Cybersecurity and Information Security Newsletter

Issue 1 | July 1, 2020

The Center for Legal & Court Technology (CLCT) at William & Mary Law School is proud to share the first issue of its "Cyber and Information Security Newsletter." To promote the mission of the Commonwealth Cyber Initiative (CCI), CLCT's Senior Research Fellow, Daniel Shin, Esq., will curate a monthly selection of news stories related to cybersecurity and general information security, and share them with CCI's Coastal Virginia Node and beyond.

Table of Contents

Security researchers discover eBay is port scanning visitors' computers

Background

- Port scanning is used to determine what computer applications are actively listening for connection requests from other computers. IT security professionals use it for legitimate security-audit purposes to ensure that only authorized programs are actively seeking to be connected to third party computers. However, hackers use port scanning to evaluate what type of attacks can potentially be carried out against a target machine.
- While visiting eBay's website, security researchers noticed that port scanning was triggered via JavaScript execution on the visitor's browser. eBay did not provide any prior notice, nor has it acknowledged any port scanning as of the date of this newsletter.

Analysis

- It is unusual for websites to conduct port scans of a visitor's computer. Such practice is intrusive because it can potentially reveal what software and services are running on the visitor's computer.
- Security researchers speculate that eBay might be attempting to detect compromised visitors' computer systems. The evidence of a remote desktop service running *inadvertently* on visitors' computers might be a sign that a computer has been compromised by malicious code, such as a trojan horse.
- It is arguable that port scanning can provide a proactive early detection method of identifying compromised systems. However, since eBay's core business is facilitating e-commerce, not cyber threat detection, it is not immediately obvious why eBay would implement a port scanning system.
- Visitors to eBay were not given any prior notice to the port scanning operation. There are few court cases evaluating whether port scanning third-party systems without consent constitutes a criminal or civil violation. A federal court in the Northern District of Georgia held that port scanning a third-party's system without consent, but without any additional actions, did not violate the Computer Fraud and Abuse Act (CFAA), 18 U.S. Code § 1030. The reasons are that (1) port scanning alone does not cause any alternation, damage, or malfunction of the third party's network, an explicit requirement of the statute; and (2) port scanning alone does not allow unauthorized access to the third-party's network. *See* Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901, at *6 (N.D. Ga. Nov. 7, 2000).
- Although port scanning third-party systems without authorization may not automatically fall under the CFAA, there may be additional legal liabilities stemming from other "anti-hacking" federal statutes, including the Stored Communications Act, the Electronic Communications Privacy Act, and the Defense Trade Secret Act.
- Port scanning can also be used to digitally fingerprint visitors' computers in order to facilitate broader surveillance analytics for data-harvesting companies. As more people use aggressive ad and script blocking software while surfing the web, data-

harvesting companies may rely more on port scanning and other digital fingerprinting techniques to track users' browsing habits.

Tips

- To prevent websites from port scanning your computer, you can block "check.js" from loading or executing on the web browser as suggested by Avast.

Read the full article here.

A National Security Research Agenda for Cybersecurity and AI

Background

- Georgetown University's Center for Security and Emerging Technology released a white paper exploring the intersection between cybersecurity and artificial intelligence. The paper assesses machine learning technologies and their potential effects on cyber offense and defense.
- These include:
    - bolstering cyber offense by rapidly finding exploitable software vulnerabilities of an adversary system through code analysis;
    - executing more potent spear-phishing attacks by "generat[ing] credible messages that appear to come from plausible senders";
    - enhancing cyber defense. For example, machine learning can be utilized to identify and isolate malicious-*looking* code, even when that specific code string has not been identified as such in any malicious code databases; and
    - detecting and thwarting potential cyber attacks via network traffic analysis.

Analysis

- Once machine learning is mature enough for industry-wide cybersecurity adaptation, organizations should consider integrating some machine learning tools into existing cybersecurity functions. These should supplement, not replace, critical cybersecurity operations.
- Organizations should use machine learning tools to supplement and not replace critical cybersecurity operations.
    - Machine learning is vulnerable to adversarial learning. For example, a malicious adversarial learning tool could potentially dismantle a machine learning cybersecurity protection and prevent it from operating properly.
    - Machine learning has a degree of unpredictability, which can lead to undesired results. Organizations may take on additional liability when machine learning

plays a critical role in the organization's cybersecurity functions if those functions cannot be reliably anticipated.

Read the full article here.

External actors motivated by monetary interests drive most breaches (Verizon's 2020 Data Breach Investigations Report)

Background

- Verizon released its 2020 Data Breach Investigations Report ("DBIR"). The findings are based on Verizon's analysis of 32,002 security incidents worldwide, which includes 3,950 confirmed breaches.
- Examining the perpetrators of breaches, DBIR found that external actors conducted 70% of all confirmed breaches. The report also found that organized criminal groups conducted 55% of all confirmed breaches.
- Focusing on the victims of breaches, DBIR found that 58% of all confirmed breaches involved the compromise of personal data. The report also found that 72% of all confirmed breaches involved large business victims.
- DBIR concluded that 86% of all confirmed breaches were financially motivated, while only 10% were linked to espionage.

Analysis

- Having an overall view on data breaches can provide insight into how cyber attacks may evolve in the near future. However, big picture statistics can leave out the useful context within the data points. I would encourage reading this report in its entirety to appreciate the analysis.
- Although a data breach may potentially trigger a civil lawsuit, the legal liability of the breach generally does not turn on whether the breach actually occurred. Instead, it depends on whether the organization took the necessary steps that are either required by statute or considered legally reasonable, to protect private information before and after a breach.

Read the full article here.