



Introduction

During Q4-2020, **Pixm detected and stopped over 60 breaches** for its consumers at point of click with its Al 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.

Details					
Email	d5c0bb@anon-user.com	C Screenshots	HTML	💽 Vision Analysis	
Brand	Microsoft				
Status	Unverified				
P	185.142.239.87			Monark	
Opened	3:38 PM, November 9th			te narourd	
Jel	https://login.microsoftonline.msxkw.com/com_		1	ier pasaworu.	
				Series	

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

- → Targeting Users on Personal Devices and Social Media
- → Stealth Tactics to Evade Protection
- → Featured Attack









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

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.









Email	b537d0@anon-user.com	a Screenshots	() HTML	(e) Visi	on Analysis	
Brand	American Express		Terrecont Scout	A const O service	-	providence interpretations interpretation
Status	Unverified					
IP	NA		You must be logged in to	continue. Please log in bei	0W.	
Opened	10:52 PM, October 7th		Log In to Your Acco	unt Passed	DON'T	HT BIL
Url	https://2901 , com/indexa.php?cmd=lo		Ramoritan po Employees da facement Conservation Annual Annualy New Card Vita Annualy Card Vita Annualy Card			
			American Express Cards	New Products & Sections Review on Travel	Provided Lines	Company Information Accus Generation Teaching
			Particular Carlo Constitution (Design Representation of Constitution Carlos Antonian Carlos (1997 Lands Antonian Carlos (1997 Lands Antonian Carlos (1997 Lands	Research Constantion Research Constantion Research Constantion Research Constantion Research Constantion	Broad Agents Broad Contribution Sees Mitty Party Name Tra- Distance (Contribu-	The set of a second set for the set of the set of the set for the set of the set of the set of the Kinema Marianity

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.

Indi	c7e7ca@anon-user.com	Creenshots CHTML Revision Analysis
Brand	Facebook	facebook
status	Unverified	 Received, terents to write your account information to allow access this video
Р	87.229.70.249	
pened	7:56 PM, December 19th	Logier
Iri	http://aegtsrhref-aegtsrhge26.wezzpage.hu/?fb	Chiefe New Alcount
		(Annual Ageneration)
		Found 1 and 1 Found 1 and 1 Found 1 And 1 Found 1 And 1 Found 1 Found 1 Found 1 Found 1 Found 1 Found 1
		num 122

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.

nttp:	segtsthref-aegtstrige26.wezzpage.hui?fbclid=lwAR3JNENbGePbBS5nWLd4FJ0BSleJE8N-PrvwKGFT2dyJR/uPkyOHYVIRc					Q 🛎 🖁	😫 🖵 Sign in 🤇
	0	o engines detected this URL					C 26
	intp://w e.JIEBN	egtschref-aegtschge26.wezzp PrwKGFT2dyJR7uPkyOH9V1	age hui??fbclid-lwAR3JNENbGePb8SshWLd4FJ08Sl Rc	200 Stillie	text/html: charset=UTF-6 Coolerst Table	2021-02-23 02:23:30 UTC	ŝ
	2 aegtari X. Commune V	vef-aegtirfige26.wezzpage.h	4				
	DETECTION DETAILS	LINKS COMM	UNITY				
	ADMINUSLabs	🕗 Clean	Ac	igisLab WebGuard	🕗 Clean		
	AICC (MONITORAPP)	Clean	Al	enVault	🕗 Clean		
	alphoMountain.al	💮 Clean	Αr	itiy AVL	📀 Clean		
	Armis	Clean	Ar	tists Against 419	🕢 Clean		
	Avira (no cloud)	Clean	B/	DWAREINFO	🧭 Clean		
	Beidu International	Clean	Bit	Defender.	🕗 Clean		
	DiockList	 Clean 	DA	atifiv	🕗 Clean		
	Certego	Clean	0	NS Army	🕗 Clean		
	CLEAN MX	 Clean 	C	MC Threat Intellige	nce 🥥 Clean		
	Comordia Valkunia Ventrict	C Dean		RDF.	Cieno		

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.

Details					
Email	685f07@anon-user.com	Screenshots	HTML	Vision Analysis	
Brand	Netflix	NETFLIX	Rid 1	C T SHUMPY	(A second se
Status	Unverified				and the second
IP	134.209.213.56	Antonia Antonia Antonia	Bold 1	Bign In	Comment of the second
Opened	8:23 PM, December 10th		E FRONTIER,		1 20- 7
Url	https://accesneflixsadobill.com/login	Sel games	Ten		1822120 78
		and the second s	1159	Sign in Next fail?	
					Part Rac
		Carrier	the Inc		121638
			× /0,	Stature with susanian	SEXTUPIET
					COLUMN TO A DE LA COLUMNT TO A DE LA COLUMNTA A DE LA COL





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.

https://accesneflixsadobiil.com/login				9. ± #	🛛 🖓 Sanin Sanup
0	No engines detected this URL				0.2
1 de 19	itps://accesnefflasadobill.com/login .ccesnefflix5adobill.com		20	021-02-23 02:43:01 UTC moonerit ago	G
DETECTION DET	ALS COMMUNITY				
ADMINUSLabs	Clean	AegisLob WebGuard	🕑 Clean		
AICC (MONITORAPP)	Clean	AllenVault	🧭 Clean		
alphaMountain.al	() Clean	Antly-AVL	🕑 Clean		
Amis	🚫 Clean	Artists Against 419	🕢 Clean		
Avira (no cloud)	🕗 Clean	BADWAREINFO	⊘ Clean		
Baldu International	 Cinan 	BitDefender	Clean		
BlockUst	🕑 Clean	Blueliv	💮 Cléan		
Certego	Clean	CINS Army	Clean		
CLEAN MX	Olean	CMC Threat Intelligence	🧭 Clean		
Comodo Valkyne Wirdict	Clean	CRDF	Ciean		

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.

Details					
Email	e3bd14@anon-user.com	C Screenshots	HTML	🕫 Vision Analysis	
Brand	Facebook	10 		facebook	
Status	Unverified		-	And and the set of the	
IP	78.155.216.216				
Opened	4:59 PM, November 14th				
Uri	https://static-ru insales.ru/files/1/3446/143967,			Charles have Account	
			Alexandreau Maria a Maria		Darie Lawe Main Jagon
				(marked (9)00)	







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

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



WIRED

Bloomberg

The Boston Blobe

