Saint Paul Public Schools

Independent School District 625
360 Colborne Street
Saint Paul, MN 55102-3299

Phone: 651-767-8100 • website: www.spps.org

Saint Paul Public Schools—2023 Information Security Incident Investigation Report

Date: November 06, 2023

Introduction

This investigation report has been prepared by Saint Paul Public Schools (SPPS). The contents are based on investigations conducted by SPPS, Unit 42 by Palo Alto Networks, Inc. ("Unit 42"), and Raytheon Technologies ("Raytheon").

Facts

On or about February 13, 2023, SPPS learned from law enforcement that it was possible that several SPPS-issued email addresses may have been illegally obtained. Specifically, SPPS learned that the Federal Bureau of Investigation ("FBI") and the Minnesota Department of Public Safety ("DPS") believed that a third party had the intent to sell several students' SPPS-issued email addresses. The actor stated that they had acquired information from SPPS's servers and was willing to sell all of that information online.

Between February 13, 2023 and March 2023, SPPS performed the following actions:

- Requested a copy of allegedly exposed directory list of student SPPS-issued email addresses. None of the organizations assisting SPPS at that time was able to provide the directory list.
- Attempted to recreate an export of our Google Workspace Directory. The attempt was unsuccessful.
- Met with Raytheon on a weekly basis to review any concerns; however, nothing unusual was reported by Raytheon.

In March 2023, SPPS formally engaged Raytheon to conduct a forensic investigation to determine if there was any concrete evidence of potential data exfiltration. As explained in further detail below, Raytheon found no concrete evidence of potential data exfiltration as of the time of its investigation. However, the FBI and DPS provided SPPS with a screenshot depicting that a limited number of SPPS-issued email addresses were posted online.

In May 2023, SPPS provided notice of this incident to the families of those few students whose SPPS-email addresses were believed to have been posted online.

On July 17, 2023, SPPS received information from an interested community member indicating that an unknown individual online claimed responsibility for releasing the names and SPPS-issued email addresses. In reviewing the link provided by the interested community member, the alleged perpetrator claims that SPPS "suffered a data breach that exposed over 105,849 customer records. The exposed data included email addresses, and Full Names." Within that page was a link to a list of staff and student names and SPPS-issued email addresses.[1] SPPS does not have any information indicating that any information about SPPS students or staff was released aside from names and SPPS-issued email addresses.

On July 20, 2023, SPPS engaged Unit 42 to assess the feasibility of exporting a directory listing of SPPS's Google Workspace Directory given student-level permissions. Unit 42 also performed research related to the actor that appeared to have posted the directory listing online. As explained in further detail below, Unit 42 determined that a directory listing could have been successfully obtained via at least two methods by someone with student-level permissions.

Unit 42 also reviewed a website post made on or about May 29, 2023 by a user claiming responsibility for an incident involving the publication of names and SPPS email addresses.

As part of its investigation, SPPS has also coordinated with the FBI, DPS, and Minnesota IT Services ("MNIT"). In August 2023, SPPS learned that the actor who had posted the staff and student names and SPPS-issued email addresses online had been identified, was not an SPPS student, and a law enforcement investigation was ongoing.

Approach

Raytheon was engaged to perform a forensic investigation to determine if there was any concrete evidence of potential data exfiltration.

Raytheon Technologies reviewed a post mentioning SPPS from Dark Web sources, however nothing in the post threatened SPPS, nor appeared to relate to anything malicious. Nothing related to SPPS and the Dark Web (such as data dumps, usernames, emails for sale, etc.) at the time of Raytheon's analysis was found. SPPS also engaged Unit 42, and SPPS provisioned an account for Unit 42 with student-level permissions. Unit 42 attempted to use several publicly-available tools to obtain a directory listing with the credentials for this account. Unit 42 was unable to successfully obtain a directory listing using several freely available tools which they tested. However, Unit 42 did determine that a directory listing could be obtained via at least two methods.

[1] Staff names and SPPS-issued email addresses are public data. *See* Minn. Stat. § 13.43.

Conclusions

On or about February 13, 2023, SPPS learned that the FBI and DPS believed that a third party had the intent to sell several students' SPPS-issued email addresses.

Investigations by SPPS, Raytheon, and Unit 42 revealed no evidence that SPPS servers were compromised, but rather that student level permissions were used by an actor to access SPPS' Google Workspace Directory and to post the directory listing online.

SPPS is not aware of any evidence that information about SPPS students or staff was released aside from names and SPPS-issued email addresses.