PerksConnect Attack Simulation Campaign

South Carolina Department of Employment and Workforce

Ali Jamil & Kyra Bethea

February 23rd, 2023

Overview

On February 16th 2023, security analysts Ali Jamil and Kyra Bethea launched the first SCDEW agency wide campaign to its 653 employees. The purpose of the simulation was to aid employees in recognizing, avoiding and reporting potentially suspicious emails. Just one compromised user can be detrimental to an organization. In August 2012, one Department of Revenue employee clicked on a malicious link triggering malware and allowing intrusion into DOR's database. The delivery platform for the campaign was "link to malware" based where recipients received an automatically downloaded attachment stating that they've been phished upon clicking.

Procedure

The spoofed email appeared to have been sent from SCDEW HR Director Katie Herrmann, announcing that the agency will be participating in an employee discount program with PerksCard (*Figure 2*). The program offer stated that for $5 a month state employees could save on everyday purchases from vendors. Information on both, Katie Herrmann's prestige within the agency and a legitimate PerksCard program from the Department of Admin were all public, and could be obtained with ease through little research. Coming from the perspective of an external threat actor, all information that was spoofed is easily accessible, via DEW's blogs and other agency websites.

Cost Analysis

How much does ONE user compromised email cost the agency? Considering the Security Operations Center (SOC) team consists of 15 analysts that work for $15/h, one compromised user would halt all further security operations. Any tickets, potential security risks and website categories needing to be reviewed would be halted, all man hours requiring the 15 analysts to collaborate. An incident of this scale would halt business operations. Say, if it took analysts 6 hours to remediate 20 accounts, it would take 46.2 hours to remediate all 154 compromised accounts. This would cost $10,395 solely compensating the security team for the time spent resolving accounts.

Results

The attack simulation campaign was successfully delivered to 1,663 recipients, of which 154 or 9.26% users were compromised (*Figure 1*). Due to a forthcoming holiday, the campaign lasted seven days. The timeframe was provided to give those that may have been out of office time to participate. There were 1,663 personnel in the target audience in the DEW agency including admin, contractor and noreply accounts. Of the 1,663 recipients, 154 employees clicked on the malicious link and 123 forwarded the email to the SOC to report as a phishing attempt. The rest of the recipients either deleted or disregarded the email. The rate of compromise was 9.26%. The rate of reporting to the SOC for the email was 7.3%. A possible way to raise awareness would be including training for those that clicked on the link. Microsoft Defender offers it, allowing users to gain some insight on what to look for.Throughout crafting

the simulation, it was agreed that training would not be required. Overall, the SCDEW employees are now more vigilant than ever that one click could prove detrimental to the agency.

Figure 1 - Results overview

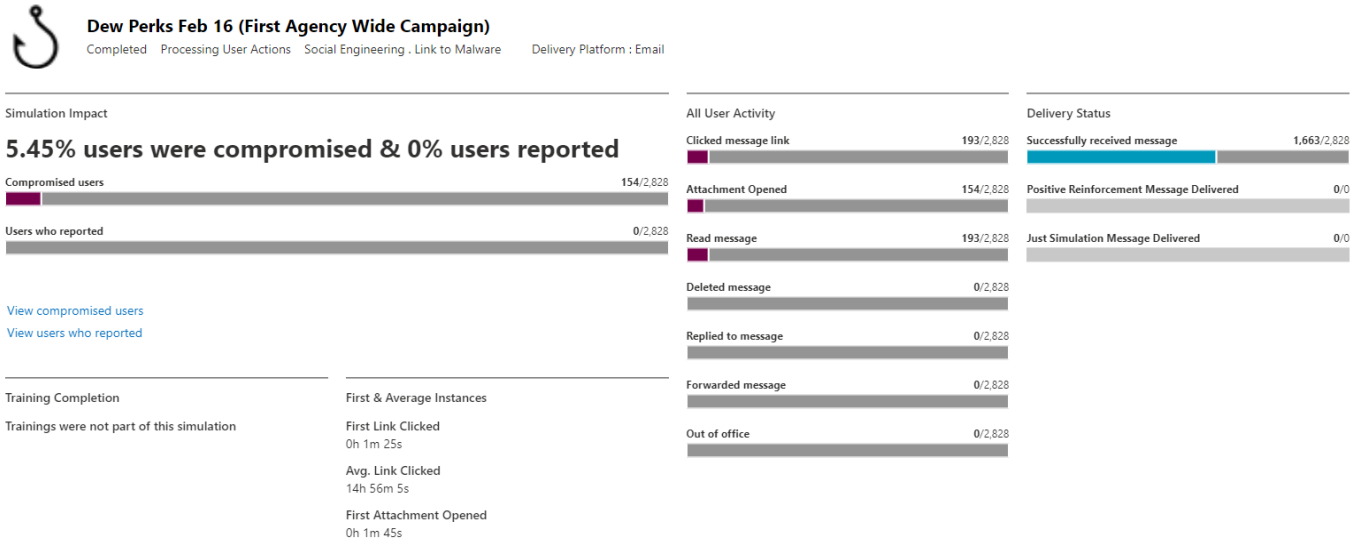

Figure 2 - Phishing email

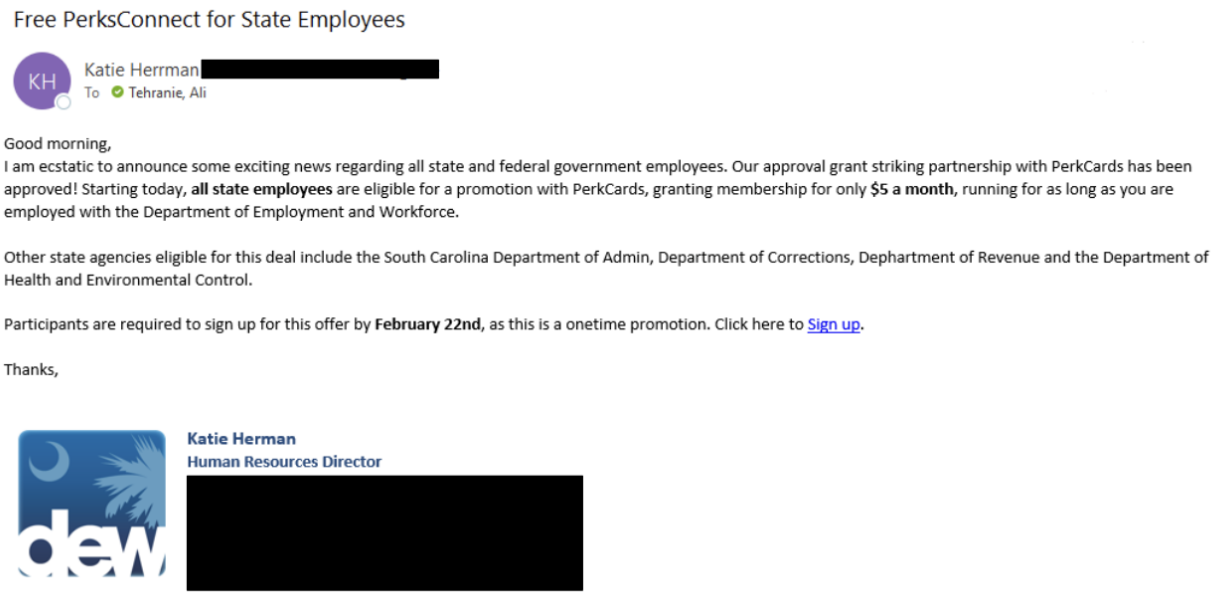

Figure 3 - Reported phishing email