FS-ISAC

Navigating Cyber 2021

The Case for a Global FinCyber Utility

About This Report

This is a thematic summary of FS-IAC Global Intelligence Office (GIO) in-depth report of cyber trends in 2020 and predictions for 2021.

The full report is only available to member financial institutions via the *FS-ISAC Intelligence Exchange.*

FS-ISAC membership is **exclusive** to financial institutions headquartered in eligible countries. FS-ISAC's full suite of intelligence products is solely available to members who are **directly** connected to *FS-ISAC Intelligence Exchange.*

As cybersecurity becomes a more pressing issue, the quality of cyber intelligence you receive is paramount. FS-ISAC is the only global cyber intelligence sharing community solely focused on financial services. Make sure you get your cyber intelligence from reputable sources.

If your financial institution is not yet a member of FS-ISAC, apply to become a member here.

Executive Summary

In 2020, the global pandemic disrupted the daily business operations of FS-ISAC members and the world. Cybersecurity teams in financial services had to adapt strategies and operations to the onslaught of digitization of products, services, and work while contending with fraudsters capitalizing on fear and uncertainty. Changes that normally happened gradually over years were implemented within weeks.

In the addition to the **cyber challenges of remote work** and fast and furious digitization, other concerns emerged to keep CISOs awake at night: **geopolitical tensions** manifesting in cyber warfare and crime; the continued **commoditization of malware** that makes it easy for any would-be cybercriminal to wage attacks; **new business models for ransomware** that complicate the response calculus; **cross-border campaigns** that sweep across continents and different types of institutions in mere weeks; and heightened **third party risks** in a global financial industry with many common suppliers.

This report details the themes that have emerged in fincyber over the past year and explores where they are heading in 2021 and beyond. The themes are based on the contributions of our members and the resulting trend analysis by FS-ISAC's Global Intelligence Office (GIO). In 2020, FS-ISAC launched its new secure chat and intelligence sharing platform, the *Intelligence Exchange*, which provided a new way for members to discuss threats and security trends. Adding choices for members with different communication preferences increased sharing across borders and boosted actionable alerts, which GIO then incorporated into its analysis.

In 2021 we anticipate that **third party risks** and **geopolitical tensions** especially will escalate as factors cybersecurity teams need to manage. While they are constantly evolving, one thing is clear. Today's cyber threats consistently affect several, and often a great many, institutions. They transcend borders and oceans. The same threat actor may target a wide variety of verticals and sub-verticals. And they move swiftly. In this context, cross-border intelligence sharing has never been more critical for the financial services industry to defend against cyber threats, protecting both firms and customers.

Cyber Snapshot 2020 Timeline

January

Geopolitical and Nation-State Threat Activity

2020 kicked off with increased vigilance against nation-state threats following tensions between the US and Iran. While no large-scale incident materialized for the financial system, a quarter of the Iranian internet was taken down via a cyber attack, which heightened tensions even further. The geopolitical tensions raised awareness and scanning around the types of TTPs typically associated with Iran and other sophisticated nation-state actors.

February

COVID-19: The Ultimate Market Driver

65% Members surveyed reported increase in phishing in early months of pandemic

The pandemic forced the world into rapid digitization of financial products and services and an almost wholesale shift to remote work within weeks. With the demise of the firm perimeter, a dispersed workforce, and a distracted customer base, fraudsters took advantage and amped up phishing with COVID-19 as a lure.

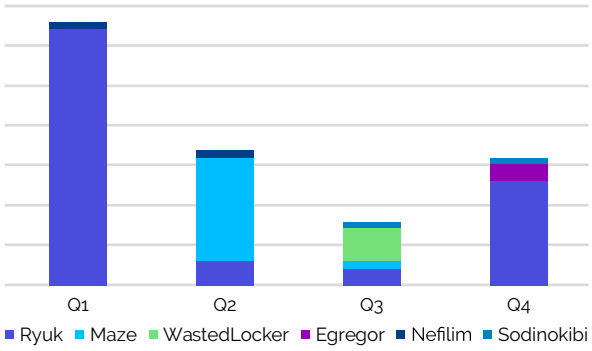
From a security perspective, what were originally short-term emergency measures are now being adapted and cemented into new modus operandi, with migrations to cloud and SaaS planned over years taking place in months.

Digitization is here to stay. These new business opportunities come with increased cyber risks as well as a new competitive landscape, with fintechs increasingly gaining ground on traditional financial institutions.

March

Ransomware: New Business Models

Top 5 Ransomware Threats 2020



In 2020, financial firms around the world were impacted by innovative new ransomware tactics that maximized ROI for the threat actors. While financial firms represent a small percentage of victims directly targeted by ransomware attacks, they can and have been impacted by **attacks on third parties**, who are prime targets.

Key Innovations

- Ransomware actors now predominantly target at the **enterprise level**, a shift enabled by commoditization of malicious code and the **ransomware-as-a-service** (RaaS) model that lowers barriers to entry for relatively unsophisticated cyber criminals.
- *Double tap*, also known as double extortion, where attackers threaten to **release data publicly** or auction it off on the dark web.

Potential Impact

- Data integrity
- Loss of intellectual property
- Fraud using employee or customer data
- Legal and compliance issues
- Reputational damage
- Customer retention

April

May

Malware Commoditization

Formbook Ursnif IcedID Emotet
Dridex Remcos RAT
Zloader Agent Tesla Qakbot
TrickBot Ryuk Ransomware
JsOutProx LokiBot BazarLoader
AZORult

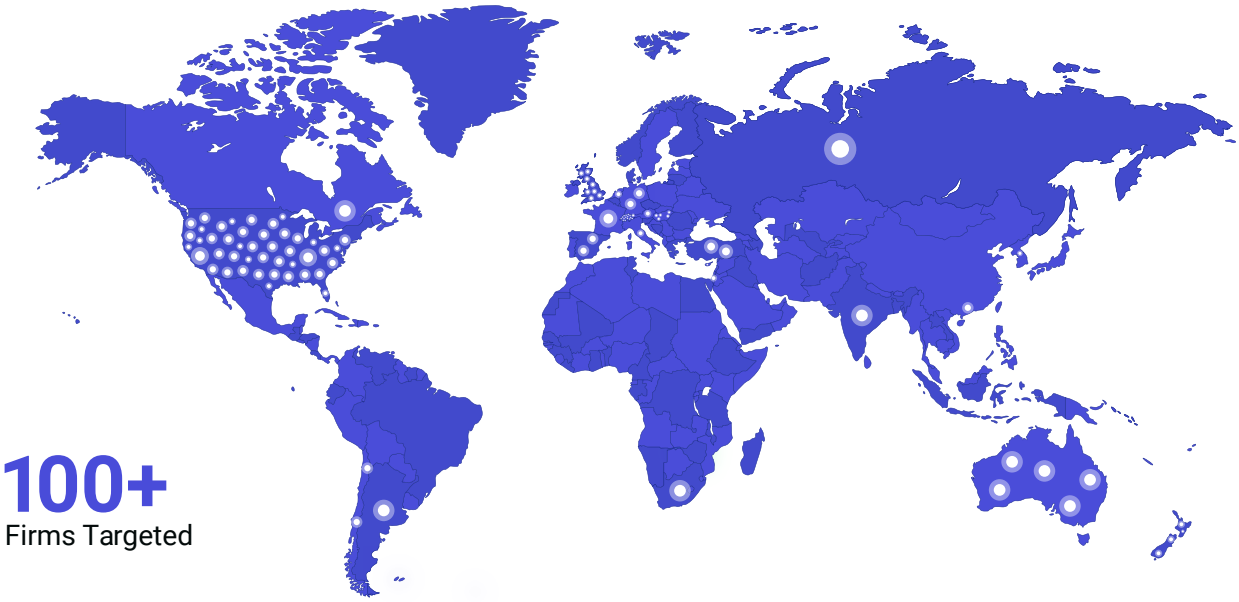
Increasingly, malware developers not only use their products themselves, but sell them as specialized components on the dark web for assembly into kits. Some of the top malware attacks reported by members are these commoditized strains.

Emotet, the most reported malware seen by members in 2020, is highly modular. After a lull in Q2, *Emotet* resurged in Q3 with a new twist: using stolen email attachments to add credibility to the spam it generates to infect targeted systems. It also hijacks email threads—a social engineering strategy employed to increase the likelihood of infection.

In January 2021, Europol and North American law enforcement announced an effort to take down *Emotet* operations. FS-ISAC is following.

June

Cross-Border Campaigns: Build Once, Distribute Globally



100+
Firms Targeted

July

More than 100 financial firms received DDoS extortion threats. The threat actor hit dozens of institutions across multiple sub-verticals around the world within weeks. The threat actors were more sophisticated than in years past; leveraging the brands of well-known threat actors such as *Fancy Bear* and *Lazarus Group* by impersonating them, and capitalizing on media reports of victims for use in subsequent extortion demands.

FS-ISAC members shared intelligence early and often, keeping up with the rapid pace of attacks using the *FS-ISAC Intelligence Exchange's* secure chat and intelligence sharing capabilities, which enables industry collaboration and discussion in real time.

Read the *Wall Street Journal* article here.

August

September

October

Trickbot, Disrupted

FS-ISAC joined Microsoft in a legal action – the first of its kind -- to disrupt operations of the *Trickbot* banking trojan, the #4 most reported malware by members in 2019 and 2020.

Members had received thousands of emails per month, resulting in account takeovers. *Trickbot* was also used as a malware-as-a-service to drop *Ryuk* ransomware, the most reported ransomware in 2020.

November

Third Party Risk: SolarWinds and Beyond

The *SolarWinds* compromise revealed the scope and severity of third party breaches for the financial sector. The breach happened through a weaponized security update that was downloaded by 18,000 firms, many of them smaller financial institutions and other third party suppliers. The US government, itself impacted by the breach, has attributed the hack to an unknown Russian threat actor.

In terms of impact to the financial sector, the dominoes are still falling. What data was compromised and how the threat actors intend to use it remains unknown. More third party attacks have already hit in 2021; they will not be the last.

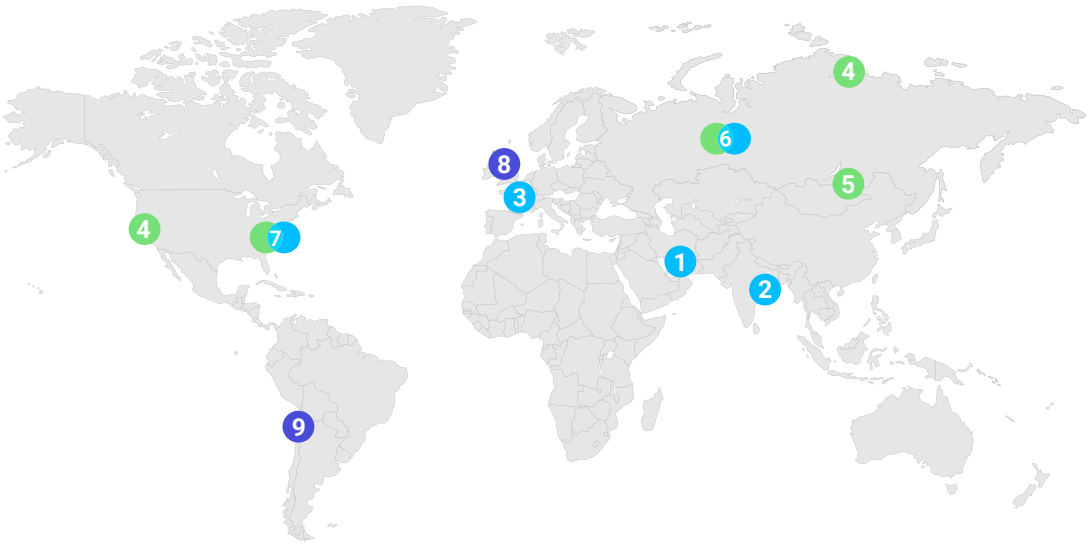
FS-ISAC worked with thousands of its members, "offering 'strategic and tactical reports detailing the attack vectors and offering best practices to mitigate risk.'"

Read the Bloomberg article here.

December

2020 Cyber Threats Around the World

The following are just a few incidents that give a sense of the breadth of threats impacting members and the wider financial sector in 2020. Most notable is where themes converge, such as where geopolitical tensions and third party risk intersect.



Geopolitical Tensions · Third Party Risk · Geopolitical Tensions & Third Party Risk · Ransomware

Geopolitical Tensions

1 **February:** Soon after the killing of popular Iranian military leader Qasem Soleimani by a US airstrike, a cyber attack reportedly took down 25% of the Iranian internet, fueling tensions between the country and the US and Israel.

2 **July:** The physical clash between Chinese and Indian military forces at the Ladakh border was followed by a significant spike in cyber activity by Chinese actors against the Indian government and businesses. Traditionally a 'non-aligned' country, India may begin to build new cybersecurity alliances with other democratic nations to counter future Chinese threats.

3 **December:** The UK officially leaves the EU. Key data sharing and cyber regulations such as GDPR and the NIS Directive have already been adopted in UK legislation. It is unclear how Brexit will affect data sharing between UK and EU law enforcement, although the UK has lost access to crime fighting tools like the Schengen Information System (SIS).

Third Party Risk

4 **January:** 250 million customer records for Microsoft, spanning 14 years, exposed online. Microsoft moved immediately to secure the servers and reported that "no malicious use" was found in their investigation.

5 **June:** A backdoor was discovered in China's 'Golden Tax' software, dubbed 'Golden Spy.' Local software companies Aisino and Baiwang were licensed by the central bank to sell the tax software and are most likely responsible for embedding the backdoor.

Geopolitical Tensions & Third Party Risk

6 **April:** Internet traffic for 200 major networks and providers were redirected through Russian state-owned Rostelecom. Impacted companies included Google, Amazon, Cloudflare, Akamai and LeaseWeb.

7 **September:** US Treasury Financial Crimes Enforcement Network breached. Large amount of anti-money laundering Suspicious Activity Reports leaked, which contain sensitive information provided by banks. Russia's President Vladimir Putin was among those exposed with links to large suspicious international financial transfers.

Ransomware

8 **January:** Foreign exchange company Travelex hit with *Sodinokibi* (AKA *REvil*) ransomware, causing a two-week outage at major financial institutions around the world. US$6 million was reportedly demanded by the ransomware operators in exchange for decryption of the data and not exposing sensitive data online.

9 **November:** The largest retail company in Chile, Cencosud, was reportedly hit by *Egregor* ransomware. This was not the first major attack in Chile in 2020; BancoEstado closed for a few days in September due to the *Sodonikibi (AKA REvil)* ransomware.

Predictions for 2021 and beyond

01 Nation-states and cyber criminals collide

Wittingly or otherwise, criminals will support nation-state operations through selling initial access or tools to achieve those ends. Nation-state cyber actors will benefit from the mass "workforce" of the cybercriminal underworld constantly seeking to compromise networks who will handle the first step of a kill chain that they can then take advantage of. By using the initial access gained by others or tools developed by the underground, nation-state operators can obfuscate their activity and complicate attribution. Nation-states with developing cyber programs can also use cybercriminal tools, exploits, and access to enhance their own capabilities.

Risk & Business Impact

- **Operational disruption**
- **Material customer loss**
- **Increase in insurance premiums**
- **Lawsuits or fines**
- **Systemic destabilization**
- **Credit downgrade**
- **Reputational damage**

02 Third party risk will dominate the discussion

Cloud service providers, managed service security providers, and other third parties performing critical services for multiple valuable clients will continue to be lucrative targets for threat actors with a variety of motivations, from financial to destructive. This may trigger a push towards overly zealous zero trust models to try to better understand third- and fourth-party security environments. Discussions on using zero trust as a mindset should be stressed over more enhanced questionnaires to vendors.

Risk & Business Impact

- **Operational disruption**
- **Material customer loss**
- **Systemic destabilization**
- **Reputational damage**

03 Attacks will cross borders, continents, and verticals, with increasing speed.

As we saw with many of the large-scale attacks in 2020, cyber criminals will test attacks in one country and quickly scale up to multiple targets in other parts of the world. An attack on an insurance company in Asia could be a harbinger for a fintech in Europe or a community bank in the US. It is critical to have a global view on cyber threats facing the sector in order to prepare and defend against them.

Risk & Business Impact

- **Operational disruption**
- **Material customer loss**
- **Systemic destabilization**
- **Reputational damage**

04 Ransomware-as-a-Service will evolve

Threat actors will capitalize on the success of the *double tap* methods employed in 2020. While financial targets should remain harder to hit, third party suppliers and providers will continue to be impacted. Ransomware operators will exploit third parties' need to remain functional for their clients and perhaps be more willing to pay a ransom. Shutdown of these dependencies can have operational impact to members.

These ransomware operators may continue partnering with other threat actors to have multi-faceted impact from a single attack, such as using access for cyber espionage purposes.

Risk & Business Impact

- **Operational disruption**
- **Lawsuits or fines**
- **Reputational damage**

05 Remote working, and its cyber risks, are here to stay

Threat actors will continue to exploit the remote working environment: exploiting vulnerabilities in VPNs and social engineering that capitalizes on a lack of personalized interaction—such as business email compromise, gaining access to cloud environments or targeting virtual meeting spaces. As some firms consider keeping portions of their workforce remote indefinitely, they must re-evaluate and re-tool their cybersecurity profiles.

Risk & Business Impact

- **Operational disruption**
- **Material customer loss**
- **Reputational damage**

06 Economic drivers towards cybercrime will increase

The persistence of economic contractions and unemployment due to the pandemic make cybercrime an ever more attractive alternative, especially in certain areas of the world with high concentrations of technically skilled workers with few career options. Dramatic increases in cryptocurrency valuation may drive threat actors to conduct campaigns capitalizing on this market, including extortion campaigns against financial institutions and their customers.

Risk & Business Impact

- **Operational disruption**
- **Material customer loss**
- **Increase in insurance premiums**
- **Reputational damage**

FS-ISAC

Global Intelligence Office

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyber threats. FS-ISAC members represent over $35 trillion in assets under management, with 15,000 users in more than 70 countries. Headquartered in the United States, the organization has offices in the United Kingdom and Singapore. To learn more, visit **fsisac.com**. To get clarity and perspective on the future of finance, data and cybersecurity from top C-level executives around the world, visit **FS-ISAC Insights**.

The FS-ISAC Global Intelligence Office (GIO) coordinates and disseminates analysis of member-submitted intelligence as well as threat alerts to its member financial institutions around the world. GIO regularly issues reports and convenes member calls as well as spotlight calls on emergent issues to ensure members are prepared for current threats.

GIO also coordinates with other cybersecurity organizations, companies, and agencies around the world to ensure actionable and timely cyber intelligence is disseminated to our members. GIO is a 24-7, follow-the-sun operation with teams in Singapore, the Netherlands, UK, and US.

If your financial institution is not yet a member of FS-ISAC, apply to become a member here.