LAWYERS JOURNAL

LAW PRACTICE MANAGEMENT

Verizon releases its highly anticipated 15th annual Data Breach Investigations Report

By Caitlin Counihan

Verizon recently released its highly anticipated 15th annual Data Breach Investigations Report (DBIR), with a valuable data-driven review and analysis of the past year's major security events. As a leader in the field of cybersecurity services and incident response, bit-x-bit is pleased to have contributed to the DBIR again this year. This information is intended to raise awareness and assist in identifying the security needs of your business. Reflecting on the methods commonly used by attackers can help to better defend against them.

The DBIR is the result of the analysis of more than 23,000 (anonymized) incidents, including 5,200 confirmed data breaches. Your organization can leverage this information to raise awareness and assist in identifying important security needs. We recommend that our clients utilize the DBIR to reflect on the methods commonly used by attackers, which can help organizations anticipate, mitigate, and remediate these threats.

Some important takeaways from the DBIR to consider:

• With a rise as large as the last five years combined, ransomware has increased approximately 13% and continued its upward trend. Ransomware is a strain of malicious software intended to halt access to a computer system until an amount of money (ransom) is paid. The most common way ransomware is spread is through desktop sharing software (remote access tools), followed closely by phishing emails that contain malicious attachments or links. See bar graph below:

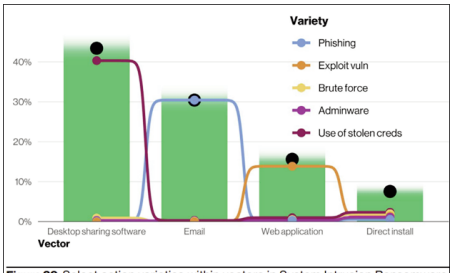

Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

• Incidents are driven by four main types of access to the victim's estate: botnets, credentials, exploiting vulnerabilities and phishing.

– Botnets – This is a network of internet-connected devices which can be used to steal data, send spam and allow an attacker to access devices.

– Credentials – Attackers will use a victim's credentials to gain access to computer systems.

– Exploiting vulnerabilities – Attackers will find issues in software, then use those weaknesses to their advantage to gain access to systems.

– Phishing – Attackers will send phishing emails which often contain malicious attachments or links. Others will simply trick the user to take an action that weakens or compromises the security of their system.

• The Human Element is still a pervasive issue across the breach landscape. According to Verizon's report, "This year 82% of breaches involved the human element. Whether it is the use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike." Security awareness training – which should be iterative, consistently provided and adapted based on the learning needs of the target community – is a key component to addressing the human element of security breaches. Training can be provided online and can be adapted based on the subjects' grasp of the concepts in the various modules.

• With 80% of breaches stemming from those external to the organization, external actors are steadily more prevalent than Internal. Vulnerability scanning can be a useful method of detecting potential points of exploit on a computer or network to identify security weaknesses that should be addressed.

As a member of the Center for Internet Security (CIS), bit-x-bit helps clients mitigate the risk of cyberattacks through the assessment of CIS controls. Within that control environment, we can provide security awareness training, vulnerability scanning and other helpful services to reduce the likelihood of a successful attack. To obtain a more in-depth view of this year's key findings, the full DBIR report is available on Verizon's website. ■

Caitlin Counihan is a Digital Forensic Analyst at bit-x-bit, LLC. Looking for assistance with your cybersecurity needs? Contact bit-x-bit at info@bit-x-bit.com.