Let’s Learn: Introducing Latest TrickBot Point-of-Sale Finder Module

vkremez.com/2018/11/lets-learn-introducing-latest-trickbot.html

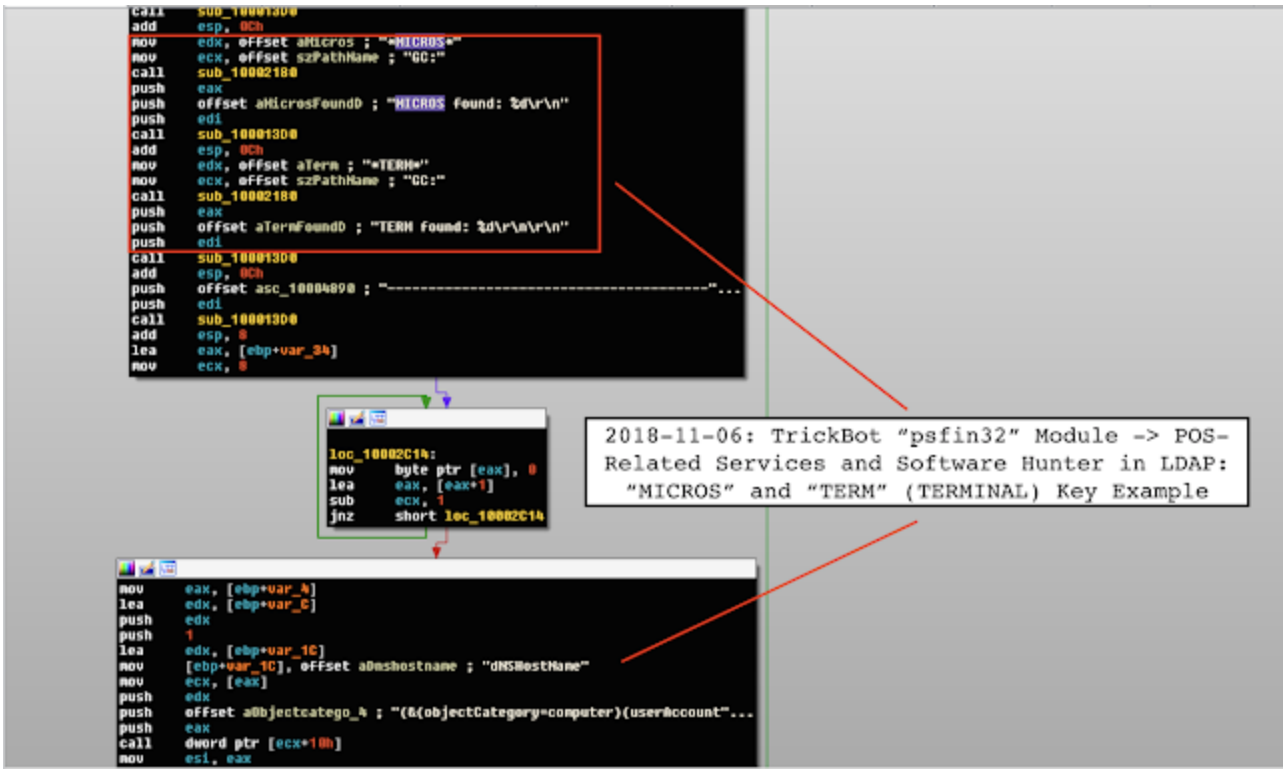
Goal: Analyze the latest TrickBot point-of-sale finder“psfin32” reconnaissance module hunting for point of sale related services, software, and machines in Lightweight Directory Access Protocol (LDAP)
Source:
Unpacked TrickBot psfin32 Module 32-Bit (x86) (MD5: 4fce2da754c9a1ac06ad11a46d215d23)
Outline

```
I. Background
II. Decoded TrickBot Point-of-Sale Finder “psfin32” Module 32-Bit (x86)
III. TrickBot Point-of-Sale Finder Module vs DomainGrabber Module: Code Analysis
IV.  TrickBot Point-of-Sale Finder Module LDAP Analysis
V.  TrickBot Point-of-Sale Finder Module POST Command
IV. Yara Signature
```

I. Background

This is not the first time the TrickBot development group leverages LDAP; they also developed a DomainGrabber module specifically to harvest sensitive domain controller information, as detailed earlier. The group behind the TrickBot malware development remains to be one of the most resourceful in the e-crime ecosystem continuously releasing various modules (for example. password grabber “pwgrab32Dll” on October 19, 2018). The module itself does not steal any point-of-sale data but rather used to profile corporate machines of interest with possible point-of-sale devices. This module arrives just in time for the holiday shopping season highlighting the group interest in exploring possible point-of-sale breaches. The question is: What point-of-sale malware would the group behind TrickBot deploy on identified machines of interest, and/or would they auction this access to another group? This question is yet to be answered.

II. Decoded TrickBot Point-of-Sale Finder “psfin32” Module 32-Bit (x86)

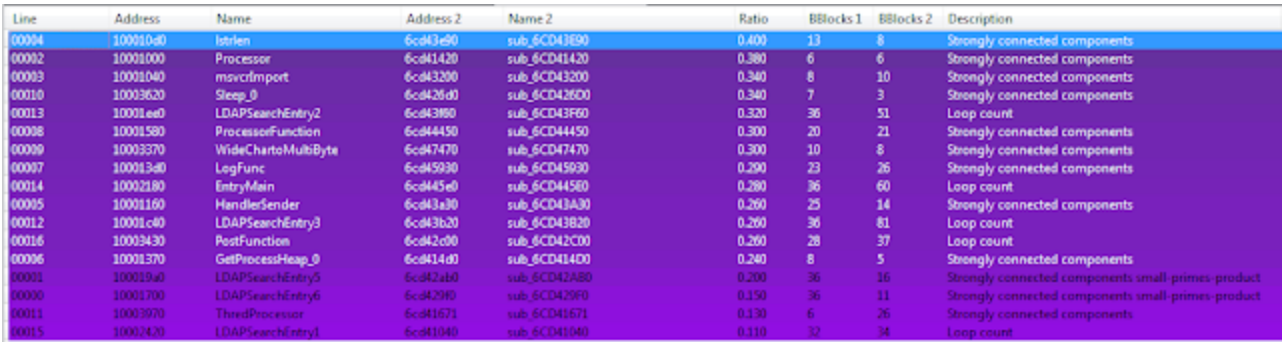


This tiny "psfin32" module DLL with the size of 18.13 KB (18568 bytes), compiled on Monday, November 5, 09:00:47 2018 UTC, is originally called "dll[.]dll." The module itself consists of only 24 functions.

The decoded Trickbot "pfin32Dll" module contains the usual Trickbot export functions:

```
Control
FreeBuffer
Release
Start
```

III. TrickBot Point-of-Sale Finder Module vs DomainGrabber Module: Code Analysis



Line	Address	Name	Address 2	Name 2	Ratio	BBlocks 1	BBlocks 2	Description
00004	100010d0	lstrlen	6cd43e90	sub_6CD43E90	0.400	13	8	Strongly connected components
00002	10001000	Processor	6cd41420	sub_6CD41420	0.380	6	6	Strongly connected components
00003	10001040	msvcrImport	6cd43200	sub_6CD43200	0.340	8	10	Strongly connected components
00010	10003620	Sleep_0	6cd426d0	sub_6CD426D0	0.340	7	3	Strongly connected components
00013	10001ea0	LDAPSearchEntry2	6cd43f80	sub_6CD43F60	0.320	36	51	Loop count
00008	10001580	ProcessorFunction	6cd44450	sub_6CD44450	0.300	20	21	Strongly connected components
00009	10003370	WideCharToMultiByte	6cd47470	sub_6CD47470	0.300	10	8	Strongly connected components
00007	100013d0	LogFunc	6cd45930	sub_6CD45930	0.290	23	26	Strongly connected components
00014	10002180	EntryMain	6cd445e0	sub_6CD445E0	0.280	36	60	Loop count
00005	10001160	HandlerSender	6cd43a30	sub_6CD43A30	0.260	25	14	Strongly connected components
00012	10001c40	LDAPSearchEntry3	6cd43b20	sub_6CD43B20	0.260	36	81	Loop count
00016	10003430	PostFunction	6cd42c00	sub_6CD42C00	0.260	28	37	Loop count
00006	10001370	GetProcessHeap_0	6cd414d0	sub_6CD414D0	0.240	8	5	Strongly connected components
00001	100019a0	LDAPSearchEntry5	6cd42ab0	sub_6CD42A80	0.200	36	16	Strongly connected components small-primes-product
00000	10001700	LDAPSearchEntry6	6cd42f40	sub_6CD42F00	0.150	36	11	Strongly connected components small-primes-product
00011	10003970	ThredProcessor	6cd41671	sub_6CD41671	0.130	6	26	Strongly connected components
00015	10002420	LDAPSearchEntry1	6cd41040	sub_6CD41040	0.110	32	34	Loop count

The latest module consists visually a lot of similarity to their previous DomainGrabber module. During pseudo source-code level analysis, it is revealed that the code contains 6 partial function matches (including perfect match and strongly connected components), 17 unreliable function matches (including same MD index and constants, strongly connected components, similar small pseudo-code, strongly connected components small-primes-product, and loop count). By and large, the pseudo source-code analysis reveals the new module heavily borrows from the earlier DomainGrabber code and was likely coded by the same developer(s).

IV. TrickBot Point-of-Sale Finder Module LDAP Analysis

This Trickbot module was programmed leveraging Active Directory Service Interfaces (ADSI) APIs to search LDAP for objects possibly linked to point of sale related services, software, and machines. To learn more about specific access **ADsOpenObject and IADsContainer** interface, please refer to the DomainGrabber post.

LDAP provider is used to access Active Directory Domain Services. The LDAP binding string takes the following form of "GC://" binding to the root of the namespace. "GC:" uses the LDAP provider to bind to the Global Catalog service to execute queries.

The module queries for DOMAIN Global Catalog the following accesses:

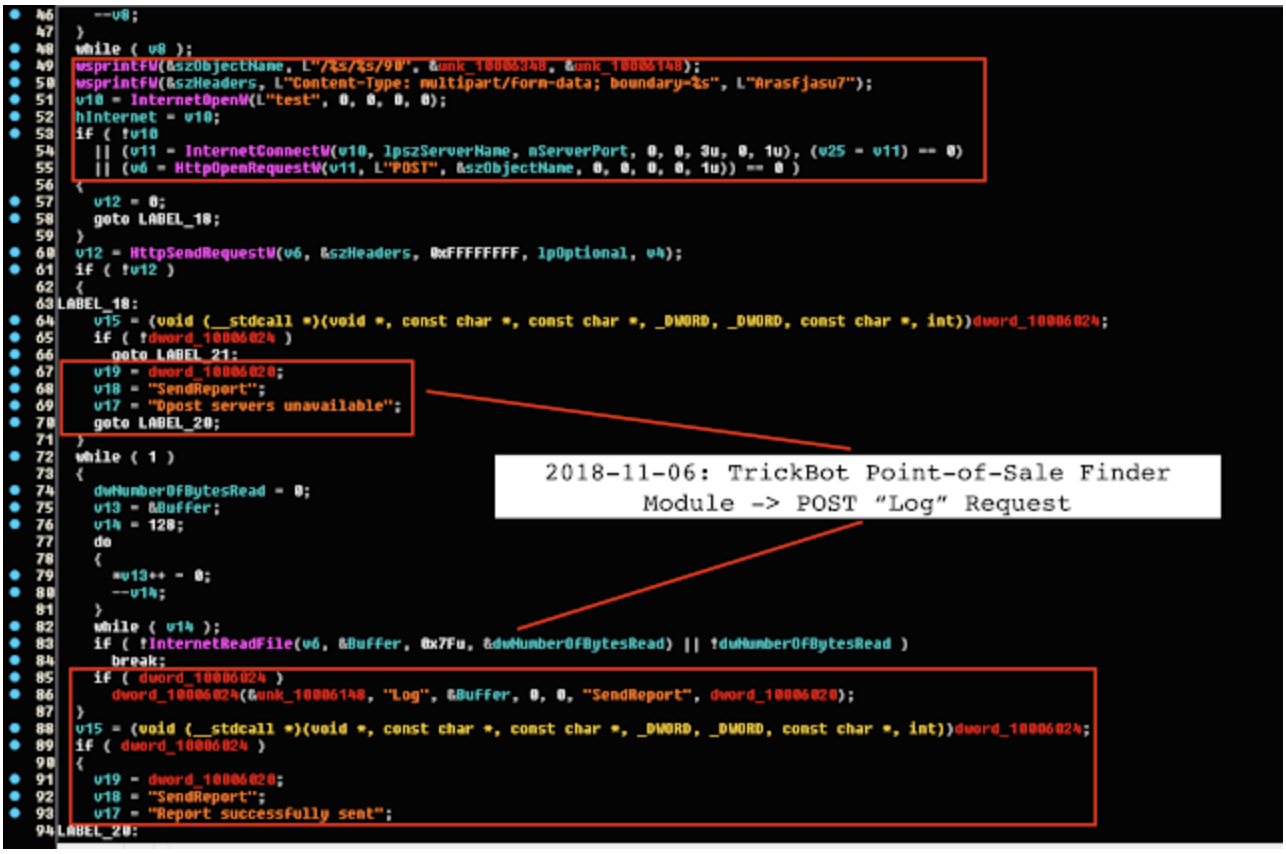
```
COMPUTERS
USERS
GROUPS
SITES
OUs
```

The point-of-sale key terms of interest are as follows:

```
*POS*
*REG*
*CASH*
*LANE*
*STORE*
*RETAIL*
*BOH*
*ALOHA*
*MICROS*
*TERM*
```

V. TrickBot Point-of-Sale Finder Module POST Command

Once the information is harvested, the "Log" file with the information would be posted to the TrickBot to "Dpost" servers via "/%s/%s/90" command.



Part of the export "Control" function, the module forms and communicates to the next-layer network via the module network path ending in .../<GROUP ID>/<CLIENT ID>/90. The /90 ending is leveraged for POST requests with its content in the following three unique formats:

```
A. Content-Disposition: form-data; name="proclist"
B. Content-Disposition: form-data; name="sysinfo"
C. Content-Type: multipart/form-data; boundary=Arasfjasu7
```

The unique value "Arasfjasu7" appears to be a marker/separator for the LDAP query collection upload to split the harvested information.

IV. Yara Signature

```
import "pe"

rule crime_win32_trickbot_psfin32_dll {
   meta:
      author = "@VK_Intel"
      reference = "Detects TrickBot Point-of-Sale Finder Module"
      date = "2018-11-07"
      hash1 = "f82d0b87a38792e4572b15fab574c7bf95491bf7c073124530f05cc704c1ee96"
   strings:
      $s0 = "(&(objectCategory=computer)
(userAccountControl:1.2.840.113556.1.4.803:=8192))" fullword wide
      $s1 = "Dpost servers unavailable" fullword ascii
      $s2 = "USERS:" fullword wide
      $s3 = "*POS*" fullword wide
      $s4 = "/%s/%s/90" fullword wide
      $s5 = "DOMAIN GC" fullword wide
      $s6 = "*MICROS*" fullword wide
      $s7 = "(&(objectCategory=person)(sAMAccountName=%s))" fullword wide

 $ldap_gc_pos_queryportion = { 85 f6 0f ?? ?? ?? ?? ?? 8b ?? ?? 8d ?? ?? ?? ?? ?? 6a
04 c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ??
?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ??
?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ??
?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7
?? ?? ?? ?? ?? ?? ?? ?? ?? 8b ?? 52 50 ff ?? ?? 85 c0 0f ?? ?? ?? ?? ?? 68 84 45 00
10 57 e8 ?? ?? ?? ?? 68 a0 45 00 10 57 e8 ?? ?? ?? ?? 68 24 46 00 10 57 e8 ?? ?? ??
?? ba 40 46 00 10 b9 e0 44 00 10 e8 ?? ?? ?? ?? 50 68 4c 46 00 10 57 e8 ?? ?? ?? ??}

   condition:
      ( uint16(0) == 0x5a4d and
         filesize < 50KB and
         pe.imphash() == "13c48c2a1eaa564e28ee00ed7cd0fc0f" and pe.exports("Control")
and pe.exports("Release") and
         ( all of them )
      ) or ( $ldap_gc_pos_queryportion and 5 of ($s*) )
}
```