New SVCReady malware loads from Word doc properties – Detection & Response

socinvestigation.com/new-svcready-malware-loads-from-word-doc-properties-detection-response/

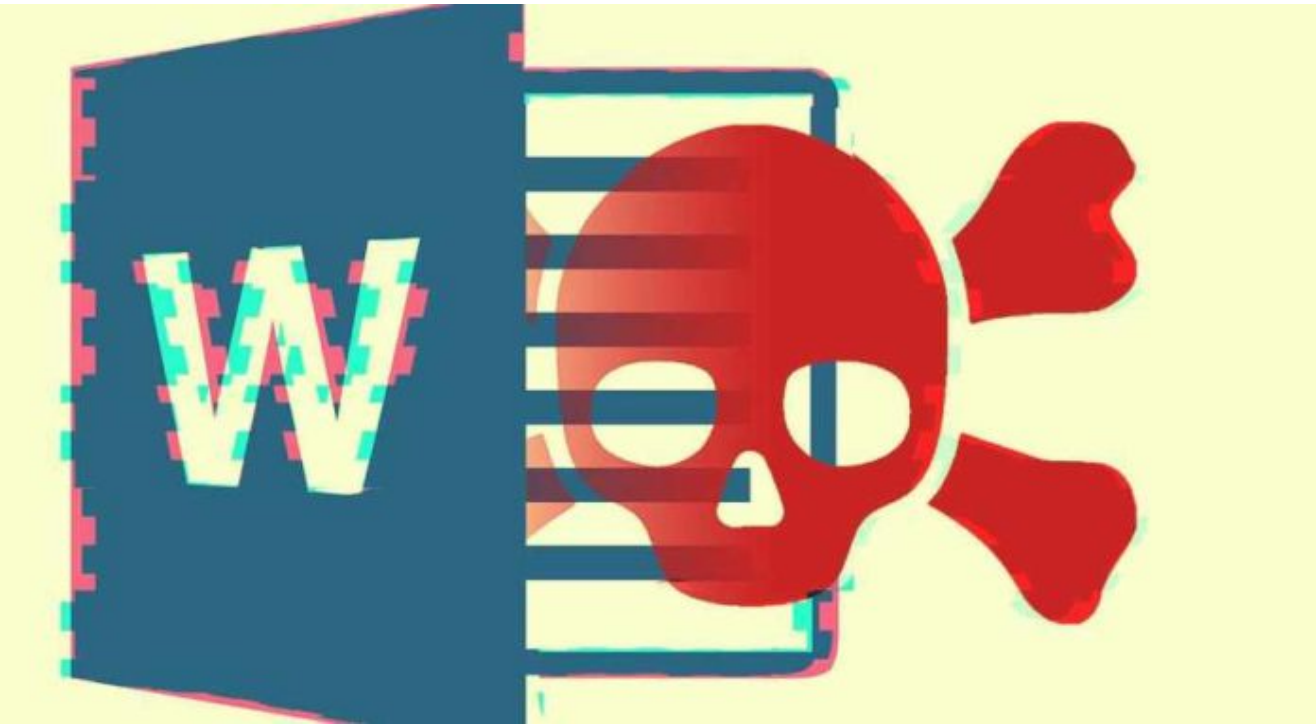
June 10, 2022

IOC

By

Vignesh Bhaaskaran
-

June 10, 2022
0



An unknown malware loader named SVCReady has been discovered in phishing attacks, featuring an unusual way of loading the malware from Word documents onto compromised machines.

More specifically, it uses VBA macro code to execute a shellcode stored in the properties of a document that arrives on the target as an email attachment.

According to a new report by HP, the malware has been under deployment since April 2022, with the developers releasing several updates in May 2022. This indicates that it is currently under heavy development, likely still at an early stage.

However, it already supports information exfiltration, persistence, anti-analysis features, and encrypted C2 communications.

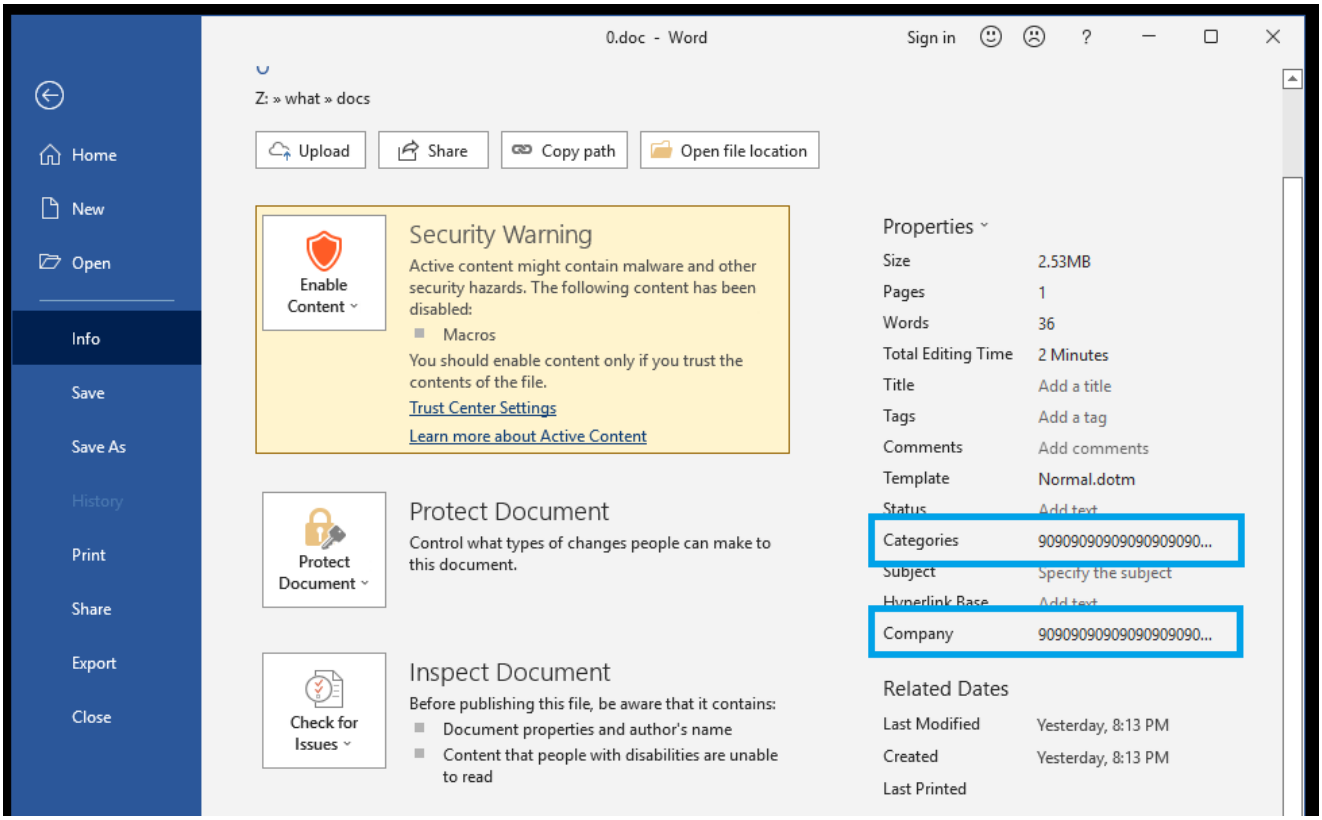
Also Read: Symbiote malware infects all running processes on Linux systems

SVCReady starts with an email

The infection chain begins with a phishing email carrying a malicious .doc attachment. However, contrary to the standard practice of using PowerShell or MSHTA via malicious macros to download payloads from remote locations, this campaign uses VBA to run shellcode hiding in the file properties.

Also Read: Black Basta Ransomware operators leverage QBot for lateral movements

As shown below, this shellcode is stored in the properties of the Word document, which is extracted and executed by the macros.



Shellcode hidden in document properties *(HP)*

By splitting the macros from the malicious shell code, the threat actors attempt to bypass security software that may normally detect it.

“Next the shellcode, which is located in the document properties, is loaded into a variable. Different shellcode is loaded depending on if the architecture of the system is 32 bit or 64 bit,” explains HP’s report.

The appropriate shell code is loaded tino memory from where it will use the Windows API function “Virtual Protect” to acquire executable access rights.

Next, the SetTimer API passes the address of the shellcode and executes it. This action results in a DLL (malware payload) dropping into the %TEMP% directory. A copy of “rundll32.exe”, a legitimate Windows binary, is also placed in the same directory under a different name and is eventually abused to run SVCReady.

Also Read: New ‘DogWalk’ Windows zero-day gets free unofficial patches – Detection & Response

Detection Queries

Microsoft Defender

```
DeviceProcessEvents | where (((InitiatingProcessFolderPath endswith @"\WINWORD.exe") or (FolderPath endswith @"\WINWORD.exe") or (ProcessCommandLine contains "WINWORD.exe")) and (ProcessCommandLine contains @"\AppData\Local\Temp") and (ProcessCommandLine matches regex @'(?i)\\[\w\.]+\.dll|\\[\w\.]+\.exe'))
```

CrowdStrike

```
(((ParentBaseFileName="*\\WINWORD.exe") OR (ImageFileName="*\\WINWORD.exe") OR (CommandHistory="*WINWORD.exe*") OR (CommandLine="*WINWORD.exe*")) AND ((CommandHistory="*\\AppData\\Local\\Temp*") OR (CommandLine="*\\AppData\\Local\\Temp*")) AND (regex field=CommandHistory "['\\\\[\\w\\.]+\\.dll|\\\\[\\w\\.]+\\.exe']" OR regex field=CommandLine "['\\\\[\\w\\.]+\\.dll|\\\\[\\w\\.]+\\.exe']"))
```

Elastic Query

```
((process.parent.executable:*\\WINWORD.exe OR process.executable:*\\WINWORD.exe OR process.command_line:*WINWORD.exe*) AND process.command_line:*\\AppData\\Local\\Temp* AND (process.command_line:/\\[\w\.]+\.dll|\\[\w\.]+\.exe/))
```

CarbonBlack

```
((parent_name:*\\WINWORD.exe OR process_name:*\\WINWORD.exe OR process_cmdline:*WINWORD.exe*) AND process_cmdline:*\\AppData\\Local\\Temp* AND (process_cmdline:/\\[\w\.]+\.dll|\\[\w\.]+\.exe/))
```

Fireeye Helix

```
(metaclass:`windows` (pprocess:`*\WINWORD.exe` OR process:`*\WINWORD.exe` OR args:`WINWORD.exe`) args:`\AppData\Local\Temp` args:/['\\\\[\\w\\.]+\\.dll|\\\\[\\w\\.]+\\.exe']/)
```

Google Chronicle

```
(principal.process.file.full_path = /.*\\WINWORD\.exe/ or target.process.file.full_path = /.*\\WINWORD\.exe/ or target.process.command_line = /.*WINWORD\.exe.*/) and target.process.command_line = /.*\\AppData\\Local\\Temp.*/ and target.process.command_line = /\\[\w\.]+\.dll|\\[\w\.]+\.exe/
```

MS Sentinel

```
SecurityEvent |  where EventID == 4688 | where (((ParentProcessName endswith @'\WINWORD.exe') or (NewProcessName endswith @'\WINWORD.exe') or (CommandLine contains 'WINWORD.exe')) and (CommandLine contains @'\AppData\Local\Temp') and (CommandLine matches regex @'(?i)\\[\w\.]+\.dll' or CommandLine matches regex @'(?i)\\[\w\.]+\.exe'))
```

Splunk

```
(source="WinEventLog:*" AND ((ParentImage="*\\WINWORD.exe") OR (Image="*\\WINWORD.exe") OR (CommandLine="*WINWORD.exe*")) AND (CommandLine="*\\AppData\\Local\\Temp*")  | rex field=CommandLine "\\(?P<payload>[\w\.]+\.dll)|\\(?P<renamed_file>[\w\.]+\.exe)"
```

Indicators of Compromise

501D971E548139153C64037D07B4E3FEA2C1735A37774531C88CFA95BA660EC3
99DF2CC2535C82B84BA23384DF290D7506242532123D8414C1CFC61967072C28
C6C080A63DD038D11CD6E724D2DE31108CABE7B6E38F674FE8189696886582AF
D270E1CA349DAA668E0807BE65ECA75CC739008A39E283F922A8728C22663417
6C9FD23D88239D819E0B494E589B665C4E7921ED9B9DD0BBD1610D71230BCF81
F47514C680135C7D4285F2284D5621245463F55A901C38F171DCE445695AC533
9F7124303F1C957F7E02F275F3501CBAA6E0645A6D78B50617A97761DC611CFF
4C1DD6A893F86A150E003118148C655044D06E8300678CF6BF3CC3107B91B66C
FCB325D21D1100269731553015D6D0F85143DAE2BFA6CBAF49AC6DA29F1F732E
939863285773B17623F0F027FAAE8B994BF5FC1AFB182C63A026431C71CD3885
65A650DD353EA767EF68CF4627436977E6D55102D699B2E8B8DE491DA5C0A5EB
134D0B10BAC1404FA1DA83C96C08E0882500819DAAD5F49E9E83C92F2A624B3E
F2FADD7A8B88DA62228DAB8981638B5C9F5512A57A0441B57C2B3A29B0A96012
0D55564A2BED4FF06BC8B1DAAB98E2032C39536DAA31878E16FED29BC987A4D1

A8EED171FDCB2A872865620FC2234E0B07201D927ABCB65344846F6D4A7B75F5
C24266CC16D65F0B8D72BB7DF80A6B2FFE343429A764AFB9FB0A9C20D53AB9AF
50FBE350CC660361B919F5E464DA6D6170F35EF497327AE5DEFC7805E76D5568
C362D9EEFAFB44D4116B4DFABD5945E974C8A010221705E021490EFBF34BC3A3
68617985E8AB455316C18172723FBD2748DE58008714C4CB3F7C6F19D326F135
65E551F7093299A9A20EAF536197C19ABBDD51B95B9570EDAC4950D7C951AD92
D8AEC5539973927EB07A23BA4DE3780D28C2DD2D6DBBC697562A44B30CD3B03F
CA61DE1E2442C16C280EB7264D6B7F79EC92CDC10D1C202EFB028DA5F242F83A
74652EAE27C9F5A5C397EACC76DAF768B3E601F106E8539C7D855712AB185E40
0224B906741F248D8BCEDAEF423B58FFB1B4577EC06711293F7065B12AE71788
FDABB1F5B7691F03B2D89FEB8B0D4E3FD036F9B4E718269CAD8741C7E4D14072
FD799D99F7E84436F8AF16D94EE7B2F1D08CA3CEE746E1CF9B36E2139D676E4C
4A2E76B57DE10C687716A1D7A295910CC5C0D04F5D10D4F4C53AE1BDE45A251C
9122092980BC0ED9C9B008C5456CC18656C41798585B8819F1D6F2620CAC3CF3
391D134B792FB660426F183755AD00DBD737F521CFF1F9A12D402CD714D34645
B67120F25963D36560CBB86B35E864F608536ABEF7C3377F46997D65BAD13CAA
5170461322CB1A79ABB84FEED75B7F871B6F1594562E7724C45D7BB98F97C86B
4B8627B5896A0656E801A95B16068F84660F1460A247E712651E0945EB4309CB
95E328A549247F900DA5747F7E2057DEF121D2EDA82CFD7E926A6955C797D317
AFA40C3157F2704ABA4838A7308B53A4853176AF86982CE2999AA4DF3AC7BB9C
00FD57B32A3DF737C274D2184663DE4EDC22A4E003419C1B10B262E66995EE23
5B7FBEC223DEB714DC7A4037348936A27D86B061CB2120213D5A69849CC9B588
FA6F5695AC2530B486FDD6FE8096AAAF65081BC092AB874545628C61E1403919
C86A477579188305132DAB40700D06FFF9E26B5CE627233FB9D20DA1DFC74B47
748352146AB86EA1A32DFED0B0D5FAC0EFC52728BCCD79476B74FB73517EFB21

DLLs

08e427c92010a8a282c894cf5a77a874e09c08e283a66f1905c131871cc4d273
16851d915aaddf29fa2069b79d50fe3a81ecaafd28cde5b77cb531fe5a4e6742
1d3217d7818e05db29f7c4437d41ea20f75978f67bc2b4419225542b190432fb
235720bec0797367013cbdc1fe9bbdde1c5d325235920a1a3e9499485fb72dba
39c955c9e906075c11948edd79ffc6d6fcc5b5e3ac336231f52c3b03e718371e
5e932751c4dea799d69e1b4f02291dc6b06200dd4562b7ae1b6ac96693165cea
d3e69a33913507c80742a2d7a59c889efe7aa8f52beef8d172764e049e03ead5
f690f484c1883571a8bbf19313025a1264d3e10f570380f7aca3cc92135e1d2e

Domains

muelgadr[.]top
wikidreamers[.]com
galmerts[.]art
marualosa[.]top
kikipi[.]art
kokoroklo[.]su

Source: https://www.bleepingcomputer.com/news/security/new-svcready-malware-loads-from-word-doc-properties/

> SVCReady: A New Loader Gets Ready

LEAVE A REPLY

Please enter your comment!

Please enter your name here

You have entered an incorrect email address!

Please enter your email address here