JULY 2021

Threat Hunter Intelligence Report

Data Breaches

splunk>

turn data into doing™

The Threat Hunter Intelligence Report is a monthly series brought to you by Splunk's threat hunting and intelligence (THI) team. We research and produce actionable reports on the latest cybersecurity threats and trends — helping organizations stay one step ahead of adversaries, one report at a time.

Data breaches 101

Few data breaches compare to the massive SolarWinds hacks that left the company — and its roster of high-profile clients — exposed for more than nine months before detection in December 2020. During the unprecedented attacks, foreign hackers infiltrated the Texas-based company's network, executing malware that gave them access to sensitive information and the ability to spy on tens of thousands of SolarWinds customers. The resulting domino effect represented every security professional's worst nightmare, raising alarms to the vulnerability of government and corporate cyber systems as more organizations fell victim in its wake.

Yet even before that, data breaches were rapidly becoming more sophisticated, destructive and costly. The average cost of a breach is $150 per data record — $175 when breached via a malicious attack. And while publicly disclosed breaches fell by 48% in 2020, the number of lost records spiked 141% to an eye-crossing $37 billion last year, evident in assaults against CAM4, BlueKai and Whisper, among others.

In this report, we'll take a closer look at the intensifying scale and impact of data breaches, some of the most common risks and vulnerabilities that lead to them and what CISOs can do to prevent their critical assets — and those of their customers — from walking out the door.

THI profile 1

Database misconfiguration

Chris Vickery, renowned security researcher, made a startling discovery: The personal information of almost 200 million U.S. voters was accessible to anyone on the web. A conservative data firm was hosting voter information on an Amazon S3 server and completely messed up its configuration. While some of the data on the server was protected, more than a terabyte of voter information was available on a public database.

Researchers also recently discovered an improperly-secured Microsoft Azure database belonging to TrueDialog, a U.S. communications firm that provides SMS-texting solutions. The database contained 604GB of data, including almost one billion highly sensitive data entries related to the company, its client base and its clients' customers.

What you need to know:

Database misconfiguration is a widespread problem that can put organizations at risk due to incorrectly configured security controls. This can happen at almost any level of the IT and security stack, ranging from the company's wireless network and custom code to web and server applications.

This type of attack usually happens because of missing patches, use of default accounts, unnecessary services, insecure default configuration or poor documentation. For example, failing to set a security header on a web server or forgetting to disable administrative access for certain levels of employees can lead to a data breach. These attacks can also happen when hackers take root in legacy applications that are inherently misconfigured because they haven't been updated.

THI profile 2

Vendor vulnerability

Companies often assume the risk of their vendors. An infamous example is the Target breach in 2019 that affected over 40 million customer accounts. Investigations into the breach revealed that attackers stole the credentials of Target's HVAC contractor, Fazio Mechanical Services, and used that third-party vendor's details to get into Target's internal web application. Once in, hackers installed malware to capture the names, phone numbers, payment credit card numbers, credit card verification codes, and other highly sensitive information belonging to Target customers.

This type of attack happens when a bad actor gains a foothold in the system via legitimate access identification — usually thanks to a stolen or spoofed vendor identity — and then moves laterally to other points of compromise within the system. Depending on the level of access these permissions provide, attackers can potentially access an entire network.

What you need to know:

Generally speaking, these vendor-based attacks happen due to a lack of safeguards around vendors' credentials (as well as sheer human folly). Hackers can also get access by spoofing login domains or using keyloggers to steal legitimate authentication credentials.

Ultimately, weak authentication methods that can be duped by external parties are usually the source of the problem. Vendors and other service providers should always be vetted on their own security controls and processes, as their security posture can directly impact the confidentiality of customers' data. Also, implementing a zero trust strategy can help deter bad actors, thanks to a number of ways to authenticate and authorize user identity before granting access.

THI profile 3

Insecure applications

Employees often download software onto their workstations to help them get the job done. But more often than not, these apps are installed without the knowledge or consent of the organization's IT department — and without the appropriate security protocols in place.

Unsurprisingly, one in five organizations experience a cyber incident originating from an unauthorized or insecure app. Since users access these apps largely under the radar, they unintentionally leave the door wide open for malicious insiders or external hackers looking for security gaps in these systems.

What you need to know:

Breaches can occur when employees upload, share or store critical or regulated data in these apps without appropriate security and data loss prevention (DLP) solutions. The exposed information then provides an easy target for insider threats and data theft, and can also lead to costly compliance violations. In addition, the apps themselves can be riddled with endpoint vulnerabilities (see Adobe Reader for just one example of a popular app with a storied history of security vulnerabilities).

Hacker profile

REvil

Wanted for extortion

REvil — a hacker group believed to be an offshoot of the now-defunct GandCrab gang— are very much still at large. Pronounced as the letter “R” followed by “evil,” REvil has an impressive rap sheet. And while it’s hard to say where they’re based, cybersecurity analysts suspect REvil is located in a Soviet state because the group avoids targets in Russia and former Eastern Bloc countries. To date, the group has made countless attempts to extort companies and public figures by stealing their personal information. In May 2020, they demanded $42 million from Donald Trump. A week later, they released over 2GB of legal information connected to Lady Gaga.

Most recently, REvil stole plans for upcoming products from electronics manufacturer Quanta Computer said to include the blueprints for new Apple laptops, an Apple Watch and a new Lenovo ThinkPad. Quanta addressed the attack but chose not to explain how it happened or how much of their proprietary information was stolen.

REvil is now threatening to release the plans publicly unless Apple pays them a $50 million ransom fee. Until then, the hackers will continue to post new files every day, REvil said on their blog.

Actor type:

Nation state, state-sponsored

Suspected country of origin and support:

Russia/Former Eastern Bloc

Motivation:

Monetary gain

Targeted sectors:

Technology, Financial, Manufacturing, Media, Healthcare, State and Local Governments, Automotive, Travel, Legal

Commonly abused technologies:

Remote Desktop Protocol, Software Vulnerabilities, AdFind, Rclone, PsExec, Bloodhound, Cobalt Strike

Go phish

Sawfish

In early 2020, Sawfish initiated a phishing attack targeting developers, cleverly duping GitHub users with a domain name and web interface that looked to be legitimately part of GitHub. Users received phishing emails claiming that their GitHub account and repositories had been compromised, leading them to a fake login form to harvest their credentials.

Sawfish used a range of tactics to hide the real link destination, including URL shorteners. They also used redirects on compromised sites with legitimate-looking URLs to trick victims into going to malicious sites.

With the stolen GitHub user account details, Sawfish then created GitHub personal access tokens or authorized OAuth apps in order to preserve their access even when the rightful account users changed their passwords. “In many cases, the attacker immediately downloads private repository contents accessible to the compromised user, including those owned by organization accounts and other collaborators,” GitHub said.

To better prevent phishing attacks like this (which collect two-factor codes), hardware security keys or WebAuthn two-factor authentication are almost always a safe bet. Also consider using a browser-integrated password manager. Many commercial and open-source options exist, including options native to popular web browsers that provide a degree of phishing protection by only autofilling or recognizing legitimate domains where a user has previously saved a password. If the password manager doesn’t recognize the website a user is visiting, it could be a phishing site.

Looking for trouble?

Stay ahead of current and emerging threats by subscribing to our monthly updates on threat hunting and investigation.

Subscribe Now

splunk>
turn data into doing™