Cyber Security Report 2019

Welcome

Dear reader,

Swiss banking has been around since the end of the 14th century. With the emergence of the modern banking system from 1850, our strengths – stability and security – have become ever more apparent. Today, in the 21st century, these strengths are more important than ever. Cybercrime is one of the biggest operational risks in our industry. In order to counter this risk, we need to join forces as the Swiss financial center. Collaboration is key. When it comes to cyber security, we must make no distinction between big and small organizations, between banks and insurance companies. We have to act together. And we must make sure that acting together is no empty phrase: SIX is ready to fully support the financial market players in their efforts.

The SIX Cyber Security Report clearly shows the potential of such collaboration. The fixed costs of cyber defense are high, we face an acute shortage of skilled professionals and there is a tendency for banks to not share enough information. SIX continuously invests in security in order to minimize cyber risks to our system-critical infrastructures. With that investment, we already help banks and insurance companies to uphold their security promise to customers today. By presenting the SIX Cyber Security Report, we are hoping to stimulate better information exchange within the industry – in a similar way to our SIX Cyber Security Hub, a forum for the local cyber security community. You can read more about the Hub on page 8. Please do get in touch with us. We love discussing cyber security.

Happy reading!

Jos Dijsselhof
CEO SIX

Table of Content

Executive Summary

This report gives an overview of the Swiss financial services industry's exposure to cyber security threats.

To do this, the report focuses on two aspects. First, a comparison of Switzerland to its international neighbors with equally or more significant financial services industries. Second, a subdivision of the Swiss financial services industry into different sectors and business-types to see where threats are concentrated and risks most pronounced.

The first part, labelled "Macro Analysis", mainly draws on data gathered from open source intelligence. The second, "Micro Analysis", uses primary evidence collected from members of the SIX Cyber Security Hub.

The report reveals that, over the last 12 months, the countries under review experienced consistent cyberattacks which explicitly targeted their financial services ecosystem. Furthermore, evidence shows that sophisticated cybercriminal groups focus their attacks on specific companies within the industry. In other words, the majority of attacks by sophisticated groups are targeted.

Of these targeted attacks, the most notable examples originated from threat groups known to be based in North Korea or Russia.

Looking at the incidents overall, both targeted and untargeted, our investigations conclude that these cyberattacks were achieved either via exploitation of exposed networks and unpatched vulnerabilities, or via widespread, nondiscriminatory attacks. Out of all malware families, banking trojans, crypto miners and mobile malware continue to be the most popular for use among threat actors.

Zooming in on the specifics of the Swiss financial sector, the analysis shows that we can assign every organization onto one of three tiers that characterize the threats they encounter.

Starting from a tier with the smallest diversity of threats, each tier accumulates additional threats in direct relation with its activity profile on the financial market.

Overall, phishing threats cause the highest number of incidents, where it can also be observed that the amount of targeted phishing compared to untargeted phishing varies from tier to tier.

This report is authored by SIX, together with research inputs from Recorded Future.

Key Findings

- The financial services industry continues to be an attractive target for cybercriminals.
- The most notable types of threat actor to target the financial services industry are cybercriminals, motivated by profit, and state-sponsored entities, motivated to gain some sort of competitive advantage.
- Of all malware families, banking trojans, crypto miners and mobile malware have had the most significant impact on the financial services industry over the past year.
- The majority of mentions on the Dark Web of targeting financial services organizations were attributable to just four platforms: Offensive Community, Raid Forums, Gaza Hacker Team Forum and Bits Hacking Forum. Threat actors operating on such platforms were found to vary in sophistication.
- In 2018, incidents of data theft via Point of Sale (PoS) malware cost e-commerce organizations and online payment systems millions of dollars in financial loss, in addition to reputational damage.
- Based on the current growth of the IoT, mobile and cloud computing markets, there will be a massive increase in the attack surface (the number of potential points of intrusion) for financial services organizations in the coming years.
- The number of references to cyber events in the financial services industry has doubled over the last year. This is likely a result of the increased severity of mobile malware threats and accessibility of mobile malware samples for cybercriminals thanks to decreasing prices among underground sources.

Why This Report

Ginni Rometty, CEO and President of IBM, stated as early as 2015: “Cybercrime is the greatest threat to every company in the world”. At SIX, our many years of experience have shown us that two elements are absolutely crucial to warding off this threat. Protection against cyber attacks must be both comprehensive and continuous; this is the only way to manage and control the risk. Apart from technical considerations, comprehensive protection should be understood in terms of its proximity to the business field: banking infrastructure is particularly system-critical and must therefore be carefully and adequately protected. Continuity requires that protection and defense mechanisms are in place around the clock, every day of the year, and can be activated within a very short space of time.

These Two Key Principles Form the Basis of SIX Cyber Security Services’ Four Pillars:

1. **From Banks, for Banks.** The systemically relevant SIX infrastructure is subject to state supervision and monitoring. This means we have a detailed understanding of the needs of our customers in the banking and insurance sector and are familiar with the strict regulatory requirements.

2. **1+1=3.** In cyber security, the economies of scale are enormous. Protecting one bank requires almost the same infrastructure as protecting 20 banks. Consequently, it makes sense for financial institutions to outsource this activity – which is not part of their core business – to external experts. Thanks to the larger volumes, SIX can provide a broader offering that considerably exceeds the protective measures a single bank could implement for itself.

3. **Sharing Is Caring.** Protected, moderated and highly transparent information exchanges among security experts are immensely important in the fight against cybercrime. The SIX Cyber Security Hub is designed specifically for this purpose. It provides a non-commercial communication platform where experts can share and discuss learnings, insights, know-how and information about vulnerabilities and cyber attacks. Participants sign a Code of Conduct; this allows SIX to guarantee a high-quality discussion.

4. **The Best Talent.** SIX addresses the shortage of skilled cyber security experts by consciously and extensively training and educating employees. Cyber security is part of our core business and as such, covers a sizeable volume. This makes us an attractive employer for cyber security experts.

Contributors

The Cyber Security Report reflects our knowledge and expertise at SIX. It analyses and interprets SIX data as well as external events such as cyber attacks, security incidents and vulnerabilities. Because cyber security is a topic that, for the most part, is not limited to national borders, we have provided space for discussing cyber security in Switzerland alongside the rest of the world.

Contributors to the SIX Cyber Security Report 2019 were:

- Recorded Future. Recorded Future is an Internet technology company specialising in real-time threat intelligence. Recorded Future automatically organises open web, Dark Web, and technical sources for analysis so information security teams can stay ahead of cyber attacks.
- Members of the Cyber Security Hub by SIX.

The Cyber Security Hub by SIX is a non-commercial platform that facilitates the constant exchange of cyber security information. It helps the cyber security community share experiences, learnings and knowledge as well as vulnerability and attack information.

All Swiss banks and insurance companies that are FINMA-regulated are invited to participate.

Become part of the Cyber Security Hub:
www.six-group.com/cybersecurityhub

Methodology

For the purpose of this report, SIX collected and investigated cyber security information in collaboration with Recorded Future.

The main data sources for this report are open source intelligence information (OSINT) and information gathered from the members of the SIX Cyber Security Hub.

The macro analysis examines a sample of the G20 nations and Switzerland with regard to cyber threats of their financial sectors. The graphs in the macro section contain information about the total number of incidents as well as illustrating “sentiment” about cyber attacks, which is based on an interpretation of opinions expressed (e.g. as text in tweets).

For the micro analysis of the Swiss financial sector, Swiss financial institutions are assigned to one of three tiers based on the institutions’ main focus of activity (e.g. wealth management).

Macro Analysis: Comparison by Country

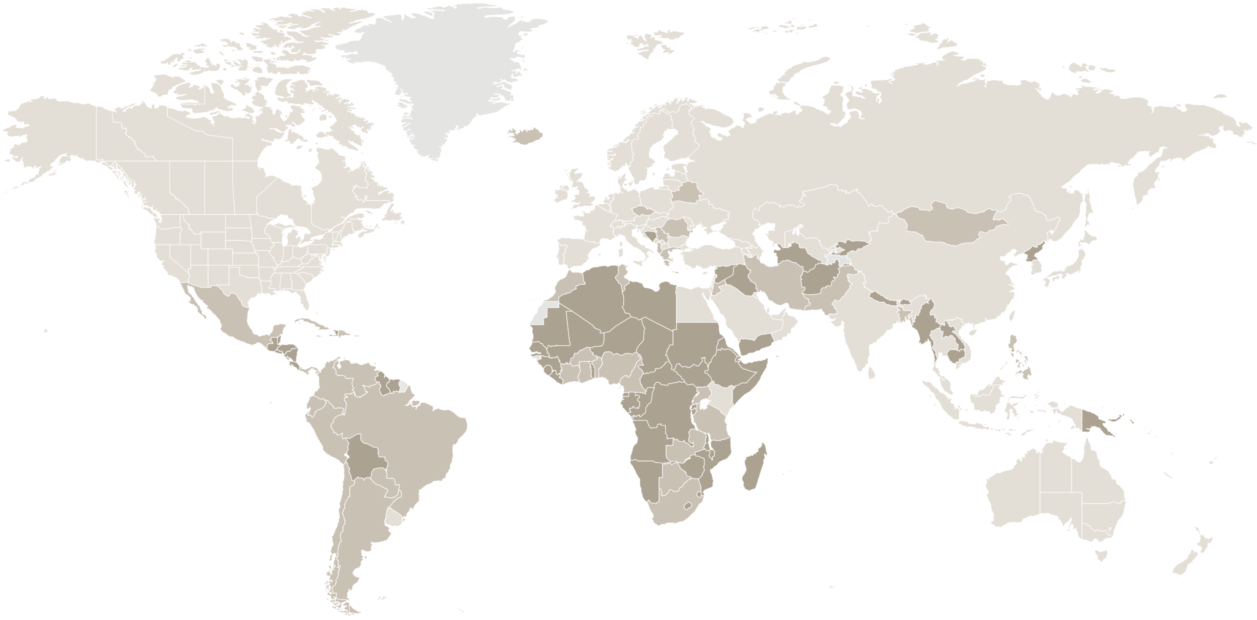
Over the past year, there has been rising concern among the press, public and financial services industry around the increasing number of cyberattacks on companies within the sector. A likely contributing factor to these attacks is the wide range of systems being used on a daily basis within the industry, many of which are either outdated or unsecured. On top of this, the amount of payment information contained within these systems renders the industry an attractive target for financially motivated threat groups and cybercriminals.

In tandem with this uptick in cyber activity, the past few years have seen a trend of underreporting cyberattacks among G20 nations. In 2017, only 49% of cyberattacks were believed to have been reported to financial authorities within G20 nations such as the United Kingdom. At the heart of this is the fact that there exists no universal standard to report these attacks. This is compounded by the increasing number of organizations with business operations spanning multiple G20 countries. Unless required by more stringent laws in a particular country, there is very little incentive to report.

Beyond reporting, there remain many visible gaps between G20 countries in terms of national cyber security strategies and legislation more broadly.

The International Telecommunication Unit (ITU), an agency of the United Nations (UN), produces an annual global cyber security index to measure a country's commitment to the cyber threat landscape through five primary pillars:

- Legal (Existing Legislation, Regulation)
- Technical (Technology Used for Defense, Standards Implementation Framework, Use of Cert or Incident Response Teams)
- Organizational (National Strategies, Regulatory Agencies, Cyber Security Metrics)
- Capacity Building (Professional Training Courses, Public Accreditation, Public Awareness Campaigns)
- Cooperation (Partnerships between Public and Private Sectors, Participation in International Forums)



Countries are classified according to their level of commitment: high, medium and low.

- □ Countries that demonstrate high commitment in all five pillars of the index.
- ▨ Countries that have developed complex commitments and engage in cyber security programmes and initiatives.
- ■ Countries that have started to initiate commitments in cyber security.

2018 Classification via the Global Cyber Security Index, Source: ITU

There is currently no acknowledged method of quantitatively measuring cyber risk within financial services by country. However, all of the G20 countries sampled in this macro analysis are officially listed as having a high level of commitment to cyber security (the highest ranking available via this standard).

At the end of 2017, the ITU attempted to construct an index accurately monitoring for cyber threat terminology associated with international banking institutions. During the process, it was noted that complete datasets on cyberattacks are incredibly scarce. While select public and commercial datasets do exist, they are often incomplete, have varying levels of coverage, and use different definitions of “cyberattack”. Ultimately, this makes analysis of cyber losses difficult.

The graphs for each country in the following subsections show two aspects of cyber attack activity relating to the countries financial sectors as observed across open source reporting. First, the bar in the graph shows the total number of events that were observed for each month. Second, the marker indicates the most negative sentiment that was expressed over all of the events of one month (for more information regarding the negative sentiment, please refer to the subsection methodology in the introduction).

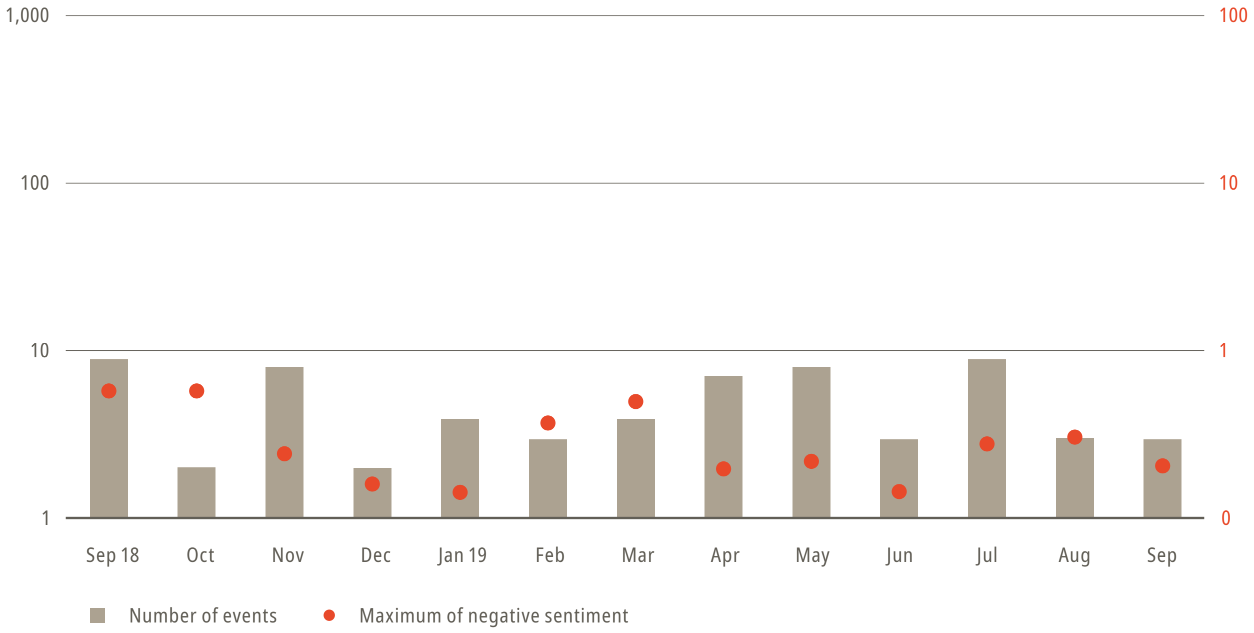
The x-axis shows each month for the period that was investigated for this report. The y-axis on the left refers to the values for the total number of events observed, while the y-axis on the right refers to the values for the maximum negative sentiment, which therefore has the same color as the respective markers. When no marker is printed for a specific month, it means that there was no expression of negative sentiment observed during that time.

As the values for the various countries in this section differ significantly, the y-axis use a “compressed” (logarithmic) scale. That means one tick shows values from 1 to 10 while the next tick of equal size shows values from 10 to 100 and so on. Please also note that the y-axis on the left ranges from 1 to 1000 while on the right it ranges from 0 to 100.

Switzerland

Switzerland's financial services industry has, at a macro level, similar cyber vulnerabilities to those of other nations detailed within this report. Common methods of attack, like phishing attacks, designed to target employees with access to critical financial systems are a concern. Over the past year, cybercriminals have also demonstrated a willingness to update variants of malware (such as Trickbot) to target firms in the region.

The graph below illustrates the cyberattack activity relating to the Swiss financial sector as observed across open source reporting. For information about how this graph is structured, please refer to the beginning of the macro analysis section.



Switzerland Cyber Event Timeline (Finance/Banking/Insurance)

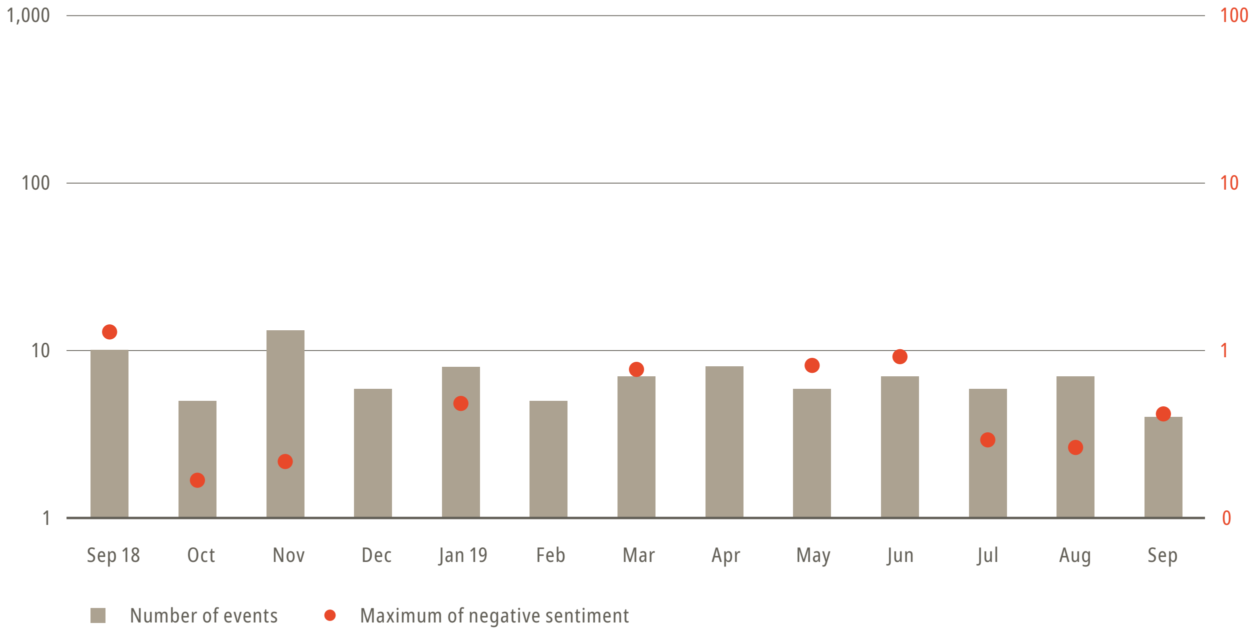
Singapore

The analysis for this report identified three advanced persistent threat (APT) groups that have directly targeted organizations within Singapore in the last year. Our findings show that the industries most likely to be targeted are healthcare, media, telecommunications, and engineering – not financial services. The APT threat groups likely targeted these industries as a result of the vast amounts of sensitive information housed within their various Singapore-based organizations (such as SingHealth). Such data could be used for corporate espionage or the sale of patient data by financially motivated cybercriminals.

In the context of the financial services industry, owing to the characteristics of this region, the national regulator (Monetary Authority of Singapore) has been particularly thorough and effective at ensuring a high cyber security baseline for the organizations it regulates. This has resulted in comparatively stronger infrastructure when compared with other industries.

The graph below illustrates the cyberattack activity relating to the financial sector of Singapore as observed across open source reporting. For information about how this graph is structured, please refer to the introduction in the beginning of this section.

However, as observed in the timeline, there are still examples of Singaporean banks being targeted within the last year. These attacks have been attributed to Russian cybercriminals, though unaffiliated with any Russian-based APT group.



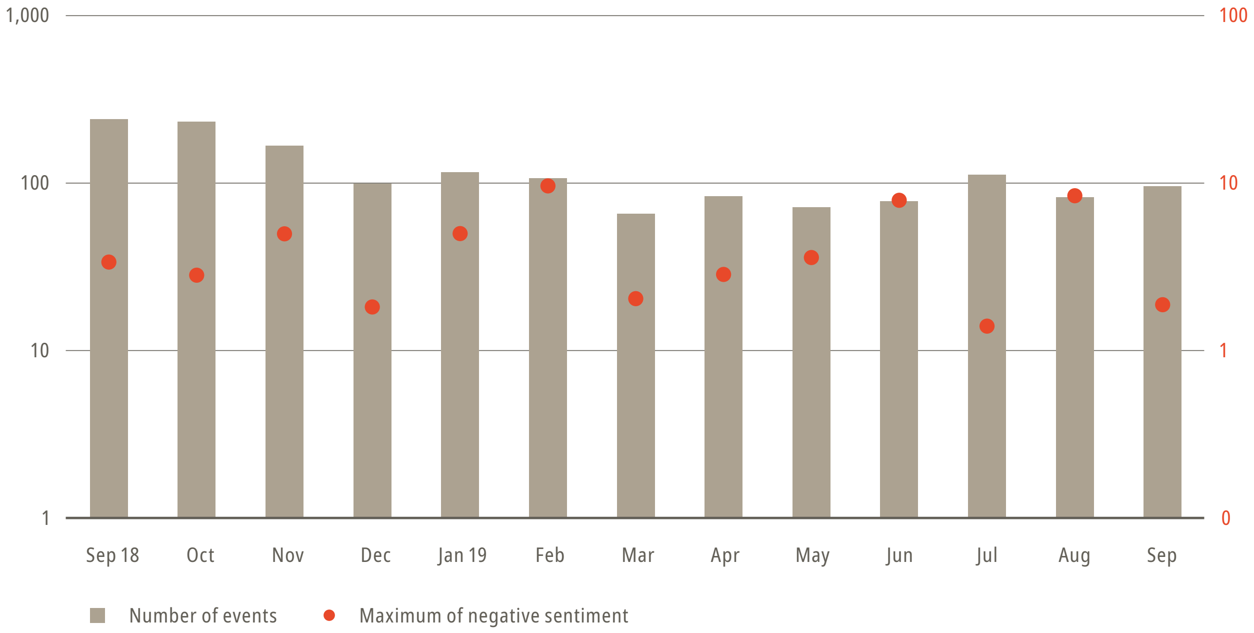
Singapore Cyber Event Timeline (Finance/Banking/Insurance)

United Kingdom

Britain's security services recently issued a warning to financial organizations on the growing danger of cyberattacks by nation-state actors, particularly those based out of Russia. The warning included a discussion around the dangers of Britain's reliance on a handful of providers of cloud computing services, exposing many organizations based in the United Kingdom to a single point of failure. If just one of these central providers were to be targeted effectively, it could theoretically take down the entire financial services industry within the UK, as well as having potential ramifications abroad.

As noted in the timeline below, our research group has observed an overall decrease in the amount of threatening cyber activity reported within the UK financial services industry over the past year. However, as identified by Britain's security services, it's critical to note that nation-state attacks are likely to operate at a level of technical sophistication that would make attribution and mitigation difficult.

The graph below illustrates the cyberattack activity relating to the financial sector of the UK as observed across open source reporting. For information about how this graph is structured, please refer to the introduction in the beginning of this section.



United Kingdom Cyber Event Timeline (Finance/Banking/Insurance)

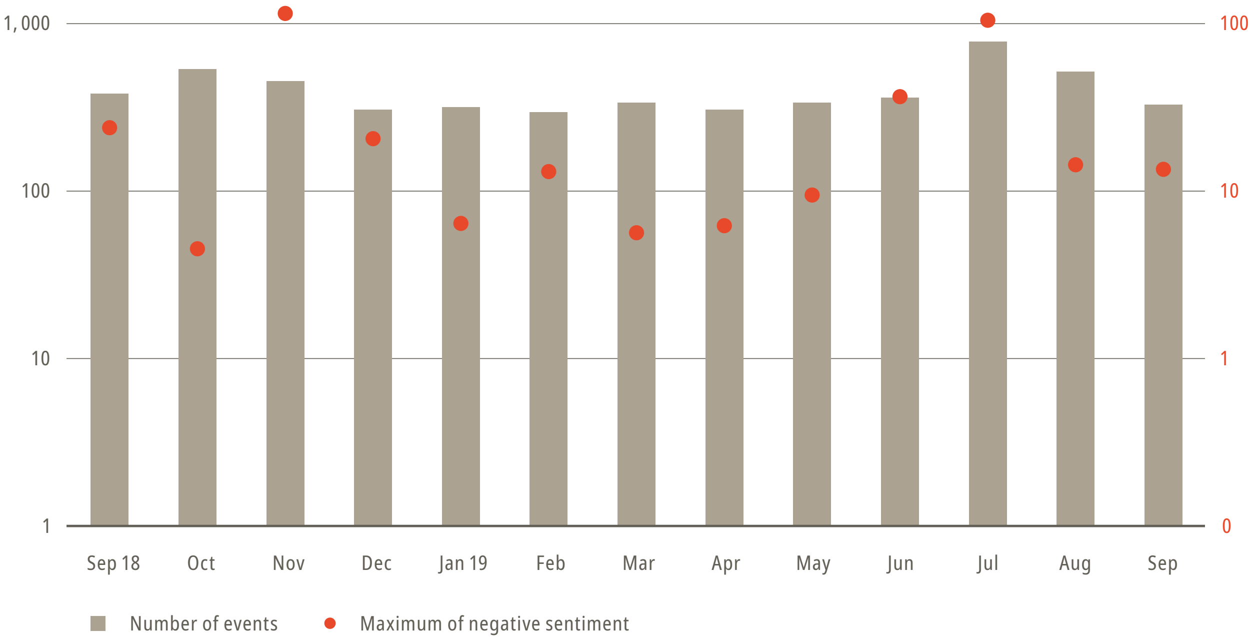
United States

The financial services industry in the United States (US) has historically been a popular target for cyberattacks, a trend which has continued into 2019. The reason for this is relatively straightforward: the rest of the economy is highly dependent on the nation's strong international business presence and access to financial information.

That said, financial organizations themselves are by no means the only, or even the preferred, target for attack. Customers, third parties, and downstream vendors appear to present more convenient avenues for gaining access to monetizable financial information. This is understandable given the financial institutions themselves have invested heavily in cyber defenses. A smart cybercriminal will focus on less well-defended parts of the value chain, as demonstrated by historic attacks on physical peripherals like ATMs and Point of Sale (PoS) devices.

Technological developments in blockchain and cryptocurrencies have also served to extend both the available threat surface and the types of organizations involved in financial transactions. On top of this, large scale US-based data breaches and leaks over the past year have substantially increased the likelihood of leaked credentials to be used in password brute-forcing and credential stuffing attacks. In each case, the predominant motivation for these attacks is attaining access to customer data for financial gain.

The graph below illustrates the cyberattack activity relating to the US financial sector as observed across open source reporting. The most negative sentiment were observed for activities around events concerning HSBC and Capital One in November 18 and July 19 respectively. For information about how this graph is structured, please refer to the introduction in the beginning of this section.



United States Cyber Event Timeline (Finance/Banking/Insurance)

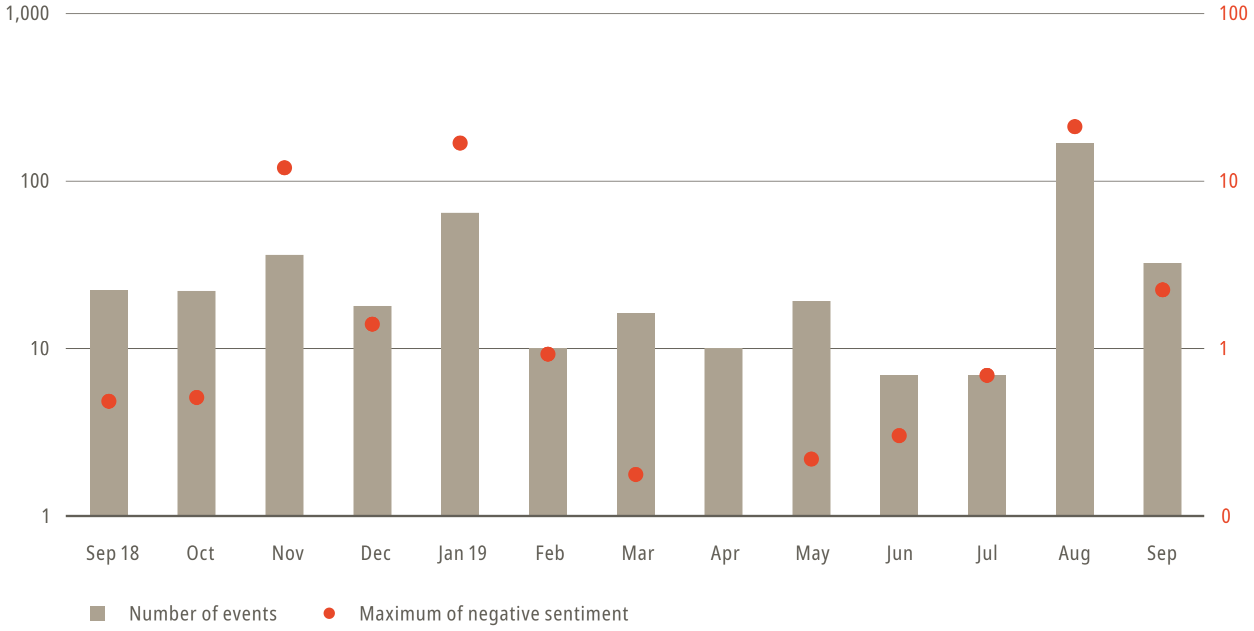
Germany

Several factors make Germany a higher risk area for potential malicious cyber activity, the most prominent being the high density of major financial institutions operating in Frankfurt – attractive targets for sophisticated cybercriminals.

In fact, the high concentration of both data centers regional and global headquarters for financial institutions likely attracts targeted operations and cyberattacks – not only from cybercriminals, but also state-sponsored groups. This is not likely to decrease in the coming years, with increasing geopolitical tensions between Russia and the West, as well as in the Middle East.

This report observed consistent Russian influence behind suspected state-sponsored activity. The degree of attribution of these cases varies, however the pattern is noticeable enough. Russian-sponsored threats should be of elevated concern when considering cyber threats to the German financial services industry.

The graph below illustrates the cyberattack activity relating to the German financial sector as observed across open source reporting. For information about how this graph is structured, please refer to the introduction in the beginning of this section.



Germany Cyber Event Timeline (Finance/Banking/Insurance)

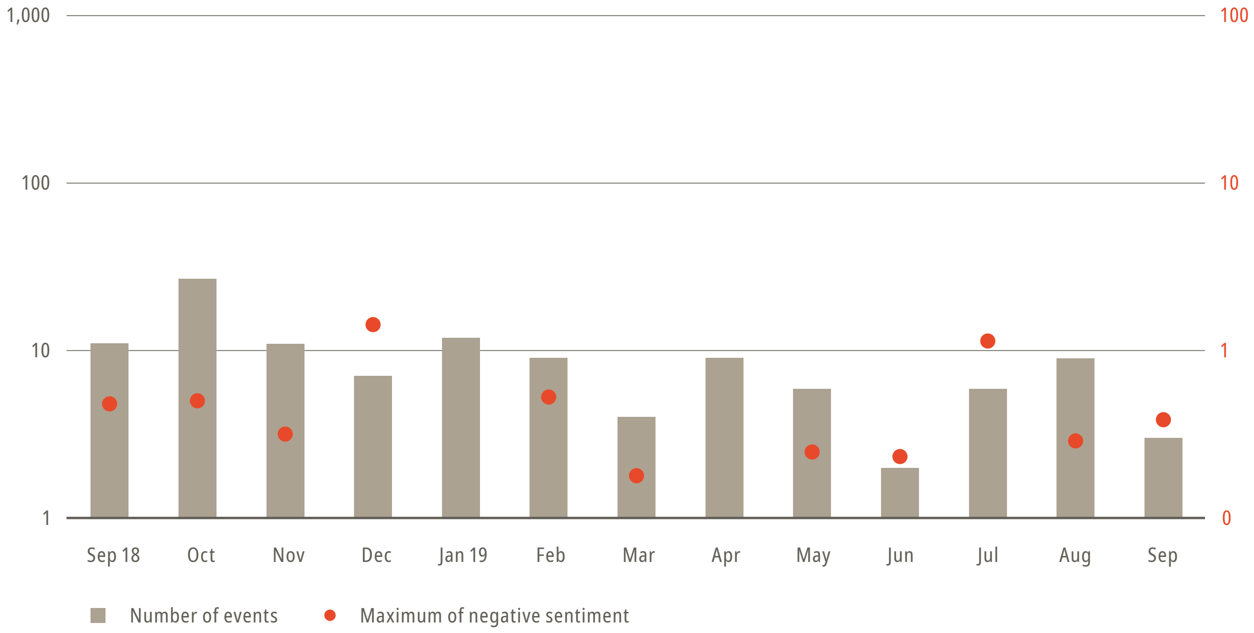
The Netherlands

Over the past year, this report has identified frequent references to Dutch organizations across the Dark Web and other underground sources, predominantly pertaining to the sale of online banking credentials, stolen credit card information, and banking malware such as web injects.

We also observed multiple references to advertisements for various account credentials and credit card data most likely belonging to customers of Dutch financial institutions.

As with most other G20 countries detailed in this section, financial institutions within the Netherlands were identified as being increasingly targeted by Russian and Iranian state-sponsored groups over the past year. Several other malicious entities that have historically targeted Dutch organizations have also been observed conducting active threat campaigns this past quarter, primarily motivated by financial gain.

The graph below illustrates the cyberattack activity relating to the Dutch financial sector as observed across open source reporting. For information about how this graph is structured, please refer to the introduction in the beginning of this section.



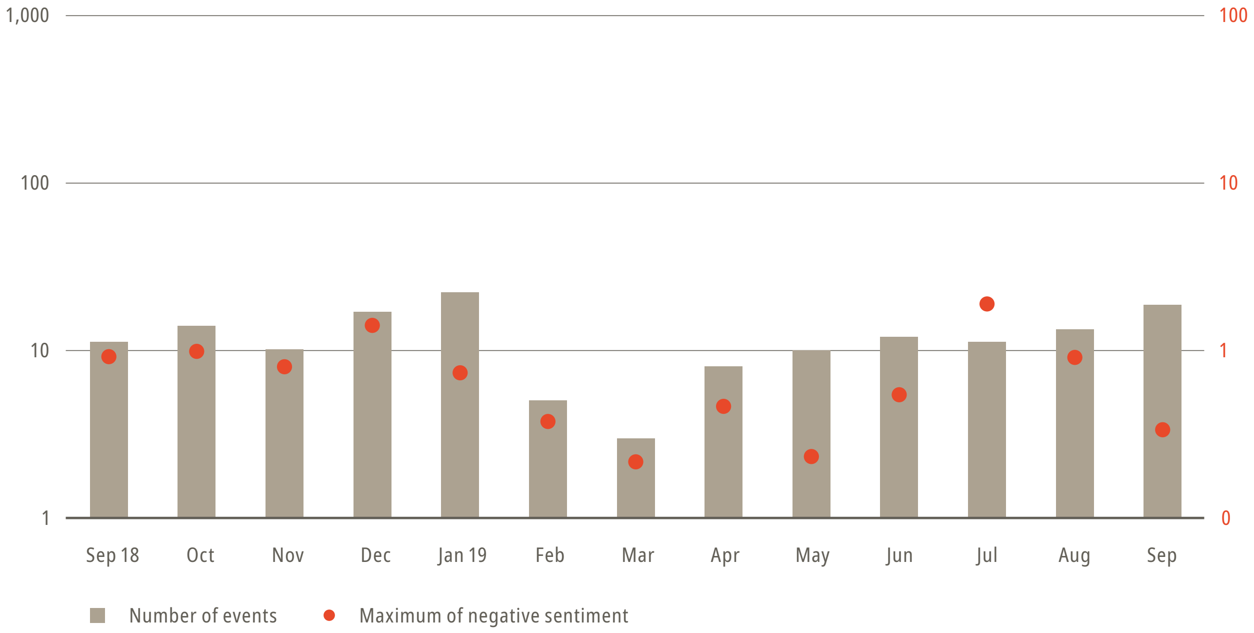
The Netherlands Cyber Event Timeline (Finance/Banking/Insurance)

France

2018 saw an increase in the number of malware attacks on financial institutions worldwide, particularly via banking trojans focused on targeting websites, mobile applications used by financial institutions, and Point of Sale (PoS) and payment processing systems used by e-commerce organizations.

The time span investigated in this report observed a temporary decrease in the volume of cyberattacks within France's financial services industry in the beginning 2019. Overall, we observed an increase in threat activity collectively targeting multiple countries across the European continent, as opposed to French organizations specifically.

The graph below illustrates the cyberattack activity relating to the French financial sector as observed across open source reporting. For information about how this graph is structured, please refer to the introduction in the beginning of this section.



France Cyber Event Timeline (Finance/Banking/Insurance)

Micro Analysis: Finance Industry in Switzerland

This report analyzes data from over forty financial services institutions across insurance, banking, securities, and investment, with headquarters or a significant presence in Switzerland. It investigates cyber events and credential leaks affecting these organizations, as well as Dark Web and underground discussions which have mentioned them over the past year.

Most of the cyber security executives participating in the SIX Cyber Security Hub program were confidentially interviewed for this report. Those interviews yielded a significant amount of highly relevant information on past incidents and near misses that organizations have suffered over the past 12 months. For apparent confidentiality reasons, all information was anonymized after collection. Wherever this report mentions individual anonymized examples, it does not contain information that originated from this confidential data collection. Confidentially shared information was only used in aggregate analysis in order to protect the interests of the Cyber Security Hub members.

Key Findings

In analyzing the collected information, we found that financial organizations with different characteristics tend to be subject to different combinations of threats. Based on this analysis, this report groups the Swiss financial services industry into three categories of organization that share common characteristics and threats. Those three tiers are:

Tier 3

- Insurance
- Investment Banking
- Securities and Trading

Over the past year, Tier 3 organizations have been subject to both targeted and generic phishing campaigns. A few have suffered significant data leakage, either directly or via third parties. There is little-to-no mention of Tier 3 organizations on the Dark Web.

Tier 2

- Small and Medium Retail Banking
- Financial Infrastructure Providers (e.g. SIX)
- Corporate Banking
- Wealth Management

In addition to the attack categories associated with Tier 3, Tier 2 organizations have been subject to a lot more phishing activity, low intensity targeted attacks, and extortion attempts.

Tier 1

- Large Retail Banking

On top of the attacks associated with Tier 2 and Tier 3 organizations, Tier 1 institutions have been regularly exposed to targeted malware attacks, as well as all categories of phishing attempts.

We also identified several targeted attacks implementing banking malware and trojans, focused on Tier 1 institutions' customers, as opposed to the organizations themselves.

The reader may note that the tiers inherit threats from each other, meaning that, for example, a Tier 2 organization faces all threats observed in Tier 3, plus additional threats associated with Tier 2.

Comparing Switzerland to Its Neighbors

It appears from the results that the Swiss financial services industry has been less affected by cyber security incidents than those of neighboring countries. The section below outlines more evidence. This prompted our team to ask why: to investigate the root causes and identify salient principles that the broader financial services community can learn from.

First, there seems to be a correlation between a large number of attacks and retail banking activity. The wider the reach of the retail banking organization, the broader the attack landscape and the higher the number of incidents.

Although Switzerland hosts several hundred financial services organizations, the Confederation does not have many sizeable retail banking organizations when compared to, say, France, the Netherlands, Germany, or the UK. Over the last year, those large retail banks that do exist in Switzerland received the bulk of attacks, supporting the correlation we observed.

Swiss Wealth Management and Private Banking: Insulated against Targeted Attacks?

Based on the data collated from the confidential interviews and open source intelligence, our analysis suggests that the wealth management and private banking sectors within Tier 2 are subject to significantly fewer cyberattacks when compared with other organizations.

We attribute the relatively low level of attempted targeted attacks towards the wealth management and private banking sector to the far more manual and labor-intensive nature of these activities. Besides, these organizations in Switzerland are usually reasonably small and have developed tried and tested control procedures. These characteristics have – by and large – insulated these institutions against attack.

Digitalizing these environments, outsourcing overseas, or delegating tasks to less sophisticated human resources would automatically increase the risk and likelihood of targeted attacks. Therefore, any such initiative should be considered from a risk/reward perspective, and combined with the deployment of adequate controls.

Beyond the Organization: Protecting Customers and Partners

Cyberthreats do not stop at the border of the organization. Our research shows numerous cybercriminal activities are aimed at Swiss financial institutions' customers, rather than at the organizations themselves. For example, fake banking applications and spoofed websites are designed to lure and profit from customers directly, with no need to compromise the actual institutions. Cybercriminals seem to find this a more convenient way to gain access to monetizable financial information. This was corroborated by the interviews conducted for this report: the compromise of customers, third parties, and downstream being a major concern for Swiss financial services organizations.

Sample Results

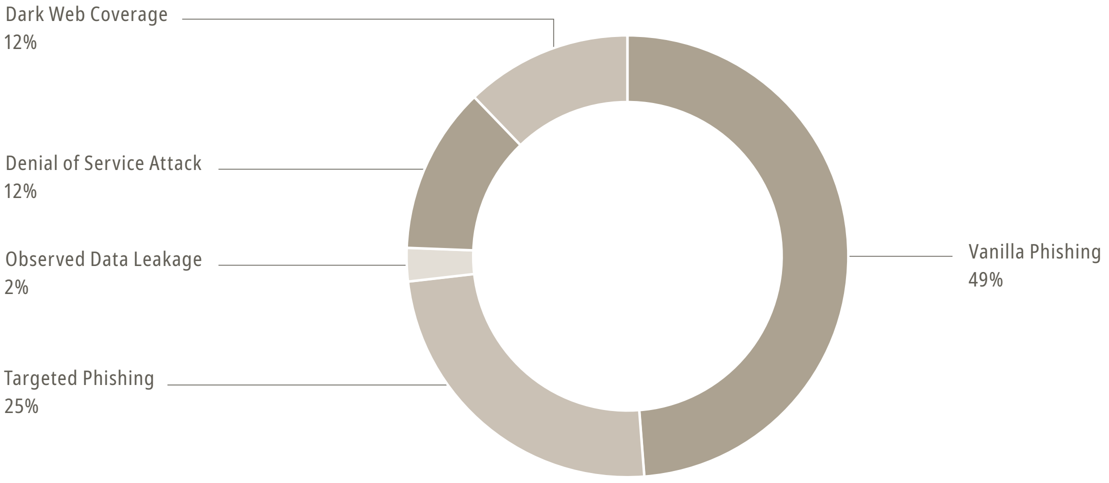
The results presented in this section are mainly based on confidential interviews conducted with the SIX Cyber Security Hub members. Additional information and examples are taken from collected open source intelligence. This report focuses on two key areas of analysis: first, how cyberattacks differ between organizational tiers, both by type and volume; second, what insights can be drawn from Dark Web conversations regarding different organizations. These results should be understood as interpretations of trends based on our data rather than precise reference values for organizations similar to the ones sampled. Examples given in this section are for illustration purposes and do not necessarily refer to any member of the Cyber Security Hub.

Tier 3 Organizations

Organizations in this tier belong to the insurance, investment banking and securities, and trading classes within the financial sector of Switzerland. Looking at the total volume of cyber events reported for this tier, phishing attacks make up by far the largest part, amounting to almost three quarters of the total cyberattacks registered. From all phishing attacks, about two thirds are vanilla phishing, meaning the attacks were not targeted at the specific organization. Dark Web coverage in this context counts every mention of one of the sampled organizations in the Dark Web. For organizations with strong international presence, a specific mention cannot be attributed to its Swiss or international presence and is therefore counted in any case. Therefore, the Dark Web coverage may appear relatively large compared to the other categories.

Some notable and representative examples of cyber events to afflict Tier 3 organizations in our timeframe include:

- Mentioning / offering of domains belonging to specific organizations on Genesis Store (see Box-out).



Qualitative chart based on anonymized SIX Cyber Security Hub information

Genesis Store is operated by the threat actor of the same name, Genesis Store. The Genesis Store forum operates by selling the browser fingerprints of compromised host machines. These host machines are first infected by malware, which turns the machine into a bot. The machine can then be used for other malicious activity such as Distributed Denial of Service (DDoS) attacks. Additionally, while the machine is a bot, the information from the machine is collected through various means and sold on Dark Web and underground forums, such as Genesis Store.

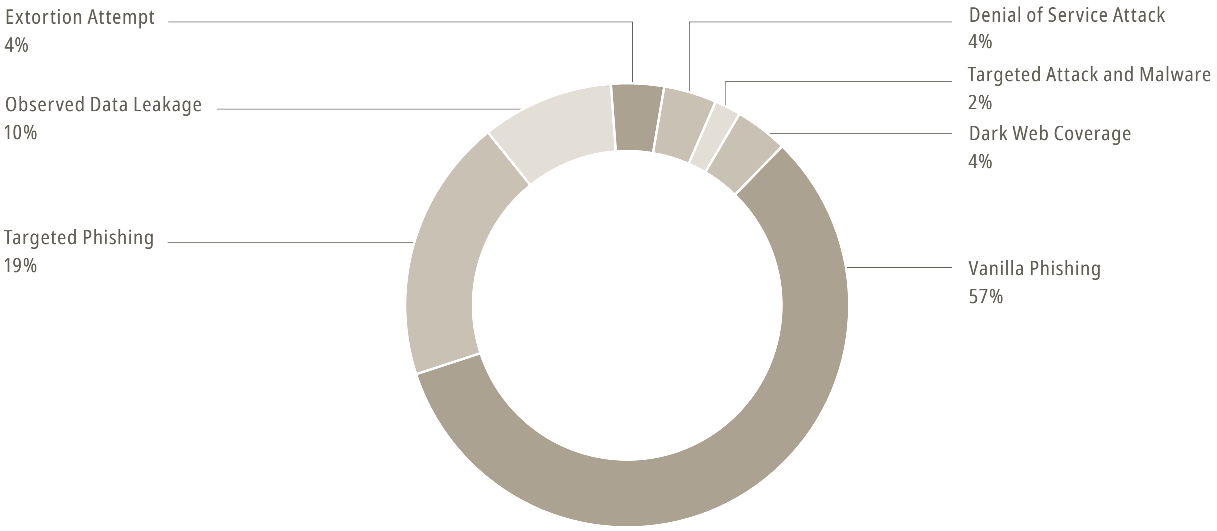
Through this, the purchaser has access to a combination of fingerprints, cookies, form-grabbing logs, account credentials and other information obtained from the victim's machine's browser. Cybercriminals can download a custom browser plugin built for Chromium, which allows them to import the victim's data. After the purchase, the cybercriminals can log into the user's browser to access various accounts for the purpose of stealing funds, personal photos, sensitive or proprietary documents, etc.

Tier 2 Organizations

Tier 2 organizations consist of small to medium retail banking, corporate banking, wealth management and financial infrastructure providers. Of the cyberattacks that our sampled Tier 2 organizations are subject to, more than three quarters are phishing attacks. Almost half of the remaining part consists of data leakage, which includes payment card information among other types of leaked information. Further breakdown of the phishing attacks reveals that most are instances of vanilla phishing with approximately one quarter targeted. In alignment with what this analysis observed for tier 2 organizations in general, also the Dark Web coverage for this tier is significantly lower than for the other tiers.

Some notable and representative examples of cyber events to afflict Tier 2 organizations in our timeframe include:

- Interest among actors operating on BHF Forum in compromising a wealth management and corporate bank's ATM machines, as recently as March 2019.
- Suspected command-and-control network traffic relating to a specific malware family regarding wealth management and corporate banking infrastructure.
- A user on SkyFraud Forum attempted to sell account or carding information linked to a wealth management/corporate bank. While no interested buyers responded to the initial advertisement on the forum, it is possible that buyers would contact the vendor via private forms of messaging available within the forum to maintain anonymity.
- Multiple events referencing an official wealth management and corporate banking domain on Genesis Store as part of an advertised bundle.
- Significant Denial of Service (DoS) attacks on a wealth managers and/or corporate bank originating from multiple countries and even including satellite links.
- Large amounts of compromised payment card information available on Joker's Stash Forum.



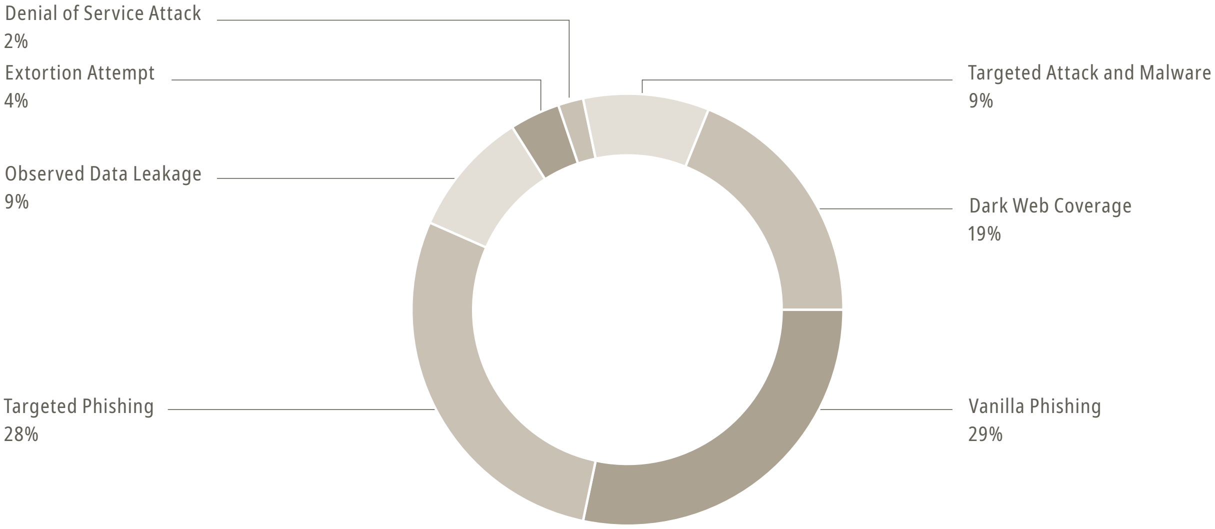
Qualitative chart based on anonymized SIX Cyber Security Hub information

Tier 1 Organizations

Tier 1 institutions – large retail banks in Switzerland – were most frequently affected by phishing attempts. These attacks amounted to just over half of the total attacks on this tier, split almost 50/50 between vanilla and targeted phishing attempts. Mentions of Tier 1 organizations on the Dark Web ranked as the next most prominent category of events, followed by targeted non-phishing attacks.

Some notable and representative examples of cyber events to afflict Tier 1 organizations in our timeframe include:

- Registration of 20+ typosquatting domains for a Tier 1 organization within one month as preparation for targeted phishing attacks.
- Consistent reporting of products/data linked to a retail bank available for sale on popular underground markets such as EpicMarket, with a noticeable spike over the past two quarters – likely in response to cybercriminals seeking alternative marketplaces in the wake of additional site takedowns by law enforcement.
- Availability of 50,000+ credit card numbers for a retail bank on underground communications channels.
- Domains affiliated with a retail bank being available on the Genesis Store.



Qualitative chart based on anonymized SIX Cyber Security Hub information

Conclusion

From a macro perspective, Switzerland fares well in terms of cyberattacks when compared with other G20 nations. Considering the total size of its banking sector compared to those of other countries, the country is a relatively low-level target for cyberattacks.

Partially, this is thanks to the structure of the Swiss financial services industry. Switzerland benefits from its high proportion of non-retail financial services organizations, as large retail banking organizations attract the most targeted attacks. However, such organizations will not remain immune to cyberattacks forever. In fact, attacks are increasing in both frequency and sophistication. It is important to remember that cybercriminals are incredibly dynamic and always on the lookout for new ways to exploit vulnerabilities for profit, such as extortion incidents.

To address these risks – both actual and emerging – financial services organizations in Switzerland should coordinate their cyber security activities to increase their surface for intelligence collection. They should also coordinate with each other to implement nationwide incident response strategies to ensure cyber protection efforts are as efficient as possible.

From a micro perspective, an interesting pattern emerges across different types of Swiss financial services firms and institutions. We categorized organizations into three tiers, finding that at each level a new set of cyber threats emerged in addition to those inherited from the tiers below.

Most notably, across all tiers, phishing is the most common form of attack. The percentage of targeted phishing increases from tier to tier, from approximately 30% among Tier 3 organizations, to over 50% among Tier 1 organizations.

Additionally, mentions of organizations on the Dark Web vary from tier to tier in both structure and frequency. While the structure is partially due to the specific financial activities in question (e.g. issuing credit cards versus wealth management), the frequency of mentions reflects the cybercriminal’s level of interest in said tier.

Finally, cybercriminals target customers and suppliers in order to find an easier way of accessing monetizable information. Current best practice mandates that the cyber security team of a given organization must be made explicitly responsible for addressing this type of risk. Such customer-orientated incidents damage confidence, with the reputation of the entire Swiss financial services industry suffering as a result. As such, it is the shared responsibility of all institutions in our sector to minimize the frequency and impact of these events.

Terms and Abbreviations

APT	Advanced Persistent Threat
DDoS	Distributed Denial of Service
DoS	Denial of Service
IoT	Internet of Things
OSINT	Open Source Intelligence
PoC	Proof of Concept

The information contained in this document does neither constitute an offer for the rendering of a service nor any advice or recommendations in the area of cyber security (or any other area). SIX Group AG or its direct and indirect subsidiaries (hereafter: SIX) accepts no liability for the completeness, accuracy, currentness and uninterrupted availability of this information, or for losses as a result of actions taken on the basis of information found in this or other publications of SIX.

SIX Group Services AG
Pfingstweidstrasse 110
Postfach
CH-8021 Zürich

T +41 58 399 2111
www.six-group.com/cybersecurity
cybersecurity@six-group.com