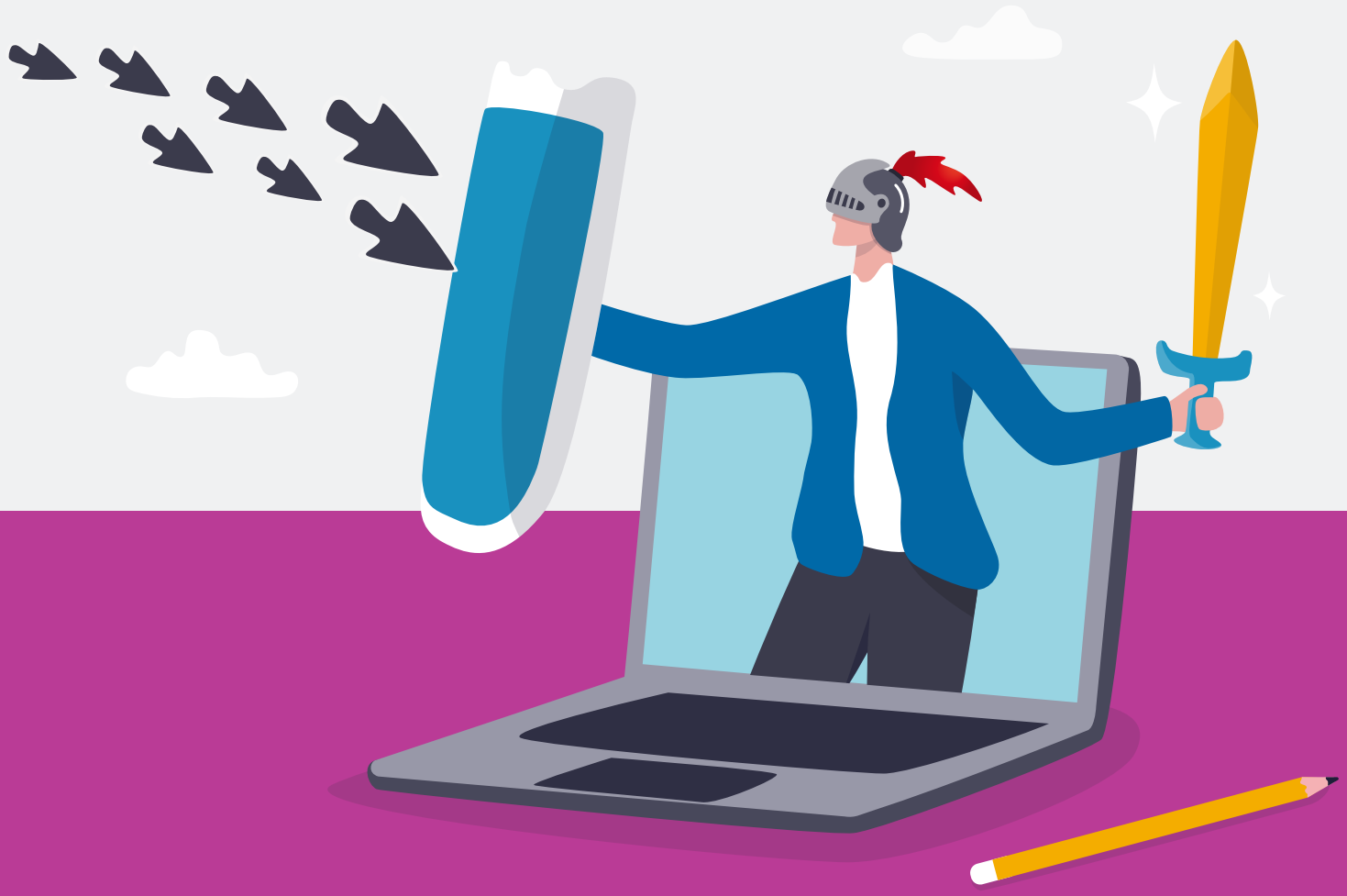
proofpoint.

EBOOK

5 Real-World Cyberattacks and How to Stop Them

Vol. 2: Technical attacks



Introduction

Cybercriminals are crafty and highly motivated. And why wouldn't they be? They're in a growth industry where the risks are low and the returns are so high that by 2027 cybercrime is expected to cost the world a staggering $23.8 trillion per year.[1]

With so much money to be made, the creativity behind today's cyberattacks is seemingly endless. New and ingenious malware, phishing, and social engineering schemes pop up daily as defenders play a whack-a-mole game to stop them. Yet although these new threats may seem infinitely varied, they all have a few basic things in common, namely: they use email, and they target people.

In this e-book series, we've collected some of the most insidious email attacks out there right now. What's notable is that many of them have slipped past multiple security tools before we've caught them. To help you understand why, we take you through each attack step-by-step to show you how each one worked and how cybercriminals tried to take advantage of human vulnerabilities. Then we tell you how they were stopped.

Previously, in volume 1, we covered attacks that rely on social engineering. This volume covers more technical attacks.

1 World Economic Forum. "2023 Was a Big Year for Cybercrime – Here's How We Can Make Our Systems Safer." January 2024.

Table of Contents

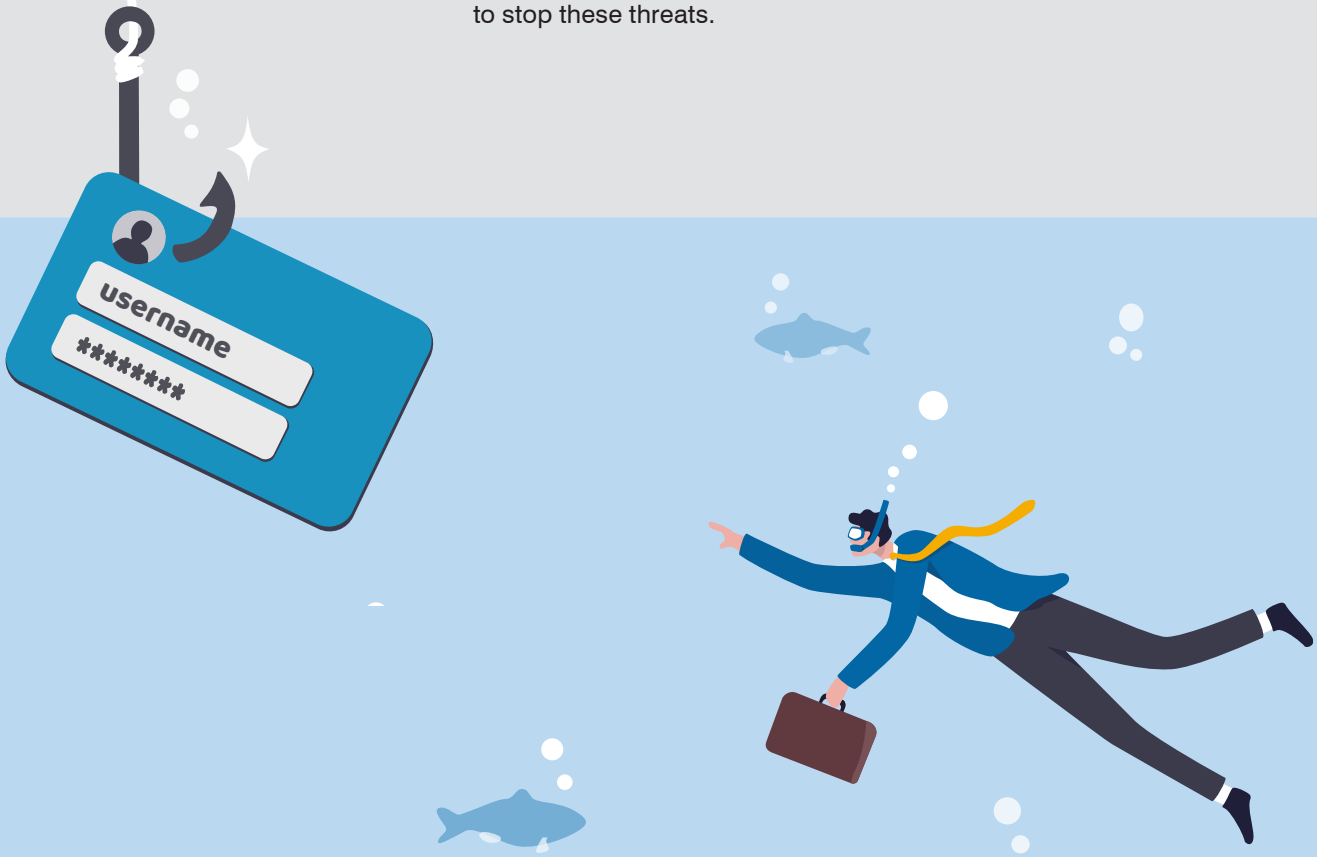
SECTION 1

EvilProxy Phishing Toolkit

EvilProxy is a phishing toolkit that can steal user credentials and multi-factor authentication (MFA) tokens.

It works by sitting behind a legitimate webpage. When the user connects to a phishing page, they are presented with a fake login page that looks and acts like a real login portal. When the user logs in, EvilProxy captures the user's credentials and authentication session token. The bad actor can then use that information to bypass MFA protections and log in on behalf of the user.

EvilProxy and other threats that bypass MFA are becoming more frequent as bad actors adapt to enhanced security controls. Traditional methods, such as IP or URL reputation, are not enough to stop these threats.



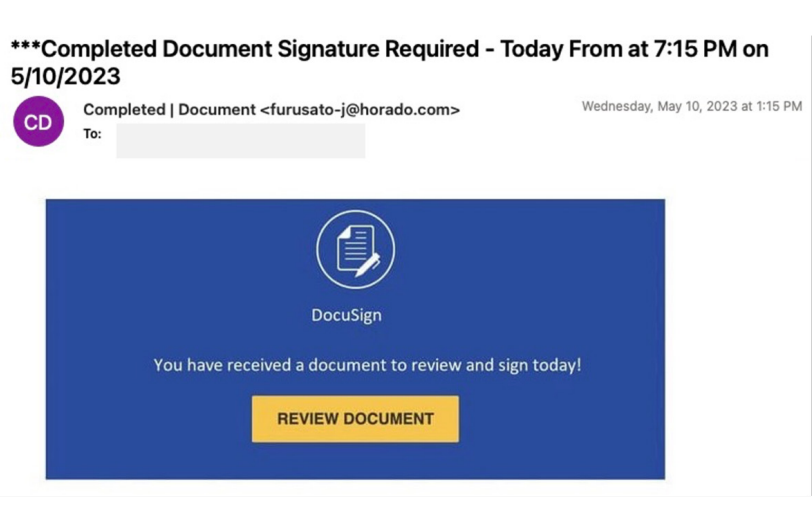
The scenario

During an email threat assessment, Proofpoint discovered that a technology company with 1,500 clients had been exposed to EvilProxy. The company already had another email security tool that failed to detect this threat.

How the attack played out

Here's a closer look at how the attack unfolded.

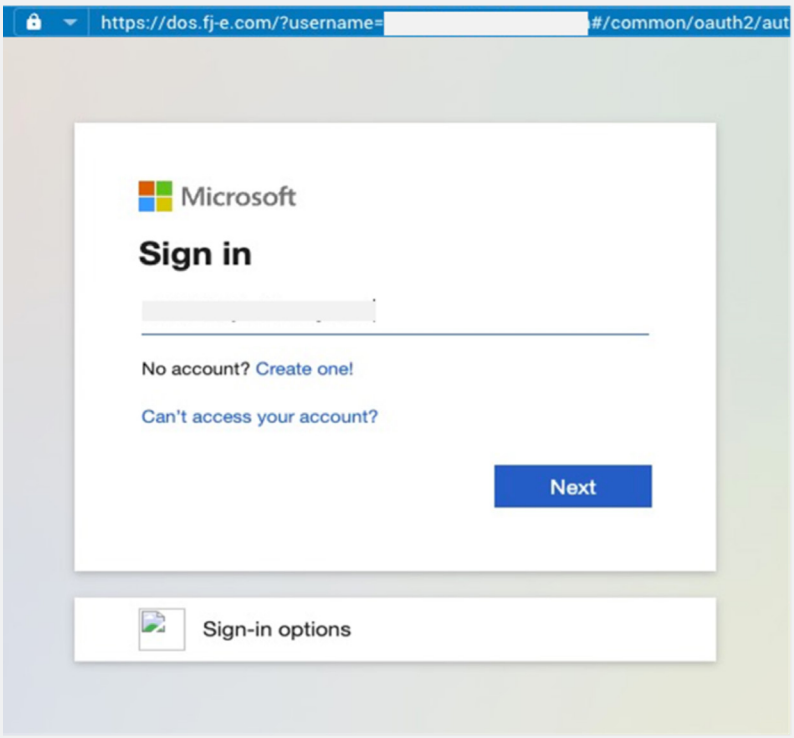
1. **The deceptive message.** The attack started with an email that looked like a legitimate DocuSign notice. It notified recipients that there was a document ready for their signature. This seemingly harmless message was actually the gateway to an advanced cyberattack.



The initial deceptive email received by the customer.

2. **The malicious URL.** When recipients clicked on the embedded URL, they were sent to their own Microsoft login page. The attackers' proxy was set up behind this page. It's there that users were deceived into entering their credentials.

3. **The EvilProxy phishing framework.** This was the driving force behind this attack. Attackers employed a reverse proxy technique to intercept user login attempts through their actual Microsoft sign-in page. This is how they secretly extracted MFA codes and user credentials.



The malicious Microsoft sign-in page.

4. **Undermining MFA verification.** With MFA codes and user login credentials in hand, attackers gained free access to the compromised accounts. Because they were able to bypass MFA verification, they were able to enter the company's environment.

How Proofpoint detected it

Proofpoint uses advanced machine learning (ML) to decipher the context of inbound messages and analyse their language for potential threats. We determine whether an email is benign, malicious or suspicious by analysing its message body and context. We also look at the sender's typical sending patterns. If the email has any suspicious payloads, Proofpoint submits them to a sandbox for an in-depth analysis. This helps us to home in on malicious content, even if it has never been seen before.

In this scenario, Proofpoint found the message was suspicious for several reasons. For starters, the recipient did not typically get emails from that sender. Also, the sender was asking the recipient to take an action (click on the URL). Since we couldn't initially see whether the URL was benign or malicious, we preemptively sandboxed it for further analysis.

As we followed the URL, we saw that it used a redirecting evasion tactic to mask its malicious nature. As we followed it further, our URL engine discovered that it led to a web page that looked a lot like a Microsoft login page. Based on the behaviour of that web page, Proofpoint detected a URL framework that used a proxy service that was intended to steal users' credentials and MFA responses in real time. These characteristics aligned with EvilProxy. By intercepting credentials and an MFA challenge response in real time, bad actors can quickly gain access to a user's account even when MFA protection is enabled.

Malicious URLs

Credential phish caught by machine learning engine

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	dc890227-7740-11e9-8d93-12ba71d80a0c

phishing url

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	2930c017-0415-11eb-bab7-12ba71d80a0c

Detected by rule e7461bcaf73c18c64b12ed7fbb7283e6

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	behavior_e7461bcaf73c18c64b12ed7fbb7283e6

Redirect Chain

A URL with multiple redirects was visited

URL	https://doc.yg-r.com/?username=redacted_email&auth=1-0.79432671181593

A summary of observations by Proofpoint about the e-signature email, which led to condemnation of the email.

Behaviors

Malicious content dropped during execution

Rule	behavior_d27be4c0bb9ef4dc79fb5309c19e5b3d

ETPRO Suricata IDS Alerts

Rule	behavior_286b6c79e0dc5b5fc7664b918c773cae

SocGholish redirect domain: trademark.jgieslaclarca.com

Rule	behavior_800bd3bcf9c9fc40f2ce1212d47b0b76

SocGholish compromised script detected: http://jc.efficasing.com/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6

Rule	behavior_800bd3bcf9c9fc40f2ce1212d47b0676

Detecting the EvilProxy phishing framework in Proofpoint.

SECTION 2

SocGholish Attack

Observed in the wild as early as 2018, SocGholish is a malware variant that continues to thrive. Because it uses a wide variety of stages, eligibility checks, and obfuscation routines, it is one of the most elusive malware families to date. The absence of details about its target selection, evasion logic, and the specific procedures in its intermediary phases all contribute to its shroud of mystery.

It works in four basic stages:

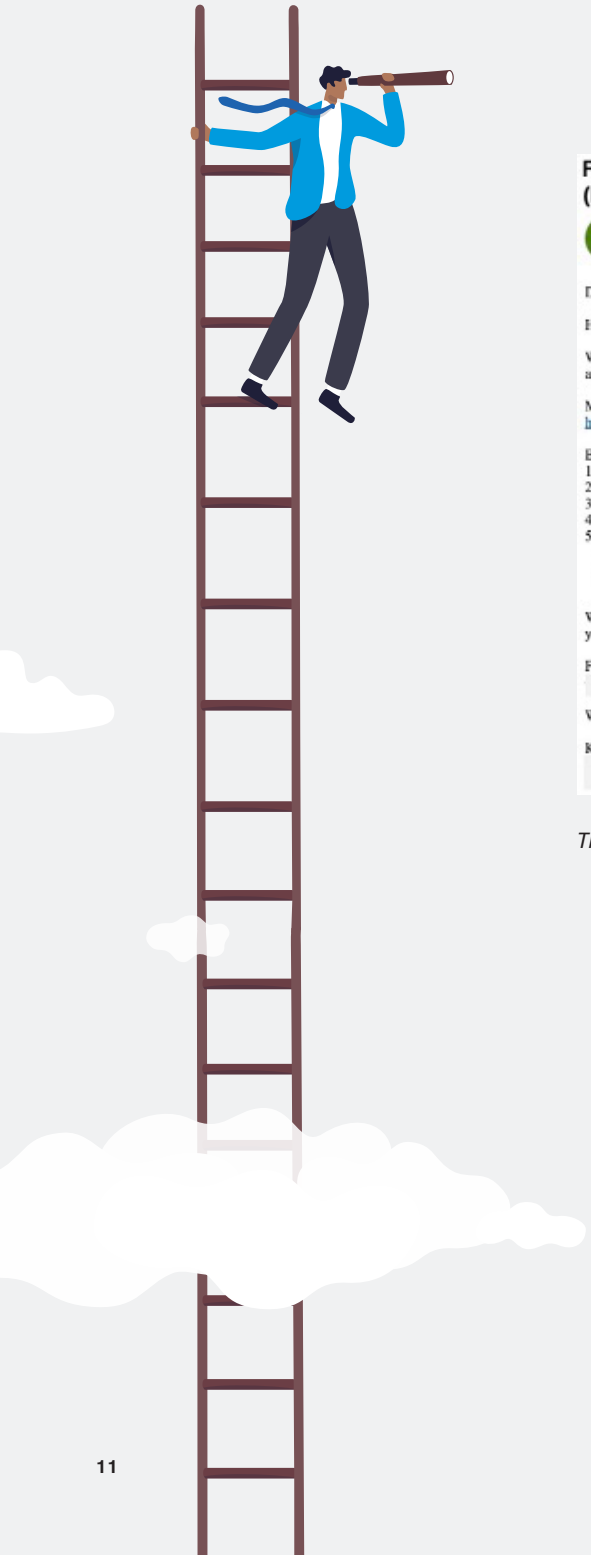
Stage 1: Malicious injects
A bad actor compromises a legitimate website and injects malicious JavaScript that profiles users in an attempt to find ideal candidates for further attack.

Stage 2: SocGholish download
If a user meets certain criteria, the JavaScript smuggles in SocGholish, which often looks like a fake browser update. If clicked, it downloads SocGholish to the user's device.

Stage 3: Phone home
Next, the malware communicates with C2 proxies to receive further instructions.

Stage 4: Follow-on malware and infection
SocGholish continues profiling the user's device and makes subsequent calls to C2 servers for delivery of follow-on malware. This often includes Remote Access Trojans or ransomware.

SocGholish is challenging to defend against. It's widespread. And it can evade even the most advanced email security tools. In just a single month in 2023, Proofpoint saw it evade detection by other layers of security in thousands of instances worldwide.



The scenario

During an email threat assessment, we found that a technology company with 4,000 users had been exposed to a SocGholish attack. Their previous email security tool had failed to catch this threat.

How the attack played out

Here's a closer look at how the attack unfolded.

1. **The initial message.** Users received an email inviting them to submit a paper for publication in a well-known academic journal. The email itself wasn't malicious. Nor was it crafted by a bad actor. As is characteristic of SocGholish campaigns, the malicious code didn't manifest itself until the user arrived at the compromised – but legitimate – website.

Follow up: Paper Invitation: [Environment and Social Psychology] (Indexed in Scopus) is Open for Submission

TS

Thursday, June 29, 2023 at 6:05 AM

To:

Dear

Hope this mail finds you well.

We were wondering if you have received our paper invitation for the journal *Environment and Social Psychology*. We are writing to inquire if you are interested in submitting a paper for publication in this journal.

More information can be found on the website:
https://esp.apacsci.com/index.php/esp/index

Benefits of publishing with ESP:
1.Open access (unlimited and free access for readers).
2.Indexed by the Scopus, NLB, Portico, and other databases.
3.Fast Publication combined with thorough peer review.
4.As indicated on the website, the APC of USD 1250 in 2023 applies to submitted papers.
5.We will provide discount for early bird submission:
*Early Bird Submission before July 31, 2023: 90%
*Early Bird Submission before August 31, 2023: 60%
*Early Bird Submission before September 30, 2023: 50%

We cordially invite you to submit a paper. In addition, we would appreciate it if you could recommend this journal to your colleagues. If you are interested, please kindly let us know.

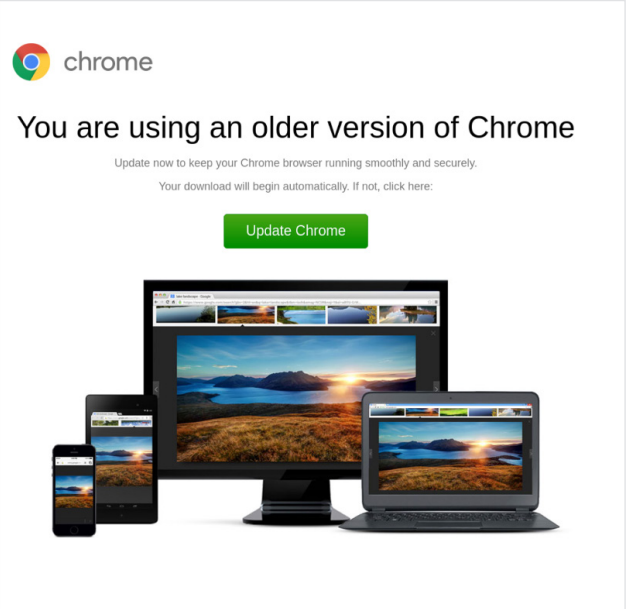
For any questions regarding technical issues or applying discount, please feel free to contact

We look forward to hearing from you.

Kind regards,

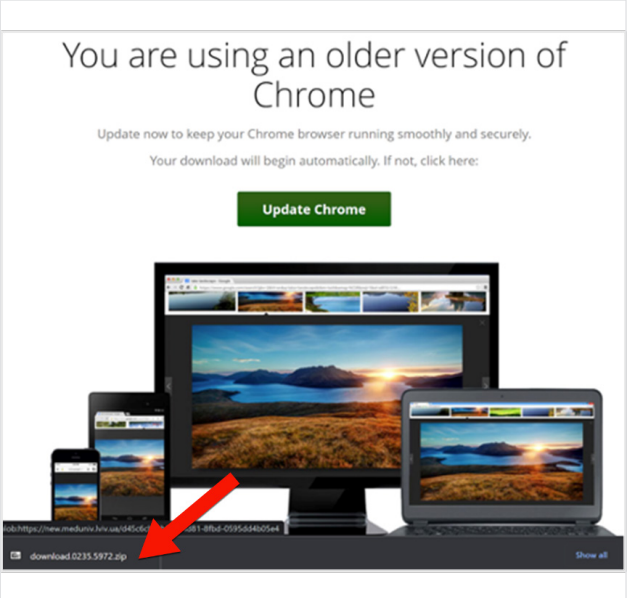
The initial email received by our customer.

2. **The compromised URL.** If the user clicked through to the URL within the email, the JavaScript injected at the destination began profiling them to find out if they were eligible for further attack. Selected users were presented with a full-page pop-up that said their browser needed to be updated.



The fake browser update request.

3. **Installation of SocGholish.** If the user downloaded the update package, SocGholish profiled the user's device, its configuration, and what it had access to. SocGholish then asked C2 proxies for further instructions and if any follow-on malware needed to be installed.



The file downloaded by initiating a fake browser update.

Why these threats are hard to catch

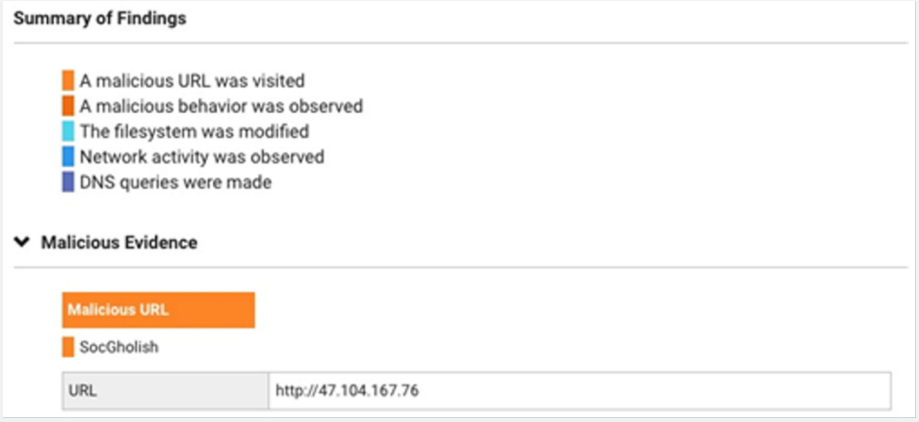
Most email security tools can detect malicious JavaScript, but SocGholish is evasive by nature. In particular, many email security tools find it difficult to detect its profiling techniques. These include looking at a device's IP address, operating system, browser, and local language. Also, tools that rely solely on anomaly detection struggle with attacks like SocGholish because the email message and the URL are both legitimate.

SocGholish also uses sandbox-aware evasion tactics. This means that it won't manifest if it detects a simulated environment such as a threat analyst's sandbox. What's more, email security tools that claim to analyse threats with AI/ML also struggle to detect SocGholish. That's because the email message itself is not malicious. It would also not be considered anomalous based on previous sending patterns.

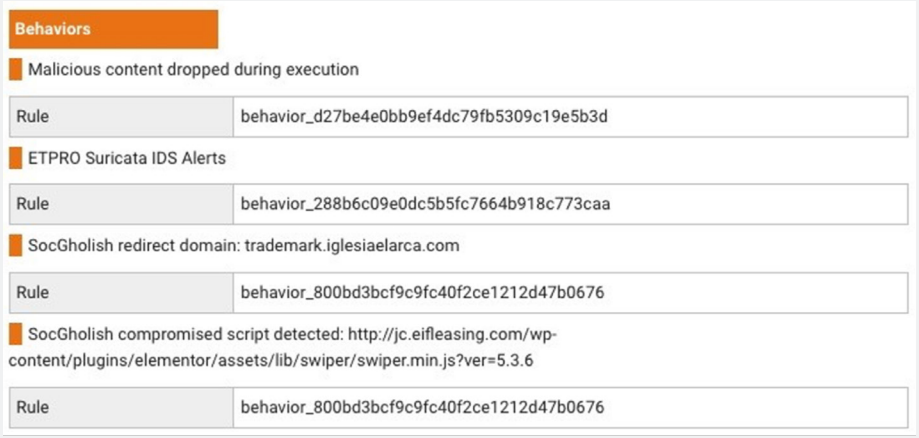
How Proofpoint detected it

Proofpoint uses deep URL behaviour analysis to detect multiple suspicious behaviours associated with SocGholish, like profiling. Because we analyse network activity, we can see the malware phoning home to C2 proxies. We also catch another tactic we've seen with SocGholish: redirecting to a DNS service and exploiting compromised scripts.

In this scenario, Proofpoint detected unusual sending patterns. So we sandboxed the URLs before users clicked on any links. The predictive sandboxing of selective URLs is a distinct feature that is unique to Proofpoint. It's one of the reasons why we can detect novel, never-before-seen URL threats.



TAP Dashboard Forensics report showing activities indicating a SocGholish attack.



TAP Dashboard Forensics report showing specific behaviours indicating a SocGholish attack.

Proofpoint also prioritises frequent and thorough scanning of URLs. The threat actor TA569, which is commonly associated with SocGholish, has demonstrated persistence in maintaining control over injected sites. We have observed instances where cleaned web pages are compromised again, with the site being reinject with similar or different attacks.

So we proactively sandbox URLs after they have been deemed safe or have been cleared. Ongoing monitoring helps to ensure that any potential compromise or weaponisation is uncovered quickly.

SECTION 3

QR Code Phishing

QR code phishing moves the attack channel from the protected email environment to a user's mobile device, which is often far less secure.

With QR codes, the URL isn't exposed within the body of the email. This approach renders most email security scans ineffective. What's more, decoding QR code scams using image recognition or optical character recognition (OCR) quickly becomes resource-intensive and difficult to scale.

The scenario

Proofpoint recently detected one of these attacks at an agriculture company with more than 16,000 employees. A bad actor had crafted a phishing lure that looked like it had information about an employee's wages. The message instructed the employee to scan a QR code with their mobile phone to access the information, rather than click on a link. Once scanned, a fake SharePoint login screen prompted them to provide their credentials.

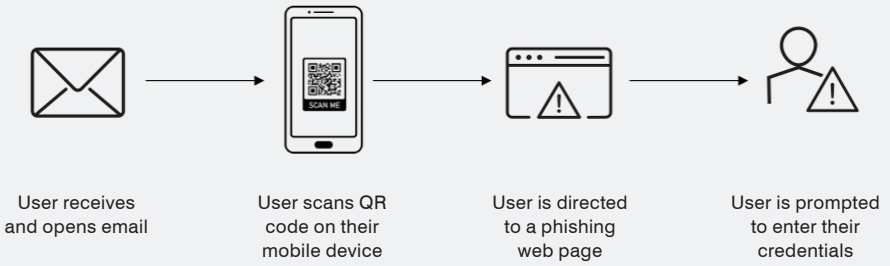
How the attack played out

Here is how the attack unfolded:

1. **The deceptive message.** The employee got an email from what looked like the company's HR team, which claimed to have payroll information.

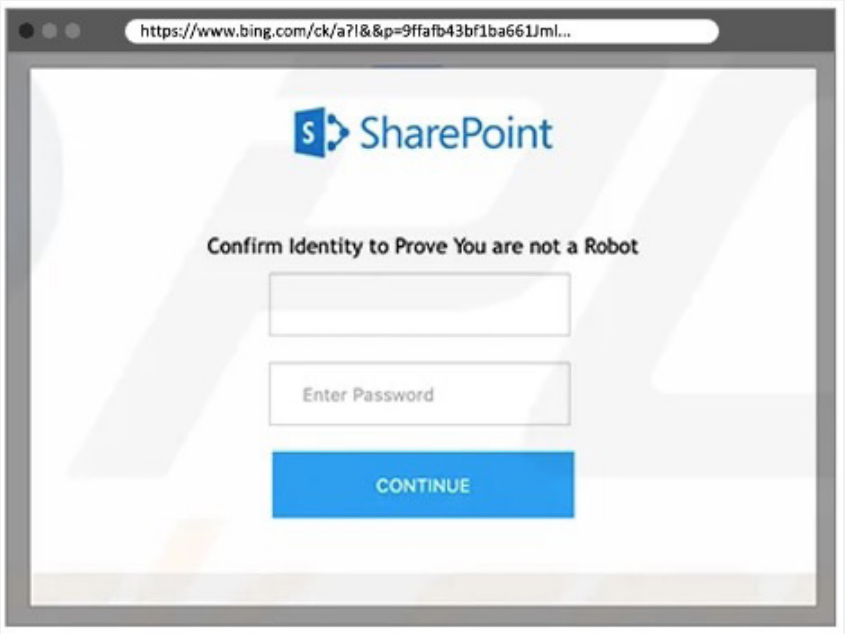
Malicious email blocked by Proofpoint before it was delivered to the user's mailbox. (Note: For safety, we replaced the malicious QR code with one linking to Proofpoint.com. The rest of the message is a redacted screenshot of the original.)

2. **QR code attack sequence.** The employee was told to scan the QR code with their mobile device.



Typical QR code attack sequence.

3. **SharePoint phishing lure.** Once the employee decoded the URL, a fake SharePoint login screen tried to fool them into entering their credentials.

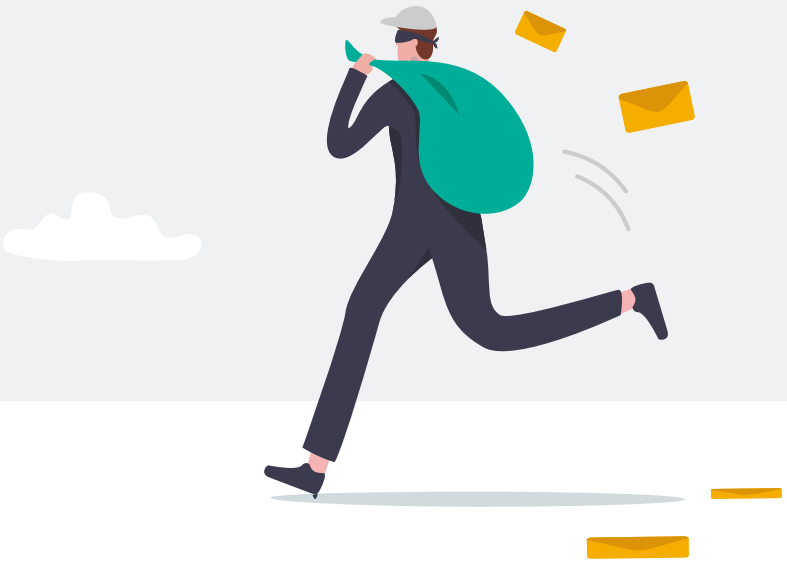


Decoded QR code redirecting the user to a SharePoint phishing page.

Why these threats are hard to catch

For starters, the phishing URL inside a QR code isn't easy to extract and scan. And then there's the challenge of the ubiquity of QR codes. Most benign email signatures contain logos, links to social media outlets embedded within images and even QR codes pointing to legitimate websites. So the presence of a QR code by itself isn't a sure sign of phishing.

Often, security tools will try to stop these threats using uncommon sender patterns alone. However, they are a weak basis for condemning a message and can result in falsely classifying a benign message as bad. That's often the case with email security tools that try to address threats post-delivery.

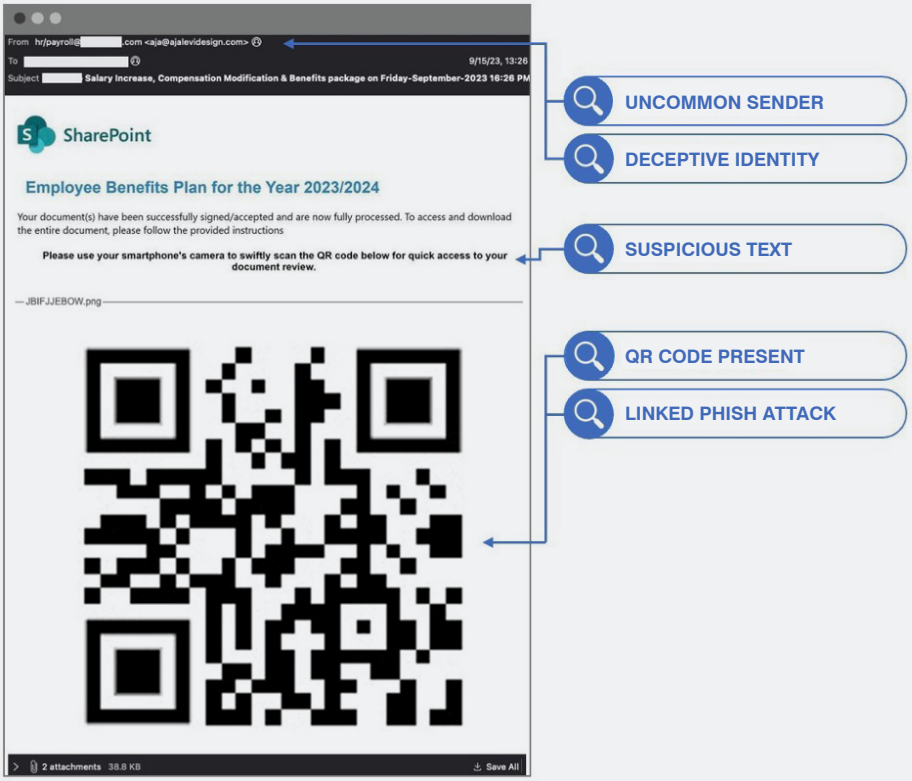


How Proofpoint detected it

Proofpoint uses an advanced blend of signals and layers of analysis to distinguish between weaponised and benign QR codes. We analyse and profile:

- The sender
- The sender's patterns
- The relationship of the sender and recipient based on past communication

All of these clues help us to identify suspicious senders and whether they are acting in a way that deviates from an established profile. In this example, our systems had never seen this sender communicate with this company or recipient.



Signals that Proofpoint used to condemn the message as a threat.

But we don't just rely on uncommon sender patterns. To reduce the number of false positives, we combine many other signals to extract the nature and metonym of the email's content. (A metonym is a word or phrase used to represent something else, such as "the crown" is used for British royalty. This type of analysis helps us to infer a sender's intent no matter what words they use to phrase it.)

We analyse the sender's email history along with a linguistic and semantic analysis of the email's body. Using this approach, we identified language that revealed the email was asking the recipient to take action – in this case, to scan a QR code with their mobile device.

Outside of the behavioural and language analysis, we also detected deception tactics within the headers of the message. Bad actors often try to spoof trusted entities or other employees to gain trust. In this case, the bad actors crafted the email headers to appear to be from the employer's HR and payroll team.

We also went a step further – and deeper – by analysing the QR code. By using the OCR and image recognition technology in our detection engines, we scanned and condemned the malicious URLs hidden within the QR code itself. We extract both URLs and text to ensure that any messages that should be delivered are delivered and those that shouldn't are blocked or remediated.

SECTION 4

MFA Manipulation

Multi-factor (MFA) manipulation poses a significant threat to cloud platforms. It's an advanced technique where bad actors introduce their own MFA method into a compromised cloud account.

Bad actors have multiple options for getting around MFA. One way is to use an adversary-in-the-middle (AiTM) attack. This is where the bad actor inserts a proxy server between the victim and the website that they're trying to log into. Doing so enables them to steal that user's password as well as the session cookie.

There's no indication to the user that they've been attacked – it just seems like they've logged into their account as usual. However, the attackers have what they need to establish persistence. This means that they can maintain access even if the stolen MFA credentials are revoked or deemed invalid.

MFA manipulation attacks are used after a cloud account takeover attack (ATO). Unfortunately, ATOs are alarmingly common. In 2023, Proofpoint threat researchers found that almost all businesses (96%) were targeted by cloud-based attacks. What's more, 60% were successfully compromised and had at least one account taken over.

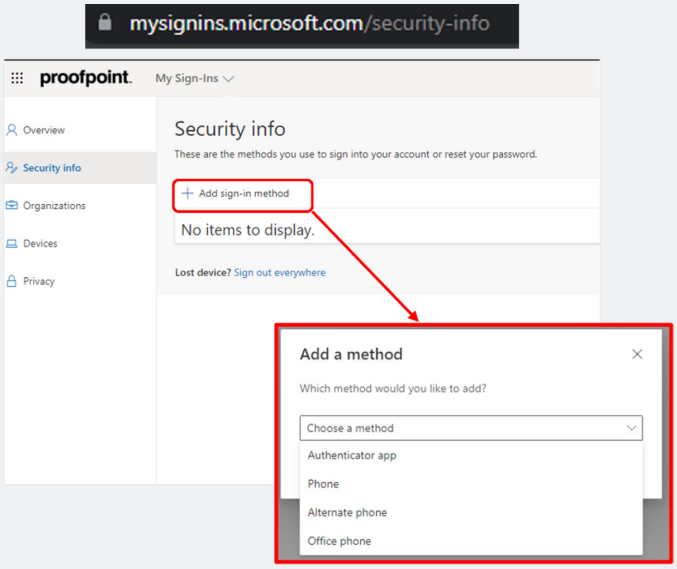
The scenario

Proofpoint intercepted a series of MFA manipulation attacks on a large real estate company. In one case, the bad actors used an AiTM attack to steal the credentials of the firm's financial controller as well as the session cookie. Once they did that, they logged into that user's business account and generated 27 unauthorised access activities.

How the attack played out

Here's a closer look at how the attack unfolded.

1. **Secure a foothold.** Bad actors used the native "My Sign-Ins" app to add their own MFA methods to compromise Microsoft 365 accounts. We observed that the attackers registered their own authenticator app with notification and code. They made this move right after they gained access to the hijacked account as part of an automated attack flow execution. This, in turn, allowed them to secure their foothold within the targeted cloud environment.



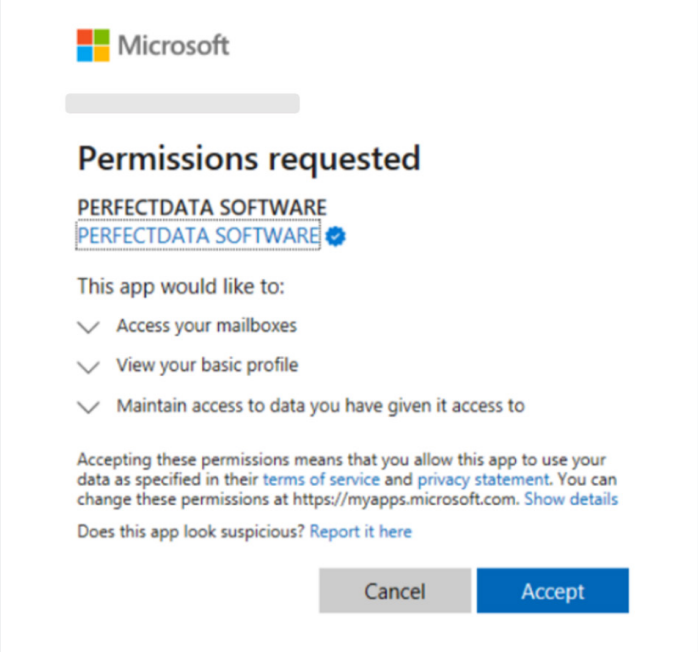
The typical MFA manipulation flow using Microsoft's "My Sign-Ins" app.

2. **Combine attack tactics.** Attackers used a very sophisticated approach. They combined MFA manipulation with OAuth application abuse. Essentially, OAuth abuse is when an attacker uses a third-party app to steal data, spread malware or cause havoc.

3. **Gain persistent access.** Attackers also use an abused app to maintain persistence even after their initial access to a compromised account has been cut off. In this case, attackers authorised the seemingly benign application, "PERFECTDATA SOFTWARE," to gain persistent access to the user's account and the systems, as well as their resources and applications. Here are the permissions that the attackers requested for this app:

    - Complete permanent access to the user's mailbox
    - Offline access to data
    - User profile access

If these permissions had been granted, attackers would have been free to steal sensitive data continuously. It would have been easy for them to spread malicious threats to internal or external user accounts.



The permissions request for the "PERFECTDATA SOFTWARE" app, which shows its associated scopes.

Why these threats are hard to catch

These multi-step attacks exploit legitimate cloud functionalities. Plus, they blend seamlessly with regular activities. That's why they often slip by traditional security measures. Focused on isolated events, other vendors struggle to connect the dots.

How Proofpoint detected it

Proofpoint used several strategies to find where attackers got in and what they did post-compromise. These included using internal intelligence feeds as well as user and entity behaviour analytics (UEBA).

Our next steps were to automate the remediation of the malicious sessions and revoke the abused PERFECTDATA SOFTWARE app. This allowed the real estate company's security team to take immediate, corrective action.

Proofpoint cloud threat researchers also advised the company as it was investigating this incident. They helped to ensure that all attacker-controlled MFA methods were removed for good, helping to reduce risk in the future.

The app details for the revoked third-party app.

SECTION 5

Multi-layered QR Code Attack

Typically, in a QR code attack, a malicious QR code is directly embedded in an email. But recently, attackers have come up with a new and sophisticated variation. In these multi-layered attacks, the malicious QR code is hidden in what seems like a harmless PDF attachment.

To slow down automated detection and confuse traditional email security tools, attackers use evasion tactics like adding a CAPTCHA on the landing page. This means that tools using traditional URL reputation detection face an uphill battle in trying to identify them.

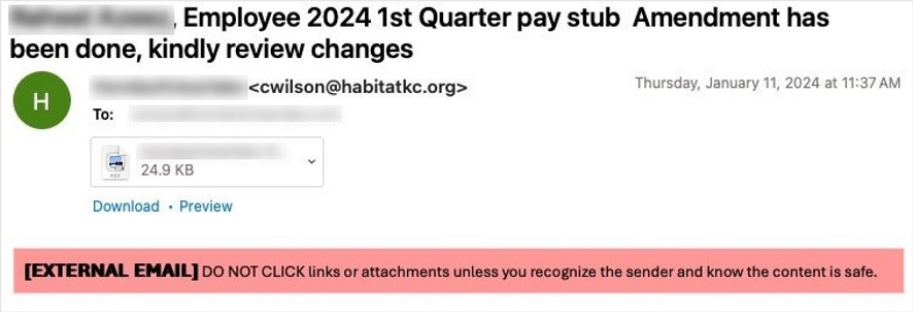
The scenario

Proofpoint recently found one of these threats as it conducted a threat assessment at a US-based automotive company with 11,000 employees. The company's incumbent security tools – an API-based email security tool and its native security – both boasted QR scanning capabilities. Yet both classified the email as clean and delivered it to the end user.

The threat: How did the attack happen?

Here's a closer look at how the attack unfolded.

1. **A deceptive lure.** The email was designed to appear legitimate, and it played on the urgency of tax season. This prompted the recipient to open an attached PDF.

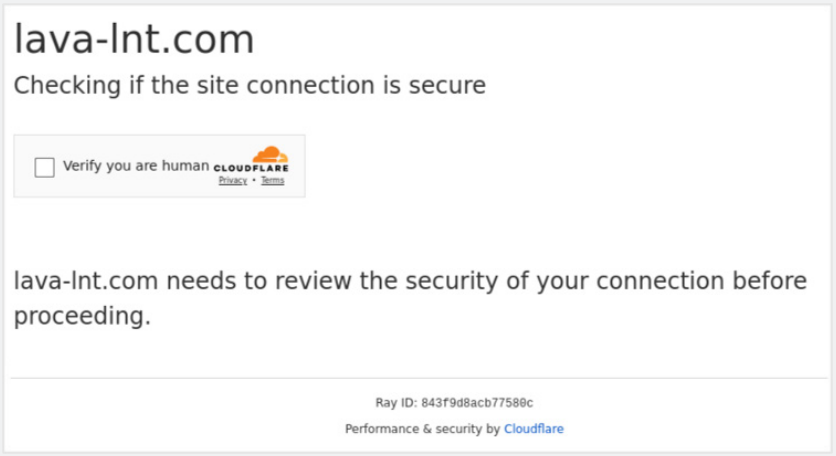


The initial email to the end user.

2. **Malicious QR code embedded in the PDF.** Unlike previous QR code attacks, the malicious URL in this attack was not directly visible in the email. Instead, it was hidden in the attached PDF. Given the ubiquity of QR codes, this might not have seemed suspicious to the recipient.

The attached PDF with the embedded QR code (obscured).

3. **Cloudflare CAPTCHA hurdle.** The attacker added another layer of deception. They used a Cloudflare CAPTCHA on the landing page from the QR code URL to further hide the underlying threat. This step aimed to bypass security detection tools that rely solely on analysing a URL's reputation.



Cloudflare CAPTCHA on the QR code URL landing page.

4. **Credential phishing endgame.** Once the CAPTCHA was solved, the malicious QR code led to a phishing landing page set up to steal user credentials. The theft of user credentials can give a malicious actor access to a user's account to spread attacks internally. Or they might use them externally to deceive partners or suppliers as with supplier email compromise attacks.

Why these threats are hard to catch

The use of optical character recognition (OCR) or other QR code scanning techniques plays a vital role in defending against QR code threats. But QR code scanning is only the mechanism that's used to extract the hidden URL. It does not act as a detection mechanism to decipher between legitimate or malicious QR codes.

Many tools, including the incumbent email security tools used by the automotive company, claim to parse QR codes and extract the URL for analysis. However, they cannot scan URLs within an embedded image in an attachment.

How Proofpoint detected this attack

Few tools have engineered the ability to use in-depth URL analysis on a scale like Proofpoint. We use QR code scanning combined with a multi-layered detection stack that uses advanced AI and ML. Because we analyse both the URL and its behaviour, we can understand the context of email messages and detect advanced URL threats that other tools can't.

Here's what we used to detect and stop this threat:

QR code scanning. Proofpoint used QR code scanning to convert images into a machine-readable format. This allowed us to extract the hidden URL for further analysis. Our QR code scanning supports PDF, email body, images, Microsoft Word files, and many others.

Behavioural indicators. Proofpoint analysed user behaviour, email context and the thematic nature of the email. And we found patterns that indicated it was very likely that the email was malicious.

URL sandboxing. With the URL extracted within a sandbox, Proofpoint can analyse visual elements, redirect patterns, endpoint processes, network activity, DNS calls and CPU and memory processes. We can detect anti-evasion tactics like CAPTCHAs as well. Even if the URL appears to be clean – despite showing behavioural indicators associated with malicious activity – we continue to monitor and scan the URL for later compromise or weaponisation.

SECTION 6

Conclusion

All of these scams are just the latest reminder of the critical need for multi-layered and robust cybersecurity measures.

To stay ahead of evolving dangers like them, you need a comprehensive approach to protecting against threats targeting your people:

- **Detect threats pre-delivery.** The only way to keep users safe is to block malicious messages before they are delivered. Proofpoint research shows that one in seven users will click on an email within one minute. Look for a tool that combines ML algorithms and advanced threat intelligence to identify and block advanced threats.
- **Educate your users.** Your employees, contractors, and partners are your first line of defence. Make sure that they get security awareness training for all types of attacks. Remind them to move fast to report any unusual account behaviours.
- **Conduct regular security audits.** Audits can help you identify any potential vulnerabilities in your environment. As part of that work, be sure to look for irregularities in your configurations and access logs.
- **Set up your system to monitor for misconfigurations.** Besides checking for misconfigurations, don't forget to enable auto-remediation. This will ensure that you detect unauthorised changes and mitigate them promptly, which will stop attackers from establishing persistence.
- **Create an incident response plan.** Map out multiple attack scenarios. Then, define how you will investigate and mitigate them. Be sure to test how effective your plan really is by conducting regular simulated exercises.

Next Steps

More than ever, it's important to protect your organisation from rising email threats. You need to take a proactive approach to keep your business, employees, and customers safe from advanced attacks like ransomware, BEC and credential phishing.

The Proofpoint Email Rapid Risk Assessment provides you with comprehensive visibility and insights into your vulnerability to attacks. It helps you discover who is being targeted by email-based threats across your organisation.

Don't wait until it's too late to test your email security. Contact Proofpoint for a free **Email Risk Assessment.**

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0503-007-02-01 08/24