CYBERRISKS+LIABILITIES

IN THIS ISSUE

JRG
ADVISORS

DHS Warns of Utilities Malware

Two cyber security firms have uncovered malicious software that they believe caused a Ukraine power outage last December. The software was recently uncovered by two cyber security firms—ESET, a Slovakian anti-virus software maker, and Dragos Inc., a U.S. critical-infrastructure security firm.

The two firms released details of the malware, which goes by two different names, Industroyer and Crash Override. They also issued alerts to governments and infrastructure operators to help them defend against the malware, warning that it could be easily modified to harm critical infrastructure operations around the globe.

The U.S. Department of Homeland Security (DHS) hasn't seen any evidence to suggest that its critical infrastructure has been affected, but it will continue to investigate, as there is the possibility of more attacks using the same approach. In an alert posted on its website, the agency stated that "the tactics, techniques and procedures described as part of the Crash Override malware could be modified to target U.S. critical information networks and systems."

In the same alert, the DHS posted a list of technical indicators that a system had been compromised by Crash Override and asked firms to contact the agency if malware was suspected.

Power firms are concerned that there could be more attacks, especially considering the malware could attack other types of infrastructure, such as transportation, water and gas providers.

The two companies do not yet know who masterminded the attack, although Ukraine blames Russia. Officials in Moscow have denied the claims.

Target to Pay Settlement from 2013 Data Breach

Target has agreed to pay $18.5 million to settle claims made by 47 states and the District of Columbia as well as to resolve an investigation into the retailer's massive data breach in 2013.

The investigation found that Target's gateway server was accessed by cyber hackers through credentials stolen from a third-party vendor. As a result, data from up to 40 million credit and debit cards were stolen during the 2013 holiday season.

The total cost of the data breach was $202 million, according to Target. The state receiving the largest share of the settlement is California, which will receive more than $1.4 million.

Michigan Utility Company Loses Employees After Cyber Attack

A Lansing utility company is still recovering from a 2016 cyber attack that temporarily disabled its internal network and asked for a $25,000 ransom. According to officials, an employee unsuspectingly clicked on an infected email attachment, which shut down the company's accounting and email systems.

Since the cyber attack, 14 employees have voluntarily left the company—13 of which were IT employees. The company is devoting its resources to minimize the odds of an attack and to quickly recover in the event it is hit again.

WannaCry Came from North Korea

According to British security officials, the May 2017 global ransomware attack that affected over 200,000 computer systems came from North Korea. The hackers are believed to be a hacking group known as Lazarus—the same group that targeted Sony Pictures in 2014.

In the wake of increasing tensions resulting from North Korea's missile tests, the DHS and the FBI have issued an alert to businesses about another possible cyber attack led by North Korea, warning people to update old software.

Microsoft Warns of Cyber Attacks

Citing an elevated risk of cyber attacks, Microsoft has released several security updates during its June "Patch Tuesday" in an effort to protect against widespread hacking. A recent blog post by Adrienne Hall, General Manager of Microsoft's Cyber Defense Operations Center, stated, "In reviewing the updates for this month, some vulnerabilities were identified that pose elevated risk of cyber attacks by government organizations, sometimes referred to as nation-state actors or other copycat organizations."

WannaCry

In May 2017—after the WannaCry ransomware locked hundreds of thousands of machines around the world and demanded that victims paid a ransom in bitcoin—Microsoft was prompted to release updates for software that it no longer supports. This was an unexpected move that preceded more updates for old, outdated systems.

Microsoft's motives for June's most recent security updates are speculative, and it is unclear whether the company has been warned of another cyber attack using exploits similar to those of WannaCry. A Microsoft spokesperson stated that the decision to release the most recent updates is "an exception based on the current threat landscape and the potential impact to customers and their businesses."

Recent Findings

British security officials have recently linked the North Korean government to the creation of WannaCry, based on tactics, techniques and targets. The ransomware was originally built around a hacking tool belonging to the National Security Agency and spread through a flaw in Windows.

The Importance of Performing Updates

WannaCry is believed to be a flawed attempt to raise revenue for the North Korean regime, considering the hackers have not yet cashed in the $140,000 in bitcoin they stole. That is likely because the transactions are easy to track. Despite the failed attempt, one of the reasons why WannaCry was so powerful was because many of the facilities attacked hadn't updated their software to patch holes in security.

The most recent security update includes patches to its Windows XP, Windows Vista and Server 2003 products, which are all unsupported but still widely used. Microsoft suggests customers enable Windows Update if they haven't already.

JRG Advisors, LLC
7000 Stonewood Drive, Suite 251
Wexford, PA 15090
412-456-7000
http://www.jrgadvisors.net/

This publication is for informational purposes only. It is not intended to be exhaustive nor should any discussion or opinions be construed as compliance or legal advice. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.