W-2 Wage and Tax Statement Phishing Attacks in the Wild

Current Assessment Date: Friday, 18 March 2016 17:00 GMT

Executive Summary:

A pattern of successful phishing attacks against organizations across multiple industries has occurred within the last month targeting finance or human resources personnel. In recently documented attacks, successful phishing emails were made to look like C-suite executives sent them. These phishing attacks are designed to elicit improper release of a company's employee Wage and Tax Statements for 2015 to unauthorized third parties with the intent to file fraudulent Federal and State tax refund requests. Form W-2s contain sensitive personal information to include Names, Addresses, Social Security numbers, and salary information.

Details:

On Wednesday, February 24, 2016, Alaskan telecommunications company, *GCI,* was targeted by a phishing attack purportedly sent by the Chief Financial Officer. The email requested "employee payroll information, specifically copies of the W-2 Wage and Tax Statement forms for everyone who worked for GCI during calendar year 2015." All GCI, Denali Media, UUI and Unicom employees paid in 2015, approximately 2,500, were affected.

Social media company, *Snapchat*, was targeted on Friday, February 26, 2016, by a phishing email impersonating the Chief Executive Officer, Evan Spiegel. That email targeted the payroll department and requested employee payroll information. It was not recognized to be a fraudulent request and targeted personnel disclosed payroll information on current and former employees to a malicious third-party.

Seagate Technology learned Tuesday, March 1, 2016, that the "2015 W-2 tax form information for current and former U.S.-based employees was sent to an unauthorized third party in response to the phishing email scam," according to the company spokesman. After receiving an email appearing to have been sent by Seagate CEO, Stephen Luczo, requesting 2015 W-2 data for current and former employees, a Seagate employee sent that information to an outside email address. Seagate did not disclose how many employees were affected, but put the number under 10,000.

Environment Resources Management, or *ERM,* was also the target of a successful phishing attack on Monday, February 29, 2016, in which a targeted employee received a spoofed email purportedly from a member of the company's senior management team. That employee released PDF versions of the company's Form W-2s for employees formerly within EMR's Northern Division.

Details:
(continued)

In a similar incident, *Mansueto Ventures*, publisher of *Inc*. and *Fast Company* magazines, was the victim of a breach that exposed employees' wages and Social Security numbers to attackers. According to reports, that information has already been used to fraudulently file federal and state tax returns.

Notably, the Internal Revenue Service recently discontinued the ability to retrieve Identity Protection Pins (IP PIN) via its website due to heightened security concerns after the feature was demonstrated to be used by malicious actors to hijack tax refunds or file false refund requests. Users were able to retrieve their IP PIN by answering questions generally associated with consumer credit bureaus. The likelihood of compromise by an attacker could be substantially increased when utilizing stolen W-2 data.

Recommendations:

Alvarez & Marsal recommends personnel with access to sensitive employment and payroll data receive immediate notice of the highlighted phishing attacks along with supplemental training to guard against social engineering. Relevant employees should demonstrate heightened vigilance, scrutinizing and verifying all wage and tax-related requests. Executive leadership should ensure guidance is communicated down to relevant employees to reiterate existing policies to defend against improper disclosure of sensitive information. Further, requests of this nature should follow a process that includes multiple approvers.

Contact:

Richard Moore
rmoore@alvarezandmarsal.com
(+1) 212 759 5532

Brady Willis
bwillis@alvarezandmarsal.com
(+1) 602 459 7051

Links:

More than 2,500 GCI employees' W-2 information stolen in phishing scam
http://www.ktva.com/more-than-2500-gci-employees-w-2-information-stolen-in-phishing-scam-524/

An Apology to Our Employees
http://snapchat-blog.com/post/140194434840/an-apology-to-our-employees

Seagate Phish Exposes All Employee W-2's
https://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/

Hackers victimize Inc., Fast Company staffers
http://nypost.com/2016/03/04/hackers-victimize-inc-fast-company-staffers/

IRS Suspends Insecure 'Get IP PIN' Feature
http://krebsonsecurity.com/2016/03/irs-suspends-insecure-get-ip-pin-feature/