PIXM

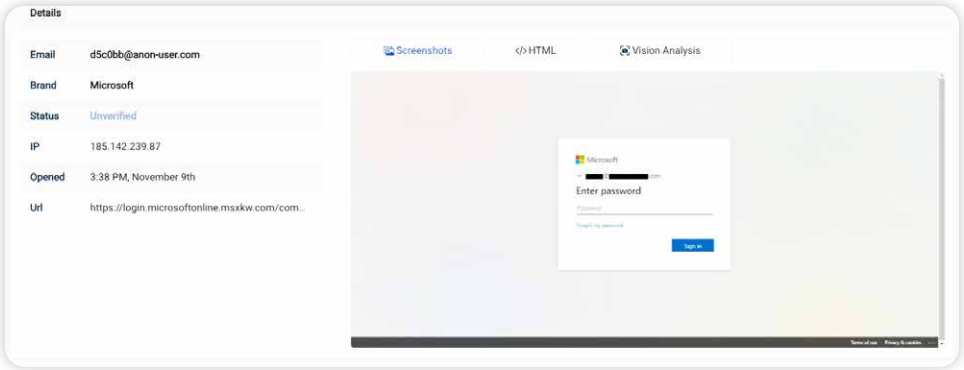
Consumer Threat Report Q4-2020

Introduction

During Q4-2020, **Pixm detected and stopped over 60 breaches** for its consumers at point of click with its AI real time browser protection. **These phishing attacks were detected after they bypassed existing security protections and after they were actually clicked by users.** This report explores Pixm's breach data to uncover common tactics hackers use to bypass corporate security protections and to target users on personal devices and social media. It further studies the consequences of campaigns that evade detection for prolonged periods.

Targeting Personal Devices and Social Media

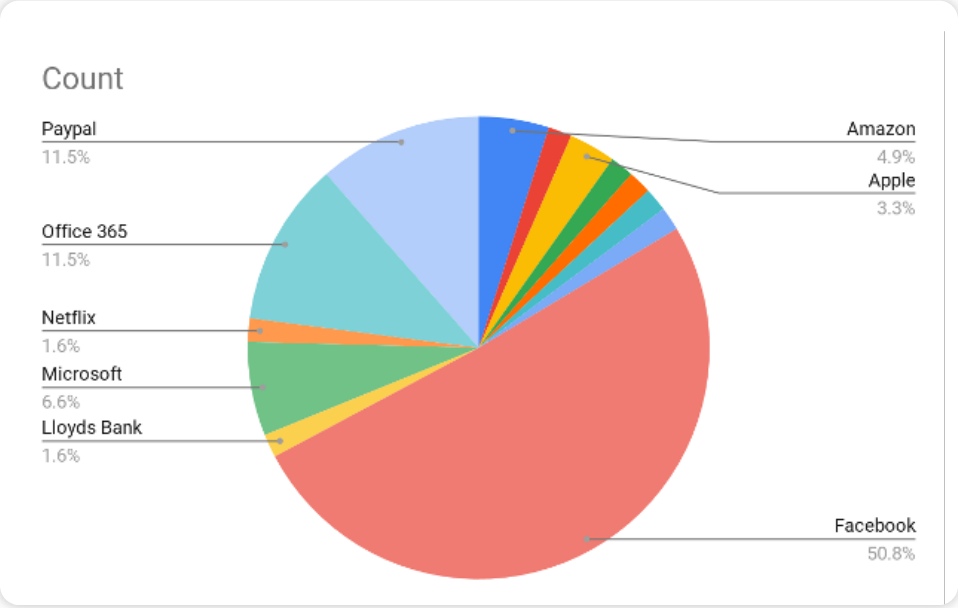
Our consumer breach data shows an alarming number of work related phishing clicks on personal devices. 18% of the breaches Pixm stopped were on Office 365 related applications. Moreover, nearly half of these exhibited spear-phishing indicators, including email addresses with corporate domains either in the URL or pre-populated in the phishing page itself. We can observe an example below that was clicked at 3:38pm ET on Nov 9th with the user information anonymized.



Industries targeted in other spear-phishing breaches Pixm prevented include pharmaceutical, aerospace, and news media among others. Instances like these confirm the high risk of corporate users accessing work email and applications on personal devices.

CONTENTS

The other key risk Pixm's breach data indicates is social media phishing. If we observe the below breakdown of phishing attacks prevented by Pixm, it's hard not to notice the predominant 51% of Facebook phishing attacks.



OVER 50%
of breaches were completely outside the scope of any corporate security protection.

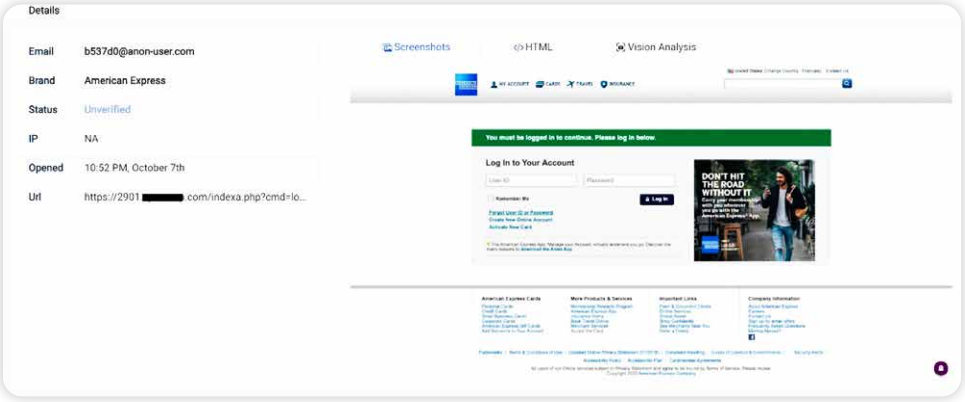
These links were delivered entirely through personal email or the Facebook platform itself. Thus, over 50% of breaches were completely outside the scope of any corporate security protection.

Stealth Tactics to Evade Protection

This section explores common tactics hackers use to evade security protections based on URL reputation or email and cloud based analysis.

"Reputation Hijack": Hackers are Compromising Reputable Websites to Target Users

To evade the plethora of reputation based security tools, hackers will first compromise a third party legitimate webpage in order to host their phishing attack. Below we can see an American Express phishing page that was clicked on October 7th at 10:52pm ET with the legitimate root domain anonymized for privacy.

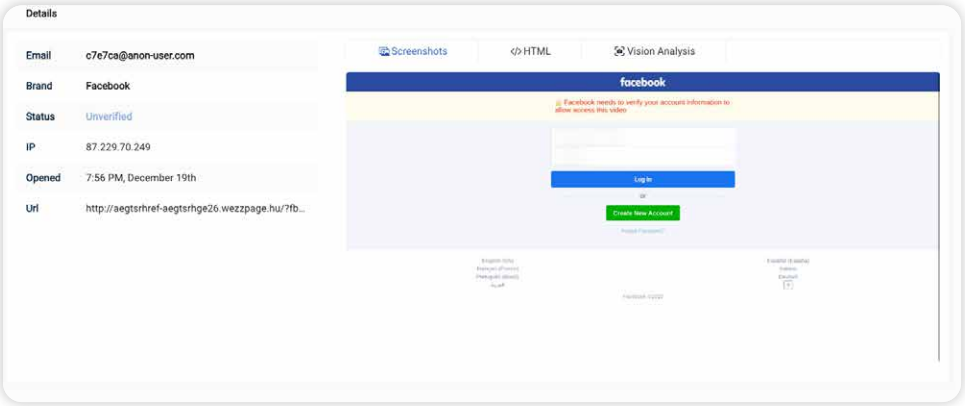


In this instance, the root domain is an accounting education website providing online CPA degrees. We can observe that the attacker deployed this phishing page on a '2901' subdomain. Pixm observed dozens of similar cases over the quarter, where hackers breached and hijacked the reputations of online service, small business, and community organization websites to deliver their attacks undetected.

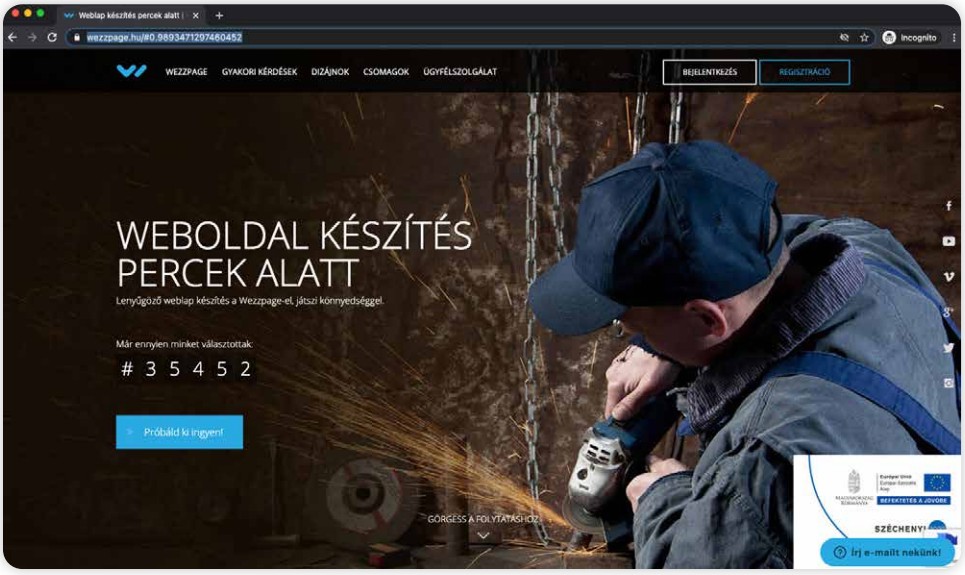
Hackers are Flying Under the Radar

Hackers can further evade Advanced Threat Protection and other email or cloud based security tools by redirecting incoming page requests depending on the request origin and time.

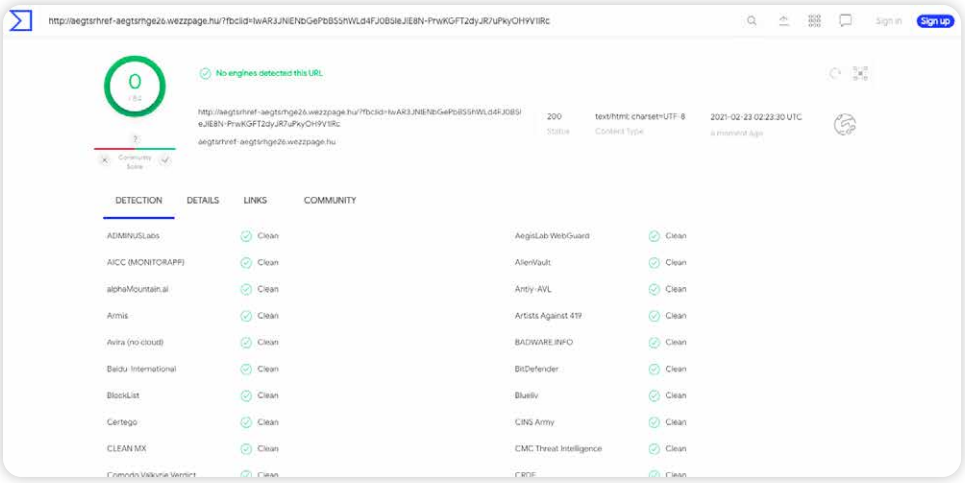
The below Facebook phishing page was clicked by a user on December 19th at 7:56pm ET.



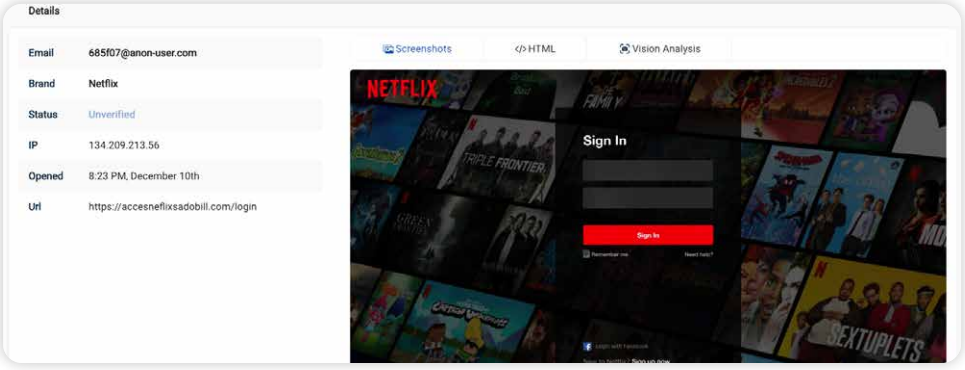
We can observe the root domain is wezzpage.hu, which is a popular Hungarian website builder. When an analyst opens the same URL in an Incognito browser an hour later, they are redirected to the webuilding domain itself.



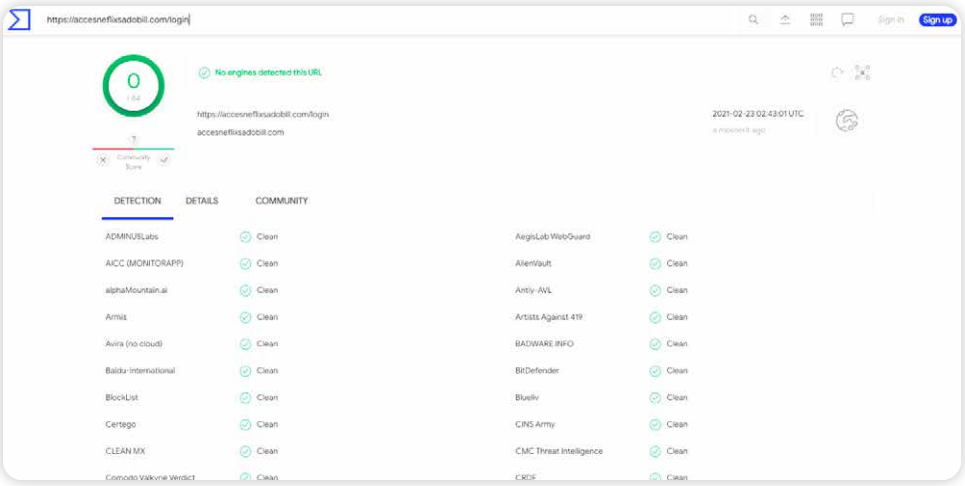
Even two months later, the same URL continues to redirect to the same location and remains unknown to 84/84 detection engines on Virus Total.



Pixm observed numerous cases of this strategic redirect, often leading to the legitimate page of the brand being phished. Below is a Netflix phishing page a user opened on December 10th.



The same analyst who opened the URL immediately following the incident was redirected to the Netflix homepage: https://netflix.com. Meanwhile, all 84/84 Virus Total engines are completely in the dark, even two months later.



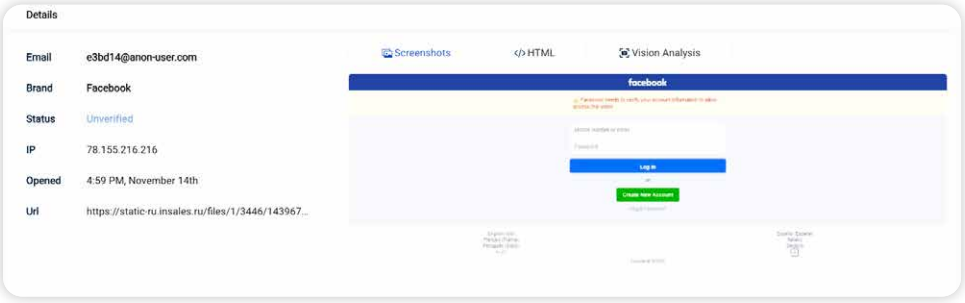
Pixm observed similar phishing redirects to the domains of the targeted brands for Microsoft, Paypal, and AT&T among others.

Featured Attack

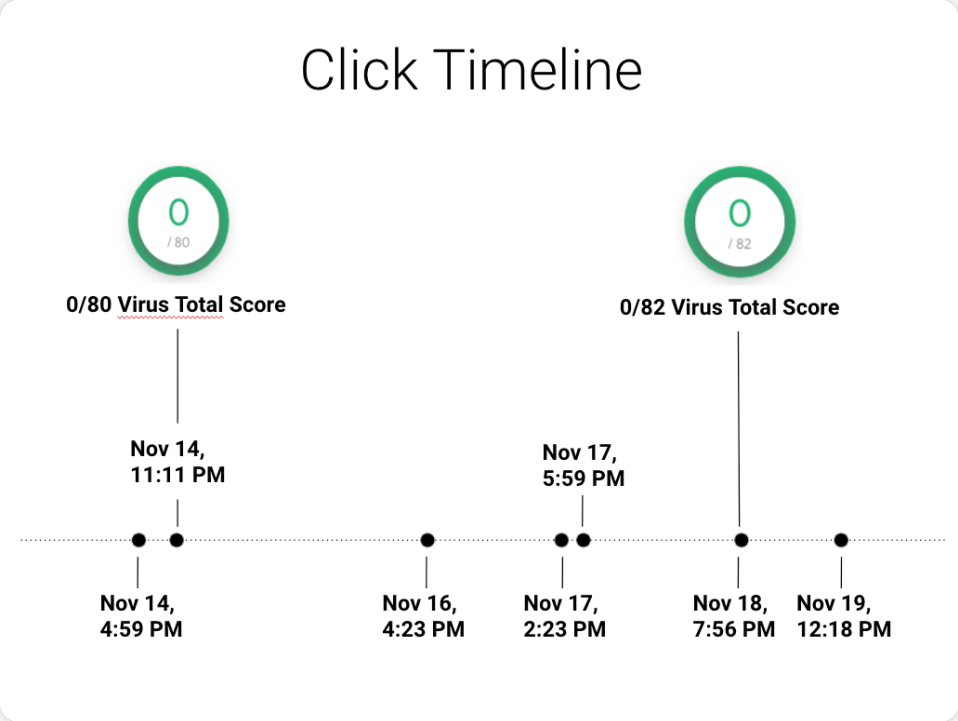
As a consequence, under the radar phishing attacks evade detection and continue to be clicked for long periods without any security stakeholders being aware.

From Russia Without Detection

Pixm initially picked up a Facebook phishing attack hosted on a Russian e-commerce domain when a user first clicked on it on November 14th at 4:59pm ET.



This same URL was clicked by a new user later that evening at 11:15pm ET. It was not only missed by Google Safe Browse. A Virus Total scan run at the time of the second click showed 80/80 detection engines marking it as clean. The same URL with a couple of path variations was clicked by five additional users over the next 4 days: on Nov 16th at 4:23pm, on Nov 17th at 2:23pm and 5:59pm, on Nov 18th at 7:56pm, and on Nov 19th at 12:18pm. An additional Virus Total scan run at the time of the Nov 18th click resulted again in the entire detection engine suite marking the URL as clean. We can observe the user click timeline below alongside the VirusTotal scans.

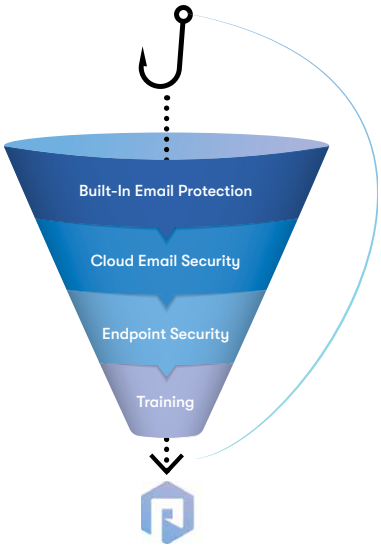


So a phishing attack hosted on a Russian server was delivered to and clicked by seven distinct users over a five day period, during which time it went entirely undiscovered by the entire VirusTotal community. Without Pixm's protection, seven users would have been at high risk of a data breach without any security authorities and stakeholders being the wiser. Pixm observed numerous similar instances where its protection stopped URLs that would have been clicked by many users over prolonged periods.

Conclusion

Pixm's breach data reveals just a few tactics hackers use to bypass various layers of corporate security funnels. It also shows a concerning amount of corporate spear phishing attacks being delivered entirely outside corporate detection on personal devices and phishing activity delivered through non-work accounts like social media.

Pixm's real-time computer-vision AI technology identified these attacks at point to click in the browser. The report reflects the statistics of these detections, which were also stopped at the same time.



FEATURED IN

CSO FROM IDG WIRED Bloomberg The Boston Globe