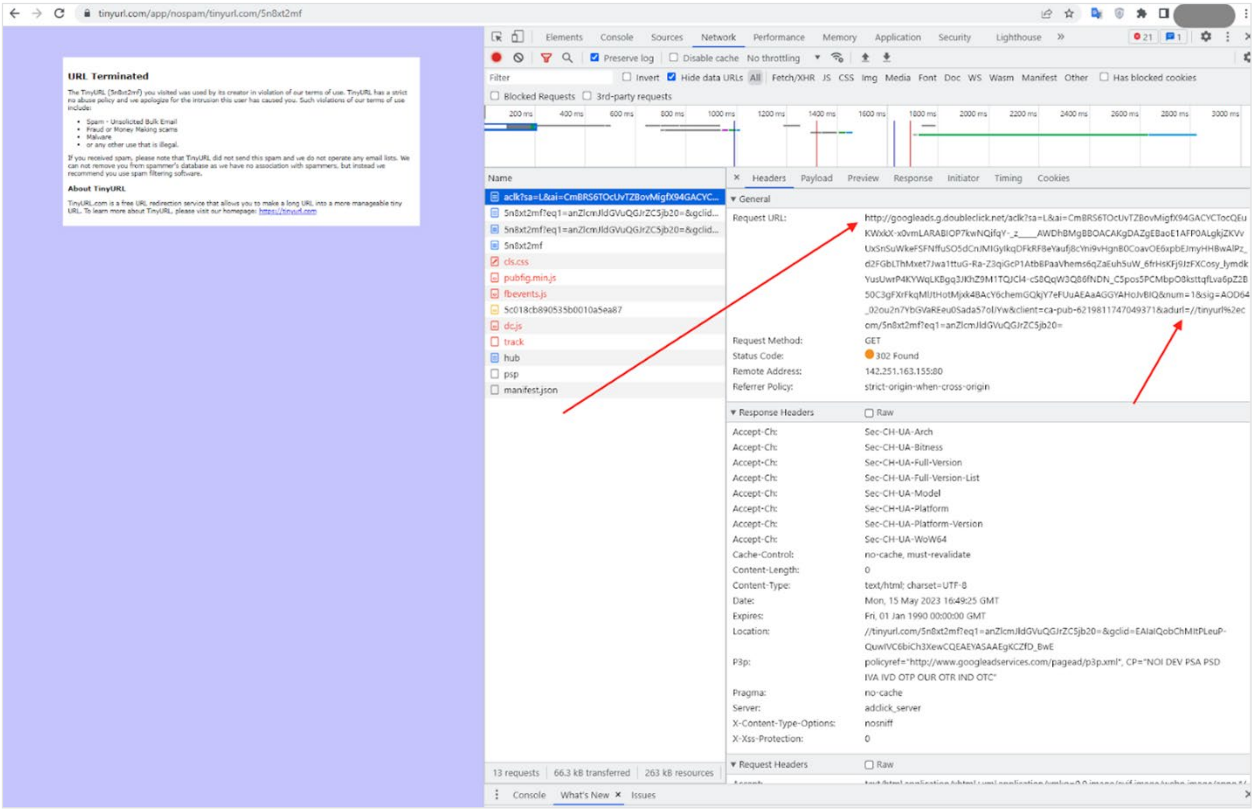
`Click Play To Listen to Voice Message`

Microsoft

We respect your privacy. To learn more, please read our Privacy Statement.

Microsoft Corporation, Redmond, WA 98052 USA

http://googleads.g.doubleclick.net/aclk?sa=L&ai=CmBRS6TOcUvTZBovMigfX94GACYCTocQEuKWxkX-x0vmLARABIOP7kwNQifqY- z AWDhBMqBBOACAKgDAZgEBaoE1AFP0ALqkjZKVvUxSnSuWkeFSFNffuSO5dCr



tinyurl.com/app/nospam/tinyurl.com/5n8xt2mf

URL Terminated

The TinyURL (5n8xt2mf) you visited was used by its creator in violation of our terms of use. TinyURL has a strict no abuse policy and we apologize for the intrusion this user has caused you. Such violations of our terms of use include:

- Spam - Unsolicited Bulk Email
- Fraud or Money Making scams
- Malware
- or any other use that is illegal.

If you received spam, please note that TinyURL did not send this spam and we do not operate any email lists. We can not remove you from spammer's database as we have no association with spammers, but instead we recommend you use spam filtering software.

About TinyURL

TinyURL.com is a free URL redirection service that allows you to make a long URL into a more manageable tiny URL. To learn more about TinyURL, please visit our homepage: https://tinyurl.com

```
Name
aclk?sa=L&ai=CmBRS6TOcUvTZBovMigfX94GACYC...
5n8xt2mf?eq1=anZlcmJldGVuQGJrZC5jb20=&gclid...
5n8xt2mf?eq1=anZlcmJldGVuQGJrZC5jb20=&gclid...
5n8xt2mf
cls.css
pubfig.min.js
fbevents.js
5c018cb890535b0010a5ea87
dc.js
track
hub
psp
manifest.json
```

```
▼ General
Request URL:              http://googleads.g.doubleclick.net/aclk?sa=L&ai=CmBRS6TOcUvTZBovMigfX94GACYCTocQEu
                          KWxkX-x0vmLARABIOP7kwNQifqY-_z____AWDhBMgBBOACAKgDAZgEBaoE1AFP0ALgkjZKVv
                          UxSnSuWkeFSFNffuSO5dCnJMIGylkqDFkRF8eYaufj8cYni9vHgnB0CoavOE6xpbEJmyHHBwAlPz_
                          d2FGbLThMxet7Jwa1ttuG-Ra-Z3qiGcP1AtbBPaaVhems6qZaEuh5uW_6frHsKFj9JzFXCosy_lymdk
                          YusUwrP4KYWqLKBgq3JKhZ9M1TQJCl4-cS8QqW3Q86fNDN_C5pos5PCMbpO8ksttqfLva6pZ2B
                          50C3gFXrFkqMlJtHotMjxk4BAcY6chemGQkjY7eFUuAEAaAGGYAHoJvBIQ&num=1&sig=AOD64
                          _02ou2n7YbGVaREeu0Sada57olJYw&client=ca-pub-6219811747049371&adurl=//tinyurl%2ec
                          om/5n8xt2mf?eq1=anZlcmJldGVuQGJrZC5jb20=
Request Method:           GET
Status Code:              ● 302 Found
Remote Address:           142.251.163.155:80
Referrer Policy:          strict-origin-when-cross-origin
▼ Response Headers        □ Raw
Accept-Ch:                Sec-CH-UA-Arch
Accept-Ch:                Sec-CH-UA-Bitness
Accept-Ch:                Sec-CH-UA-Full-Version
Accept-Ch:                Sec-CH-UA-Full-Version-List
Accept-Ch:                Sec-CH-UA-Model
Accept-Ch:                Sec-CH-UA-Platform
Accept-Ch:                Sec-CH-UA-Platform-Version
Accept-Ch:                Sec-CH-UA-WoW64
Cache-Control:            no-cache, must-revalidate
Content-Length:           0
Content-Type:             text/html; charset=UTF-8
Date:                     Mon, 15 May 2023 16:49:25 GMT
Expires:                  Fri, 01 Jan 1990 00:00:00 GMT
Location:                 //tinyurl.com/5n8xt2mf?eq1=anZlcmJldGVuQGJrZC5jb20=&gclid=EAIaIQobChMItPLeuP-
                          QuwIVC6biCh3XewCQEAEYASAAEgKCZfD_BwE
P3p:                      policyref="http://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA PSD
                          IVA IVD OTP OUR OTR IND OTC"
Pragma:                   no-cache
Server:                   adclick_server
X-Content-Type-Options:   nosniff
X-Xss-Protection:         0
▼ Request Headers         □ Raw
```

The image above showcases the website and the source code. This phishing page has been taken down. But when looking at the source code, we can see a few things.

It starts with this: http://googleads.g.doubleclick.net/aclk?

This is the base URL for Google Ads' click tracking and redirection service.

Next, you'll notice more in the URL string:

sa=L&ai=CmBRS6TOcUvTZBovMigfX94GACYCTocQEuKWxkX-x0vmLARABIOP7kwNQifqY-_z_____AWDhBMgBBOACAKgDAZgEBaoE1AFP0ALgkjZKVvUxSnSuWkeFSFNffuSO5dCnJMIGylkqDFkRF8eYaufj8cYni9vHgnB0CoavOE6xpbEJmyHHBwAlPz_d2FGbLThMxet7Jwa1ttuG-Ra-Z3qiGcP1AtbBPaaVhems6qZaEuh5uW_6frHsKFj9JzFXCosy_lymdkYusUwrP4KYWqLKBgq3JKhZ9M1TQJCl4-cS8QqW3Q86fNDN_C5pos5PCMbpO8ksttqfLva6pZ2B50C3gFXrFkqMlJtHotMjxk4BAcY6chemGQkjY7eFUuAEAaAGGYAHoJvBIQ&num=1&sig=AOD64_02ou2n7YbGVaREeu0Sada57olJYw&client=ca-pub-6219811747049371&adurl=//tinyurl%2ecom/5n8xt2mf?eq1=anZlcmJldGVuQGJrZC5jb20=

These are the parameters used by Google Ads for tracking and analytics purposes, as well as the destination URL where the user will be redirected.

Instead of placing a business URL, the hacker places the TinyURL. That's where the end-user will go, and in this case, it's a malicious site.

```
adurl=//tinyurl%2ecom/5n8xt2mf?eq1=anZlcmJldGVuQGJrZC5jb20=
```

Essentially, attacks are setting up a campaign using Google ads, and placing the redirect link on the URL.

By leveraging the trust and legitimacy of services like Google Ads, hackers are having a successful time getting their intended URL or payload to users.

In this case, by sneaking in a URL redirect into the parameters of a Google Ads script, the hackers can insert want they want with little notice.

We believe this is a true evolution in how hackers are operating. We predict that, by year's end, this attack will become more and more popular.

And, we predict, more and more damaging.

Attack: Google Looker Studio

Google Looker Studio is a powerful data visualization software tool. Cyber criminals figured out they can use it to create visualizations to send realistic phishing materials. This attack was first seen on July 13, 2023, and we have seen over a hundred of these attacks since then.

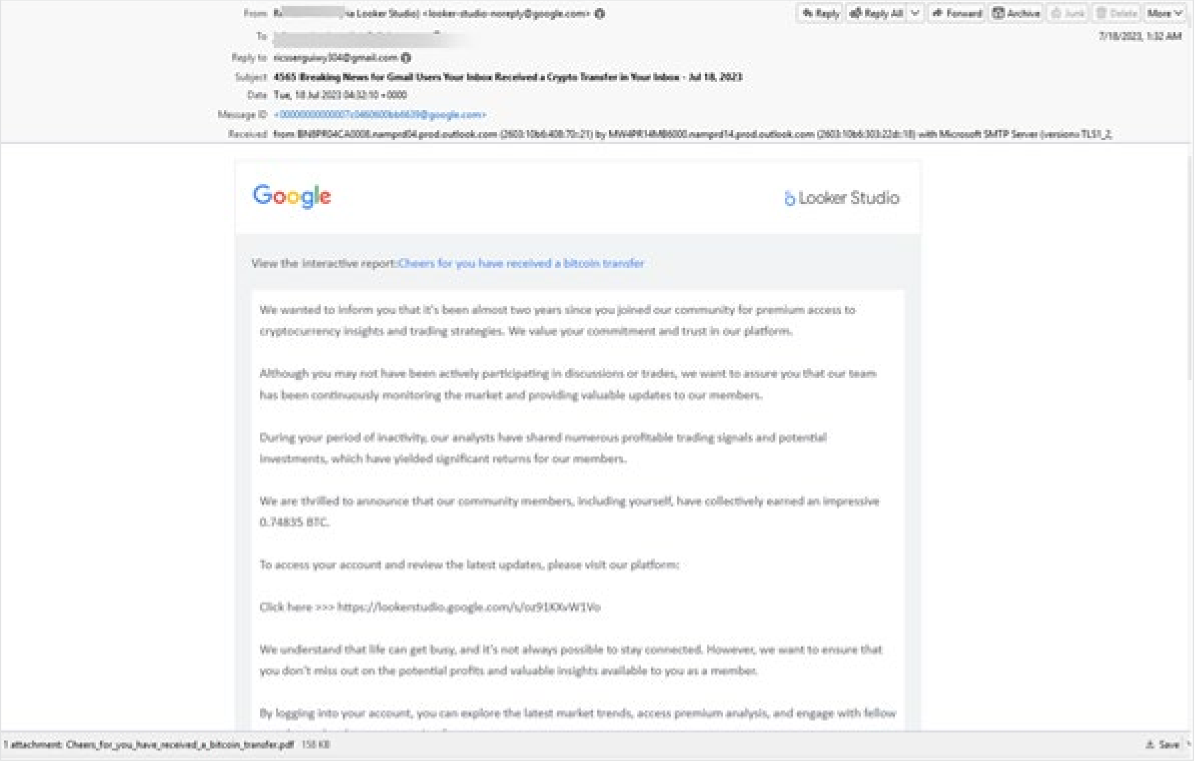
Here's how it works. Someone creates a Google document or Google Looker Studio page and shares it with a colleague or friend. The recipient receives a notification directly from Google, saying that someone has shared content that is awaiting comment or reply, via a click. The email comes directly from Google and is in fact legitimate. The recipient's email security service would not and should not block that, because it is legitimate from Google. When the link is clicked, it directs to the Google Looker Studio page, Google Doc or Google Slide. That page is also legitimate—it is a Google page. There's no spoofing. But embedded *within* that page, is a link that redirects the recipient to an external page designed to try to steal their credentials and other crypto-related information.

Why is this significant? Previously, cyber criminals spoofed Google in their phishing emails. They did this by using email accounts that were similar to google.com. The URL might have an extra 'o' in it, or an extra 'g'. Or maybe the URL is completely different and the logo is a bit off. These types of phishing attempts are easy to identify.

But in this new attack, it's more difficult. The email is actually coming from Google—the call is coming from inside the house. Google is not being hacked or exploited here. Rather, hackers are creating free Google accounts like anyone can, and then putting malicious content onto a Google page. When they send that page, both email security services and users see that it comes from Google and think it's safe. And then when they click on the link in the email, that also goes to a Google page. It's only when they *click on the link on the Google page* that the danger is apparent. And by then it's too late.

This attack starts with an email that comes directly from Google, in this case Google Looker Studio.

Hackers have created a report within Looker Studio. The email has a link to the report, saying that by following these investment strategies, users have seen a nice return. To access your account, just click here.



From R[redacted]ia Looker Studio) <looker-studio-noreply@google.com>
To [redacted]
7/18/2023, 1:32 AM
Reply to ricsserguiwy304@gmail.com
Subject **4565 Breaking News for Gmail Users Your Inbox Received a Crypto Transfer in Your Inbox - Jul 18, 2023**
Date Tue, 18 Jul 2023 04:32:10 +0000
Message ID <00000000000007c0460600bb6639@google.com>
Received from BN8PR04CA0008.namprd04.prod.outlook.com (2603:10b6:408:70::21) by MW4PR14MB6000.namprd14.prod.outlook.com (2603:10b6:303:22d::18) with Microsoft SMTP Server (version= TLS1_2,

View the interactive report:Cheers for you have received a bitcoin transfer

We wanted to inform you that it's been almost two years since you joined our community for premium access to cryptocurrency insights and trading strategies. We value your commitment and trust in our platform.

Although you may not have been actively participating in discussions or trades, we want to assure you that our team has been continuously monitoring the market and providing valuable updates to our members.

During your period of inactivity, our analysts have shared numerous profitable trading signals and potential investments, which have yielded significant returns for our members.

We are thrilled to announce that our community members, including yourself, have collectively earned an impressive 0.74835 BTC.

To access your account and review the latest updates, please visit our platform:

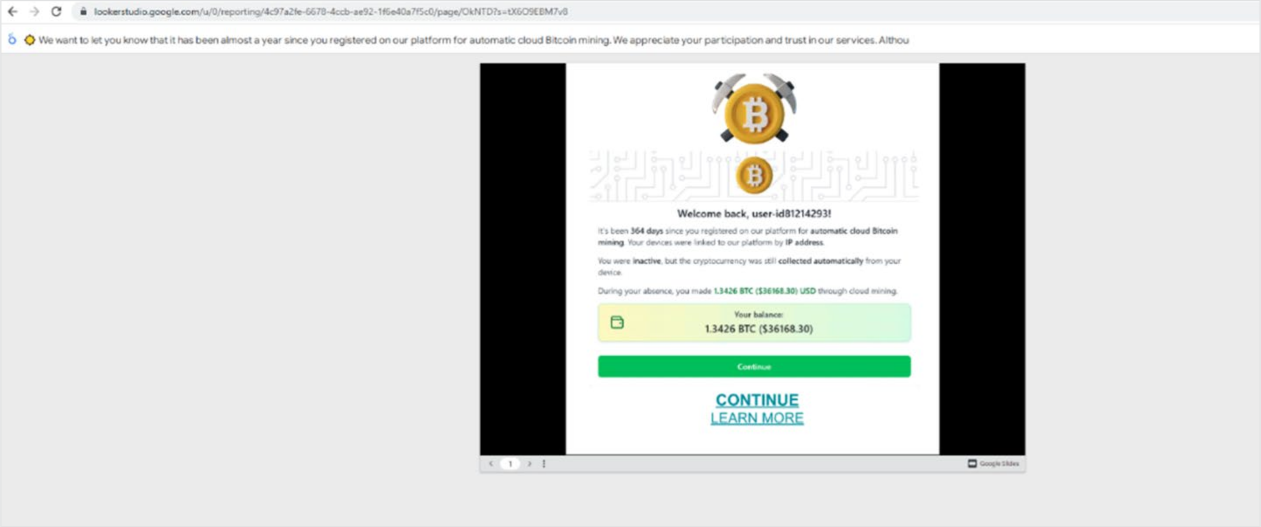
Click here >>> https://lookerstudio.google.com/s/oz91KXvW1Vo

We understand that life can get busy, and it's not always possible to stay connected. However, we want to ensure that you don't miss out on the potential profits and valuable insights available to you as a member.

By logging into your account, you can explore the latest market trends, access premium analysis, and engage with fellow

1 attachment: Cheers_for_you_have_received_a_bitcoin_transfer.pdf 158 KB

When you click, you'll be redirected to this page. Again, it's a legitimate Google Looker page.



lookerstudio.google.com/u/0/reporting/4c97a2fe-6678-4ccb-ae92-1f6e40a7f5c0/page/OkNTD?s=tX6O9EBM7v8

We want to let you know that it has been almost a year since you registered on our platform for automatic cloud Bitcoin mining. We appreciate your participation and trust in our services. Althou

Welcome back, user-id81214293!

It's been **364 days** since you registered on our platform for **automatic cloud Bitcoin mining**. Your devices were linked to our platform by **IP address**.

You were **inactive**, but the cryptocurrency was still **collected automatically** from your device.

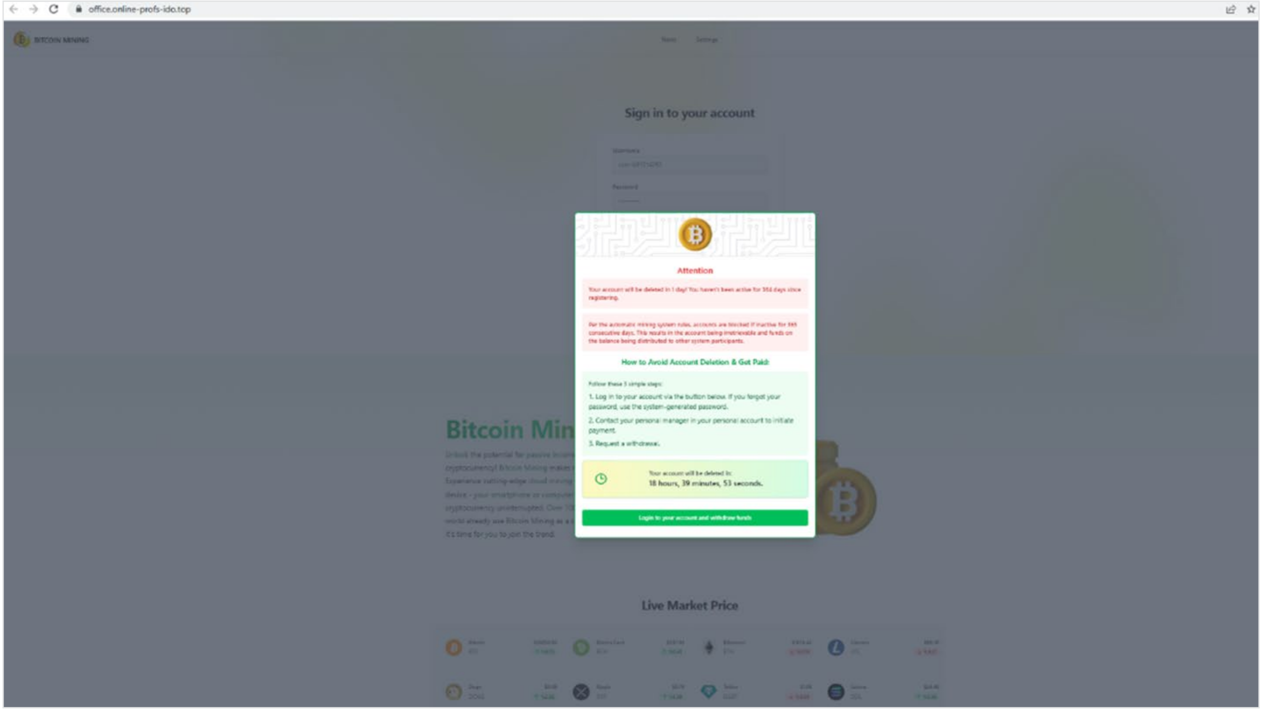
During your absence, you made **1.3426 BTC ($36168.30) USD** through cloud mining.

Your balance:
1.3426 BTC ($36168.30)

Here, the hackers have hosted a Google Slideshow, saying how you can claim more Bitcoin.

From there, it goes to a login page that is designed to steal your credentials.

But first, they give you even more urgency.



office.online-profs-ido.top

Sign in to your account

Attention

Your account will be deleted in 1 day! You haven't been active for 364 days since registering.

Per the automatic mining system rules, accounts are blocked if inactive for 365 consecutive days. This results in the account being irretrievable and funds on the balance being distributed to other system participants.

How to Avoid Account Deletion & Get Paid:

Follow these 3 simple steps:

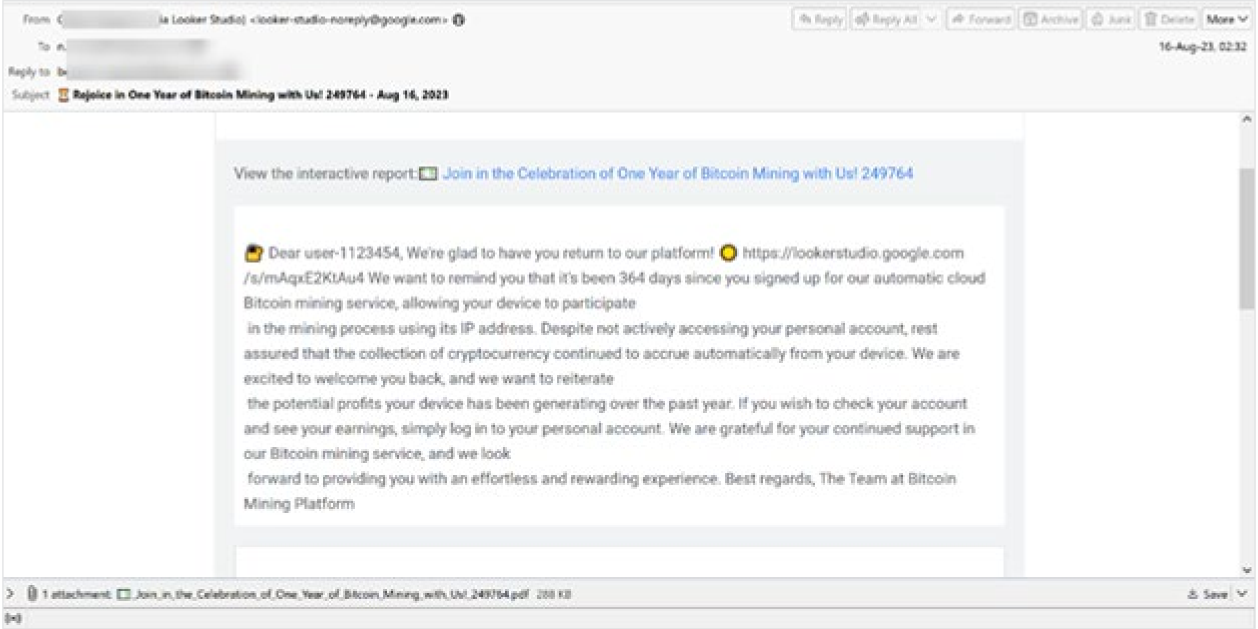
1. Log in to your account via the button below. If you forgot your password, use the system-generated password.
2. Contact your personal manager in your personal account to initiate payment.
3. Request a withdrawal.

Your account will be deleted in:
18 hours, 39 minutes, 53 seconds.

In order to save your account, you have to login immediately.

Then, of course, your credentials are stolen.

Here’s another example:



From C[redacted]ia Looker Studio) <looker-studio-noreply@google.com>
To [redacted]
Reply to [redacted]
Subject Rejoice in One Year of Bitcoin Mining with Us! 249764 - Aug 16, 2023

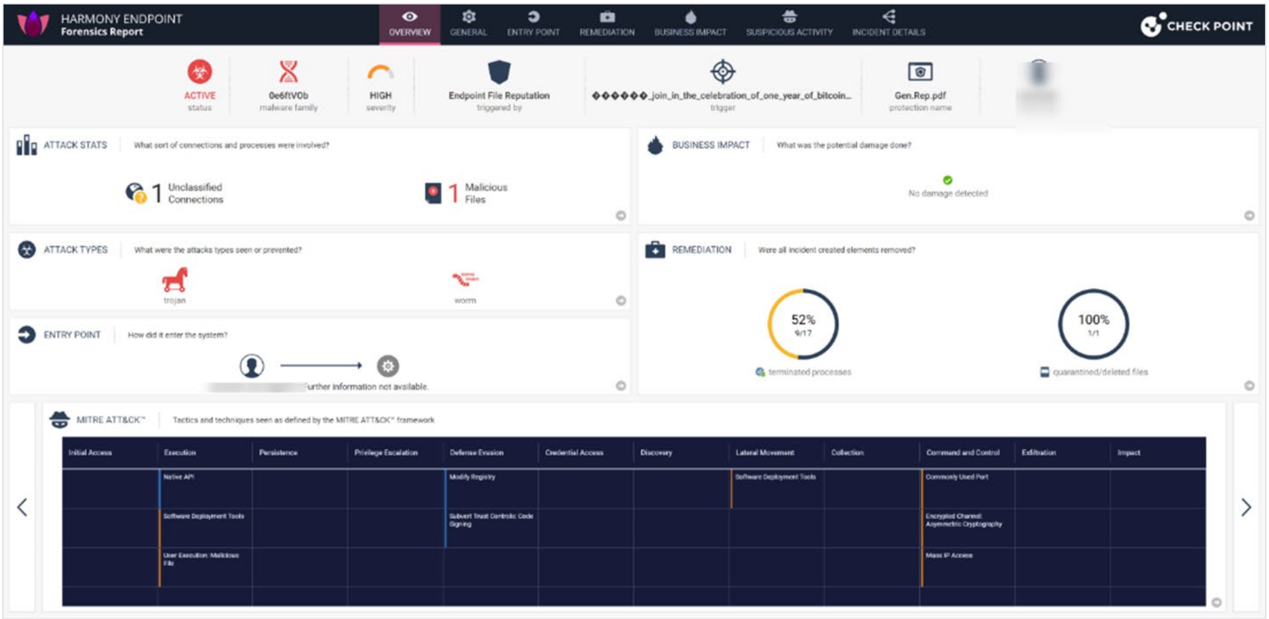
16-Aug-23, 02:32

View the interactive report: Join in the Celebration of One Year of Bitcoin Mining with Us! 249764

Dear user-1123454, We're glad to have you return to our platform! https://lookerstudio.google.com/s/mAqxE2KtAu4 We want to remind you that it's been 364 days since you signed up for our automatic cloud Bitcoin mining service, allowing your device to participate in the mining process using its IP address. Despite not actively accessing your personal account, rest assured that the collection of cryptocurrency continued to accrue automatically from your device. We are excited to welcome you back, and we want to reiterate the potential profits your device has been generating over the past year. If you wish to check your account and see your earnings, simply log in to your personal account. We are grateful for your continued support in our Bitcoin mining service, and we look forward to providing you with an effortless and rewarding experience. Best regards, The Team at Bitcoin Mining Platform

1 attachment: Join_in_the_Celebration_of_One_Year_of_Bitcoin_Mining_with_Us!_249764.pdf 288 KB

This is a similar example, hoping to get the user to click on the report and allow the user to give access to their IP address to mine bitcoin. This one has a slight difference, in that there’s a malicious PDF attached at the bottom. This malicious PDF is actually a Trojan:



ACTIVE
status

0e6ftVOb
malware family

HIGH
severity

Endpoint File Reputation
triggered by

������_join_in_the_celebration_of_one_year_of_bitcoin...
trigger

Gen.Rep.pdf
protection name

[redacted]

ATTACK STATS | What sort of connections and processes were involved?

1 Unclassified Connections

1 Malicious Files

BUSINESS IMPACT | What was the potential damage done?

No damage detected

ATTACK TYPES | What were the attacks types seen or prevented?

trojan

worm

REMEDIATION | Were all incident created elements removed?

52%
9/17
terminated processes

100%
1/1
quarantined/deleted files

ENTRY POINT | How did it enter the system?

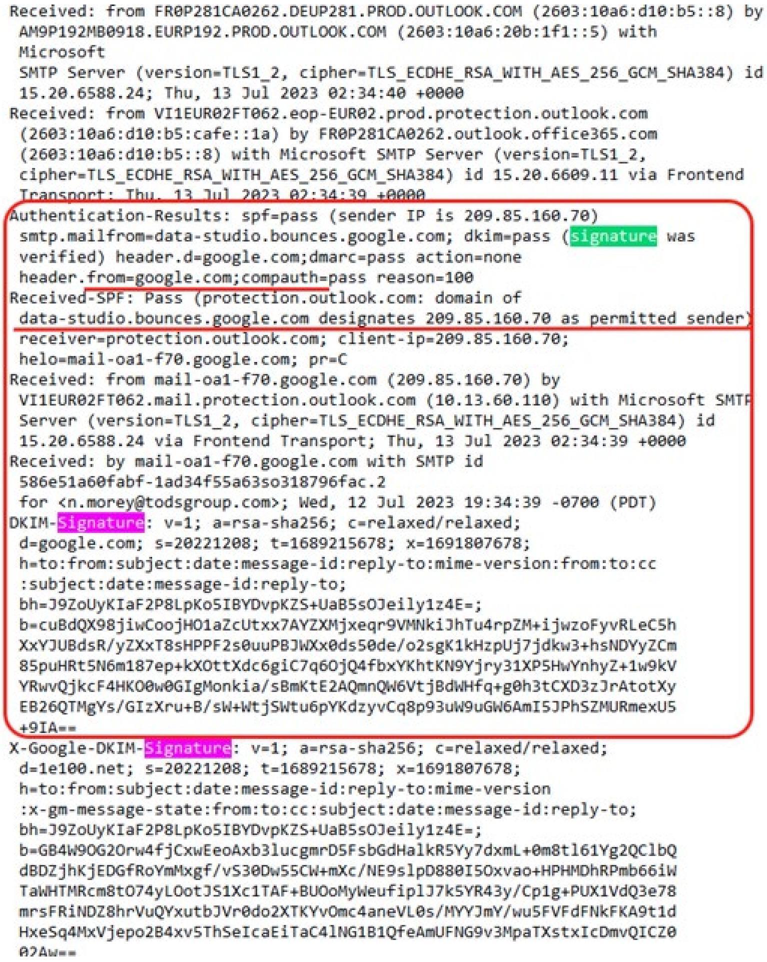
[redacted]urther information not available.

MITRE ATT&CK™ | Tactics and techniques seen as defined by the MITRE ATT&CK™ framework

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Native API			Modify Registry			Software Deployment Tools		Commonly Used Port		
	Software Deployment Tools			Subvert Trust Controls: Code Signing					Encrypted Channel: Asymmetric Cryptography		
	User Execution: Malicious File								Mass IP Access		

The clever part here is that hackers are using Google Looker to get their malicious PDF into the inbox. Because Google is a trusted service, it often soars right into the inbox, malicious PDF or not.

In the backend, you can see the signatures that Google uses to legitimize this page.



```
Received: from FR0P281CA0262.DEUP281.PROD.OUTLOOK.COM (2603:10a6:d10:b5::8) by
 AM9P192MB0918.EURP192.PROD.OUTLOOK.COM (2603:10a6:20b:1f1::5) with
 Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.6588.24; Thu, 13 Jul 2023 02:34:40 +0000
Received: from VI1EUR02FT062.eop-EUR02.prod.protection.outlook.com
 (2603:10a6:d10:b5:cafe::1a) by FR0P281CA0262.outlook.office365.com
 (2603:10a6:d10:b5::8) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6609.11 via Frontend
 Transport; Thu, 13 Jul 2023 02:34:39 +0000
Authentication-Results: spf=pass (sender IP is 209.85.160.70)
 smtp.mailfrom=data-studio.bounces.google.com; dkim=pass (signature was
 verified) header.d=google.com;dmarc=pass action=none
 header.from=google.com;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of
 data-studio.bounces.google.com designates 209.85.160.70 as permitted sender)
 receiver=protection.outlook.com; client-ip=209.85.160.70;
 helo=mail-oa1-f70.google.com; pr=C
Received: from mail-oa1-f70.google.com (209.85.160.70) by
 VI1EUR02FT062.mail.protection.outlook.com (10.13.60.110) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.6588.24 via Frontend Transport; Thu, 13 Jul 2023 02:34:39 +0000
Received: by mail-oa1-f70.google.com with SMTP id
 586e51a60fabf-1ad34f55a63so318796fac.2
 for <n.morey@todsgroup.com>; Wed, 12 Jul 2023 19:34:39 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
 d=google.com; s=20221208; t=1689215678; x=1691807678;
 h=to:from:subject:date:message-id:reply-to:mime-version:from:to:cc
 :subject:date:message-id:reply-to;
 bh=J9ZoUyKIaF2P8LpKo5IBYDvpKZS+UaB5sOJeily1z4E=;
 b=cuBdQX98jiwCoojHO1aZcUtxx7AYZXMjxeqr9VMNkiJhTu4rpZM+ijwzoFyvRLeC5h
 XxYJUBdsR/yZXxT8sHPPF2s0uuPBJWXx0ds50de/o2sgK1kHzpUj7jdkw3+hsNDYyZCm
 85puHRt5N6m187ep+kXOttXdc6giC7q6OjQ4fbxYKhtKN9Yjry31XP5HwYnhyZ+1w9kV
 YRwvQjkcF4HKO0w0GIgMonkia/sBmKtE2AQmnQW6VtjBdWHfq+g0h3tCXD3zJrAtotXy
 EB26QTMgYs/GIzXru+B/sW+WtjSWtu6pYKdzyvCq8p93uW9uGW6AmI5JPhSZMURmexU5
 +9IA==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
 d=1e100.net; s=20221208; t=1689215678; x=1691807678;
 h=to:from:subject:date:message-id:reply-to:mime-version
 :x-gm-message-state:from:to:cc:subject:date:message-id:reply-to;
 bh=J9ZoUyKIaF2P8LpKo5IBYDvpKZS+UaB5sOJeily1z4E=;
 b=GB4W9OG2Orw4fjCxwEeoAxb3lucgmrD5FsbGdHalkR5Yy7dxmL+0m8tl61Yg2QClbQ
 dBDZjhKjEDGfRoYmMxgf/vS30Dw55CW+mXc/NE9slpD880I5Oxvao+HPHMDhRPmb66iW
 TaWHTMRcm8tO74yLOotJS1Xc1TAF+BUOoMyWeufiplJ7k5YR43y/Cp1g+PUX1VdQ3e78
 mrsFRiNDZ8hrVuQYxutbJVr0do2XTKYvOmc4aneVL0s/MYYJmY/wu5FVFdFNkFKA9t1d
 HxeSq4MxVjepo2B4xv5ThSeIcaEiTaC4lNG1B1QfeAmUFNG9v3MpaTXstxIcDmvQICZ0
 02Aw==
```

Let's break this down a little bit. Sender Policy Framework, or SPF, is an email authentication method that is designed to prevent email spoofing by specifying which IP addresses or servers are authorized to send emails for a particular domain.

In this case, the SPF check has passed (spf=pass) because the sender's IP address (209.85.160.70) is listed as an authorized sender for this domain: data-studio.bounces.google.com

Then, there's DomainKeys Identified Mail, or DKIM. It's another email authentication tool that uses cryptographic signatures to verify that the email's content has not been altered during transit, and that it actually comes from the domain it says it does. In this case, the DKIM signature has passed (dkim=pass) and was verified for the domain google.com

Next is Domain-based Message Authentication, Reporting, and Conformance, or DMARC. DMARC is a policy framework that builds on both SPF and DKIM to further enhance email authentication. It allows domain owners to specify what actions should be taken for any emails that fail SPF or DKIM. In this particular case, the DMARC check has passed (dmarc=pass) for the domain google.com, and the action specified is none. That means that no specific action is taken for failed emails.

This is a long way of saying that hackers are leveraging Google's authority. An email security service will look at all these factors and have a good deal of confidence that it is not a phishing email, and that it comes from Google. And it does! Because the attack is nested so deep, all the standard checks will pass with flying colors.

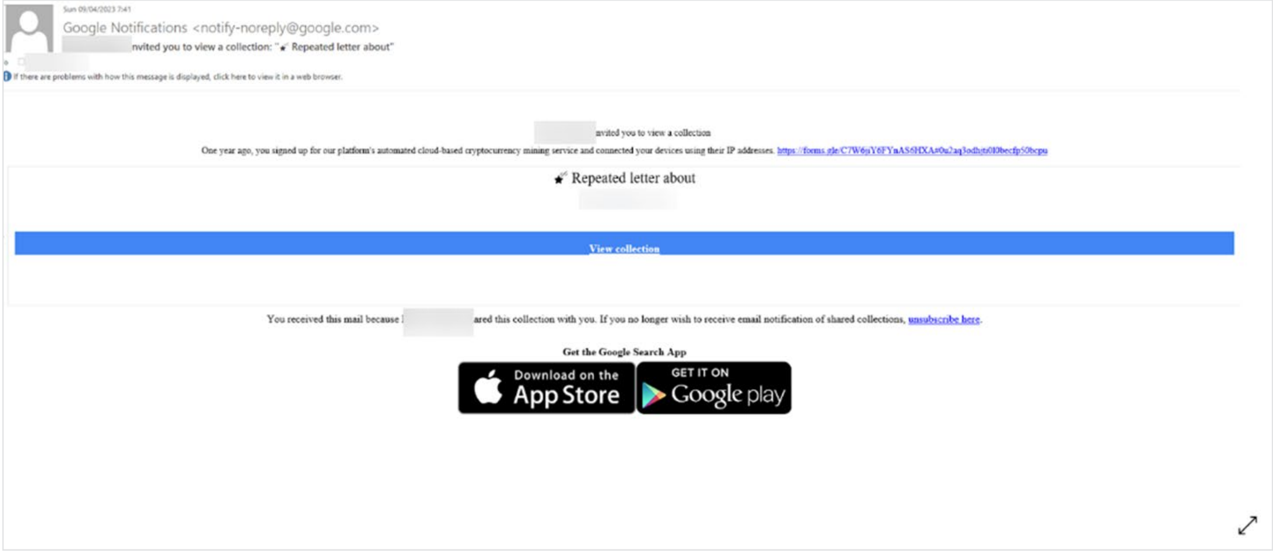
Now, this does require cooperation on the part of the user, to go through all the links and enter the required information. Not every user will do that. But as we say often, it just takes one successful attack.

Attack: Google Collection

Google Collection is a cool tool that allows you to save links, images and videos and share them with others.

In keeping with the spirit of the BEC 3.0 attacks, we're going to highlight how hackers are using this tool to spread phishing. By leveraging the legitimacy of Google, hackers are able to hide malicious links within legitimate sites.

This BEC 3.0 attack is yet another way hackers are tricking users into giving up sensitive information.



Sun 09/04/2023 7:41
Google Notifications <notify-noreply@google.com>
[redacted]nvited you to view a collection: "★ Repeated letter about"
[redacted]
If there are problems with how this message is displayed, click here to view it in a web browser.

[redacted]nvited you to view a collection
One year ago, you signed up for our platform's automated cloud-based cryptocurrency mining service and connected your devices using their IP addresses. https://forms.gle/C7W6jiY6FYnAS6HXA#0u2aq3odh/n0I0becfp50bcpu

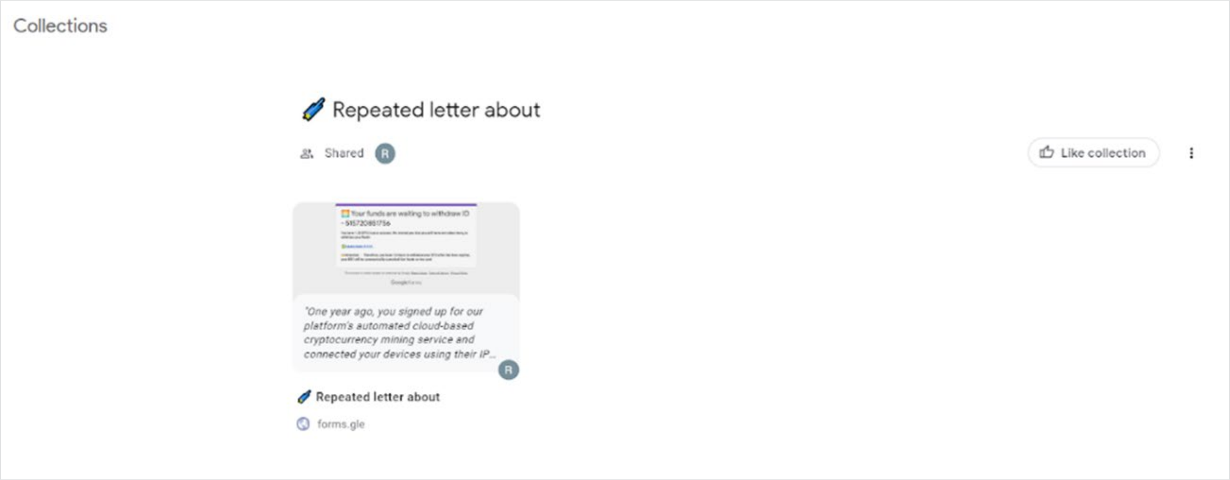
★ Repeated letter about
[redacted]

View collection

You received this mail because [redacted]ared this collection with you. If you no longer wish to receive email notification of shared collections, unsubscribe here.

Get the Google Search App

The first email comes in typical fashion, via a notification directly from Google. This is because the hacker shared the collection with the end-user. The email comes from a **no-reply@google.com** address. That address is legitimate and would be recognized as such by hackers and end-users alike. Clicking on the link is also okay–hovering over the URL will show a legitimate Googe link. Going to the page below is also, you guessed it, a legitimate Google page.

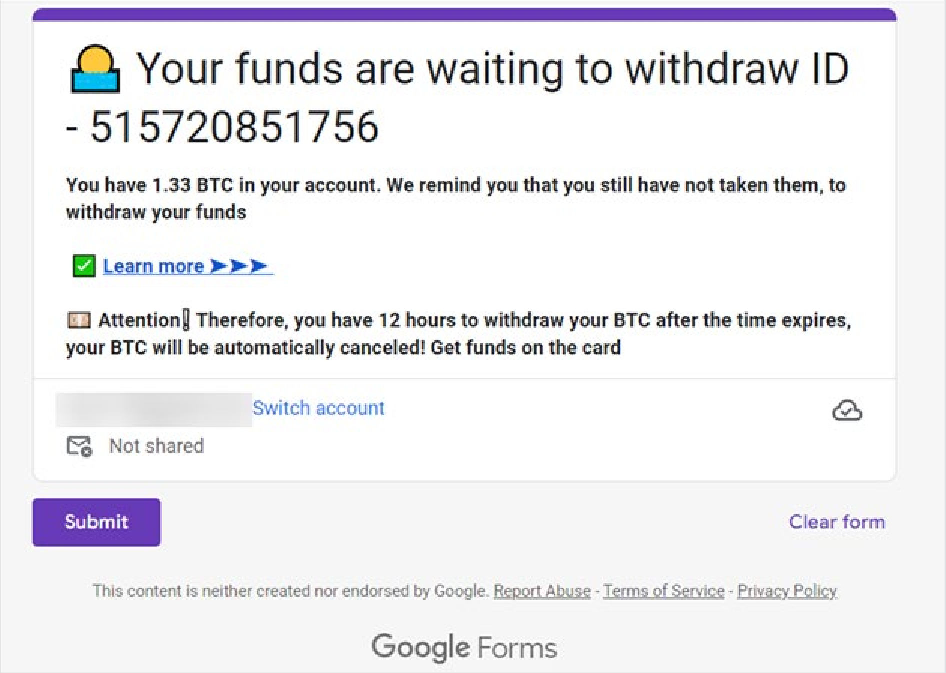


Repeated letter about

"One year ago, you signed up for our platform's automated cloud-based cryptocurrency mining service and connected your devices using their IP...

Repeated letter about

Google collections work like above, with a number of different card like figures. You can link to images, webpages, etc within that collection. Clicking on the card leads to the below page:



Your funds are waiting to withdraw ID - 515720851756

You have 1.33 BTC in your account. We remind you that you still have not taken them, to withdraw your funds

✅ Learn more ➤➤➤

Attention▯ Therefore, you have 12 hours to withdraw your BTC after the time expires, your BTC will be automatically canceled! Get funds on the card

[redacted] Switch account

Not shared

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

This is the link that they eventually want you to get to, which is a Google form. This will redirect to a fake cryptocurrency site, which will eventually steal money.

The bottom of the Google page tells an important distinction: "This content is neither created nor endorsed by Google."

What we're saying here is critical: This isn't to say that Google is now illegitimate or dangerous. Quite the contrary. But Google, like many sites, allows you to put any content on their page. Hackers are abusing this privilege by placing illegitimate, malicious sites.

To better ensure that their payloads get to their target, they are nesting it. It's not in the first link in the email. It's not in the second link that you click. It's hidden in the third link.

So yes, end-users have to get through all these links and layers, and that's certainly not a guarantee.

But when they see Google link after Google link, the hesitancy might start to drop. And when the guard drops, users might be more freewheeling with their mouse clicks.

That's the hope of BEC 3.0. It's not trickery, but rather using what the user knows against them. Because it seems so standard–because it is so standard–users might be more willing to cooperate.

That, in turn, could lead to some real damages.

Summary

Google is a safe service. It has not been hacked by an army of hackers around the world.

Rather, hackers are using its services as a springboard to launch their attacks.

The legitimacy of Google, in other words, is being taken advantage of. By starting the phishing trail via Google, it makes security services think that email is clean. That's because it is clean! The end-user is more likely to click on a legitimate link from Google than they are a suspect link.

The end-user does have to take a few steps to give over their credentials. But most phishing attacks work that way. What hackers are doing is making the steps more believable and realistic.

BEC 3.0, our term for these attacks, can happen on pretty much any free service that can send out emails. But blocking these services isn't an option, either.

That's the brilliance of these attacks.

Harmony email researchers expect these attacks to skyrocket in the end of 2023 and beyond.

It's time to get ready.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com