VOTIRO

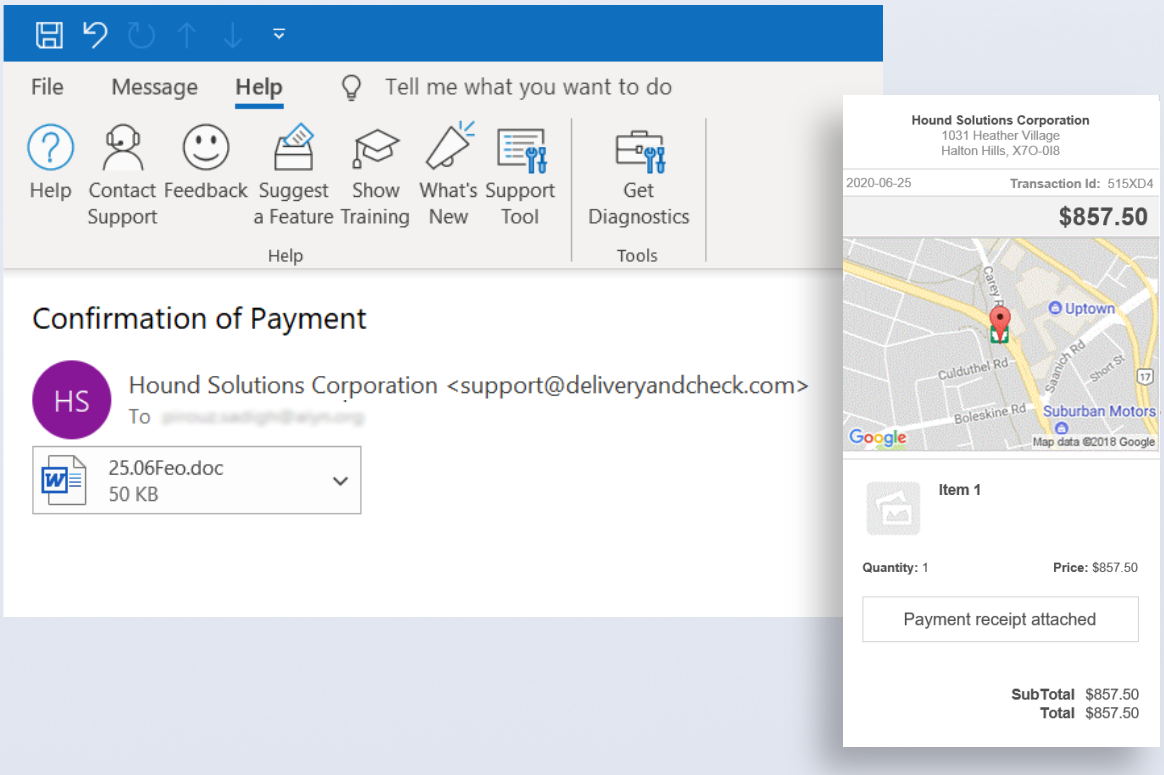
How Votiro Prevented an Attack on ALYN Woldenberg Family Hospital

The Client

ALYN Woldenberg Family Hospital (ALYN Hospital) is a Jerusalem-based rehabilitation center for physically challenged and disabled children, adolescents and young adults. ALYN's holistic approach, incorporating the treatment of physical symptoms, as well as taking into account the emotional and communal needs of the children and their families, has proven itself throughout the eight decades since ALYN was first established.

The Attack

On June 25th, an unsuspecting ALYN employee received an innocent-looking email from Hound Solutions with a Sender address of support@deliveryandcheck.com and with a subject line of "Confirmation of Payment."

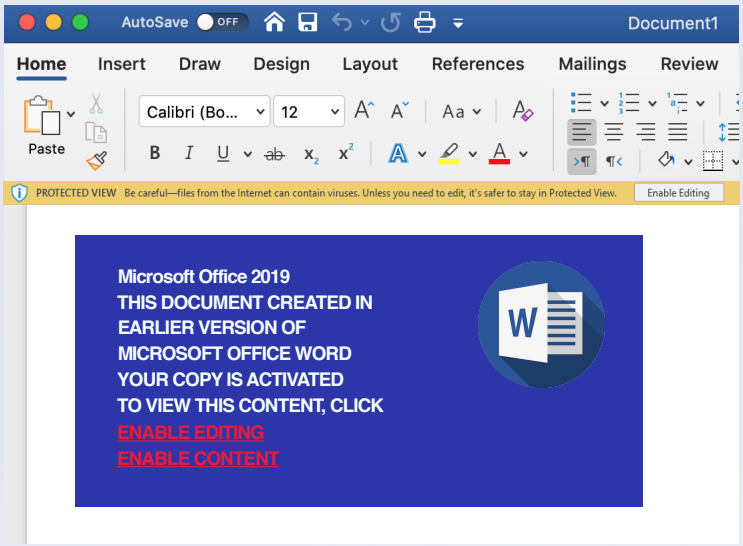


The email included a Word file attachment, which contained the following malicious macro code:

```
Public G, strTemp$, strReturn$, Biola$, CurFolder$, saveFolder
Private Tijd
Private Declare Function ShellExecure Lib "shell32.dll" Alias
"ShellExecuteA" (ByVal hWnd As Long, ByVal lpszOp As String, ByVal
lpszFile As String, ByVal lpszParams As String, ByVal lpszDir As String,
ByVal FsShowCmd As Long) As Long

Private Declare Function GetDesktopWindow Lib "USER32" () As Long
```

When the employee opened the attachment, the following appeared, requesting that the employee enable editing and content within the Word file.



If the attacker's scheme had gone according to plan, as soon as the employee clicked to enable the macro, a malicious file would have been downloaded onto the victim's machine.

The attack in this malware case study example was especially clever as the ShellExecute Win32 API call provides an opening for the attacker to covertly launch an application later on the victim's machine. The code makes use of frequent "while" loops in an attempt to trick the organization's sandbox and evade detection, and uses VBA stomping, a powerful malicious document generation technique that is **effective at bypassing anti-virus detection**.

In addition, the malicious payload is hidden using an ActiveX control button. When the employee closes the document, the code is programmed to run automatically and execute the payload.

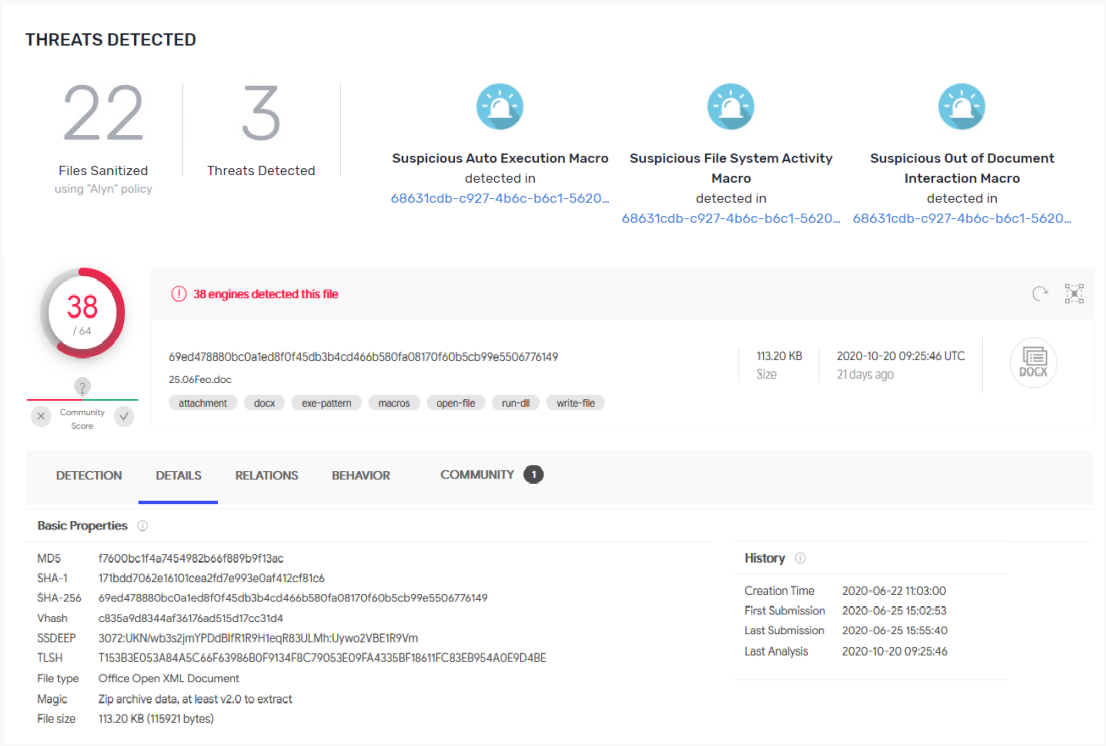
How We Prevented This Attack

Luckily for ALYN and the children they serve, their IT department has partnered with Votiro to ensure their life-saving network is secure from file-borne threats. With Votiro providing our Votiro Cloud solution as a free goodwill service, there was no need to detect the malicious code or for the sandbox to pick up the malware. That's because, with Votiro Cloud, powered by Positive Selection™ technology, complete protection against weaponized files is guaranteed.

Votiro Cloud Prevents What Detection Cannot

Unlike detection-based security solutions that scan for suspicious elements, identify and then block just some malicious files, Votiro's revolutionary Positive Selection technology copies only the safe elements of each file into a new, clean template. This ensures every file that enters the organization is safe, without compromising file functionality or usability.

Without any effort on ALYN's part, in this specific real-world case study example of malware, Votiro automatically neutralized the threat before it could wreak havoc on the hospital and its operations.



When the employee clicked on the file, no negative consequences occurred because Votiro's technology—which automatically neutralizes all file-borne threats—had already removed the macro from the document, sanitizing the file and eliminating the threat. To learn more about how Votiro's innovative approach to file security can keep your organization as safe as ALYN's, click here.

"Because of Votiro, we can safely allow downloads. I think about 70% of the files we wanted to download weren't allowed with our previous vendor. Votiro gave us the greatest flexibility in file downloading throughout our organization." – ALYN

Experience Zero Trust File Security For Yourself

Schedule A Demo

About
Votiro

Votiro protects organizations from weaponized files without slowing 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, regardless of the channel it entered on, 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 over 400 companies and 2 million users worldwide to safely access files with complete peace of mind.

Contact Votiro

info@votiro.com
votiro.com