Recorded Future®

CYBER THREAT ANALYSIS

Database Breaches Remain the Top Cyber Threat for Organizations

By Insikt Group®

CTA-2020-0521

Executive Summary

With the number of affected victims growing every year, some of today's most serious threats to organizations are database breaches and releases. These breaches compromise millions of pieces of sensitive information like personally identifiable information (PII), credentials, payment information, and proprietary data. Criminals gain access to the data through various tactics, techniques, and procedures (TTPs), such as phishing, malware, exploiting existing vulnerabilities in software, insider threats, password reuse, and a number of other methods, taking advantage of holes in security infrastructure. After breaching an organization's network, criminals may access the data themselves or sell the access off at dark web auctions. The information gathered as a result in turn frequently leads to further breaches through techniques like business email compromise (BEC).

Key Judgments

- Recorded Future observed that cybercriminals obtain access to networks using different TTPs, including compromised third-party software, domain controllers, remote desktop protocols (RDP), virtual private networks (VPN), internet routers, web shell and powershell attacks, compromised credentials, or remote access trojans (RATs).
- Recorded Future analysis indicates that the following industries are the most targeted: healthcare, education, transportation, logistics, travel and hospitality, and finance.
- Database breaches provide the underground economy with an inflow of new data that can be used in various ways, such as spamming and phishing, credential stuffing attacks, social engineering, business email compromise (BEC), tax fraud, and various other types of financial fraud.
- Recorded Future observed that leaked databases are primarily monetized via their sale through open auctions, direct sales, or subscription-based services.

Background

A database breach is not an attack on its own, though some may result from attacks, but rather a result of cybercriminals obtaining unauthorized access to a network. This access provides cybercriminals with significant capabilities for privilege escalation, data exfiltration, and other impacts. Ransomware operators can encrypt devices in the compromised network, and hackers can exfiltrate databases with PII, payment data, PHI, corporate documents, email addresses, job titles and organizations, social media profiles, and account usernames and passwords. Frequently, these leaks provide the underground economy with an inflow of new data, which can be used in various ways:

- Spamming and phishing using exfiltrated email addresses
- Credential stuffing attacks using exfiltrated email addresses and accounts
- Financial and tax fraud using exfiltrated PII
- Social engineering using exfiltrated PII
- Business email compromise (BEC) attacks

The number of database breaches increases every year. According to Norton, there were 3,800 publicly disclosed breaches in 2019, exposing 4.1 billion records.

Some of the notable database breaches reported in 2019 include the following:

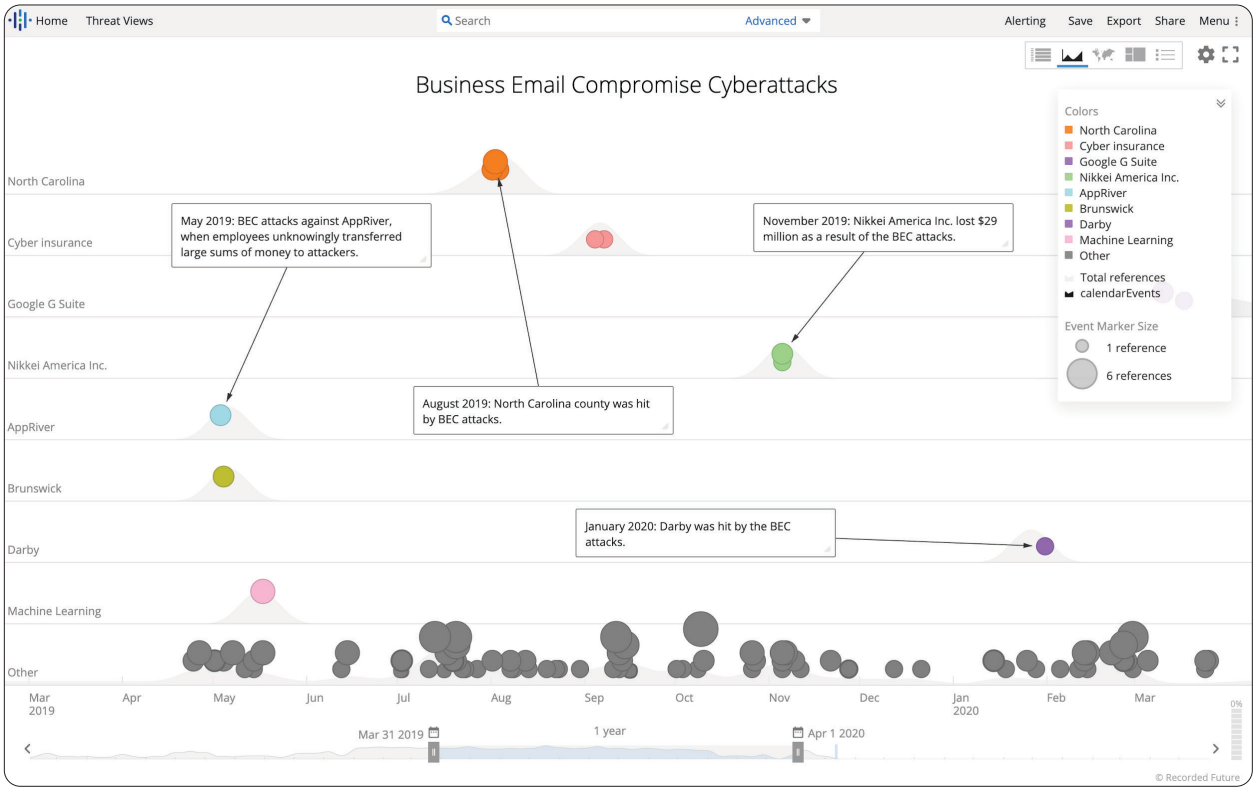
- First American Financial Corp: 885 million records
- Facebook: 540 million records
- Fortnite: 200 million records
- Elasticsearch Cloud Storage: 108 million records
- American Medical Collection Association: 20 million records
- Capital One: 106 million records
- Biometric Records (BioStar 2): 27 million records
- Ecuadorian Data: 20 million records
- Hostinger: 14 million records
- DoorDash: 4.9 million records
- Verifications[.]io: 809 million records

Threat Analysis

Business Email Compromise

Another TTP closely related to and often facilitated by database breaches and access to networks is business email compromise (BEC). This method is similar to social engineering and phishing techniques in that a threat actor attempts to compromise companies by pretending to be a legitimate employee or manager of the company, using access to their compromised email accounts or spoofing the addresses they obtained from the compromised databases. Frequently, the victim believes that they are communicating with a real employee because of the use of a legitimate email address and will reveal confidential corporate information or initiate wire money transfers to accounts controlled by cybercriminals.

According to the FBI's Internet Crime Complaint Center (IC3), as of February 27, 2017, "BEC scams continue to grow, evolve, and target businesses of all sizes." They further note that since January 2015, "There has been a 1,300% increase in identified exposed losses, now totaling over $3 billion."



BEC cyberattacks observed on the dark web over the last year. (Source: Recorded Future)

BEC is often performed in combination with other TTPs like romance scams and retirement account fraud aimed at stealing money from individuals, sometimes ranging up to millions of dollars.

Breaches and Sales, Step by Step

In the past, most threat actors had to hack a company's network to extract their databases and other valuable information. Now, much of the hacking and exfiltration has already been done by threat actors who specialize in obtaining access, and this information is offered for sale, or sometimes even provided for free, on dark web forums and markets. This access to networks is often the first step for hacking corporate databases, and the high-level threat actors who specialize in gaining access are likely the key to much of the cybercriminal activity involving everything from theft of PII and PHI (personal health information) to ransomware attacks and corporate espionage. These criminals, who often work in small teams, can perform the whole process from obtaining access to the company's network to selling it on the dark web. The subsections below discuss this process in more detail:

1. Sale of access to compromised networks
2. Sale of databases
3. Dumping of free databases
4. Sales of new and composite databases through subscription-based services

1. Sale of Access to Compromised Networks

The sale of access to compromised networks of government, business, educational, and other entities can be a highly lucrative business, with price per access varying from hundreds to thousands of dollars. Cybercriminals obtain access to networks using different methods such as compromised third-party software, remote desktop protocol, virtual private network, internet routers, performing web shell and PowerShell attacks, or using remote access trojans.

Analysis of dark web sources indicates that cybercriminals primarily target organizations in the following industries:

- Healthcare (hospitals and medical offices)
- Manufacturing
- Transportation and logistics (airline and logistics companies, airports)
- Travel and hospitality (hotels, travel agencies/services, and travel metasearch engines)
- Education (universities and colleges)
- Government (U.S. state and city administrations, police departments, regional healthcare authorities, election committees, international government agencies, and organizations)
- Finance and e-commerce (accounting and insurance companies, banks, and e-commerce organizations)
- Legal (law firms)

The victims are a combination of targets of opportunity, organizations with vulnerabilities, and targeting of sectors that provide particularly rich fields for things like PII and PHI such as healthcare institutions, government and educational entities, or for financial information such as the finance and e-commerce sectors.

Sales Through Auctions

Unlike other products and services that are offered for sale on dark web resources at a fixed cost, much of the listed compromised data is usually sold via auctions. The auctions are considered a fair and open mechanism for conducting sales on dark web forums that offer participants (threat actors) prices that they think are reasonable. One top-tier forum on the dark web, for example, has strict requirements that all members must follow:

- The seller has to sell the auctioned product or service if it is purchased (they cannot back out of a deal)
- The seller announces a starting price, bid step, and the highest bid allowed to purchase the product or service directly without participating in the auction
- The buyer who offers a price has to buy the auctioned product or service
- The seller and the buyer use an escrow service to complete the deal
- If the seller refuses to use an escrow service, they can be banned from the forum

Another type of compromised access sales on dark web forums is a direct sale, which does not have the limitations described above and is usually a private negotiation between buyers and sellers. The main advantage of direct sales is advanced privacy and security (it can be done without a third-party guarantor through secure communication methods).

Sales Through Escrow Services

In addition to auctions, the majority of top- and mid-tier forums also offer their escrow service to members, which is a universal security mechanism where a third party (threat actor or automated system) receives and disburses money according to the agreement between the seller and buyer to prevent fraud. There are two types of auctions on the dark web that use escrow services: regular and automated.

Regular Escrow Service

As a rule, this function is performed by one or two reputable threat actors or forum staff members who act as guarantors. Their usernames and contacts are usually listed in the “Rules” or “Escrow” sections on a forum. They must provide the following:

1. The seller: Their username and Jabber account
2. The buyer: Their username and Jabber account
3. The subject of the deal with a detailed explanation of the product or service, technical specifications, and so on
4. The exact amount of the deal in USD and Bitcoin, including the escrow commission (Typically, the commission costs 3-10% of the listed price, but not less than $20 USD, and is paid to the guarantor)
5. Terms of delivery and verification of the product or service
6. Additional terms of the deal, if required

Automated (Auto) Escrow Service

This type of escrow service is a special section on many cybercriminal forums that allows threat actors to conduct deals 24/7 with minimal risk and does not charge a service commission. The rules can vary on every forum but the primary steps for auctioning are as follows:

1. Members negotiate all the terms of the deal privately.
2. The buyer creates a thread in the section titled "Automated Escrow Service" or "Escrow Service," tags the potential seller, and outlines all terms and conditions of the deal. The thread is only visible to the parties of the deal and the forum's admins. Some forums secure escrow threads using a password. In this case, the buyer should provide it to the seller to get them access to the thread.
3. The buyer specifies the total amount of the deal they are going to pay and saves the thread.
4. The second participant of the deal confirms the offered amount and saves this information.
5. The buyer sees the seller's confirmation and approves the final amount.
6. The escrow system accepts the deal and finishes only when the forum representative receives the product from the seller. The seller is automatically informed about receiving payment in a private message on the forum.
7. The auto escrow service allows parties to transfer and replenish funds.

2. Sale of Databases

Database breaches are sold or shared among threat actors across dark web sources. Threat actors use the username/password combinations frequently found in these databases for credential stuffing attacks against popular online services.

As a rule, cybercriminals do not announce breaches immediately, sometimes waiting several months to sell the data on the dark web while attempting to establish the best way to monetize the access. Many breached databases are not sold in their entirety but rather in parts: For example, a sale might include a combination of email addresses with passwords, financial information, PII, and so on, but not all of the information. Not all threat actors who actually breach networks are also necessarily their sellers. Cybercriminals use strategies to obfuscate their connection to breaches for security reasons, sometimes using multiple monikers or operating within a group. Moreover, access to the database is frequently sold by individuals not directly involved in the hacking of the targeted companies, instead working primarily as a proxy.

3. Dumping of Free Databases

In addition to access and databases being sold on dark web forums, Recorded Future has also observed multiple leaked databases publicly shared for free on several forums on the dark web.

For example, one notorious threat actor, who is the creator and administrator of a forum on the dark web, started publicly sharing voter databases from different U.S. states taken from 2017 to 2018 that contained voter IDs, full names, physical addresses, previous addresses, dates of birth, gender, phone numbers, voter status, and voter history. Databases from nearly two dozen states were shared, with each one containing anywhere from hundreds of thousands to several million unique records.

4. Sales of New and Composite Databases Through Subscription-Based Services

Some threat actors buy and harvest leaked databases on different underground platforms, file-sharing platforms, and other available services to organize subscription-based services where cybercriminals can find composite leaked databases, stored both encrypted and unencrypted. These services update their databases frequently, have regular and premium tiered membership plans, and even offer customer service via Telegram. One such service was available for $64 USD for the first month and $37 for each subsequent month.

Network Compromise Mitigation Techniques

Recorded Future recommends the following measures to protect against exploitation of vulnerabilities targeting organizations' websites and networks resulting in database breaches:

- Keep all software and applications up to date; in particular, operating systems, antivirus software, applications, and core system utilities.
- Filter email correspondence for spam and scrutinize links and attachments prior to accessing them; ensure malicious attachment monitoring, if available, is on.
- Make regular backups of your system and store the backups offline, preferably offsite so that data cannot be accessed via the network.
- Adhere to strict compartmentalization of company-sensitive data. In particular, look at which data anyone with access to an employee account or device would have access to (through device or account takeover via phishing). Verify access control for users, and ensure employees have a business need to access resources.
- Strongly consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.

- Monitor vendors' security or assess risks that could be passed on by use of a third-party technology.
- Apply data encryption standards for stored databases to protect them from being used maliciously by individuals who were able to get unauthorized access to the internal network of the organization.
- Monitor available databases or account shops for employee accounts.

BEC Mitigation Techniques

According to the FBI, these steps will reduce the risk of being compromised by BEC attack:

- Create intrusion detection system rules that flag emails with extensions that are similar to a company email.
- Create an email rule to flag email communications where the "reply" email address is different from the "from" email address is shown.
- Differentiate the email using color coding, prepended tag in the subject that will help to identify emails from employee/internal accounts and emails from non-employee/external accounts.
- Enable two-factor authentication via SMS or authenticator applications such as Google Authenticator, Duo Mobile, FreeOTP, Authy, or Microsoft Authenticator to securely access devices.
- Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication; verify the number from other sources, such as the company's website or previous billing or correspondence, not the numbers provided in the email request.

Recorded Future recommends paying particular attention to the following unusual email requests to prevent BEC fraud:

- Requests that bypass normal channels of communication and request immediate actions such as money transfers or access to documents or information.
- Senior-level management sends unusual requests, especially to employees who are not their direct reports.
- Language, grammar, or format issues revealing errors, typos, and format flaws in emails.
- Requests that the recipient does not communicate the content of the email to others.

Outlook

Data breaches can have a devastating effect on an organization's reputation and financial stability and can facilitate further malicious activity using the information and access obtained as a result of the breach. The sale of database breaches and the resulting leak of information will remain one of the primary cyber threats for the foreseeable future. The sale of access by sophisticated threat actors specializing in breaches will foster related malicious activities such as BEC, tax fraud, phishing, ransomware, and many others.

Recorded Future has identified the most vulnerable industries and a list of the threat actors who are involved in much of this commoditized activity and recommends implementing the mitigation techniques outlined in this report. Additionally, it is highly recommended that entities closely follow the threads, posts, and offerings of these threat actors by monitoring dark web auctions, sale threads on the dark web forums and marketplaces, as well as underground subscription-based services.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.