



VOTIRO
SECURED.

Protecting you from tomorrow's
threats today.

Contents

Advanced Content Disarm and Reconstruction Technology.....	2
Advanced Content Disarm and Reconstruction API.....	10
Email Content—Disarming Gateway.....	14
Case Study: One Bank’s Story.....	18
Case Study: Ransomware Protection.....	22
Conclusions.....	26

About Votiro

Established in 2010, Votiro is a leader in cyber-protection technology for organizations that are a target for cybersecurity attackers and are underprotected by conventional enterprise IT solutions. Votiro was founded by a team of senior security experts with vast experience in intelligence, government, and enterprise security organizations. Familiar with such organizations’ requirements for safeguarding their sensitive proprietary data, the Votiro team develops and licenses unique solutions that protect networks and infrastructures from external cyber threats.

Among Votiro’s customers are network equipment providers, software vendors, government and defense agencies, financial institutions, telecom enterprises, pharmaceutical companies, and health-care organizations.

To learn more, visit www.votiro.com or contact us at info@votiro.com.



Advanced Content Disarm and Reconstruction Technology

Executive Summary

Cyber defenses are a must for all enterprises, yet many companies deploy solutions that are powerless in an environment where undisclosed and zero-day attacks abound. With cybercriminals becoming more sophisticated than ever and investing enormous effort in preparing successful targeted attacks, a revolutionary approach to cyber protection is required. The patented Advanced Content Disarm and Reconstruction technology from Votiro provides the ultimate solution for stopping undisclosed and zero-day threats before they come through an organization's door.

The Need

Today's ever-increasing reliance on data brings with it elevated risks, threats, and vulnerabilities for organizations and communication networks, and many of these vulnerabilities are undetectable by traditional network security devices. In the past, cyber threats affected only a small portion of business activity. However, as the reliance on data continues to grow, so too does the impact of cyber threats on organizations' business activity. With the increasingly aggressive nature of cyber attacks, novel approaches to security are needed to successfully protect organizations.

Exploiting a Vulnerability via Targeted Attacks

By design, an exploit targets a vulnerability in an application and typically triggers an intruder's code.




A vulnerability is a “hole” in an application—say, Adobe Reader—that can be exploited to launch an attack on a computer or network system. A common method used by attackers to exploit vulnerabilities is spear phishing: sending targeted email messages that contain a malicious attachment and look harmless to the recipients. When a recipient opens the attachment, malware is deployed and the targeted attack begins.

Life Cycle of a Vulnerability

A software vulnerability opens the door to cybercriminals. A person who discovers a vulnerability can use it to gain entry to a system and then obtain unauthorized access to data.

A vulnerability has a life cycle consisting of three stages: undisclosed, zero-day, and patched.

Life Cycle of a Vulnerability and Its Exploitation

	 Stage 1 Undisclosed	 Stage 2 Zero-Day	 Stage 3 Patched
Threat	High	High	Low
Duration	Years	Months	N/A
Usage	Cyber warfare and cybercrime	Cyber warfare and spray attacks	Opportunistic attacks by script kiddies
Signature-Based Detection	No	According to provided samples	According to provided samples
Votiro Protection	Yes	Yes	Yes

 **Stage 1**
Undisclosed

At this stage, a vulnerability in an application, a system, or even hardware is unknown to the vendor or the security community but has been discovered by someone, possibly a researcher in a cyber warfare organization—or worse. This type of vulnerability presents a high security threat to everyone and can go undetected for years. Because the application’s vendor does not know of the vulnerability, countermeasures cannot be developed to prevent or block its exploitation. Undisclosed vulnerabilities are frequently used by groups that gather cyber intelligence or trade information to receive large cash payouts.

 **Stage 2**
Zero-Day

At this point, the vulnerability has been disclosed to the vendor and the security community. A zero-day vulnerability is a software weakness that has just appeared for the first time, and no patch has been developed to overcome it. This type of vulnerability presents a high risk of exploitation; intrusion detection systems or traditional protection systems using signature-based detection might identify exploitation activity after gathering and extracting several samples, but an exploit that a hacker has manipulated will be able to avoid signature detection.

Zero-day vulnerabilities can go unaddressed for some time, because vendors may take 90 days or even more to respond to reported threats.

 **Stage 3**
Patched

At this stage, although the vendor has already issued a patch for the vulnerability, it can be opportunistically exploited in non-patched environments of out-of-date applications. Large organizations may be particularly susceptible to opportunistic attacks, because patch management is more cumbersome than in smaller organizations. The threat level at this stage is low, because the vendor has provided a patch.

Votiro technology protects organizations from cyber attacks brought on by exploits at all three stages of the vulnerability life cycle.

The Solution: Disarming Undisclosed and Zero-Day Exploits

Votiro's Advanced Content Disarm and Reconstruction technology is a proactive, signature-less method that targets the file formats that are most commonly exploited via spear phishing, other advanced persistent threats, and cyber attacks (Figure 1). The technology disarms exploit attempts before they reach the end-user environment.

To ensure a successful exploit, malware writers often carefully design and build multiple suspicious objects and embed them in a malicious complex file. For example, a Microsoft® Word file may contain an ActiveX® or OLE object to execute an attack, plus shellcode that is triggered by a malicious image or macro. (Shellcode is a small piece of code used as the payload in the exploitation of a software vulnerability). The Votiro Advanced Content Disarm and Reconstruction engine carefully inspects the file to identify malicious or suspect content and then, after extracting the malicious content, rebuilds the file in such a way as to retain its usability.

"As malware sandbox evasion techniques improve, the use of content disarm and reconstruction (CDR) at the email gateway as a supplement or alternative to sandboxing will increase."¹

¹ Neil Wynne, Andrew Walls, Peter Firstbrook, "Fighting Phishing: Optimize Your Defense," Gartner, March 17, 2016 (<https://www.gartner.com/doc/3256817/fighting-phishing-optimize-defense>)

All the functionality that users need for working with a file, such as copying text, handling bookmarks, keeping content on the original pages, and searching, is preserved.

How Votiro Advanced Content Disarm and Reconstruction Technology Works

The Votiro Advanced Content Disarm and Reconstruction Technology disarms files in a three-phase process.

PHASE 1 | Identifying the format

Every file must adhere to a strict specification that is unique to that particular file format. Votiro's Advanced Content Disarm and Reconstruction technology thoroughly examines each file to verify that its format adheres to the vendor's specifications and to detect impersonation.

The Advanced Content Disarm and Reconstruction technology uses an intelligent fingerprinting technique that identifies a file's content type and format. Next, the file is examined and compared to the vendor's format specifications. For example, a Microsoft Word document will be checked to ensure that it complies with the required Microsoft file format. The Votiro engine then scans the file structure for malformed fields and attributes that could indicate a possible exploitation attempt. The Advanced Content Disarm and Reconstruction algorithm determines, on the basis of the file's unique "fingerprint," whether the file is malicious and disarming is required. Malformed files are blocked, and an alert is generated.

PHASE 2 | Disarming the file

In this phase, the Votiro Advanced Content Disarm and Reconstruction technology injects microchanges and roadblocks into the exploit's execution flow. Macros, scripts, and other suspicious embedded objects and elements are identified and removed. Additional active content, such as OLE objects and attachments, is processed recursively. The exploit-protection process then converts the file to a raw format.

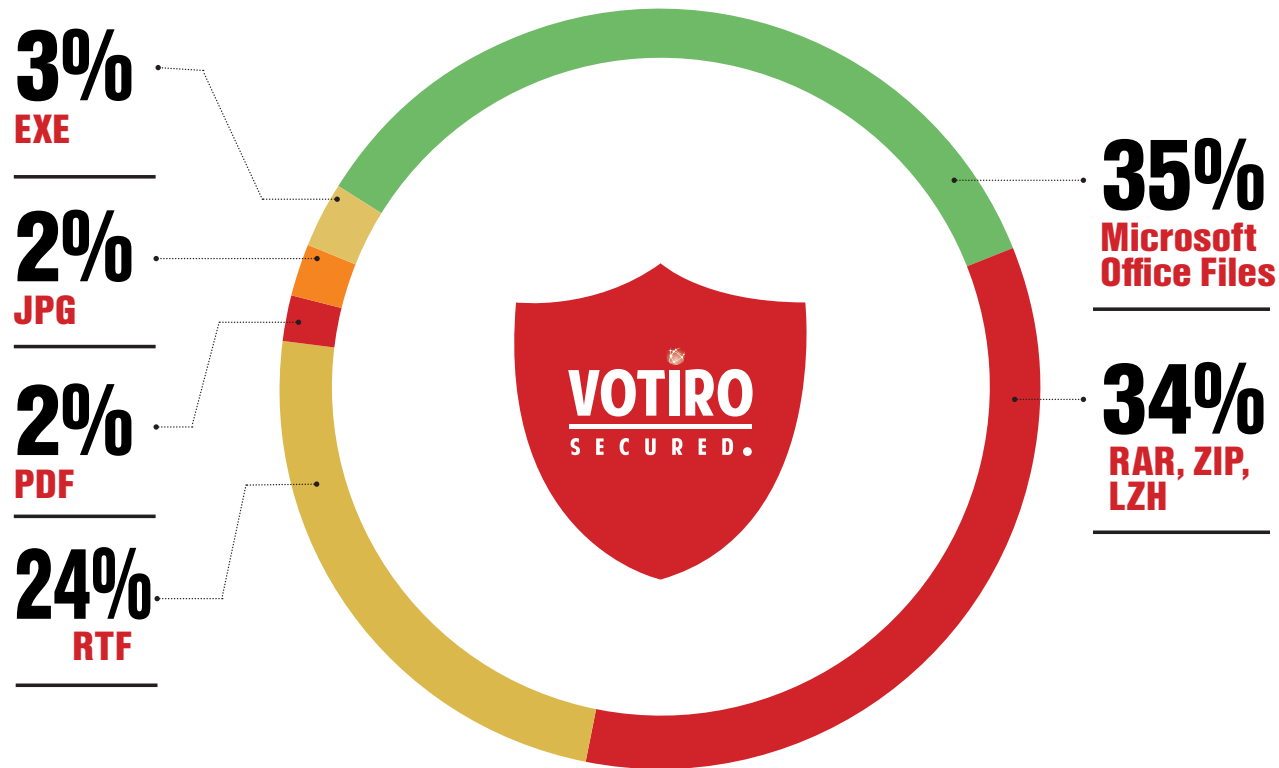
These actions interfere with the execution of the shellcode, thereby neutralizing the exploitation attempt.

PHASE 3 | Generating a disarmed version of the file

In this phase, the file is reconstructed somewhat differently from the original file and exhibits a well-known structure based on the file format's specifications. All malicious code and exploit threats have been disarmed, and all the original functionality of the file is intact.

The entire process is invisible to users, does not disrupt business activity—and normally takes less than a second!

File Types Often Used in Targeted Attacks



Trend Micro, "Targeted Attack Trends: 2014 Annual Report" (<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-targeted-attack-trends-annual-2014-report.pdf>).

The Votiro Advanced Content Disarm and Reconstruction technology supports containers, such as ZIP and other archive files, as well as the files within the containers. In the latter case, multiple compressed layers are recursively decompressed, disarmed, and recompressed, preserving the files' original functionality.

Supported File Formats

Votiro's Advanced Content Disarm and Reconstruction technology handles many types of files.



Documents

The Votiro technology supports PDF, RTF, HWP (Hangul Word Processor from Hancom Office suite) and JTD (Ichitaro Word Processing from JustSystems) formats. The Advanced Content Disarm and Reconstruction inspects the structure of the file and extracts the text, embedded objects, layout, images, scripts, bookmarks, and other elements recursively. Depending on the policy set for the particular user, the process disarms active content, such as JavaScript. Then the content is packed, and the file is returned to its original structure



Microsoft Office files

The Advanced CDR process unpacks a Microsoft Office file, recursively checking embedded objects such as images, documents, and OLE objects. Invalid or prohibited objects are stripped and replaced with placeholders or textual notations. After the file is deemed safe, it is reconstructed and delivered to the recipient or target location.



Archives

The Votiro technology supports all common archive formats: ZIP, RAR, 7-Zip, and CAB. As the container is unpacked, the Advanced Content Disarm and Reconstruction process runs recursively. After the content is successfully secured, it is repacked into the original container format.



CAD

The Advanced CDR process supports DWG and DXF formats (by Autodesk), the standard planning formats used by government, construction and manufacturing organizations. The Advanced Content Disarm and Reconstruction process runs recursively while disarming active content such as JavaScript, macros and OLE objects. After the content is successfully secured the file is reconstructed.



Email containers

The Advanced Content Disarm and Reconstruction technology supports several email containers, including EML and MSG. An email message is broken down into the subject, the body, MIME-encoded attachments, and other elements. The process runs recursively. After the content is successfully secured, the email container is rebuilt and the message is delivered to its recipients.



Images

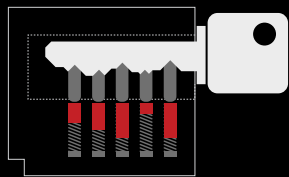
The technology removes malicious content from all the common image formats: JPEG, GIF, BMP, PNG, TIFF, EMF, and WMF.

Example

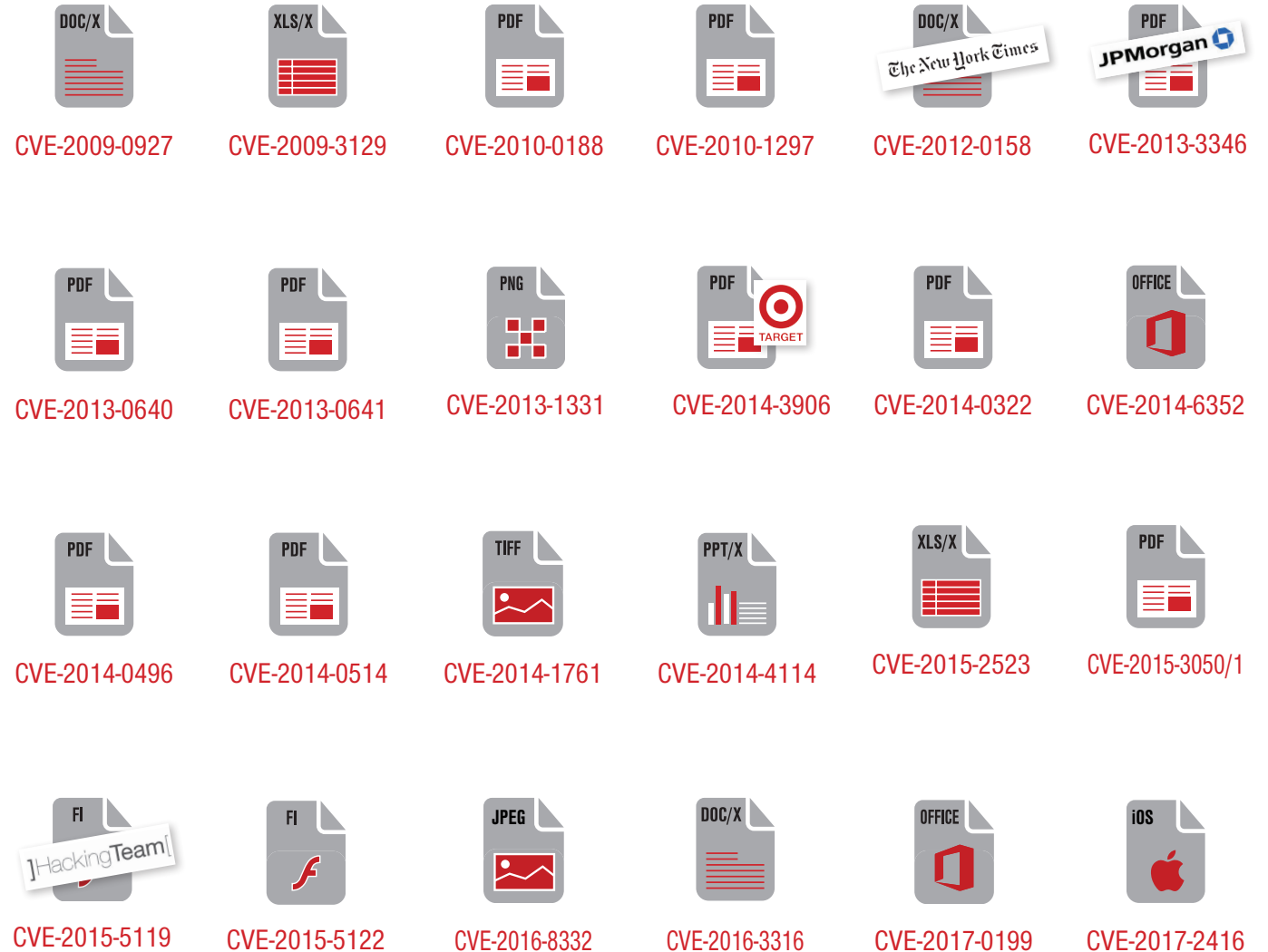
A malicious image has been attached to a targeted email message. The image contains embedded shellcode. For successful exploitation, the shellcode must run on the processor exactly as written, bit by bit. Think of shellcode as a lock in which all the pins must be precisely positioned for the lock to open.

An image viewer is supposed to display the pixels of the attached image. However, the image contains an exploit, so an image viewer application that has a vulnerability will execute the exploit when displaying the image's pixels.

The Votiro Advanced Content Disarm and Reconstruction process dissects the raw image data, restructures the bits (the exploit code embedded in the image), and then reconstructs the original file without the exploit code. Now the image viewer can display the pixels without running the exploit.



Technology is able to neutralize attacks with **No Signature Required**





Advanced Content Disarm and Reconstruction API

Solution provider?

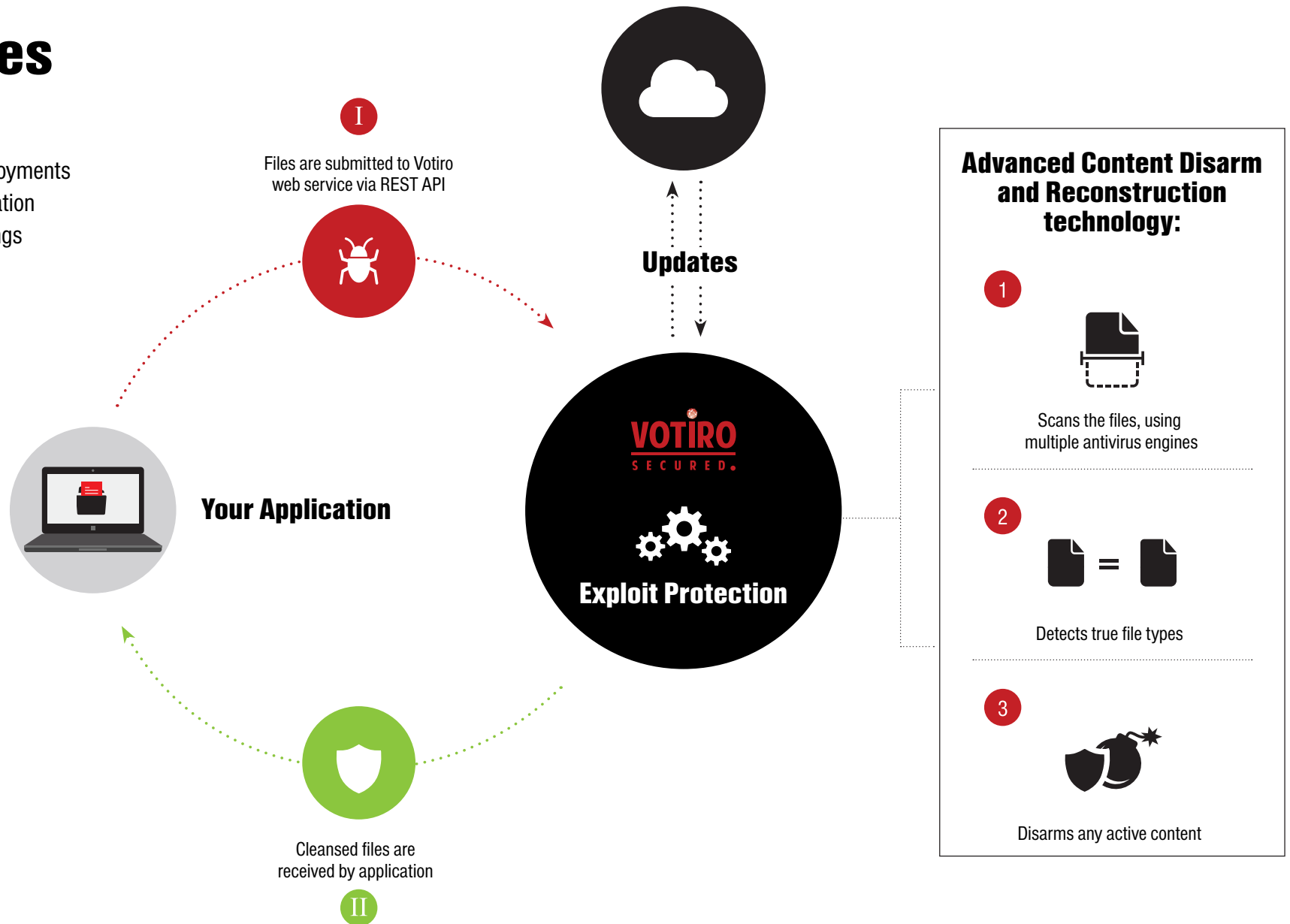
Empower your security solutions with Votiro's patented Advanced Content Disarm and Reconstruction (CDR) technology.

With zero latency and scalable deployment, Votiro's technology fits any size application.

Get your FREE API key now!
www.votiro.com/api

API Features

- › RESTful API
- › Easy integration
- › Cloud and on-premises deployments
- › Queuing for threat neutralization
- › Control of policies and settings
- › Generation of full reports





Votiro API Benefits

Patented active content disarm technology

100% advanced protection against exploits embedded in documents

Preservation of file type and functionality

Zero latency

Zero false positives

Advanced threat protection

CISO-friendly design

Flexible deployment options (cloud-based and on-premises)

What Is Votiro Advanced Content Disarm and Reconstruction Technology?

Votiro's Advanced Content Disarm and Reconstruction technology is a proactive, signature-less technology that targets the file formats that are most commonly exploited in cyber attacks, in advanced persistent threats, and especially in spear-phishing attacks. The technology neutralizes exploits before they reach the end-user environment and compromise the organization's system.

Votiro's technology protects mobile and desktop editions of many file formats, including Microsoft® Office files, Adobe® PDF files, image files, archives, RTF files, and more.



Votiro-cleansed files are safe to edit and preserve all functionality

The Votiro Advanced Content Disarm and Reconstruction API enables you to easily integrate the innovative Votiro security technology into your application, enhancing your application's capabilities and offering a superior security solution.

Through the Votiro API, all threats are neutralized and users retrieve a totally cleansed version of the files. The original functionality of these safe files is preserved, so users can edit the files in the normal way.



Email Content- Disarming Gateway

Powered by Votiro's patented Advanced Content Disarm and Reconstruction technology

Protect Your Data With Votiro's Email Content-Disarming Gateway

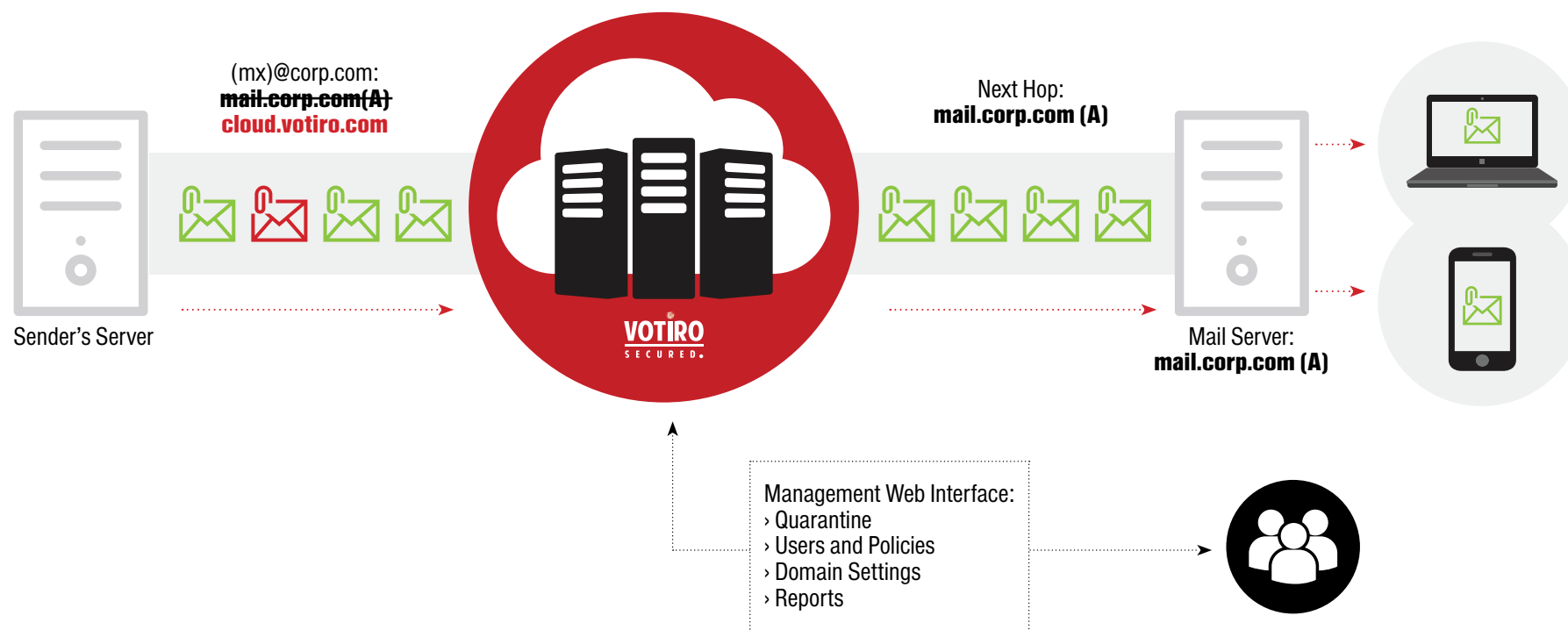
Imagine that an employee opens an email message that seems to have come from a colleague. Suddenly, malware enters your network silently, ready to steal your confidential data. Using sophisticated methods of creating genuine-looking messages, cyber criminals too often succeed in luring recipients—even those who have been well trained in security risks—to go ahead and open

- attachments.

Meet the Votiro™ Email Content- Disarming Gateway

Powered by Votiro's patented Advanced Content Disarm and Reconstruction technology, the cloud-based Votiro Email Content-Disarming Gateway helps keep your customers' credit card information, passwords, and other sensitive data safe by sanitizing all threats embedded in incoming email messages. In use worldwide at institutions such as banks, government and defense agencies, pharmaceutical companies, and utilities, Votiro's secure Content-Disarming Gateway offers you the quality of a mature, proven technology.

Figure 1. Votiro Data Center





Votiro Email Content-Disarming Gateway Benefits

.....
Applies Votiro's patented Advanced Content Disarm and Reconstruction technology to cleanse incoming email, protecting your organization against undisclosed and zero-day exploits
.....

Harnesses commercial antivirus and anti-malware solutions to safeguard your network against known threats
.....

Is delivered as a managed security service, saving your organization the effort and expense of maintaining additional servers and carrying out time-consuming endpoint installations
.....

Works automatically, eliminating your dependence on employee vigilance or actions to safeguard your organization
.....

How Does It Work?

Email messages sent to your organization are automatically routed directly to the Votiro cloud-based email server. To detect known threats, the Votiro Content–Disarming Gateway applies antivirus programs to all files attached to the messages. To block undisclosed and zero-day exploits, the Content–Disarming Gateway extracts and disarms any malicious content from an attachment while keeping the original attachment's functionality intact. Cleansed and harmless, the email messages and their attached files continue on to your organization's email server. The entire process usually takes less than a second.

To help ensure your organization's privacy, Votiro stores no email messages on its servers, nor does it store the original or cleansed versions of the attachments.

With the Votiro Advanced Content Disarm and Reconstruction technology, Votiro's Gateway supports the file formats most commonly used in highly targeted spear-phishing attacks. Among them are Microsoft® Word, Excel®, and PowerPoint® files, as well as RTF, PDF, image, and archived files. In addition, the technology detects executable and encrypted files and can block them if you so opt. Votiro's Gateway works out of the box with Microsoft Office 365®, hosted and on-premises Microsoft Exchange, Google Apps, and other mailbox services.

Setup and Management

To set up the Votiro Email Content-Disarming Gateway, you simply redirect all email to the Votiro cloud by modifying the DNS MX record. Using the intuitive, straightforward Votiro web interface, you can easily define file-scanning policies for employees. The service automatically processes every incoming email message according to the policies and parameters that you have defined and displays cyber-attack reports broken down by employee.

“An organization may expect to be targeted at least four times during the year. The attackers only have to succeed once, whereas the businesses must thwart each and every attack to remain secure. Businesses should already be thinking about what to do when (not if) such a breach occurs.”

—Symantec 2016 Internet Security Threat Report



Case Study: One Bank's Story

Background

Seeking a solution to defend its email gateway against rising security threats, a bank issued a request for proposals in 2013. In early 2014, the bank equipped itself with one of the best-known mail relay servers and a leading sandbox solution for detecting all threats trying to penetrate the bank. In addition, the bank licensed the Votiro Email Content–Disarming Gateway solution.

The bank also implemented a second sandbox (from a different vendor) for backup protection in case a threat managed to evade the Votiro Gateway. This sandbox was configured to perform retroactive scanning of all original email messages—incoming messages that had not yet been modified by any defense process. The scanning would take place a few days after a message's arrival and again a few months later, to check for signatures of new threats.

“Ensuring the safety of our organization’s sensitive information is our number one priority. Votiro’s Content Disarm and Reconstruction technology is absolutely doing the job.”

—CSO of a multibillion-dollar bank

The Threat and the Defense

In 2016, a potentially serious incident occurred at the bank.

About the Bank

The bank is among the busiest ones in the country, with over 200 branches, 11,000 employees, millions of customers, multiple subsidiaries around the world, and an annual income of \$6 billion. Every day, thousands of email messages come into the bank's network.



02:06:23

Penetration

An incoming exploit bypassed the mail relay server's defenses because the sender's IP address and email account were not on the mail relay's blacklist, and the threat's signature was unknown to the mail relay.



02:06:24

Detection Attempt

The exploit evaded the sandbox by monitoring the services on the sandbox machine and locating services (on the Internet) associated with a specific sandbox vendor.



02:08:48

Neutralization

The Votiro solution's patented active content disarm technology, designed to remove unknown and zero-day exploits, successfully sanitized the exploit.



02:08:50

Validation

The cleansed email message was sent to a second sandbox machine for analysis.



02:11:20

Delivery

With all threats eliminated, the email message was delivered to the user's mailbox.

Figure 1. On-Premises Threat Neutralization



Subsequent Developments

A few days later, a retroactive scan of original email messages identified a signature that had been added in a recent update. A threat alert was issued. That threat was the exploit that the Votiro solution had successfully eliminated without identifying the signature! If it had not been neutralized, the exploit could have created a backdoor that would enable unknown ransomware to enter the bank's network.

“We chose Votiro because of its unique concept and its known success in stopping any exploit arriving through the email channel. The Votiro technology has really proved its worth for us.”

— The bank's CISO

“I must admit that seeing the alert during the retroactive scan really spooked me,” said the bank's IT manager. “We immediately began checking for signs of damage. Each time we saw that a network segment hadn't triggered an alert for the same signature, we breathed a sigh of relief. When all the segments had been scanned and no evidence of the threat had appeared, we looked into the history of the threat's signature. “The only traces of the threat's presence were in the original message, before it had undergone the Votiro cleansing. We reprocessed the original message with the Votiro gateway solution, and the exploit was completely neutralized!”

Eventually, it became clear that the bank would not need to renew its license for the second sandbox, because no exploit had evaded the Votiro gateway.



Case Study: Ransomware Protection

Preventing Ransomware Attacks with Votiro's Advanced CDR

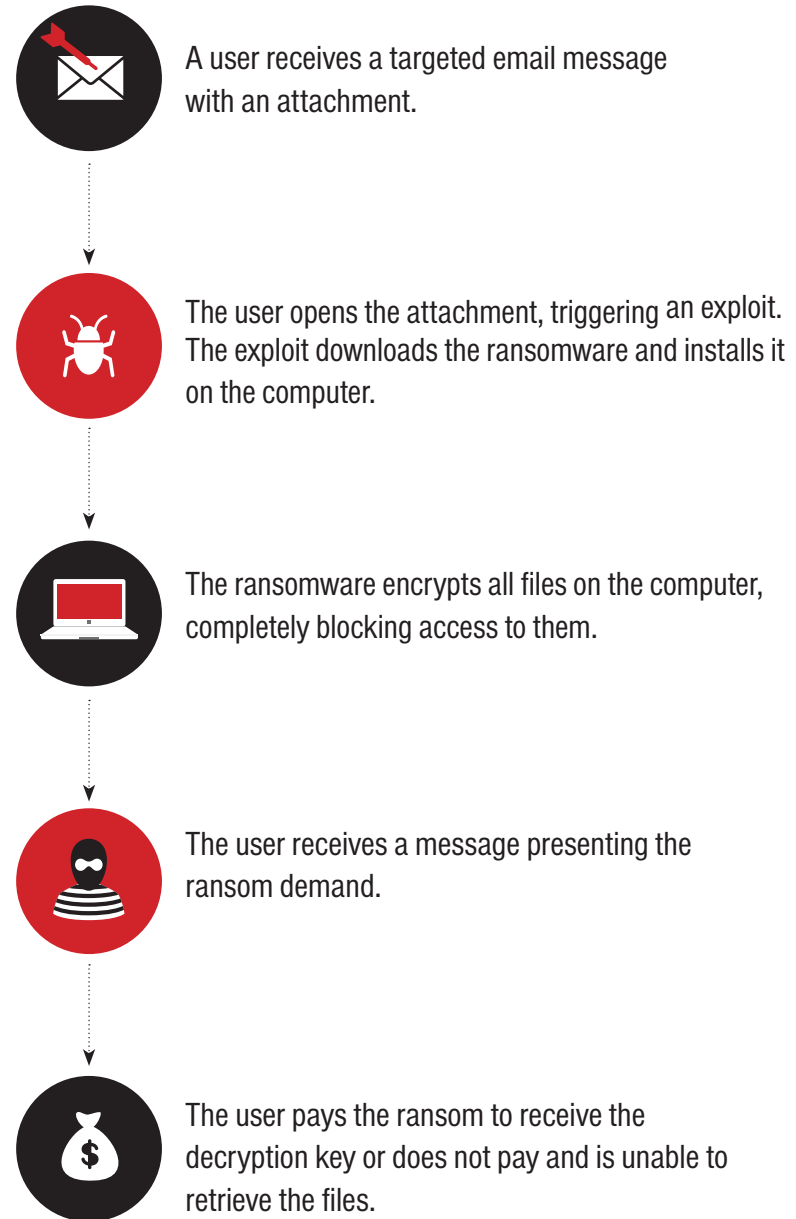
The Bar-Oz insurance company was a victim of multiple ransomware attacks that disrupted its day-to-day operations and threatened to cause serious damage to the company's finances and reputation. After deploying Votiro's Email Gateway, with its Advanced Content Disarm and Reconstruction technology, Bar-Oz experienced no more ransomware intrusions.

What Is Ransomware?

Ransomware is malicious software that, when activated, locks the victim's computer or encrypts the files in the computer. To regain access, the victim must pay a ransom to the hacker who injected the ransomware. One of the most popular types of ransomware among today's cybercriminals is Cryptolocker, which encrypts a victim's files. Only after paying a ransom does the victim obtain the decryption key for unlocking the files. Several ransomware removal tools are available online, but most of them are useless, especially on newer types of ransomware.

Votiro's patented Advanced Content Disarm and Reconstruction technology actively disarms malicious content in a file and reconstructs a clean, safe-to-edit version of the original file, keeping all of its functionality intact.

Votiro's technology does not rely on signatures and does not need to recognize a threat in order to sanitize it. Ransomware attacks depend on the manipulation of a file's active content to exploit a vulnerability in an application. Votiro's proven Advanced Content Disarm and Reconstruction technology renders any ransomware attack inert.



The Cost of Ransomware

According to a 2015 report from the Cyber Threat Alliance, CryptoWall ransomware was accountable for \$325 million in damages in 2015.

Losses from a ransomware attack don't stop with the ransom itself. In a 2016 attack, Hollywood Presbyterian Medical Center was forced to pay \$17,000 in Bitcoin to regain access to its files. However, the other costs involved in such an incident can easily surpass the ransom that is paid. Citing InfoSec Institute, Brad Brooks notes that “the cost of a computer forensic investigation varies greatly (\$100-\$600 per hour), depending on the number and types of systems involved and the complexity of the recovery of evidence.”¹ Add to that the financial harm stemming from the system's downtime, the loss of current and future customers because of the organization's damaged reputation, and the outlay required for patching the vulnerabilities in the system. In the end, ransomware attacks are expected to cost about \$1 billion in 2016.

How Do You Get Infected by Ransomware?

The most common way of getting infected by ransomware is via a targeted email attack—specifically, a spear-phishing email message. The message contains an attachment, perhaps a Microsoft Office or Adobe PDF file, from what appears to be a reliable source. A user who opens the attachment unintentionally triggers an exploit, which installs the ransomware in the computer.

Employee Education

Although the employees at the insurance company had undergone multiple cybersecurity training sessions and were told on many occasions how to detect and prevent a cyber attack, those same employees opened potentially malicious attachments that might have enabled ransomware to be deployed.

¹<http://resources.infosecinstitute.com/computer-forensics-investigation-case-study/>

Combating Attacks

Over a two-week period, the company received multiple email messages containing ransomware attacks in the form of Microsoft Word attachments.

Votiro implemented its Email Content-Disarming Gateway, with the patented Votiro Advanced Content Disarm and Reconstruction (CDR) technology. The Gateway blocked the ransomware by actively sanitizing all incoming traffic and delivering safe-to-edit files with their original functionality intact. The entire sanitization process takes less than a second and does not disrupt the company's business activity.

Malicious email messages keep on coming, but the Votiro technology continues to sanitize the files and successfully defeats the attacks.

"We receive thousands of emails a day, so we needed a solution that can work fast without interrupting day-to-day activities. As a cloud-based service, the Votiro Gateway was simple to deploy and started working immediately. We still receive malicious emails but now they are sanitized by Votiro."

— Amir Bar-Oz, CEO

About Bar-Oz Insurance Company

Specializing in homeowners insurance, Bar-Oz has been serving customers for many years. As a well-known company, Bar-Oz receives many email messages and files on a daily basis, exposing the company's sensitive data to cyber attacks.

Conclusions



The patented Advanced Content Disarm and Reconstruction technology from Votiro provides the optimal method of shielding your organization from current exploits and future undisclosed and zero-day threats. Votiro solutions neutralize cyber threats without having to identify them in advance. By removing threats on their first attempt to penetrate a network, the Votiro technology provides true protection against zero-day exploits and advanced persistent threats.

Threat neutralization is achieved by making microchanges to the structure and metadata of a file.

Invisible to users, these changes do not affect the file's usability but do eliminate the possibility that malicious code will run from the file. For typical files, threat neutralization is completed in less than one second. By actively processing all files without having to detect threats in advance, Votiro protection surpasses standard methods and removes zero-day threats before they penetrate an organization. Votiro's Advanced Content Disarm and Reconstruction process offers you the quality of a mature, proven technology.

What's Next?

Experience our online demo. Upload a file to the demo on our website (<http://www.votiro.com/demo>). The Votiro Advanced Content Disarm and Reconstruction technology will sanitize all threats, without changing the file's user experience in any way. Your file will come back to you with functionality and content intact.

Try our solution for free. See for yourself how easy it is to safeguard your organization. Register for a free trial today at www.votiro.com.

Future-Ready **Protection** Against Targeted Attacks

Europe, Middle East & Africa

126 Yigal Alon St.
Tel Aviv 67443, Israel
Tel: +972 73 737 4102
Email: sales-emea@votiro.com

North & South America

1325 Avenue of Americas, Floor 28th,
New York, NY, 10019, USA
Tel: +1 415 231 3725
Email: sales-us@votiro.com

Asia Pacific

435 Orchard Road
238877, Singapore
Tel: +65 3159 1224
Email: sales-apac@votiro.com

Australia

20 Martin Place,
Sydney, Australia
Tel: +02 9239 3165
Email: sales-au@votiro.com

