Avoid these TOP 10 digital attack vectors this holiday season

A CyberInt eBook ~ November 2018

Cyberint

The Digitalization of Businesses and the Opening of Attack Surfaces for Cybercriminals

The topic of cybersecurity becomes more critical with each passing year. Global spending on information security reached approximately $90 billion in 2017, which is 7.6 percent more than 2016, is expected to reach $96 billion this year, and $113 billion by 2020, according to Gartner.

Cybersecurity Ventures predicts cybercrime will cost businesses globally more than $6 trillion annually by 2021. This prediction includes damaged data, lost productivity, theft of intellectual property or money, theft of personal and financial data, embezzlement and fraud, disruption of business continuity, forensic investigation, restoration of hacked data and damaged reputations. In 2017, the Identity Theft Resources Center (ITRC) recorded 1,293 data breaches in the U.S. which exposed over 174 million confidential records which represent an increase of 21 percent over 2016.

Enhancing detection and response capabilities will continue to be a key priority to keep businesses secure, especially as they become increasingly reliant operationally on digital transactions and more susceptible to cyberattacks. The accelerated process of digitalization has created a highly dynamic environment for both businesses and criminals requiring constant adjustments to stay current on the latest technologies, making it an ongoing battle to fight ever-shifting threats and insidious attacks. Additionally, increasing omnichannel experiences to meet customer needs across multiple touchpoints opens up vulnerabilities that must be protected and secured by retailers; end users' digital experiences across different verticals must be at once prioritized with the opening of attack surfaces for cybercriminals.

How much will it cost us?

Cybersecurity Ventures predicts cybercrime will cost businesses globally more than $6 trillion annually by 2021

Current Top 10 Digital Attack Vectors

We recognize that companies cannot afford – for even a moment – to fall behind in understanding which attack methods are being used and with which technologies. The cybercrime landscape continues to shift as quickly as ever.

With this in mind, we've ranked the most common attacks vectors you should be concerned about to .at least be sure that you are doing the most to protect yourself.

1 Social Engineering

The term social engineering includes a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

A common new social engineering attack – pretexting – occurs when individuals impersonate another individual, either using a fake persona, creating a brand new identity, or simply using a legitimate role improperly. These can take place face-to-face, over the phone, or by email. Surprisingly, 63% of data breaches originate from internal sources, which makes vigilance on the part of each organizational member more critical. Organizations are encouraged to provide regular user training and awareness, and social engineering tests should be part of an overall security penetration test.

2 Phishing

A phishing attack is when a criminal sends an email pretending to be someone s/he's not, to extract sensitive information from a target. Essentially, the perpetrator attempts to elicit fear, curiosity, or a sense of urgency from the target, so that the target will open an attachment, click on a link, or otherwise provide their sensitive information.

Spear phishing is when a criminal is targeting a single, or a limited number of people using a customized approach. Spear phishing attacks are generally more effective because the attacker uses language and methods specific to each individual.

For small and medium-sized businesses, phishing is one of the most feared attack forms. According to the Verizon Data Breach Investigations Report (DBIR Report), 30% of phishing messages get opened by targeted users, and 12% of those users click on the malicious attachment or link. Increasing employee awareness is the best defense against phishing attacks.

Did you know?

Surprisingly, 63% of data breaches originate from internal sources, which makes vigilance on the part of each organizational member more critical

3 Ransomware

Of the 10 types of crimeware cited in the Verizon DBIR report, the overwhelming attack vector is ransomware - a type of malicious software designed to block access to a computer system until a sum of money is paid. Generally, the attack is sent to a target via an email attachment or web link. The email is designed to appear to be from a believable source to encourage the recipient to open the attachment or click on the link.

Ransomware comprises close to half of the crimeware incidents and is the most significant malware threat today. Cybersecurity Ventures predicts ransomware damages will reach $11.5 billion in 2019. Prevention should include a robust malware strategy at the endpoint, at malware gateways, application whitelisting, and attachment sandboxing.

Did you know?

Ransomware comprises close to half of the crimeware incidents and is the most significant malware threat today

77 percent of compromised attacks in 2017 were fileless

4 Fileless Attacks

Fileless malware leverages applications already installed on a user's computer. For example, exploit kits can target browser vulnerabilities to make the browser run malicious code, or take advantage of Microsoft Word macros, or use Microsoft's Powershell. Fileless malware can be the basis to launch a variety of attacks from ransomware to using the infected machine to mine Bitcoin. With access to PowerShell, there are practically no limitations to the type of attack that can occur.

According to the Ponemon Institute's The State of Endpoint Security Risk Report, 77 percent of compromised attacks in 2017 were fileless. The report estimates that fileless attacks are ten times more likely to succeed than file-based attacks. In early 2017, a fileless attack infected more than 140 enterprises, including banks, telecoms, and government organizations in 40 countries. Software already installed that contains vulnerabilities is required to carry out a fileless attack. Patching and updating the operating system as well as applications and browser plugins are the most effective prevention.

Did you know?

In early 2017, a fileless attack infected more than 140 enterprises, including banks, telecoms, and government organizations in 40 countries

5 Malicious Apps

In 2017, McAfee Labs detected more than 16 million new incidents of mobile malware. One malicious app called HummingBad infected over 10 million Android operating systems in mid-2016. User details were sold, and advertisements were tapped on without the user's knowledge which generates fraudulent advertising revenue.

Mobile expert Gagan Singh from Avast notes, "We are seeing a steady increase in the number of malicious applications for Android devices that are able to bypass security checks on popular app stores and make their way onto consumers' phones."

Banking and retail businesses need to be acutely aware of this avenue of attack. Avast identified a malicious software called "BankBot." If a user downloads it onto their smartphone, it can exploit major banking apps by creating a fake overlay of the real banking app and collect the user's banking credentials to be sent to the attacker. Anti-virus software for Android devices can help and use two-factor authentication if available.
We all use mobile devices in nearly every aspect of our lives. With BYOD policies more common, state actors and cyber criminals are looking at ways to infect mobile devices with spyware to access corporate data.

6 Credential Reuse

Exploiting your reused passwords begins when your credentials are stolen from a site with a database of user credentials. A hacker will then sell your credentials on the dark web or use your credentials to commit identity theft, extortion, or money laundering. Cybercriminals will use your stolen credentials in what's called a credential stuffing attack. The cybercriminal will choose a target site and analyze the site's login sequence and processes. Then, they can either create an automated script or use a configurable credential stuffing software to systematically test if the stolen credentials successfully login to the target site.

In 2016, about 3.3 billion credentials were compromised in data breaches. The success rate for credential stuffing attacks was between 0.1 percent and 2 percent. To protect your accounts from credential stuffing attacks, use a unique password for each account, a password manager, and enable two-factor authentication.

7 Supply Chain

A supply chain attack occurs when someone infiltrates a system through an outside partner or provider with access to the systems and data. This dramatically changes the attack surface of the typical enterprise, with more suppliers and service providers touching sensitive data than ever before.

According to a survey conducted in 2017 by the Ponemon Institute, 56 percent of organizations have had a breach that was caused by one of their vendors. On average, a U.S. company pays over $7 million per breach in remediation costs, fines, and lost customers. To reduce the likelihood of a breach, keep a strict audit of all your vendors, and which of them have access to sensitive data. Implementing tools to constantly monitor your supply chains to centralize workflows and documentation of third-parties – creates systems to properly evaluate your security practices and thereby reducing the potential of a breach through a third-party. From there, create a Third-party Risk Management Committee to create standards to review and assign someone to take ownership of a Third-party Risk Accountability Program.

8 Denial of Services

Overwhelming an application, system, or network is one of the easiest ways for attackers to shut down a network or website temporarily. An attacker will flood a target with excessive connections, usually from multiple sources. This results in an overload of bandwidth or network resources which prevents legitimate traffic from being processed. And, while DDoS attacks themselves aren't the means by which data is breached, a DDoS attack can give attackers an entry point by overwhelming security appliances. According to Neustar's internal security data, 45 percent of DDoS attacks were over 10Gb/s while 15 percent consumed at least 50Gb/s. These bandwidth rates are nearly twice than reported in 2016.

According to a survey of mid-to-large corporations in Europe and the U.S., a DDoS attack can cost financial service businesses anywhere from $250,000/hr to over $1 million/hr in revenues. The impact of these attacks isn't just loss of revenue but can be used as a smokescreen to cover up thefts of intellectual property, customer data, and other attacks.

How much will it cost us?

Cybersecurity Ventures predicts ransomware damages will reach $11.5 billion in 2019

56% of organizations have had a breach that was caused by one of their vendors

$7 million per breach in remediation costs, fines, and lost customers

DDoS attack can cost financial service businesses anywhere from $250,000/hr to over $1 million/hr in revenues

9 SQL Injection Attack (SQLi)

SQL Injection is a web application vulnerability that allows hackers to inject malicious Structured Query Language (SQL) code to web inputs to determine the structure and location of key databases. During the 2016 U.S. election year, hackers were able to steal the personal data of 200,000 Illinois voters with a SQL injection attack. The affected database was offline for 10 days in order to recover from the attack. Besides personal data being stolen, there was a potential for other consequences such as influencing election results. In 2017, a SQL Injection vulnerability was discovered in one of the most popular Wordpress plugins, installed on over 300,000 websites, which could be exploited by hackers to steal data and possibly hijack the affected sites remotely.

Mitigation techniques to prevent SQL injection attacks include setting database permissions correctly, require input validation, using prepared statements, and using stored procedures for loading data.

10 Cross Site Scripting (XSS)

A cross-site scripting attack occurs when malicious scripts are injected into otherwise benign and trusted websites. For an XSS attack to take place, the vulnerable website needs to include user input in its pages directly. An attacker can then insert a string that will be used within the web page and treated as code by the victim's browser. Potential costs could include lost revenue, damaged reputation, and even allowing criminals to exploit the site to mine cryptocurrencies. Even the likes of Google are not immune to this vulnerability. Over a 2 year period, Google paid over $1.2 million in bug bounties to security researchers that found and reported XSS bugs in Google applications. To combat this attack, regularly test if your website or web application is vulnerable to XSS and other vulnerabilities by running a web vulnerability scan.

How much will it cost us?

Google paid over $1.2 million in bug bounties to security researchers that found and reported XSS bugs in Google applications

Staying Safe In a Digital World

The payoff for cybercriminals increases dramatically as digitalization opens up more attack vectors. Cyberattacks, more diverse and sophisticated as ever, requires an advanced security platform because the technology changing constantly translates to ever changing attack vectors. These rapid changes have opened the working surface for cybercriminals that are looking to exploit new vulnerabilities. Continuous adaptation requires organizations to employ a dynamic security system that continually tests for vulnerabilities with the ability to adapt to past incidents and changing hacking methods. **There will be more attack vectors but it isn't all doom and gloom. Equip your business and stay safe out there!**

Cyberint

United Kingdom
Tel: +442035141515
sales@cyberint.com
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +1-646-568-7813
sales@cyberint.com
214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

Israel
Tel:+972-3-7286777 Fax:+972-3-7286777
sales@cyberint.com
Ha-Mefalsim 17 St | 4951447 | Kiriat Arie Petah Tikva | Israel

Singapore
Tel: +65-3163-5760
sales@cyberint.com
10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com **www.cyberint.com**