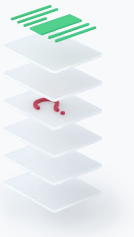
VOTIRO

How Votiro Prevented an Password-Protected Zip File Attack



On March 2nd, 2021, a hacker, having infiltrated the email inbox of a legitimate law firm, sent a malicious password-protected zipped file to a large insurance company.

The insurance company and the law firm had been engaged in back-and-forth communications for some time. Therefore, when the insurance company employee received the email with the password-protected file and instructions to review the legal documents inside, it raised no suspicions.

This style of attack is **vendor email compromise (VEC)**—a method wherein a hacker impersonates a trusted vendor in order to execute an attack. Because of the existing relationship and trust between the vendor and victim, these attacks are highly successful.

In fact, this attack was—at face value—successful:

1. The attack made it through its existing secure email gateway and other email security solutions and protections.

2. The insurance company employee typed in the password for the zip file unlocking the infected files.

3. The employee opened the files inside of the Zip archive upon opening these files; it normally would have released the virus on the corporate machine.

4. In this case, nothing happened.

The attack made it to the victim, but the threat inside—a Valyrian trojan—didn't execute. That's only because the **Votiro Cloud solution had proactively cleansed the file of any threats before it reached the victim**. While the mechanisms of threat delivery worked, the actual threat code had been removed in a foolproof process using Votiro's patented **Positive Selection® technology**.

Details about the Threat: Malware: VB:Trojan.Valyria.3963

The threat that would have executed if Votiro had not been in place is a zero-day Valyrian trojan, name after the indestructible steel from the series Game of Thrones. This malware contains wide-ranging functionality and multiple propaganda methods, with devastating consequences when deployed.

This malware family is also very stealthy: Valyria remains concealed in the victim's system by writing itself to the Windows startup folder, executing automatically on computer startup.

The timeline from this malware's point of creation to delivery to the employee inbox was just 2.5 hours. Traditional security solutions are not capable of detecting and preventing zero-days and unknown threats, as they operate based on signature databases. This is why the attack evaded the insurance company's existing email solutions, along with the fact the malicious code was obfuscated by being password-protected encrypted ZIPPED, which traditional malware scanners deem **UNSCANNABLE**.

It took antivirus software an additional 6 days to identify this attack.

This line of attack was replicated by the hacker several times throughout multiple businesses before the malware was recognized in antivirus databases 6 days later.

How Votiro Prevented the Threat from Executing

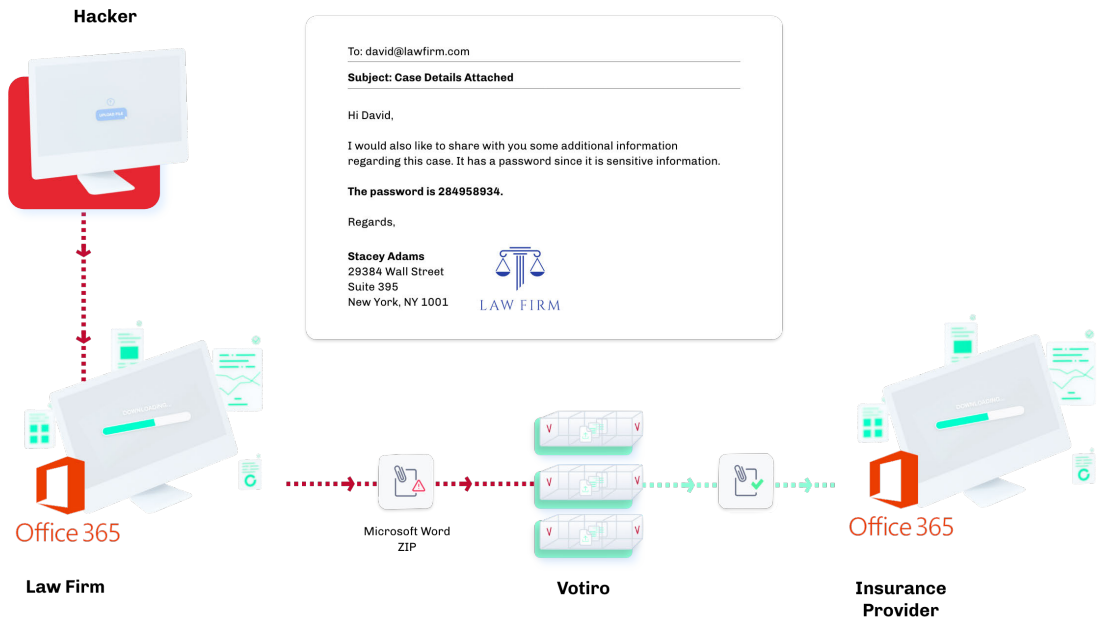
Because the insurance company had Votiro Cloud for Email, when the employee received the malicious password-protected email, they entered the ZIP file's password to Votiro's password-protected file portal. The portal exists in the same email that contained the ZIP file, so it did not interrupt the employee's work or require intervention from the security team.

Votiro's Positive Selection technology is a revolutionary approach to file security. Instead of seeking out and detecting known bad hashes, files, and code—**which would have missed this** zero day attack!

Instead, Votiro identified only the known good elements of the file, allowing those elements through to the end-user, leaving behind the malicious code.

Therefore, the employee received a safe and secure file. (A useless file, as there were no promised legal documents inside, but a safe and secure file none-the-less!)

✔ **Result: VEC phishing attack unsuccessful**



What Would Have Happened Without Votiro Protection

Without Votiro Cloud, the sequence of events would have been much different:

1. The email was sent from a hacked account and recognized, bypassing all reputation and validation checks of the Insurance Company's existing Secure Email Gateway, including:

    A: Headers specifying McAfee and Sophos embedded engines are up-to-date

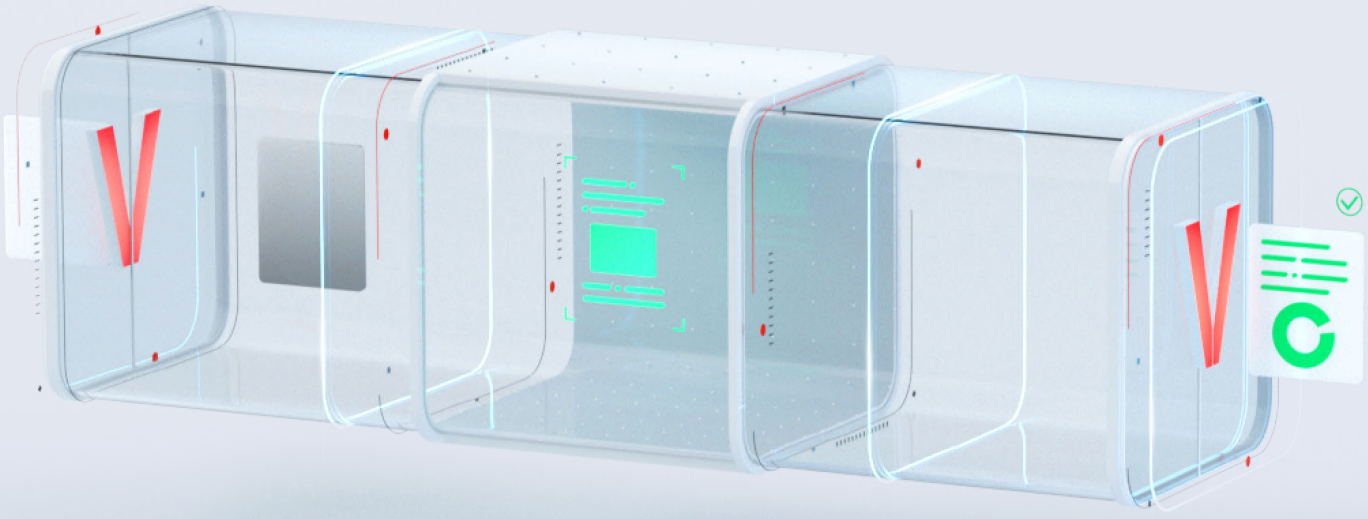
    B: The ZIP file was considered UNSCANNABLE

2. The VB_Trojen.Valyria.3963 malware has penetrated the Secure Email Gateway.

3. The employee receives the familiar email from a trusted known sender; the message included regular content: logo, footer, disclaimer, and ZIP attachment.

4. The employee opens the ZIP file by typing in the provided password, opens the embedded threats, and unwittingly triggers the malware attack, resulting in a successful attack.

✗ **Result: phishing attempt would have been successful without Votiro.**



Experience Votiro Secure For Yourself

Contact Us to Learn More

About
Votiro

Votiro Cloud protects from weaponized files without disrupting business. Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Votiro's revolutionary Positive Selection® technology singles out only the safe elements of each file, ensuring every file that enters your organization is safe.

Founded by leading file security experts, Votiro's new approach to file security works invisibly in the background, completely eliminating threats while ensuring zero interruption to business. Votiro is trusted by large enterprises globally, including top Fortune 500 companies, to completely eliminate file-based threats while ensuring business continuity. Headquartered in the United States, with offices in Australia, Israel and Singapore, Votiro is trusted by hundreds of companies and millions of users worldwide to safely access files with complete peace of mind.

Contact Votiro

info@votiro.com
votiro.com