Symantec™
by Broadcom Software

WHITE PAPER

RANSOMWARE AND FINANCIAL SERVICES

Drivers, Developments, and Defenses

WHITE PAPER

RANSOMWARE AND FINANCIAL SERVICES

Drivers, Developments, and Defenses

TABLE OF CONTENTS

RANSOMWARE GOES PUBLIC

Global currency exchange Travelex started the year 2020 fighting a **ransomware attack**. The attack deprived international travelers of services from their 1,200 stores, kiosks, and counters in transportation terminals across 70 countries. It also deprived global banks—including HSBC, Royal Bank of Scotland, and Barclays—of automated currency exchange services. Travelex fell back on manual operations for weeks, and months later was **forced into administration**, attributed in part to the costs of recovery from the attack.

The attack, launched by Russian-speaking gang **REvil**[1], was not exceptional in toolset, scale, origin, or damage done. But it was groundbreaking in that REvil announced their (unproven) theft of Travelex customer data and their threat to publish it if a $6 million ransom demand was not paid.

At the time of the attack, ransomware was already a well-recognized threat. But it was discussed only in abstract, aggregate terms: $16+ billion **in losses**, one billion **attempts per year**, and so on. Business, IT, and banking press covered the trend, but without ever identifying successful attacks on individual named banks. Their sources in banking, IT, and risk-management were comfortable discussing the pervasiveness of the ransomware threat and the damage done industry-wide, but were uniformly silent about successful attacks on their employers or clients. Even public lists of attacks still **lack any reference to major financial institutions**. The insistence on anonymity comes as no surprise: as with any kind of extortion, acknowledging the success of one attack just encourages the next. But REvil's choice to add public pressure to their threat brought the fight into the open.

The DarkSide gang's May, 2021 attack on Colonial Pipeline raised the public stakes. A six-day pipeline shutdown, panic buying and shortages of gasoline, and emergency declarations by the Georgia Governor and

RANSOMWARE GOES PUBLIC

US President raised public awareness of the ransomware threat. This awareness triggered a more aggressive public and private response to attacks, and a new stage of ransomware evolution.

[1] For more information on organized criminal gangs, see Broadcom's Ransom and Malware Attacks on Financial Services Institutions.

INTRODUCTION

Ransomware is the latest front in the **forever war** between financial institutions and cyber criminals. Even though ransomware delivery, encryption, and payment technologies have reached high states of maturity, the tactics, targets, and operations of the criminal gangs behind the attacks continue to evolve.

This white paper reviews the status of ransomware aimed at the financial-services industry at the beginning of 2022, including the following topics:

- A recap of the mostly technological drivers that defined ransomware's first thirty years, and its current, mature, state
- A summary of the economic, organizational, and other nontechnology factors driving its current evolution
- An outline of the operational, legal, and regulatory actions underway to block and mitigate future attacks

DRIVERS AND DEVELOPMENT

Ransomware is extortion for financial gain, using encryption or exfiltration of sensitive data as a threat. It requires efficient, covert delivery of malicious payloads and messages, credible threats, and secure, untraceable payments. The first documented ransomware attempt, 1989's AIDS Trojan, failed in every factor: delivery by physical disks, easily reversible encryption, and payment by cashier's check.

But thirty years of technical progress has transformed and weaponized every one of these factors:

Delivery by 2004 was by passive unintentional downloads of code from malicious websites. In 2018, more active email phishing attacks were added to the mix, often precisely targeted using data from the victims' social media footprint. By 2022, automation had taken over, and there were two primary vectors:

- Two-stage attacks in which spam campaigns first create worldwide botnets, which are then used to infect target computers
- Exploitation of vulnerabilities in public-facing applications

DRIVERS AND DEVELOPMENT

Threats themselves have grown far more credible and severe:

- Asymmetric cryptography, in use since 2013, makes it impossible for users to recover their data without a decryption key.
- Double extortion threats to disclose confidential data, on the rise since 2019, add risks of reputational damage to the costs of data recovery, raising incentives for victims to comply with ransom demands.
- Public threats, as with Travelex, are powerful. But they may backfire, by increasing public calls for government action.

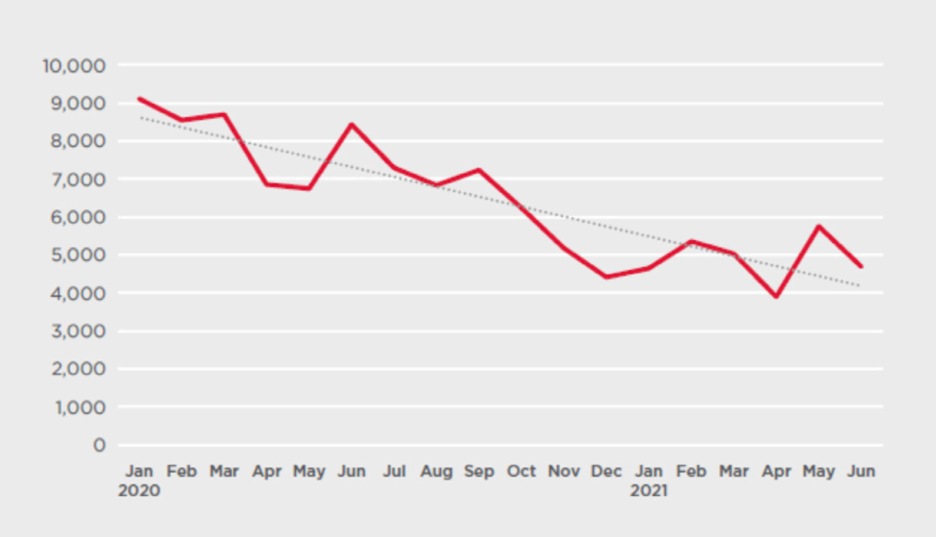
Ransom payments since 2012 have moved to bitcoin, and lately to **Monero** and other cryptocurrencies engineered to be even more difficult to trace.

Table 1: Evolutionary Milestones in Ransomware Delivery, Encryption Threats, and Payments, 1989 through 2021.

Year	Malware	Innovation
1989	AIDS Trojan	First known ransomware attempt
2004	PGPCoder	Infection using drive-by download
2013	CryptoLocker	Use of 2048-bit RSA encryption Payment in bitcoin
2017	WannaCry NotPetya	State-sponsored attacks
2018	Targeted attacks	Social-media-backed phishing Focus on banking, medical, public
2019	Maze	“Double extortion” attack
2020	Sodinokibi	Disclosure threats made public
2021	Colonial Pipeline attack	Raised public awareness and government involvement

DRIVERS AND DEVELOPMENT

Figure 1: Ransomware Detections, January 2020 to June 2021. (Source: Symantec)



STATUS AND TRENDS

The ransomware front has shifted from technologies to tactics, making threats even more concentrated, targeted, and specialized.

Frequency and Scale

Paradoxically, the ransomware problem grew more severe in 2021, even as the frequency of attacks declined. The drop in attack frequency (almost 50% over 18 months) was due primarily to a fall in untargeted mass-mailing attempts, often aimed at individual consumers.

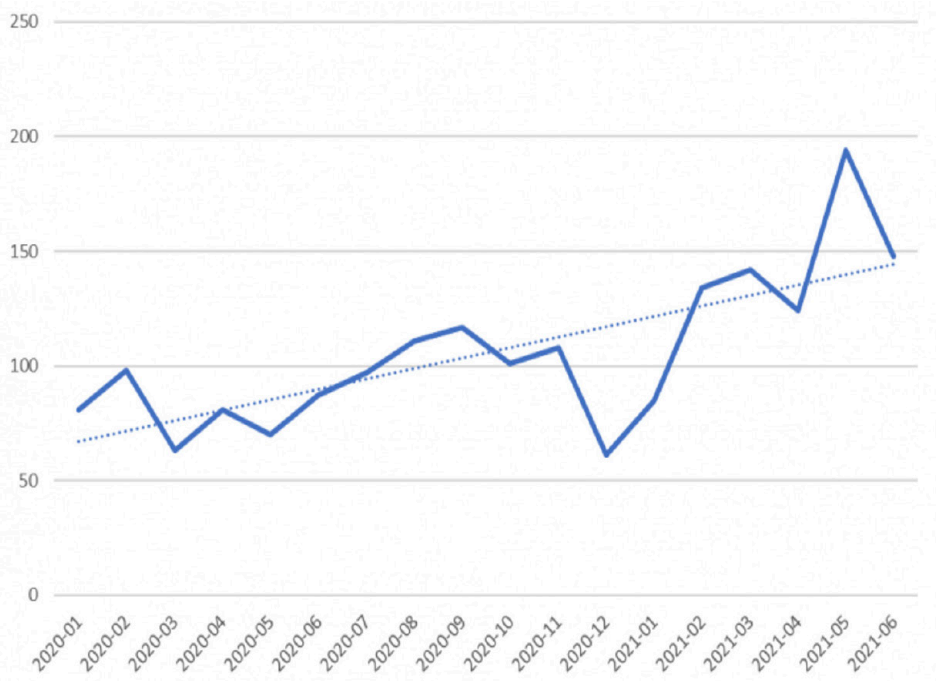
Targeted attacks on organizations show the other side of the picture. As shown in Figure 2, victims of these more effective attacks increased 83% over the same 18-month analysis period. Total payments also rose: **cryptocurrency payments** to known ransomware sites quadrupled from 2019, reaching at least $412 million in 2020, and **$590 million** in just the first six months of 2021. These numbers are certainly lower bounds to the actual damage, since many ransomware payment sites are yet to be identified, and many incidents go unreported. The numbers also exclude indirect costs, which can amount to **many times the ransom itself**. Concentration of the ransomware market on fewer, more valuable targets is multiplying the payoff—and the damage.

STATUS AND TRENDS

New Tactics

American Banker magazine **points out** that while banks are tempting targets for ransomware and spear phishing, they “are relatively well-prepared for these kinds of attacks—after all, they spend so much money deterring them.” Deloitte estimated that banks spend about **11% of their IT budgets** on cyber security—and Bank of America puts its own budget at **more than $1 billion** per year. Faced with strong defenses at the largest institutions, ransomware actors have changed their tactics—attacking smaller banks, and attacking financial institutions indirectly through vulnerable third-party service providers.

Figure 2: Organizations Affected by Targeted Ransomware Attacks, January 2020 to June 2021. (Source: Symantec)



Attacks on Smaller Banks

There are **almost 5,000** FDIC-insured banks in the US, and most are small: unlike the giants, 11% of their IT budgets might not buy adequate defense. Shortly after the Colonial Pipeline attack (and shortly before stopping all activities), ransomware groups DarkSide and Ragnar Locker announced that they had broken into three community banks’ servers, stolen data, and demanded ransom. A **review of ransomware** from the community bank perspective reveals that smaller banks rely more on third parties for help with prevention, mitigation, and response. These third parties include specialist consultants, insurance companies, and law firms, providing support that a larger bank might bring in-house.

Supply Chain Attacks

Even when banks secure their own operations from top to bottom, third parties on which they rely for specialized technologies, consulting, or other services may be vulnerable. And because these supply-chain partners typically serve multiple clients, attacks on them serve as force multipliers for ransomware actors. In 2021, third-party attacks came into their own, culminating in July's **Kaseya attack**, in which the REvil organization deployed ransomware to more than 1,500 organizations by exploiting a data leak—first identified in 2015 in its customer support site.

A nightmare scenario would be a third-party attack on an operating system, data provider, cloud service provider, or other entity relied on throughout the banking sector: banking experts often cite Amazon Web Services as a candidate for such a single point of failure that connects broadly across the financial sector.

The Ransomware Economy

Ransomware technologies have reached a high level of refinement. But while technical innovations continue, the current evolution of ransomware is driven primarily by the participants and operation of the underground economy that supports it.

Organized Criminal Gangs

The US Federal Bureau of Investigation tracks more than **100 active ransomware groups**, including Maze, DarkSide, and reputed market-share leader REvil/Sodinokibi. These groups frequently merge, rebrand, or stop all activity, often after execution of a successful attack—as did **DarkSide after the Colonial Pipeline attack**, and **REvil after the Kaseya third-party attack**.

Specialization

Primitive ransomware was typically the work of individuals, but modern campaigns are much more complex. It is no surprise that as criminal gangs grew, they also began to specialize in one or more activities along

STATUS AND TRENDS

the supply chain, sorting themselves out along the following lines of technical capability and risk tolerance:

- Creators craft software that performs reconnaissance, **inserts malware** on target networks, or encrypts target files. Software packages range from do-it-yourself kits sold on the Dark Web to packages with custom backdoors and **file-extraction tools**, with negotiated pricing. This role requires the most skill, but carries the least risk.
- Distributors of ransomware use techniques ranging from broad-spectrum indiscriminate techniques backed by botnets and **virtual machines**, through targeting of privileged insiders, often backed by months of research into insiders' social-media footprints and their companies' networks. The longer attackers linger on target networks, the more they are at risk of detection.
- **Payment specialists** use cryptocurrency, and often nest transactions through multiple exchanges that obscure the ultimate recipient—a kind of money laundering. As is true of extortion in general, the payment chain is typically a vulnerable spot in ransomware.

Ransomware-As-A-Service

Ransomware-as-a-Service is an emerging model that insulates ransomware creators from the some of the risks of distribution and payment, by offering ransomware on a prepaid or revenue-sharing basis. It also puts sophisticated extortion tools in the hands of criminals whose risk tolerance greatly exceeds their technical capabilities. By tying together the specialized activities that undergird ransomware, it also increases the number of potential attackers.

ENFORCEMENT AND COMPLIANCE TRENDS

In a sweep shortly after the Kaseya third-party ransomware attack, the European Union Agency for Law Enforcement Cooperation (Europol) **announced the arrest** of two hackers who had purchased Russia-linked REvil ransomware, and other REvil affiliates in Europe and South Korea. While it is by no means clear that the arrestees had anything to do with the Kaseya event, the arrests are a deliberate signal that the US government is increasing its enforcement activity. The message was clearly understood by other ransomware gangs; the group behind BlackMatter ransomware, for example, **announced its dissolution** a short while later.

ENFORCEMENT AND COMPLIANCE TRENDS

Information Sharing

Multiple agencies of the US government aggregate information about ransomware attacks. Historically, the agency responsible for regulating an industry aggregated and maintained records of cyber attacks in the industry: HSA for healthcare, DOE for energy, FDIC for banks, and so on. But the emergence of ransomware attacks on energy infrastructure raised its profile as a national-security threat, and spurred cross-government coordination.

The **Cybersecurity and Infrastructure Security Agency** (CISA) leads the cybersecurity effort for US government civilian networks, and coordinates public and private efforts for infrastructure security and resilience. Its **stopransomware** website is an education and resource-sharing portal that simplifies reporting of ransomware events to the FBI, CISA itself, or the US Secret Service.

Sanctions for Facilitating Payment

Despite the emergence of cryptocurrencies like Monero which was explicitly designed to obscure the identities of transaction counterparties, uncovering payment trails remains an important way for the government to identify and punish ransomware actors. The US Department of the Treasury has issued **an advisory** that facilitating payment of ransomware runs afoul of Office of Foreign Assets Control regulations established by the International Emergency Economic Powers Act, the Trading with the Enemy Act, and other laws.

The US Department of the Treasury advisory is careful to point out that these regulations apply to financial institutions and their partners, not just to the malicious ransomware actors. In other words, a cyber insurance provider or incident response team that helps process ransom payments **may violate money-laundering or other regulations**. Early and complete filing of Suspicious Activity Reports is suggested as a method to avoid penalties.

Implications for Ransomware Victims

Whether implicitly or by design, government initiatives over the past two years are nudging financial services firms in the following direction:

- Sharing information about ransomware attempts with the government as early as possible
- Negotiating hard before paying any ransom, to avoid complicity in financial crime

ENFORCEMENT AND COMPLIANCE TRENDS

The Harvard Law School Forum on Corporate Governance has issued a **guide to the new regulatory landscape**, emphasizing that while paying ransom is not itself illegal, organizations must be careful not to violate statutes and regulations in a new, more highly restrictive, enforcement environment.

BEST PRACTICES FOR RANSOMWARE PREVENTION

The **CISA Ransomware Guide** includes a set of best practices for organizations to avoid becoming ransomware victims. The guide includes the following key points:

- Maintain regular, encrypted, offline data backups and test them frequently
- Maintain and exercise an incident response plan with communications, notification, and response procedures
- Defend key vectors for ransomware infection, specifically:
    - Internet-facing vulnerabilities
    - Email phishing attacks
    - Ransomware precursor malware injected at endpoints, networks, and gateways
    - Third-party service providers, including managed service providers

SYMANTEC OFFERS TECHNOLOGY, CAPABILITIES AND EXPERIENCE

Symantec by Broadcom Software solutions address the security and compliance challenges the financial services industry now faces. The company is dedicated to providing solutions to secure, automate, standardize, and streamline operations and transactions, and is a pioneer in security and data-protection solutions aligned with Zero Trust and Secure Access Service Edge concepts.

About Us

Broadcom Software is one of the world's leading enterprise software companies, modernizing, optimizing, and protecting the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables innovation, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com