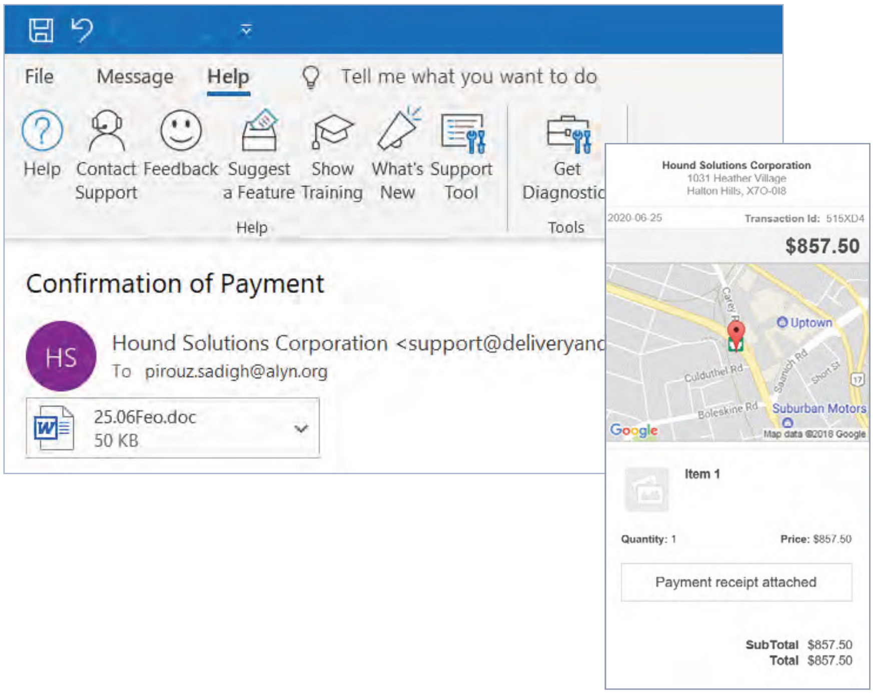
How Menlo Security Prevented an Attack on ALYN Woldenberg Family Hospital

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."



Confirmation of Payment

HS Hound Solutions Corporation <support@deliveryanc
To pirouz.sadigh@alyn.org

25.06Feo.doc
50 KB

Hound Solutions Corporation
1031 Heather Village
Halton Hills, X7O-0I8

2020-06-25 Transaction Id: 515XD4

$857.50

Item 1

Quantity: 1 Price: $857.50

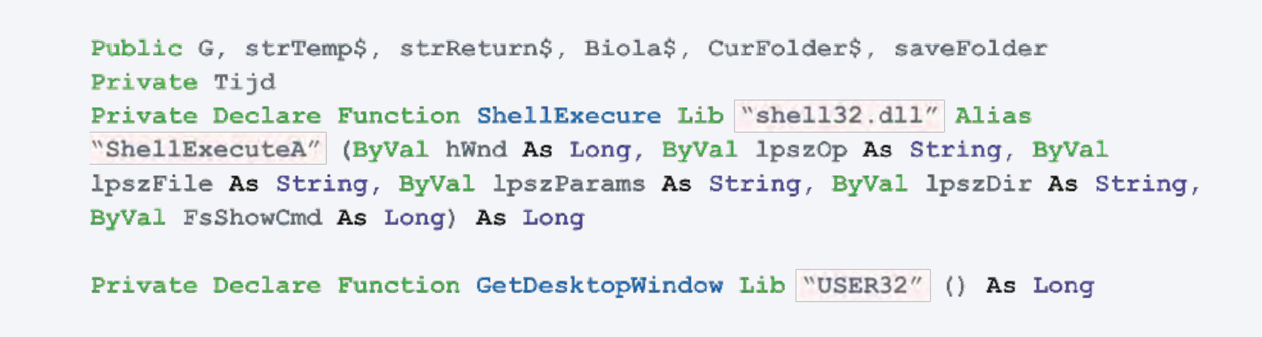
Payment receipt attached

SubTotal $857.50
Total $857.50

ALYN WOLDENBERG FAMILY HOSPITAL

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

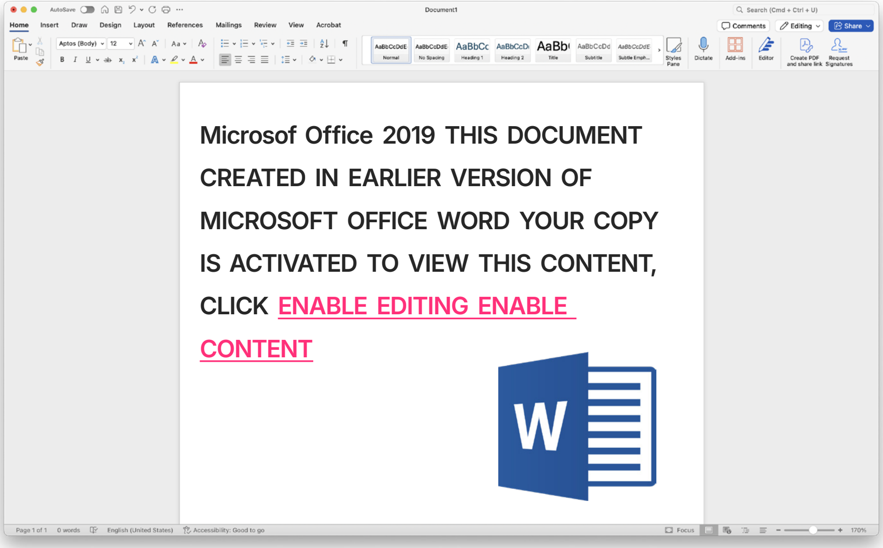


```
Public G, strTemp$, strReturn$, Biola$, CurFolder$, saveFolder
Private Tijd
Private Declare Function ShellExecure Lib "shell32.dll" Alias
"ShellExecuteA" (ByVal hWnd As Long, ByVal lpszOp As String, ByVal
lpszFile As String, ByVal lpszParams As String, ByVal lpszDir As String,
ByVal FsShowCmd As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



Microsof Office 2019 THIS DOCUMENT CREATED IN EARLIER VERSION OF MICROSOFT OFFICE WORD YOUR COPY IS ACTIVATED TO VIEW THIS CONTENT, CLICK ENABLE EDITING ENABLE CONTENT

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 Menlo Security to ensure their life-saving network is secure from file-borne threats. By providing the Menlo 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 Menlo Security, powered by Positive Selection® technology, complete protection against weaponized files is guaranteed.

Menlo Security Prevents What Detection Cannot

Unlike detection-based security solutions that scan for suspicious elements, identify and then block just some malicious files, Menlo 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, Menlo 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 Menlo File Security had already removed the macro from the document, sanitizing the file and eliminating the threat. To learn more about how our innovative approach to file security can keep your organization as safe as ALYN's, click here.

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

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.

MENLO SECURITY

Learn more: https://www.menlosecurity.com

Contact us: ask@menlosecurity.com