Scam Radar BD

Protecting the Integrity of Financial and Client Data in the New World Order

(whitepaper revision 2021-MAR)

SecureBrain
A Hitachi Group Company

Overview

The world reeled as the COVID 19 pandemic spread. It impacted not just the lives around the world but global economies as well. The World Bank says that the pandemic had an extensive humanitarian and economic toll causing a global recession, shrinking growth by almost 8%, and trillions of dollars. While the world wrestled with the pandemic, the cybersecurity sector still needed to maintain systems crucial to entire industries' continued operations. In 2019 alone, close to 2 billion people made online transactions. The year before that, there were 368.92 billion purchase transactions for goods and services worldwide. But because of the pandemic, 2020 saw an explosion in eCommerce and mobile transactions. More companies pivoted and put their digitization initiatives into overdrive. In a Mckinsey Global Institute report, about 85% of companies with multi-billion-dollar revenues have accelerated digitization. Cyberattacks took on a fevered pitch using the confusion and chaos to defraud and hold hostage companies and financial institutions (FI). Account takeovers increased by as much as 80%. Phishing attacks spiked, ransomware attacks rose, and fake sites sprouted out of the woodwork. According to reports, these cyberattacks have caused FIs more than **$100 billion**.

The State of Cybersecurity in a Post-Pandemic World

But as more companies shifted immediately to work from home for business continuity, it created new challenges. Securing personal devices that could access the corporate network was the norm. Malicious actors use the pandemic confusion and chaos to carry out phishing, cybertheft, and fraud attacks.

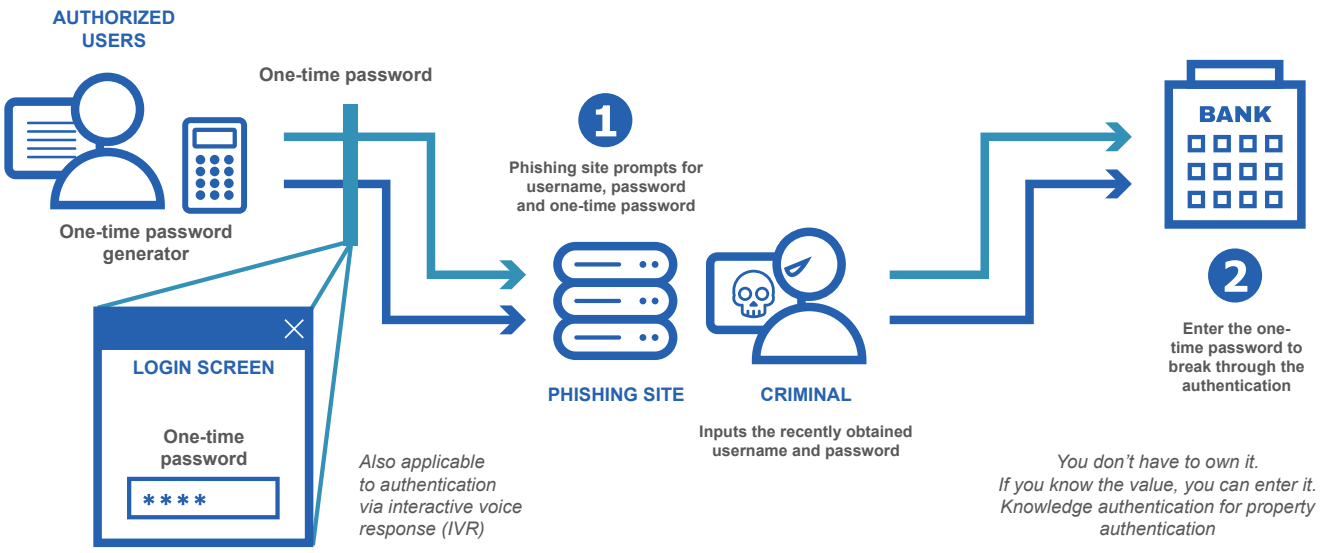
The cost of these attacks is staggering, as data breaches cost companies an average of $8.19 million. Even with a full cybersecurity suite, it could impact these companies by as much as $2.6 million.

Breaking Two-Factor Authentication and Phishing Rampancy

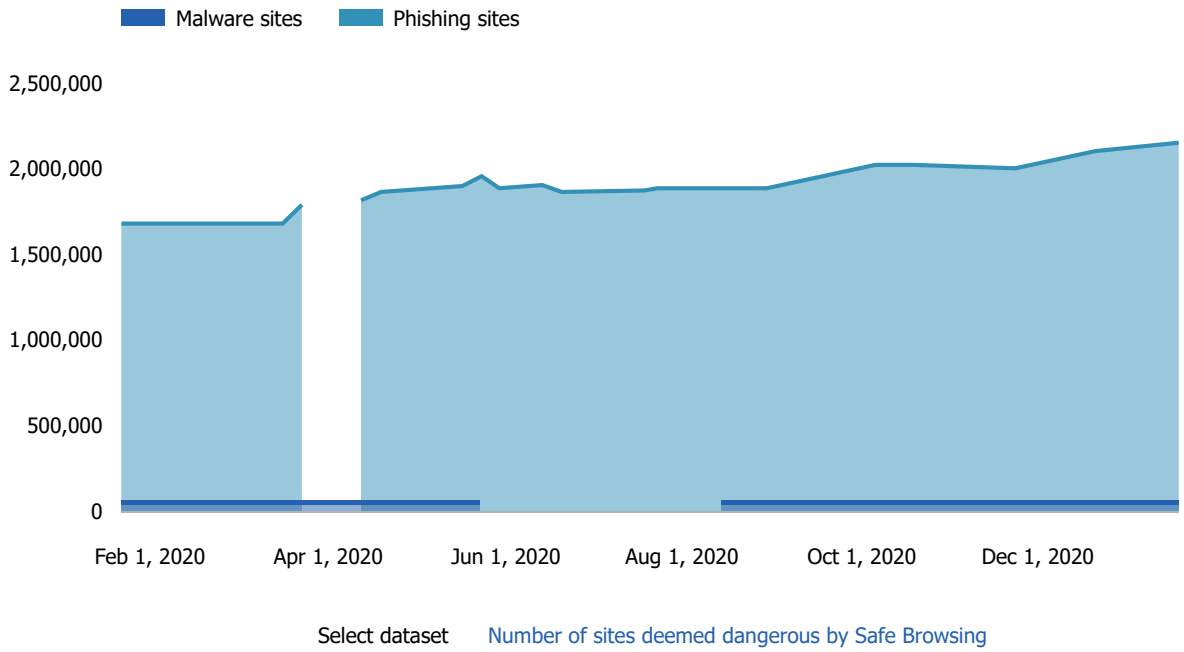
The financial sector has always been at the forefront of adopting new technologies to protect their systems' integrity and customer data. But threat actors continually develop new ways to circumvent it through sophisticated delivery systems or even simple social engineering.

Most security systems require two-factor authentication (2FA), and it has been an effective deterrent to prevent unauthorized access for several years. But even 2FA can be neutralized as it is device-dependent. It does not authenticate the individual but more on identity approximation. A stolen device with a 2FA system can easily access login, personal and financial information. Hackers were able to access these accounts illegally, even without the stolen device. Here is an example of an actual case of a 2FA broken into:

1. A user receives a phishing email that says his online banking will be suspended unless he verifies his login information by clicking on the provided URL.
2. The user clicks on the URL and gets led to a phishing site that asks for his username, password, and one-time password
3. The user uses his one-time password generator and inputs this information.
4. The hacker would then access the real bank website with this information.



Phishing has become more rampant since the pandemic. Google reports that there are more than 2 million phishing sites, a 27% increase from 1.6 million sites last year. Part technology, part social engineering, phishing continues to be some of the more difficult cyberthreats to contain. More than 60% of organizations worldwide lost data because of phishing. And the average cost of data breaches is $3.92 million. The delivery system is still mainly through email (at 96%), and Windows executables and PDFs are the usual attachments. What's worrying is that phishing campaigns have focused more on the enterprise seeing a 355% jump in August 2020. A Japanese online brokerage lost close to a million dollars when malicious actors obtained access to customers' online accounts, including their passwords, and siphoned off funds.

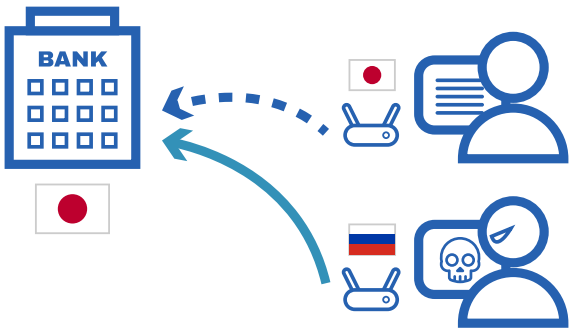


As these cyberattacks continue, the International Monetary Fund declared that Cyber Risk is the New Threat to Financial Stability. As more of the world populace move towards digital transactions, any successful attack on a global financial institution could seriously disrupt interdependent organizations and agencies. It could cause massive disruption in modern life and erode confidence in the financial industry.

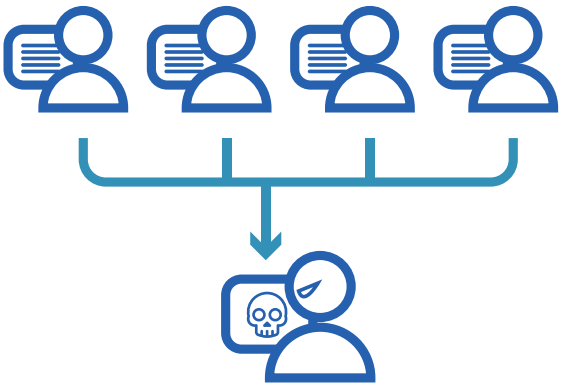
Unauthorized Login and Identity Theft

Here is a list of actual cases of unauthorized login and scenarios encountered:

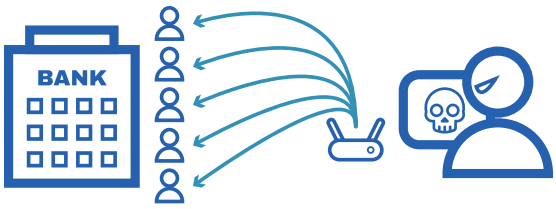
A user from a Russian IP address whose terminal's language setting is Russian tries to log in to a Japanese online banking site.



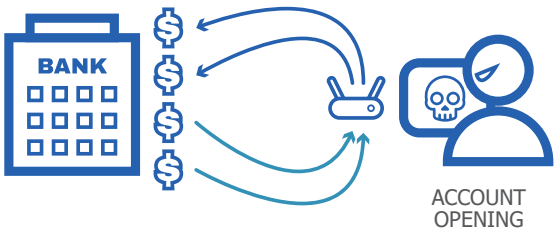
A bank account receives frequent remittances from a large number of people.



There were multiple reports of simultaneous user logins and transactions of an online banking site from the same IP address.



Large and frequent deposits and withdrawals from a bank account immediately after account opening.



Remedies and Prevention

While the usual cybersecurity suites can prevent and deter attacks and financial fraud, more intelligent and analytical systems are needed to protect vital financial system integrity and information. Establishing a cybersecurity risk framework isn't just about the tools, techniques, and solutions; resiliency is also crucial. Some of the more established and popular cybersecurity solutions such as antivirus programs, phishing, spoofed access, and MITB (Man-in-the-browser) detection platforms, multi-factor authentication can prevent unauthorized access; but they can be complicated and limited. Here's why:

- Antivirus and anti-phishing programs that are not updated reduce their effectiveness in detecting malware and phishing sites.
- Identifying spoofed access can be tricky as it might lead to false positives, potentially locking out an authentic user. For example, a Japanese online banking site can decide to block access from Russian IP addresses to deal with Russia's unauthorized login. But this would affect Japanese users who are actually in Russia and need to access their online banking. These detection systems also need continuous analysis of their logs, requiring extensive human resources to accomplish.
- Multi-Factor authentication can be complicated and cost-prohibitive. Confidence in its use has eroded through successful phishing or plain device theft.
- Phishing and MITB detection systems can be difficult to enforce due to restrictions on the user's environment and complicated maintenance of its operating system.

A well-designed, C-level supported cybersecurity risk framework needs to be in place to address these issues. Beyond that, financial institutions need to complement this framework with a full-suite telemetry and access restriction features platform.

Early detection of unauthorized use is necessary as it can minimize the damage. More often than not, the burden of protection lies on the client's side. This conventional thinking doesn't work and can be detrimental to organizations and their users. A multi-layered defense is essential. That means detection systems need to be on the server-side as well. The balance between convenience and cost is also crucial. There must be improved security without compromising user convenience.

One other aspect to ponder on is the capacity and efficiency of internal systems to handle additional operational detection loads. It's vital to secure resources, so cybersecurity teams can quickly respond and analyze vast volumes of access logs. And if there is a solution, can it be used regularly, even for day-to-day operations?

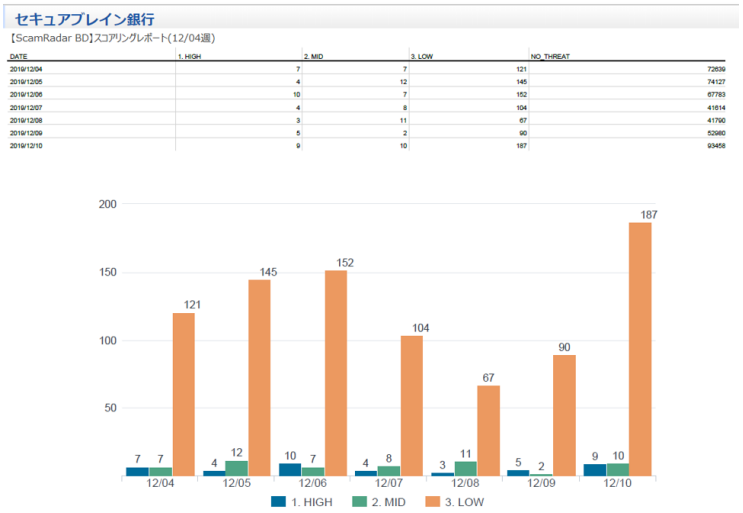
SecureBrain Cybersecurity Specialists

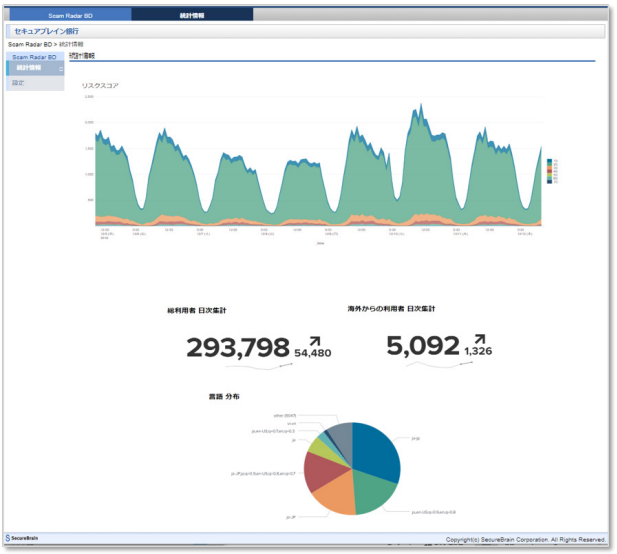
SecureBrain Corporation, a Hitachi Group Company, is a leading cybersecurity solutions provider that has been at the forefront of developing IT security solutions to protect against ever-increasing and evolving Internet-related threats to vendors and companies who offer Web services. It has innovated and evolved its software suites to address cybersecurity risks endemic to financial institutions through the years. SecureBrain **Scam Radar BD** is an independently developed fraud detection service that analyzes Big Data to help prevent fraud on companies that provide essential web transactions such as cashless payment services, Internet banking, and e-commerce systems.

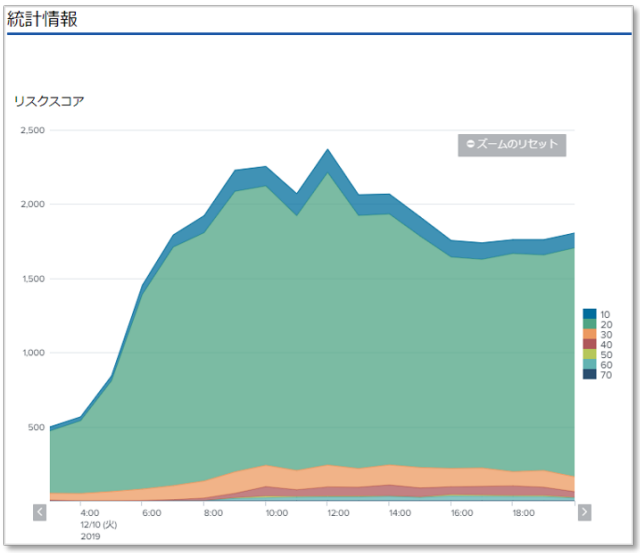
Features and Benefits of Scam Radar BD

As more cyber threat actors use more sophisticated attacks that target passwords and credit card data in the form of list-based attacks and phishing, SecureBrain saw the need to develop a solution that works beyond conventional malpractice thinking.

Scam Radar BD focuses on collecting and analyzing telemetry data generated when accessing Web services or mobile applications in real-time. Its specialists have spent years researching cybercrimes and used its considerable expertise and knowledge to build a system like **Scam Radar BD** to detect fraudulent transactions in real-time. Through Big Data analysis and its unique logic engine, users can get a visual report along with real-time alert notifications. **Scam Radar BD** performs time series analysis of the transactions, which allow it to have a holistic view to make a more accurate judgement.





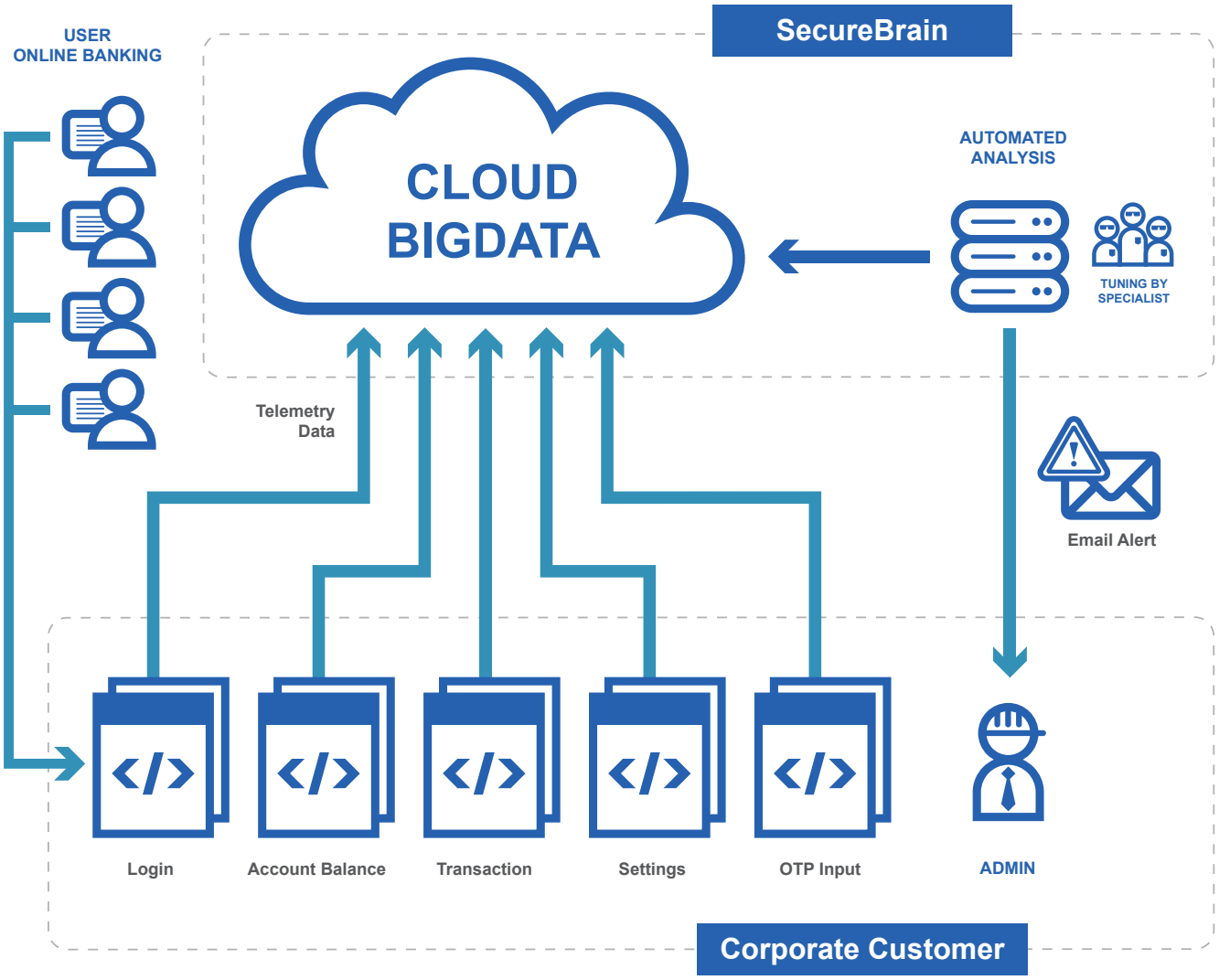


It can then share characteristics and detection patterns of different attacks with all customers who have implemented the service and detect them the first time. What's more, **Scam Radar BD** is easy to implement as there is no need to integrate with existing systems such as cashless payment or Internet banking systems.

System Architecture of Scam Radar BD

It can prevent unauthorized logins, drastically reduce manual log analysis work, visualize unauthorized access status, and detect unauthorized use in other organizations.

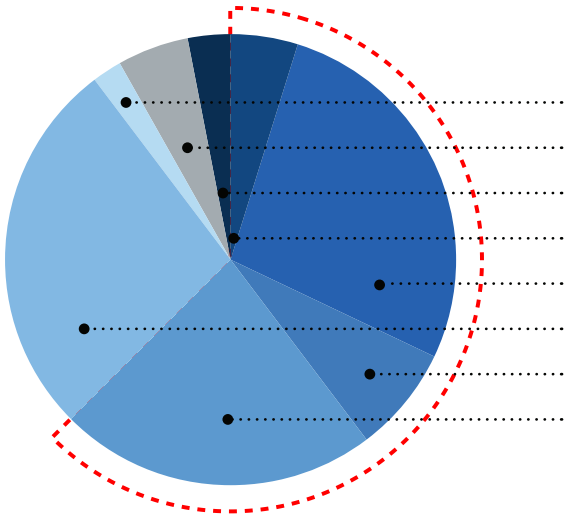
The system analyzes many different data sets, such as user telemetry data and screen transition sequences, to identify unauthorized access and detect suspicious patterns.



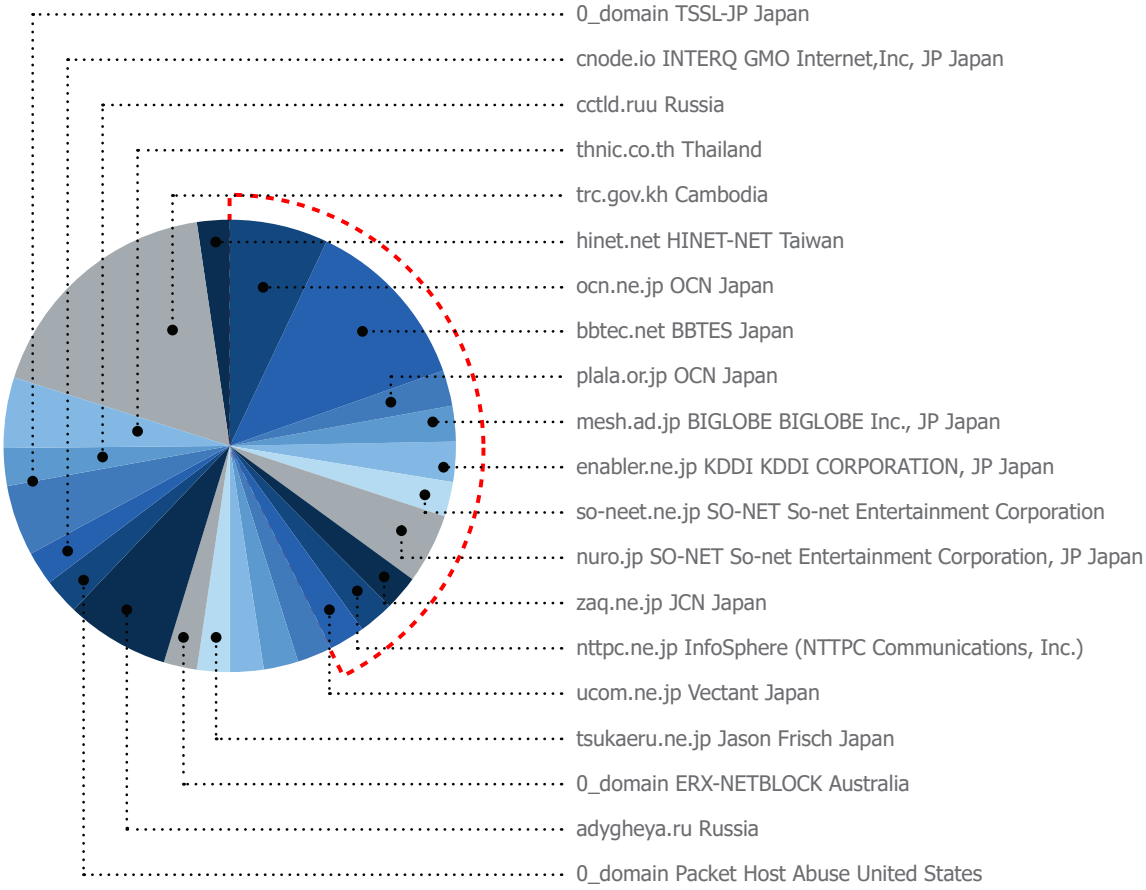
A simple Javascript snippet and a tag get placed on selected pages of the website. When a user visits these tagged pages, the snippet will collect telemetry data for real-time analysis. If suspicious behavior is detected, **Scam Radar BD** provides real-time alerting via email.

Scam Radar BD detection features go beyond conventional threat actor and blackhat thinking.

Language

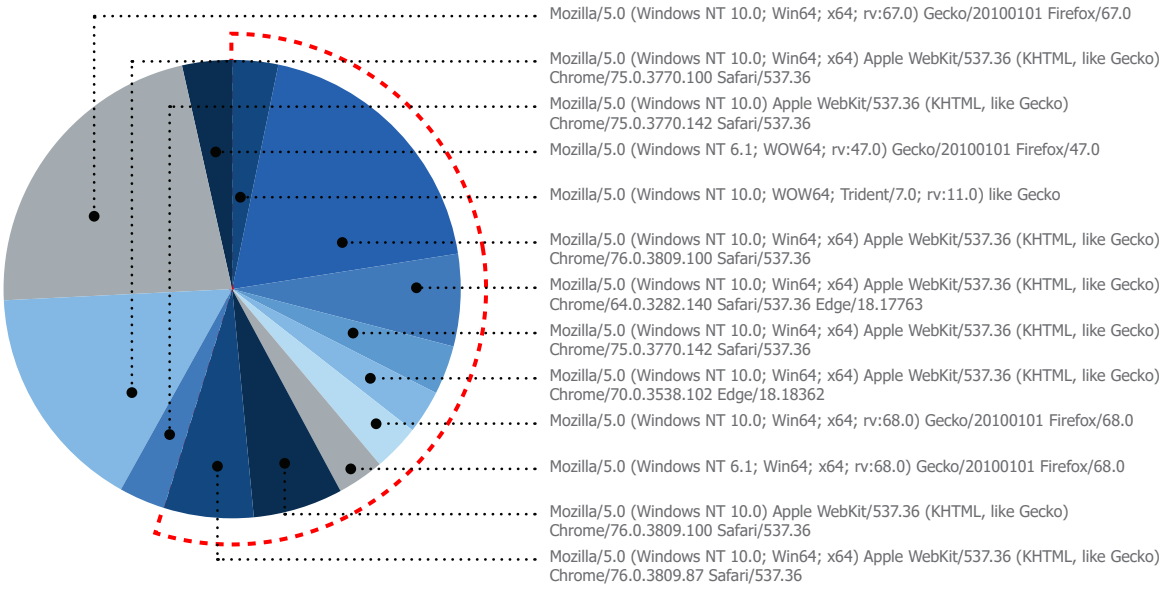


ISP Used



In the red frame is the classification of all regular users.

User Agent



Detection Based on the Attacker's Terminal Information

- It collects terminal attributes such as IP, UA, language and time zone settings. A score is assigned based on a combination of these parameters.
- In addition to the attributes mentioned above, the service performs time series analysis for highly accurate detection of various attacks.

Detection Based on the Attack's Behavior

- Scam Radar BD looks at the amount of time it takes from login up to the payment transaction. If there is a variance from the usual user behavior, it will flag this as suspicious and automatically send an alert notification.
- Scam Radar BD can detect attempts to login with multiple IDs from the same terminal, which is standard for a list-type attack.
- When a hacker is able to access a bank account online using stolen credentials, he would immediately try to change the registered email address and transaction amount limit settings. Scam Radar BD can detect this type of behavior.

Sharing Detection Logic to Prevent Future Crimes

- Our specialists can create and apply detection rules universally regardless of site configuration. These rules can detect based on terminal attributes and behavioral patterns discovered in previous attacks.
- Noise reduction algorithm applied to big data allows automatic filtering of irrelevant data, thus our specialists can focus more on investigating important data and fine tune the detection logic accordingly.

Tuning Through Continuous Analysis

- Detection logic is tuned as new threats are encountered by the system to continuously improve its detection accuracy and noise reduction for filtering out irrelevant data.
- Scam Radar BD uses a simple Javascript snippet and tag to collect visitors' telemetry data for further analysis.
- Clients can also request customized rules to be created to fit their company needs.

Scam Radar BD Competitor Comparison

SecureBrain's fraud detection service can be integrated into Internet and banking systems seamlessly and without impacting operational capacity. We compared it with another service with similar feature sets.

	SecureBrain Scam Radar BD	Vendor A	Vendor B
Ease of implementation	o (tag embedding)	x (low-level programming required)	o (tag embedding)
Mobile browsing supported	o	o	x
Price affordability	Fixed payment for a number of years.	Monthly variable payments (annual contract required)	Monthly premiums
Technology used	Big data analytics, automatic noise reduction, AI, Cloud, heuristics, calibration experts.	AI	AI, Cloud
Industry utilization/ Market segment	All segments including FIs, ECs, member service sites, web payment sites, mobile payment sites	Credit system, ECs	web payment, mobile payments
Country of origin	Japan	USA	Japan

When it comes to implementation, **Scam Radar BD** provides snippet and tag embedding into selected website pages. There's no need to install additional components or software on the server. It fully supports mobile browsing and provides monitoring at the onset. Because rules can be applied universally or customized to specific sites, various industries such as credit card companies, financial institutions, eCommerce companies, membership sites, and much more can use **Scam Radar BD**.

For customers who already have another analysis system in place, integration is possible via API instead of email notification. **Scam Radar BD** can be linked to the analysis system and used as a decision-making material in the risk assessment system. Individual customization is also available.

SecureBrain **Scam Radar BD** is the cybersecurity threat detection solution not only for the pandemic-imperiled financial industry but other business service sectors that host confidential information.

- Accurately detects fraudulent transactions and delivers alerts in real-time.
- Immediately halts fraudulent transactions when it's linked via API to existing systems.
- Respond to many types of sophisticated attacks, such as list attacks and spoofing attacks.
- Get visual reports via a Web-based dashboard.
- Easy to adapt

Transitioning to the Next Normal

2020 was the new normal. But what everyone must plan for is the next normal.

Consumer confidence will return, and more people will shop or even buy more. As more countries relax travel restrictions, the populace will travel again. Tourists will start flooding popular destinations, possibly with a vengeance. And as consumer confidence and spending return to "normal" levels, more small businesses will emerge to answer the growing need for more products and services. Digital will be the norm. More people will opt to use online payments and digital services for safety and convenience. ECommerce and mCommerce utilization will continue to grow exponentially, and there will be more opportunities for threat actors.

The majority, if not all, millennials and Gen Xers will be using mobile banking applications. But users must have a great mobile baking experience. Sixty-four percent (64%) of mobile banking users research a bank's mobile capabilities before opening an account, and if they don't have good experience using these services, they will change banks.

For organizations that offer security services, protecting individuals' and enterprises' data is always vital. Aside from providing multi-factor authentication, security service companies must detect suspicious behavior, flag it, and implement the necessary protocols. **Scam Radar BD**'s behavioral heuristics capabilities that are advanced for the industry, easy to implement, and cost-efficient, will help assure customers.

As 5G adoption gets more widespread, it can potentially transform how cryptocurrencies work is delivered. Experts believe that 5G might be a new paradigm in data transmission. With 5G, transaction management capabilities will be better because of the new band's ultra-low latency. Server distance from the crypto exchange won't matter anymore as 5G can overcome this. With this innovation, fraud detection will be essential to prevent theft and scams.

SecureBrain will continue to improve features and integrate more technologies to help digital transaction and service industries thrive in the next normal.

SecureBrain will continuously develop security products that can quickly address the latest threats under our slogan: "Protecting Your Business from Cybercrime."

Scam Radar BD by Securebrain

With almost two decades of experience, Securebrain is considered as Japan's leading security software provider. Based in Tokyo, our company aims to provide a wide array of security options for every type of business within and outside of Japan.

SecureBrain runs its own research center in order to ensure that we are providing the leading technologies in website malware detection and protection. Our team of researchers is dedicated to identifying new online website security risks and developing solutions to current and future threats.

We have secured the business of several multinational companies as well as government contracts that are specifically geared towards cybercrime and security.

SecureBrain
A Hitachi Group Company

https://www.securebrain.co.jp/eng