PUBLICATION

Human Resources and Employment Counsel Beware: Increase in Malware Attacks Raising New Concerns for Employers

Authors: Alisa L. Chestler
June 29, 2020

Human resources can no longer just rely on their IT and legal counsel to focus on the concerns and issues surrounding cyberattacks. As more companies re-open and unemployment rates grow, cyber criminals are continuing to exploit the global crisis in a myriad of ways. Cyberattacks are the best example of how this exploitation can create chaos. The month of May saw an increase in the record of cyberattacks, including employment-themed campaigns.

Frequently styled as being sent by an applicant or employee, these emails include malicious files under the guise of a CV or submission of FMLA forms. Researchers at Check Point, a leading cyber firm, have identified an increase in CV-themed campaigns in the United States, with the ratio doubling to a record of one out of every 450 malicious files being a CV-related scam. One campaign includes email subject lines referencing job opportunities. When opening the emails, employer and HR department victims enable a malicious macro to run, download and infect the device. One particular campaign featured the banking Trojan Zloader malware and was used to steal victims' credentials and other private information.

According to Check Point, another campaign targeted human resources departments with the subject line "The following is a new Employee Request Form for leave within the Family and Medical Leave Act (FMLA)." Victims are then lured into opening malicious attachments. Some FMLA-campaigns have been embedded with the Icedid malware, a Trojan used to steal users' financial data. It specifically targets banks, payment card providers and e-commerce sites. A similar campaign adopted an FMLA theme but delivers the banking Trojan Trickbot. Another campaign circulating the country includes a fake termination message. The message includes malware in the attachments, which are disguised as severance information.

These attacks continue as employers witness more COVID-19-themed phishing. Last month, the FBI issued a Flash Alert (No. MI-000124-MW), covering specific indicators for phishing email campaigns enticing victims with pandemic-based details including "Updated COVID Tracking Details" or "Updated WHO Recommendations for COVID-19." Microsoft also warned of an ongoing COVID-19-themed phishing campaign that installs the NetSupport Manager remote administration tool – all under the guise of a public health update from the "John Hopkins Center."

These and other campaigns are engineered for harvesting credentials, weaponizing other phishing sites or transmitting financial information. Employees are frequently an organization's first line of defense. Companies can protect themselves by encouraging personnel to be skeptical of email from unfamiliar sources and educating hiring managers on the risks of CV and FMLA-related attachments, and other malicious active content that could be embedded in file attachments.

For specific guidance or more information on this alert, please contact Alisa Chestler, CIPP/US or one of Baker Donelson's Data Protection, Privacy and Cybersecurity Team Members who are ready to help you identify employment or privacy issues and develop a plan to mitigate the risks. For more information and general resources on how to address legal issues related to COVID-19, please visit the Coronavirus (COVID-19): Navigating the Path Ahead page on our website.