Votiro eBook

Mitigating File-Borne Threats in the Financial Service Industry

votiro.com

Table of Contents

3 Executive Summary

4 Introduction

5 Cyber Risks Facing the Financial Industry

5 Why Target Financial Institutions?

6 The Threat Surface is Wider Than Ever Before

7 Threat Vectors

9 Why are Files Risky

11 Varieties of Malware

13 Identifying the Threat Actors

16 What are the Potential Consequences of an Attack

18 Regulatory Considerations

19 Challenges from the Pandemic

20 Why Current Security Solutions Are Ineffective

22 How Positive Selection Eliminates Risk from File-Borne Malware

23 Votiro ZT Cloud

Executive

Summary

Financial institutions face an ever-growing threat from incoming files. Every loan application uploaded to a web portal, emailed spreadsheet, or signed PDF sent to an account manager can contain malicious code that threatens the organization. All files are suspect.

Ransomware campaigns and other destructive malware are running rampant as malicious actors seek out high value targets to coerce and compromise. And the need for strong security is more critical now as the risk of file-borne threats has never been greater.

As one of the most highly regulated industries, the financial services sector faces significant pressure to uphold the highest security standards.

These institutions must overcome the challenge of providing near fail-proof security without becoming a burden on their ability to offer effective and efficient service.

...A classic example of the tension between security and usability if there ever was one.

This eBook will outline the challenges facing financial institutions in countering the risk of file-borne threats. It will review the threats and regulations, addressing why current security solutions offer inadequate protection to organizations.

The eBook will also offer recommendations for how financial institutions can confidently mitigate the threat of file-borne malware, optimizing security in conjunction with business continuity and productivity.

Introduction

There is an old joke that asks why do bank robbers rob banks? Well, because that's where the money is.

Financial firms are the most likely to be attacked by hackers. According to the Verizon Data Breach Investigation Report, financial organizations make up 14% of annual incidents across industries. Adding to the pain is the fact that banks alone suffer an average of [$5.97 million] per incident from attacks—the second highest of any industry, according to IBM. Moreover, the average number of sensitive files that could be exposed in attacks is massive, at [449,855] files on average per organization. Considering that 15% of these files are exposed to every employee on average, a single individual breach has an extensive impact.

Attacks Come in Many Forms

Social engineering tactics like phishing and whaling have netted hackers significant ill-gotten gains, tricking businesses into handing over credentials or even directing payments to the criminals with Business Email Compromise attacks.

Malware continues to be a significant threat— and since 2017 has risen from 183.6 million attacks to 493.3 million in 2022. Malware is the malicious software that allows a hacker to cause damage to their victim, taking control of the victim's machines as they move across servers and networks. This category includes a variety of hacking tools such as worms, viruses, and trojans that grant the malicious actors a footing from which to carry out their attacks.

Malware can enter a victim's system in a variety of ways. Verizon's 2022 Data Breach Investigations Report found that a small percentage of the total malware is introduced via web services vulnerabilities. But the vast majority of malware by far is still being delivered by email and web applications.

In this eBook, we will address the threats facing financial institutions from file-borne malware, explain the reasons why the financial sector is at such high risk, provide a detailed overview of the malware types facing targets, and lay out actionable steps that organizations can take to protect themselves from weaponized files.

Cyber Risks Facing the Financial Industry

Financial institutions are highly valuable targets for attackers. These organizations are our banks, trading firms, and other bodies that handle our money. We place our trust in these institutions to handle our finances with care and take the utmost precaution when it comes to

So it is unsurprising that they are often the victims of cybercrime. According to a the International Monetary Fund, more than 40% of financial institutions rate their attack monitoring, response, and recovery capabilities as “weak” or “very weak.” But to ask an obvious question, why are financials so popular among hackers?

Money on the Table

The short answer, as implied previously, is because they have the money. The longer answer is that financial institutions have both the money and the keys to accessing a lot more money and valuable data that can be used for other crimes later.

The most straightforward objective of the hackers is theft, attempting to compromise bank accounts in order to steal money. In 2016, criminals used compromised SWIFT credentials to steal $81 million from the Bangladesh Central Bank with fraudulent requests. Thankfully, a typo in one of the requests raised suspicions and prevented the thieves from making off with the $1 billion that they had been after.

Weaponizing Private Information for Fraud

But beyond stealing money directly, hackers have plenty of other valuables worth going after. Financial institutions like banks, creditors, and others all maintain a fair amount of personally identifiable information (PII) about their clients. There are good reasons that these organizations request these private details.

Personal details like our social security numbers, dates of birth, and other bits of information help to verify our identity when applying for credit or communicating with these institutions — to a minimal level to be sure. Therefore, the theft of these important personal details can be powerful tools for fraudsters looking to open illicit accounts or lines of credit. Criminals can rack up massive amounts of debt, leaving their victims to foot the bill.

The Threat Surface is Wider Than Ever Before

Financial institutions have long been cognizant of the need for strong security measures. But thick vaults and armed guards are not sufficient protections in the modern financial system.

As targets go, financial institutions are among the harder nuts for hackers to crack. Due in no small part to the expectation that they take significant steps to protect our money and data, they make significant investments in security. They have the budgets to bring on top talent for their IT security teams who are able to help mitigate many of their threat surface risks from the technology side. These risks include remote desktop protocol (RDP) connections that can give hackers access to an organization's machines if not properly updated and protected.

However, even as these organizations close many of the technical loopholes that can be exploited by talented hackers, they still have to contend with the fact that real flesh and blood humans have work to do, which includes communicating with other humans.

Allowing the sending and uploading of documents over the internet has been a great boon for the financial industry. It dramatically shortens the time to resolution of opening accounts, requesting loans, applying for credit cards, and a long list of other common fiscal activities that would otherwise have to be done by snail mail or in person.

Banks, creditors, and others that deal with money are all public facing organizations that need to communicate with each other and the outside world. Locking down behind a high wall is not an option. They must send and receive documents in order to conduct their business.

But like the stagecoach or train, criminals have identified the transfer of documents as a point of weakened security that can be exploited.

These documents can be loaded with hidden malware that can compromise your organization.

Even if sent from a trusted user, files must be treated as suspect. A colleague's email can be compromised or spoofed, so even if the user is authentic, organizations need to remain vigilant.

With great power comes great responsibility. Just as there is an expectation that banks and other financial institutions will implement strong security measures, they are also expected to offer the same ease of interaction as other service sectors. Financial organizations must balance between usability and security. However, deciding how to make informed decisions starts with understanding the types of threats that these organizations face from incoming documents.

Cyber Risks Facing the Financial Industry

Threat Vectors

In assessing the threat from malware-laden files, it is helpful to break the issue down to three threat vectors. These files can be everything from a Word or Excel file for a project to a JPEG or PDF of a signed contract, and everything in between.

Embedded Files or Attachments Sent via Email

While many financial organizations have moved to using digital signature services and cloud hosted document collaboration services, email is still a strong factor in their work. Customers, colleagues, loan-seekers, and others still send email with embedded images, links, and files that pose a risk for the organization.

In some cases, the recipient at the bank or firm is expecting to receive the email with the attachment. Other times it may come unannounced. For both instances, they can be the victim of a spear phishing campaign that targets them specifically and convincingly to gain their trust and get them to open the email with the attachment.

Documents Uploaded to a Web Portal

Offering a more streamlined method of passing on documents for various applications like mortgages and other purposes, many financial institutions have made it possible to upload files via their web applications.

These web portals are unidirectional gateways for the organization and can be an ideal way to manage the influx of documents. A classic example of this would be in a loan application where the applicant uploads identifying documents to the portal to be reviewed as part of the approval process.

This is a prime opportunity for a hacker to send through a malware laden file. Perhaps hidden inside of the JPEG with their drivers license or in a Word document.

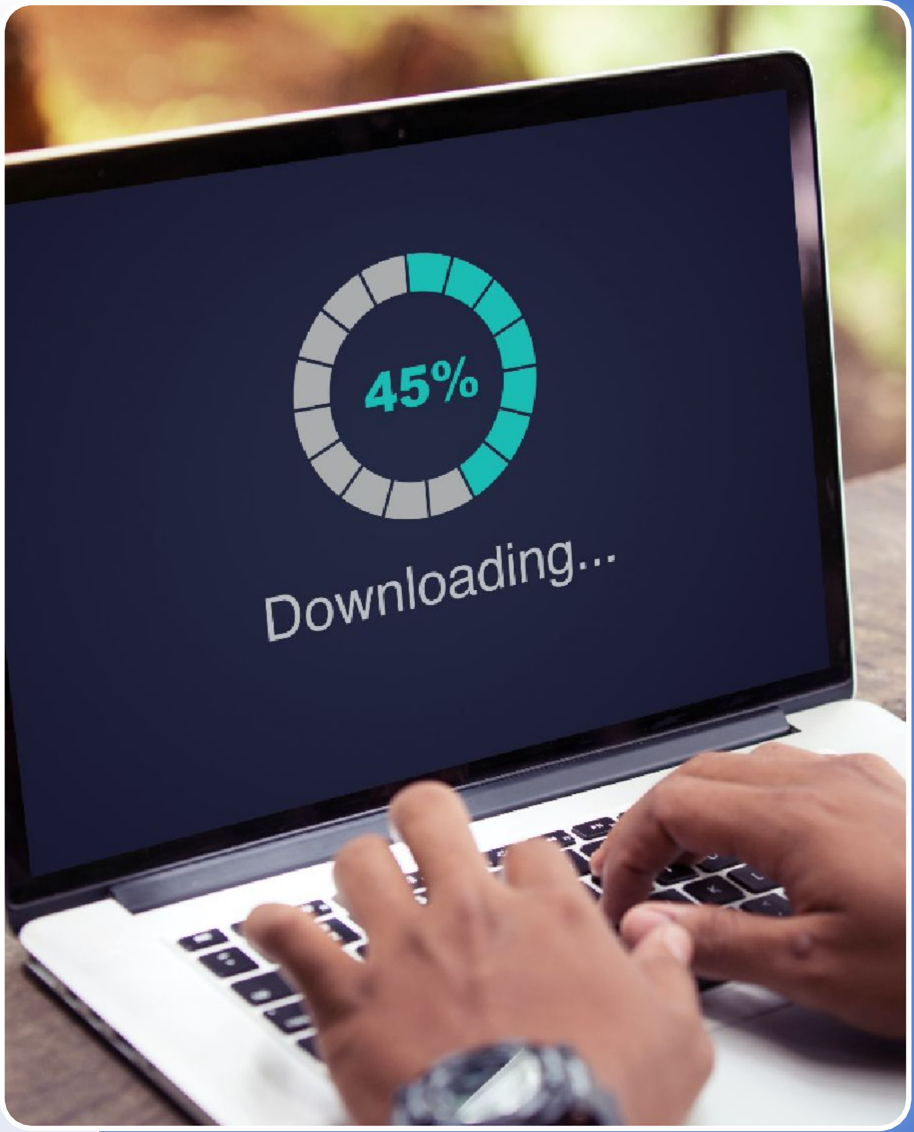
Cyber Risks Facing the Financial Industry

Threat Vectors

Web Downloads

In the course of their work, employees at financial institutions will often visit external websites. We roll the dice every time we download files, trusting that they will not cause us harm. If employees are being targeted by hackers, then they may even be redirected to a website where there is malicious content and materials for download. Unlike email attachments that require action on the part of the user, visiting a malicious website can lead to a compromise without the user making a single click.

Often referred to as “Drive-by Downloads,” these websites may attempt to download malicious software onto the employee’s machine. In some cases, it might be software that allows hackers to connect remotely. Programs like TeamViewer are hacker favorites as they are legitimate tools that can allow them to gain a foothold in their victim’s environment.



Threat Vectors

As collaboration and inter-connectivity between companies, vendors, and partners become ubiquitous, the attack surface widens. Especially when shadow IT and shadow collaboration applications (like Slack, Discord, and Telegram) sneak onto employee devices.

Content Collaboration Platforms

Content collaboration platforms underlie the most revenue-generating processes for financial institutions. Every day, employees share and download documents with and from third-parties on Slack, Teams, Discord, SharePoint, OneDrive, Box, Google Drive, and other allowed - *and not allowed* - applications.

Even Salesforce can be used as a collaborative platform for document and information-sharing.

Many IT and security teams are faced with protecting the content collaboration platforms they know - and defending against the ones they don't!

What Makes Files Risky?

Files pose a risk to financial institutions because hackers can embed malware within them. Malware refers to a range of viruses, worms, trojans, and other malicious software that they can use to cause harm.

Malicious code can be hidden within files in different ways. In Microsoft Office files, one of the most common methods is to insert the malware into the macros or a Word or Excel file. Malware can also be hidden within image files using a method called Steganography.

While malware is a catchall term used to describe malicious software that is intended to harm the victim, it is useful to think about a cyber attack according to the structure of the "Kill Chain" as it is commonly known. First published by the defense contractor Lockheed Martin, the kill chain framework describes the stages of a cyber attack.

Reconnaissance

When targeting a specific organization, hackers will first scout out the necessary intelligence for carrying out their attack. This can include researching who they intend to send the email to so as to prepare an effective phishing lure that will compel the recipient to take action and open the malicious attachment. The hackers then search out the email addresses and other relevant details such as uncovering any known vulnerabilities that can be exploited in their target.

Weaponization

With the necessary intelligence about their target in hand, hackers prepare their malware. This entails combining their exploit with the backdoor to create a deliverable payload that will allow them to take control of their victim.

Delivery

The malicious file is now ready to be sent to the target. Hackers can choose from a variety of delivery methods, such as sending an email or uploading a document to the web portal.

Exploitation

Once the file reaches the target, the payload exploits the vulnerability on the user's machine which then allows them to execute the malicious code.

Installation

Now executed, the malicious code gives the hackers the foothold they need to start carrying out their attack.

Command and Control (C2)

Having infected the victim's system, the malware can begin to communicate with the hacker's system. They can now begin to install additional malware like trojans or viruses that will enable them to secure their persistent control over the system and hide their tracks.

Actions on Objectives

Now situated, the hackers can begin their work of moving laterally across the network, collecting credentials or other information to reach their intended goals.

Time for Malice

They can now start to disrupt, steal, or destroy data on the victim's system. This is now the time to encrypt data for a ransomware attack or carry out other malicious actions for as long as they are able to maintain a presence on the target's network. The longer they sit there, the more damage they can cause.

Varieties of Malware in Malicious Files Targeting Financial Institutions

Hackers are constantly developing new versions of malware for use in their attacks. But oftentimes they make use of readily available malware that has proven its value in hacking targets, altering as needed.

These are a few examples of malware that are commonly seen targeting financial institutions.

Emotet

A polymorphic type of ransomware, Emotet is exceptionally difficult to detect until it is too late. Acting as a dropper, it is highly infectious and spreads quickly throughout a network. Along with Ryuk, Emotet has cost its victims many millions of dollars in damages.

ZeuS

Despite its age, having originated in the early 2000s, Zeus is still widely used. It is a banking keylogger trojan, which steals credentials from users when they attempt to access their bank's website. It is also widely used in building botnets for DDoS attacks.

TrickBot

Distributed through mail attachments or on compromised website downloads, TrickBot is a dropper that enables hackers to download additional malicious software onto their victim's machines. Once the malicious attachment is opened, users are asked to enable macros in a Word or Excel file that activates Powershell script that then downloads the malware.

Ryuk

One of the most prevalent ransomware types out in the field today, Ryuk hits its victims by not only encrypting their data. It also finds other copies of the data and deletes them to hinder backup attempts.

Gh0st

The Gh0st malware is utilized as a Remote Access Trojan (RAT) to manipulate compromised endpoints. It is typically deployed by other malicious software to establish a secret entry point, which grants the attacker complete control over the compromised device.

It is very common to see hacking groups combine two or more of these malwares in their attacks. If we think about a cyber attack in two stages, the initial breach and then the payload that does the damage, then we understand why they like to mix and match these. One popular combination of late has been to use TrickBot to gain access to the victim's machine and then downloading Ryuk to wreak havoc, locking down the target's files until they pay the ransom.

Hacking individual account users and financial institutions as organizations is nasty business that causes serious costs.

But who are the malicious actors that are targeting financial institutions and what are their motivations?

Identifying the Threat Actors

Banks and other financial institutions are the types of targets that everyone seems to want to break into. As noted previously, there are plenty of valuables worth going after there.

But for our purposes, we should break our threat actors down into two groups.

Criminal Groups

The most common type of hacker out there is the criminal hacker. With no overt political ideology or purpose, these scofflaws are out for profit. These can be organized gangs of hackers that coordinate with each other to create malware, phishing lures, and other tools of the trade. Some of these mercenary hacking groups like Roy/Zeon have built reputations for being effective at targeting financial institutions.

Black Basta, an offshoot of the Conti and REvil gangs, builds off of their previous tactics. This organization hit 50 organizations in the third quarter of 2022 alone, demanding millions of dollars in ransom from their victims.

There are also others who simply buy the malware and even pre-written phishing email texts that they need for their campaign off of the Dark Web prepackaged. The growth of this more “Malware as a Service” cybercrime ecosystem highlights the reduction in the need for deep technical skills in order to carry out successful hacking.

There are of course individual hackers out there in their hoodies, but cybercrime targeting the financials is big enough business that it usually requires whole teams running the different elements of the attacks.

State Actors

On the other side of the spectrum from the mercenaries are the state actors. These are hackers who work directly for, or at least in close coordination with, their government's intelligence services. Unlike criminal groups, which are often much more cognizant of the cost/benefit ratio in deciding if a target is worthwhile, state actors have the resources and time to be much more persistent in going after their targets.

North Korea is the country that is most often directly involved in cybercrime. Their groups of hackers, which have externally been named the Lazarus Group, have been cited for their targeting of banks and financial organizations. As a country with a very limited economy but big ambitions when it comes to its nuclear and missile programs, North Korea has made good use of its nation's hackers to steal currency wherever possible.

The United States includes the financial sector as part of the country's critical infrastructure and takes actions like the hacking of banks as a threat to national security.

According to the Cybersecurity and Infrastructure Security Agency (CISA), "North Korea's widespread international bank robbery scheme that exploits critical banking systems may erode confidence in those systems and presents risks to financial institutions across the world."

But North Korea is not the only bad actor that uses government resources to target the civilian financial infrastructure.

In countries like Russia and China, the intelligence services are known to work with "patriotic hackers" who also work as cyber thieves. These individuals are not always directly employed by their governments, but are often backed and protected by their country in exchange for their participation in state-directed hacking.
Specifically in Russia where hackers who do not go after Russian victims are allowed to operate in relative security, it is not uncommon for intelligence services to call on them for espionage work as well.

The US government has alleged that Evil Corp's Maksim Yakubets, one of the heads of the gang, has been employed in part by Russia's FSB for cyber spying work over the past three years.

The Russian government has even elevated cyberattacks to become a part of active warfare after the start of the Russian invasion of Ukraine. Russian 'hacktivists' hoped attacks would provide a military advantage but instead scored no decisive victories.

China has also made widespread use of its hackers to go after finance companies among other targets that are in their strategic interests. Generally less interested in theft of funds, the Chinese state-backed hackers are on the hunt for information. A series of hacks including the Office of Personnel Management (OPM), Marriott, and the credit rating agency Equifax, are believed to be an effort by the Chinese government to gather massive amounts of information about Americans for intelligence purposes.

The Globalization of Hacking

Regardless of whether a hacking group is state-backed or just out for the payday, the fact is that it is easier than ever to carry out attacks against targets across the world than ever before. The internet, proliferation of knowledge, and ease of attaining tools has led to a real globalization of crime. Once geopolitics are added to the mix, where the government in one country is unlikely to arrest a hacker who attacks targets in an adversary, the chances of the perpetrators being held responsible for their actions drops to nearly nil.

As the pace and reach of global business has expanded, financial institutions have had to deal with a growing risk factor if they are hit with an attack.

What are the Potential Consequences of an Attack on Financial Institutions?

Over the past decade, the public has grown used to cyber attacks and the need for security. Hacks happen. The question for organizations is more about how serious the fallout will be after it comes to light.

Did they follow best practices in trying to prevent the hack in the first place? Were measures taken to mitigate the damages from a breach like segmenting and encrypting their data?

Failure to act decisively can have negative consequences for the organization in the short and long term.

The Globalization of Hacking

How an organization works to protect its customers' data can have a significant impact on their ability to retain customer trust. Especially given the high stakes of the financial industry, customer trust is at a premium.

It should come as no surprise that customers' satisfaction with their bank correlates with how well they feel that their security is being managed. Those organizations that cultivate a reputation for taking strong security precautions and practices can gain an edge in an increasingly competitive market.

However the opposite is also true that if customers believe that their financial institution was careless or negligent, then it can harm their trust and incentivize them to look elsewhere for services.

Financial Losses Resulting from a Breach

As cited previously, cyber incidents cost the banking segment of the financial service industry $5.97 million per incident. This is way above the average data breach cost of $4.35 million that has been cited in other industries.

Beyond the lost business that a financial institution may incur during or after the breach, there are numerous costs that can arise.

First and foremost is the cost of making customers whole for any money that is actually stolen from their accounts. This is generally a good business decision on the part of financial companies and banks to ensure continued faith in their ability to take care of their customers. The Federal Deposit Insurance Corporation (FDIC) does not cover losses due to identity theft, so the cost is on the company and its own insurers, resulting in annual damages of **$52 billion**.

Along with repaying customers for any losses, financial institutions are likely to encounter additional costs. This pertains to payments associated with damages stemming from a data breach where personally identifiable information (PII) may have been compromised.

One of the biggest hacks on a financial services firm was the Equifax hack of 2017. The company was found liable for the cost of stolen PII when some 147 million records were stolen in a data breach of their servers. The US Federal Trade Commission (FTC) proposed settlement ordered the company to pay $575 million, which included a $300 million fund to help those affected with credit monitoring. According to Equifax, the breach has cost almost $2 billion to date.

Damages to financial institutions are likely to rise in the coming years as the rate of cyber incidents increase. An assessment Cybersecurity ventures expects that costs will grow by 15% per year until it reaches $10.5 trillion in 2025.

A part of these costs will likely come from regulatory fines as public demands for greater responsibility grow in the US and around the world.

Regulatory Considerations

In recent years, governments have stepped up their role in regulating data security. Listed here are a few of the relevant regulations that impact financial institutions:

In the European Union, the General Data Protection Regulation (GDPR) came into force in 2018, imposing significant fines on companies that mishandled personal data. Penalties for violators ranged from €10-20 million to 2-4% of the company's annual turnover, whichever was higher and depending on the severity of the infringement. GDPR is considered to be wide-reaching in its scope and has consequences for organizations that do not comply with data protection standards.

While the US does not have such a comprehensive data protection regime, there are a number of laws governing how financial institutions need to take important steps to keep data secure.

As breaches continue to be more frequent and the value that society places on data protection increases, more regulations aimed at enforcing security standards are likely. They will demand that financial institutions take more proactive measures in ensuring that they are taking significant and effective steps to keeping their customers and data secure.

Graham-Leach-Bliley Act

A consumer protection law, the GLBA requires all financial institutions that offer loans, financial or investment advice, or insurance to properly handle sensitive data and be transparent regarding their practices with their customers.

23 NYCRR Part 500

A set of regulations from the New York Department of Financial Services, this rule tackles the risks of cyber attacks to financial institutions head on. It requires financial institutions to maintain high standards in protecting their customers' data. While this is a state-run regulation set, the outsized role that New York plays in the financial sector gives it a lot of influence in moving the direction of the industry.

Payment Card Industry Data Security Standard

Governing the handling and processing of payment cards, these regulations set the rules for how companies are expected to secure their customers' data. Beyond their standard setting, this regulator works closely with merchants and financial organizations to improve how they practice security.

Post-Pandemic Challenges

The COVID-19 pandemic has changed the way that organizations of all types get work done. It has also massively changed how financial institutions manage their security. Hackers initially took advantage of the confusion and disorder of businesses moving to remote work and now are targeting employees returning to physical offices.

Since the pandemic, financial institutions that transitioned from in-person signatures accelerated the dependence on having every interaction be digital by default. As many organizations rushed in this process, security standards were not fully addressed throughout the transition. Many have since revisited their security to maintain compliance and best practices.

According to research by AT&T, the hybrid and remote work model that emerged during the pandemic is here to stay, with hybrid accounting for 81% of positions and 19% remaining fully remote.

These changes shifted towards a totally digital future, and organizations are not going to revert to paper as pandemic investments have permanently altered the traditional models. So how are we going to prepare ourselves for the future without compromise?

Why Current Security Solutions Are Ineffective

The financial industry has invested heavily in security, adopting many of the most advanced security tools available.

A report from IANS found that financial institutions invest 9.6% of their IT budget into security, more than the 6.0% invested by retail services.

Unfortunately, when it comes to the challenge of stopping file-borne malware, many of the tools such as Next Generation Anti-Virus (NGAV) are insufficient.

Why is Anti-Virus Not Enough?

Anti-virus software works by inspecting files for malware using signatures. If it identifies a file that it believes matches the signature of a known malware, then it can quarantine it in a sandbox to keep the user safe.

However, there are a number of reasons why this approach needs additional layers of control to effectively secure incoming files.

1. **Malware is constantly changing to improve its capabilities and avoid detection. Relying on AV's ability to catch every variation of a polymorphic malware like Emotet is highly risky and uncertain. The AV might not have a specific version of the malware on its "do not allow/black list" and it can get through.**

The same issue stands for dealing with 0-day exploits in malware that simply have not been identified yet. It is hard to stop what you do not know to detect.

2. **Obfuscation can also impede detection. Hackers have gotten better and better at hiding their malware inside of files. Next Generation Anti-Virus can be fooled if the hacker is clever enough.**

Surveys of information security professionals dating as far back as 2017 show that almost 73% of professionals believe traditional AV solutions are insufficient to effectively stop modern threats.

Overloaded IT Teams

Organizations train their employees to alert the IT or Security teams when they receive a suspicious email or other risky situations that require a more experienced set of eyes. Think of the corporate version of “See something, say something,” but for cyber.

This is a good instinct and employees should feel that they can reach out for assistance if needed. But this is untenable when it comes to the scale of working securely with incoming files.

Employees need to be able to open documents without jumping through multiple hoops for dealing with every file. Sending every document to IT to be manually investigated and approved before opening it is not a viable option for effective operations. Security and IT teams have their own workload to handle and their time needs to be reserved for special cases.

So how can financial institutions maintain security without sacrificing efficiency?

They need a solution that will allow them to work normally and confidently.

Zero Trust Content Security Eliminates Risk from File-Borne Malware

Countering the risk of file-borne malware to financial institutions means seeking out solutions that will not interrupt the flow of business, while ensuring that every file that comes in is safe to use.

Creating allow lists for certain "safe" file types or relying on detection only to remove the risky elements of a file is an arms race with little or no assurance, as adversaries create new malware strains as well as find new ways to obfuscate their malware.

Security that Enables Productivity

The most effective security tools are those that empower people to do more while improving their security.

For employees at financial institutions, time wasted on wondering if the file attachment that they received in an email is going to put their company at risk is not time well spent. Time here is quite literally money.

Zero Trust Content Security security processes work in the background without any need for interaction by the employee. The newly reconstructed files come through to the recipient with all of the content that they need, no matter how complex the file type. Office documents like Word and Excel transfer easily into new files. Images and PDFs where code can be hidden away come through with every detail that is needed but no more. Even large archival files with their multitude of detail are recreated.

Zero Trust Content Security is a different approach to eliminating malware. With Zero Trust Content Security, there is no "safe" file type, instead all files are sanitized by default, eliminating hidden threats. Any malware that might have been hidden in the original file stays there and the valuable safe content is passed on to the recipient.

Votiro ZT Cloud

Votiro ZT Cloud is a Zero Trust Content Security solution that directly integrates with existing solutions as an additional security layer or can replace detection-based security controls currently in place.

Votiro ZT Cloud automatically sanitize each and every file sent to or shared with your company, reconstructing a clean, safe to use, fully functional version of the original file. Votiro ZT Cloud can also be deployed with integrated AV protections in place to detect and block the first layer of known-bad files before file sanitization.

The Votiro Process:

1. **Detect.** Utilize AV to detect and block known-bad malware signatures in incoming files.

2. **Disarm.** Process every "safe" file through our content disarm and reconstruction process to proactively eliminate any hidden, evasive, or even zero-day malware threats.

3. **Analyze.** Pass the information and analytics to your SIEM, in order to provide increased visibility, threat hunting, and intelligence to your SOC or threat intelligence team.

To date, Votiro ZT Cloud has successfully cleansed over 5 billion files without a single successful 0-day or any other exploit. Available for web downloads and uploads, email, content collaboration platforms and other applications — Votiro ZT Cloud ensures you can safely and fully use files via any platform, no matter their type or where they came from.

Experience Secure & Usable Files For Yourself

Schedule A Demo

VOTIRO

Votiro is a zero-trust content security company delivering safe files to hundreds of commercial and government organizations worldwide. Votiro ZT Cloud is an open API solution to detect, disarm, and analyze fully functional content at the speed of business.

Votiro eliminates file-borne threats targeting your remote workers, content-rich apps, data lakes, supply chain, and B2C digital interactions. Votiro is headquartered in the Austin, TX, with offices in Australia, Israel, and Singapore.

Votiro is trusted by millions of users worldwide to receive safe content with complete peace of mind. Votiro ZT Cloud is a SOC 2 Type II compliant solution and certified by the international standard of Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). Learn more at www.votiro.com