VOTIRO FILE DISARMER
SECURE DIGITAL TRANSFORMATION PREVENT NEXT-GEN EVASIVE ZERO-DAY EXPLOITS

"When 30% of malware consists of zero-day threats - antivirus programs essentially have no way of stopping almost 1 in every 3 threats"

[CSO, 2017]

YOU MAY TRUST YOUR USERS. BUT CAN YOU TRUST THEIR FILES?

The age of digitalization offers immense opportunities to interact with your customers and users.

But the more digital touchpoints - the more potential breach points.

Today, more than ever, malicious macros and payloads can easily penetrate almost any organization through standard digital transactions, such as:

- Identity verification KYC processes (requiring user identification document uploads)

- Online form applications (from insurance claims to visa applications)

- Attachment uploads (such as scanned files and images)

In most cases, users are unaware of any malicious code inserted into their documents, making user identification processes ineffective, and users' files not trust-worthy.

Most incoming files are not processed through an effective sanitization system, and can easily bypass the entire organization's cybersecurity defense layers.

STANDARD CYBERSECURITY DEFENSES ARE POWERLESS AGAINST FILE-BORNE ZERO-DAY ATTACKS

Even the most advanced security ecosystems are helpless in protecting organizations from sophisticated, customized malware attacks against UNKNOWN vulnerabilities coming in via embedded macros. These attacks have proven to evade every traditional security system, including the most advanced Sandbox solutions, causing catastrophic financial and reputational damages even in the most protected industries in the world.

ONE SOLUTION ACROSS ALL PLATFORMS

Zero-day Attacks Can and Should Be Prevented

The File Disarmer integrates directly with your security ecosystem as an additional security layer within minutes, automatically sanitizing every single incoming file in less than 1 second, allowing users to store, share, download or transfer files securely, via any platform.

NOT A SINGLE SUCCESSFUL EXPLOIT IN 5 BILLION FILES

WHAT WE SANITIZE FOR YOU

The File Disarmer scans and sanitizes millions of forms, applications, and documents per month that are either:

Disarmer API
Uploaded by end-users to custom portals in custom applications.

Disarmer for Removable Devices
Uploaded via USB drives or external disks

Disarmer for File Transfer
Shared and sent via FTP, SFTP, FTPS, or any other method

Disarmer for Web
Downloaded from the web

Disarmer for Email
Received via email (the File Disarmer integrates with all existing email security solutions like Proofpoint, Mimecast, Microsoft ATP, etc.)

Disarmer for Content Collaboration Platforms (CCP)
Shared via Box Dropbox, OneDrive, etc

VOTIRO. TRUST YOUR FILES.

- Award-winning, patented solution based on next-gen Content Disarm and Reconstruction (CDR) technology
- A single solution for all channels of incoming files
- Integrates with any security system

- 100% success rate in disarming zero-day attacks
- Original content and functionality completely intact
- Trusted by over 400 customers worldwide

YOU CAN'T GO DIGITAL WITHOUT SECURING INCOMING FILES.

YOU CAN'T GO DIGITAL WITHOUT VOTIRO FILE DISARMER.

Votiro Founded by veterans of Israel's IDF elite technology intelligence unit, Votiro is an award-winning cybersecurity company specialized in neutralizing zero-day and undisclosed targeted content attacks. Our next-generation patented CDR technology disarms threats that other products fail to expose, leaving our customers with a secure, fully usable data flow across all channels of incoming files. With over 500 customers worldwide, Votiro has offices in Israel, US, Australia, and Singapore. Votiro is a Gartner Cool Vendor award-winner and certified by the international standard of Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). For more information, visit www.votiro.com.

Contact us for a free trial or just to talk:
+1 415 231 3725 | info@votiro.com

VOTIRO
S E C U R E D.
www.votiro.com