Know Your Attack Surface From the Outside In

A SANS First Look

Written by **Jeff Lomas** | August 2022

Introduction

Social engineering is a significant, yet still unaddressed, attack vector facing security teams today. Organizations seek to defend themselves and their critical assets with a wide variety of solutions, most of which are intended to train employees to spot attacks, and seek to limit risks in hybrid infrastructures and endpoints. These efforts have been largely successful at stopping infrastructure-based attacks, but they have done little to stop the rising tide of social engineering attacks that lead to ransomware, theft of intellectual property, and financial losses from business email compromise (BEC) scams, to name a few.

Although traditional solutions adequately address technology needs, they do not prevent threat actors from using open source intelligence (OSINT) to target employees through phone calls, emails, and in-person visits. Additionally, traditional cyber defenses have little sense of each employee's OSINT footprint, and employees have limited involvement in a company's cybersecurity program.

How Threat Actors Use OSINT to Power Social Engineering Campaigns

Defending against the modern-day threat actor can be difficult because the outside attack surface of many organizations constantly leaks information through breach data, social media posts, and various public databases containing employee personal identifying information. Attackers are aware of these opportunities and need to find only one instance of an employee reusing passwords on another site or discover the inner workings of an organization using context gained online. While the risks are low for an attacker to perform passive reconnaissance on employees, the reward is extremely high. IC3, a criminal database maintained by the FBI for reporting cybercrimes, recently documented that attackers pulled in $4 billion in 2020 from crimes such as BEC and ransomware. Taking advantage of openly available intelligence is a profitable business for threat actors, and they have devised tactics to achieve maximum efficiency.

How to Prevent OSINT Use

To prevent threat actors from using OSINT to socially engineer employees, an organization must know how threat actors evaluate available OSINT outside the firewall. When leveraging OSINT to defend against social engineering attacks, organizations face three expensive and time-intensive tasks:

- Gathering quality data from employees
- Analyzing vast quantities of OSINT to identify relevant paths to attack and compromise
- Neutralizing employee and company data found in online sources

Completing these tasks requires OSINT analysts to curate and analyze relevant data, then develop and manage a program that monitors company and employee online footprints. Such an analysis of any single employee would take a skilled human analyst, on average, one full workday to find reliable sources on the internet from which to collect relevant employee data, gather it, take steps to avoid attribution to the research effort itself, and analyze this data to ensure accuracy. (The job of *removing* employee personal data, also a time-consuming and meticulous process, remains with the individual employee, who must take the required action on their own time.)

SANS took a First Look at Picnic's solution for streamlining these manual processes. The platform empowers both enterprise security users and employees to know about and manage exposed OSINT, which in turn provides Picnic with a rich dataset that can be used by organizations to view and manage individual as well as organizational risk from one dashboard.

The First Look

Picnic's platform consists of two applications that work together: Command Center and CheckUp. These two applications work together to automatically and continuously identify and neutralize OSINT used by threat actors to power their social engineering attacks.

Command Center

As shown in Figure 1, Command Center shows OSINT exposures and provides direction about problem areas that need attention. The capability to filter on the most urgent exposures is easily one of Picnic's best features, because attackers view these as the most easily exploitable targets. By using Picnic's filters to identify and remediate an attacker's easiest targets in an automated fashion, an organization can remove target data before an attacker has a chance to find it.

Figure 1. Command Center

To protect employees further, Command Center does not allow administrators to view the personal identifiable information the employee provides through CheckUp (covered in the next section). Because Picnic is a SaaS solution, there is also no need to manage sensitive employee data on-premises. All things considered, the data gathered by Picnic is freely available on the internet by nature, so this extra step to maintain individual privacy is a novel (and welcome) solution to maintaining the confidentiality of employee data.

CheckUp

Picnic provides employees with a portal called CheckUp, which is accessible via a mobile app with the employees' current company information pre-populated (see Figure 2). Using this portal, employees can see how their personal identifying information and work-related accounts expose them and the company they work for to risk. When the average person discovers how many places their personal identifying information can be found, they are not only shocked but also motivated to take action against further exposure. For this reason, employee engagement is built into Picnic's ecosystem: Employees can manage and add their data to the Picnic platform for the purposes of monitoring and removal.

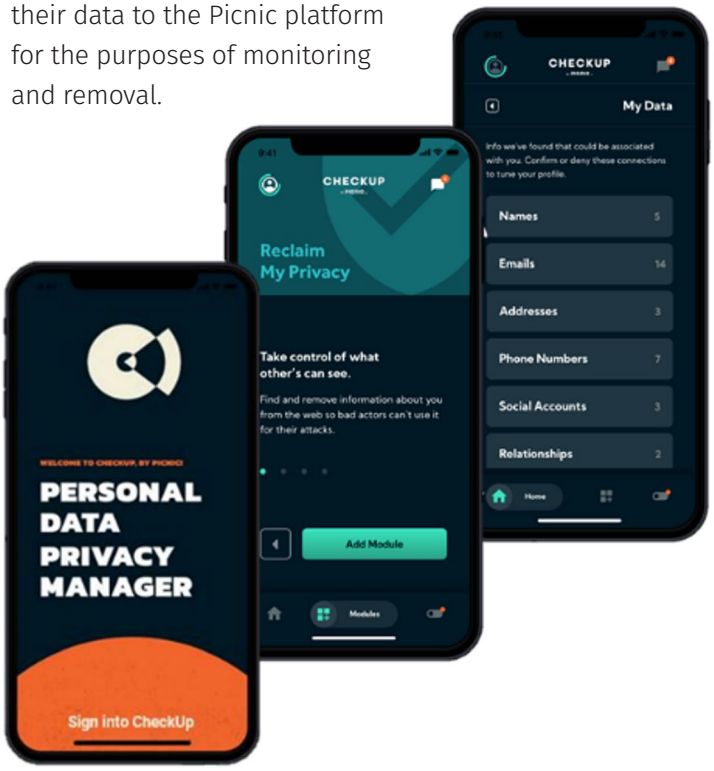

Figure 2. CheckUp

Onboarding employees through CheckUp requires only the employee's name and company email address to begin populating data. Employees can quickly see their data that is exposed to the public and the actions Picnic is taking to remove the data for them. The more data an employee provides to CheckUp, the more ways Picnic suggests to secure their online exposure.

As trust builds, employees can add more personal information for monitoring, which benefits the employee and organically builds a robust OSINT fingerprint that is fed into Command Center.

Conclusion

The use cases for Picnic's customized datasets are limited only by the imagination of the security team leveraging them. Blue teams can reduce the time it takes to find exposed employee credentials and common missteps such as password reuse. Red teams can use this same data to mimic a malicious actor's tactics, techniques, and procedures on a specified target using their OSINT footprints. Cyber awareness programs can engage employees based on their specific risks rather than the standard one-size-fits-all training regimen.

Matching Picnic's capabilities of data collection, analysis, and remediation would require several manual processes performed by various highly skilled individuals. Picnic's unique approach enhances protections for existing corporate controls and extends security to layers beyond the firewall to the root of where social engineering attacks begin. Just as attackers rely on the human element to steal sensitive information, Picnic uses it to improve an organization's overall security posture.

SANS would like to thank this paper's sponsor: PICNIC™