First published on https://www.chadhatala.com

Social Spear-Phishing: The Weaponization of Social Media Against Midsize Businesses

Chad Hatala
Certified Professional Cybersecurity Analyst, North America

Abstract

In Michael Bosetta's 2018 Report, "The Weaponization of Social Media: Spear Phishing and Cyber Attacks on Democracy," Bosetta presents a grim picture of the near-term future concerning the use of social media as an attack vector. In Bosetta's essay, he outlines a model for spear phishing on social media such as Facebook or LinkedIn.

In the model, Bosetta describes the techniques used by threat actors to leverage social platforms to connect and identify organizational relationships both inside and outside a potential target, including family members and friends. These methods directly result in highly coordinated and sophisticated spear-phishing attacks, which was empirically supported by examples from Great Britain, France, Germany, and the United States.

This study will examine how smaller criminal organizations have adopted the techniques used by both Russian and Chinese threat actors to penetrate spheres of influence within Facebook to gain intelligence on potential targets and those around them.(2)(3) This study will also examine how this method can be leveraged to ransom social media accounts, use them as platforms for malware distribution, or highly-targeted spear-phishing campaigns. The model here is supported empirically with examples from the United States and Australia.

Introduction

"Social spear-phishing" allows threat actors to create specific phishing campaigns tailored to exploit a high-value target's sphere of influence within social media platforms. These spheres of influence often overlap business owners' connections, personal relationships, customer groups, and more. In some cases, threat actors may appear as friends of friends reaching out to make a connection, while other malicious actors might appear to be upset customers posting on business pages.

These types of data-gathering and reconnaissance operations, first observed in use by nation-states— have become popular among cybercriminals of all backgrounds. The accessibility and availability of prepaid phones with swappable SIM cards allow cyber criminals to move quickly between devices and accounts when conducting attacks.

The Social Spear-Phishing Model

Figure 1: Bosetta's Model for Social Spear-Phishing

Collect	Construct	Contact	Compromise	Contagion
Discovery	*Credentials*	*Connect*	*Credentials*	*Virality*
Reconnaissance	*Photos*	*Chat*	*Malware*	*Scaling up*
	Profile Metrics	*Micro-target*	*Hijack*	

Bosetta's model consists of five phases: Collect, Construct, Contact, Compromise, and Contagion.
Source: Michael Bosetta, "The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy"

Understanding Movement in the Model

Bosetta explains in his research: "Social media platforms offer a wealth of publicly available data, and these data can be exploited to then construct fake accounts that appeal to the target's personal or professional interests. Using these accounts, attackers contact targets through any variety of communicative modes enabled by the platform, ranging from friend requests to direct messages to targeted advertisement campaigns. Depending on the attacker's intentions, the target may be tricked into revealing information or clicking a link that compromises the target's account or device. If successful, the attack can then induce a contagion effect, magnifying its scope and putting others at risk."*(1)*

The ability of attackers to move quickly through the model can blindside small to midsize businesses that have not yet adopted cybersecurity compliance or other practices like Multi-factor Authentication and Two-factor Authentication, access control, and related safeguards.

When a platform breach occurs due to poor account handling practices—such as a lack of onboarding or transfer protocol, disabled authentication safeguards, or the use of personal accounts—PR nightmares are just around the corner. As some small business owners have experienced, this can mean criminals acting on behalf of your company, or re-directing advertising dollars. The data and access provided through such social platforms can bring small businesses to a halt, especially if they rely solely or largely on social media platforms to do business.

Ramello Barnes, a small business owner in North America was quoted as saying, "He's (sic) making people think I'm stealing money," Barnes said. "It literally had put a damper on my life, social media, to the point I was panicking. This dude is killing my career."*(4).* In this instance, the small business owner turned to platform security for help but was denied. Unsure how else to recover his accounts, he ultimately did the one thing that security experts and law enforcement recommend not to do: He paid a ransom. "When I got the page back, I was able to see all the messages that he had," Barnes said. "When I tell you he was doing damage, there were so many

people talking to 'me' and I was like, wow." *(4)* Barnes' experience is far from unique: In the 2021 Verizon Wireless Data Breach Investigations Report, for instance, infrastructure auditor StrongDM found that forty-six percent of all cyber breaches impact businesses with fewer than 1,000 employees. *(7)* While not all attacks hit their targets, attackers are more commonly seeking out smaller organizations with more advanced malware and phishing campaigns. Additionally, thirty-seven percent of companies hit had fewer than 100 employees. *(7)*

These smaller businesses are often exploited with simple RDP compromises via a system administrator. While this may not always be the case with hacking social media platforms, the real issue arises due to a lack of updated training.

(replacement for "while this"): While social media hacking may have more limited consequences than ransoms or major reputational damage, the broader issue remains that rapid-paced technological development continues to outpace most small businesses' abilities to adapt to new protocols and recognize emergent threats.

Digital Marketing Agencies and "Consent Phishing"

While phishing attacks account for most compromises, businesses belonging to social platforms with advertising capabilities, or the ability to manage other clients' budgets are also becoming increasingly popular. These accounts are often lucrative for attackers looking to exploit the deliverability of the advertising platform as another attack vector. *(5)*

Smaller, less-equipped teams are increasingly susceptible to social phishing. This can be especially true if you are a digital agency. As one business owner found out in December 2021: "First, the hacker somehow gained access to my account through my mobile phone. I reset and password protected all of my smart devices. I'm still uncertain as to how they were able to get past the two-factor verification, but they did."*(6)*

I The most likely explanation is the result of a practice known as consent phishing. While the average user may easily spot a phony account sending a friend request or share requests, those who run digital agencies must always delegate and request access to multiple pages for multiple brands. This can be especially difficult if users are on a mobile device.

When consent phishing, the attacker appears to be a legitimate application, SMS, or email messaging the victim to request page access. This type of authentication abuse is not new, but has gained traction in recent years.*(9)* More recent hacks at Rockstar and Uber allegedly originated from a member of the Lapsus$ group, whose preferred method of gaining access relied heavily on this technique. *(8)*

Conclusion

When considering how many small and midsize businesses are unprepared and untrained for such a breach, social media presents a gaping vulnerability in most business models, including the explosion of growth in cloud-based services. While insiders remain the number one threat in any organization, the success of such attacks can be directly related to the size of the organization itself.

Additionally, with the impact of the COVID-19 pandemic, rapidly changing markets, and supply chains; small businesses with unprepared, stressed workforces are becoming increasingly profitable for cybercriminals. Given that the cost of a breach is always on the rise, a single breach is all it takes to permanently alter a small business's trajectory, leaving financial and reputational damage in its wake.. ▽

Chad Hatala *is a Professional Cybersecurity Analyst & Researcher. His research often covers vulnerabilities, threats and Russian-speaking hacking groups. He has 7 years experience as a Director of Information Security at a midsize business that specializes in B2B and B2C e-commerce solutions and 10 years experience as a cybersecurity consultant.*

References

1 Michael Bosetta, "The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy," Journal of International Affairs, Columbia University Sept, 20, 2018.
https://jia.sipa.columbia.edu/weaponization-social-media-spear-phishing-and-cyberattacks-democracy

2 Ian Drury and David Williams, "Foreign Spies on LinkedIn trying to Recruit Civil Servants by 'Befriending' them before Stealing British Secrets," Daily Mail, 9 August 2015.
https://www.dailymail.co.uk/news/article-3191733/Foreign-spies-LinkedIn-trying-recruit-civil-servants-befriending-stealing-British-secrets.html

3 Joseph Menn, "Exclusive: Russia used Facebook to Try to Spy on Macron Campaign – Sources," Reuters, 27 July 2017.
https://sg.news.yahoo.com/exclusive-russia-used-facebook-try-spy-macron-campaign-050414445--finance.html

4 Knowles, J., & Pistone, A. (2022, May 30). *Small business owners' Facebook pages hacked, then locked out of accounts*. ABC7 Chicago. https://abc7chicago.com/locked-out-of-facebook-account-ads-help/11909341/

5 McPherson, E. (2021, November 25). Facebook hackers target small business owners to scam money for ads. *9News*.
https://www.9news.com.au/national/facebook-hackers-target-small-business-owners-buy-up-ads-in-spending-spree/06a789e5-3085-4872-93da-6073dba30406

6 Samuel, K. (2022, March 22). What I learned from being targeted by A sophisticated facebook hack. *Forbes*.
https://www.forbes.com/sites/forbesagencycouncil/2022/03/22/what-i-learned-from-being-targeted-by-a-sophisticated-facebook-hack/?sh=52504e4f3623

7 Rahmonbek, K. (2022, October 18) "35 Alarming Small Business Cybersecurity Statistics in 2022". *StrongDM*.
www.strongdm.com/blog/small-business-cyber-security-statistics#small-business-cybersecurity-overview. Accessed 21 Oct. 2022.

8 Powell, Olivia. (2022, October 13) "IOTW: Hacker Allegedly Hits Both Uber and Rockstar." Cyber Security Hub,
https://www.cshub.com/attacks/news/iotw-hacker-allegedly-hits-both-uber-and-rockstar

9 Microsoft 365 Defender Threat Intelligence Team. (2022, September 23) "Malicious Oauth Applications Abuse Cloud Email Services to Spread Spam." Microsoft Security Blog,
https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-oauth-applications-used-to-compromise-email-servers-and-spread-spam/