(0x64 ∧ 0x6d) ∨ 0x69

- home
- 🕮 Embedded Systems Security and TrustZone (ebook)
- contact

Categories

- Advanced Networking
- Management
- Progressive Windowzing
- Reverse Engineering
- Threat Hunting
- Vulnerability Disussions

mimilib DHCP Server Callout DLL injection

With the latest commit to mimikatz the never resting Benjamin Delpy not only added the feature to load mimilib as DNS serverlevel plugin into the Windows DNS Server (see here for details) but also integrated a similar API for the Windows DHCP server. (he already blogged about that in 2012!)

I did not find any management tool to leverage this injection technique using the management RPC interface (MS-DHCPM), but I also did not spend too much time on finding one... contact me, in case you know a tool ;)

To install the DLL you just have to drop the DLL on the target system and set the following two values in the registry (everything is nicely documented here). Sadly cifs shares are not working, in my tests i could only load local files. DLLs specified on a CIFS share failed with EventID 1034 (see below)

In

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Parameters
```

set

key name	datatype	description
CalloutDlls	REG_MULTI_SZ	String that contains the local path to the DHCP Callout DLL. For example: "C:\Program Files\MyCalloutServer\my_dhcp.dll"
CalloutEnabled	DWORD	32-bit unsigned integer value that specifies 0 if the DHCP Callout server is not enabled, and 1 if it is.

The mimilib DHCP Callout plugin in the current sources of mimikatz drops all DHCP requests from VMWare MAC adresses (see here), be aware! ;)

```
$ dimi@hermes: sudo dhcpcd ens33
[...]
ens33: soliciting a DHCP lease
```

```
[...]
timed out
dhcpcd exited

$ dimi@hermes: sudo ip link set dev ens33 down && sudo macchanger --random ens33
Current MAC:   00:0c:29:1c:33:39 (VMware, Inc.)
Permanent MAC: 00:0c:29:1c:33:39 (VMware, Inc.)
New MAC:       7a:ca:20:01:96:9c (unknown)

$ dimi@hermes: sudo dhcpcd ens33
ens33: waiting for carrier
ens33: carrier acquired
[...]
ens33: soliciting a DHCP lease
ens33: offered 192.168.0.204 from 192.168.0.2
ens33: probing address 192.168.0.204/24
ens33: leased 192.168.0.204 for 691200 seconds
ens33: adding route to 192.168.0.0/24
ens33: adding default route via 192.168.0.254
forked to background, child pid 25808
```

Hunting

DLL ImageLoaded

To check whether the DHCP service additionally loads DLLs, when a Callout DLL is specified I made a intersection of the loaded DLLs in both cases.(I used ELK with Sysmon, what a great combination!) You can download the raw data here. Sadly there is no additionaly (except the specified plugin DLL) loaded DLL, so nothing to monitor here.

Windows Events triggered

I could observe the following Windows Events during my analysis in the **Microsoft-Windows-DHCP-Server** log:

- If the Callout DLL is loaded successfully we see **EventID 1033** (see attachment #1 below)
- If the Callout DLL is not loaded successfully we see **EventID 1034** (see attachment #2 below)
- There are two more Events associated with the loading or failed loading of a CalloutDll. In my tests I could not trigger them: **1031**, **1032**

Registry

Since an attacker has to modify the registry to activate the Callout DLL, we can monitor for changes in the registry with Sysmon:

Source	EventID	Fields	Details
Sysmon	13	TargetObject	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\DHCPServer\Parameters\CalloutDlls
Sysmon	13	TargetObject	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\DHCPServer\Parameters\CalloutEnabled

See attachment #3 and #4 for the full Syslog Event XML data.

attachment #1

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="Microsoft-Windows-DHCP-Server" Guid="{6D64F02C-A125-4DAC-9A01-F0555B41CA84}" EventSourceName="DhcpServer" />
<EventID Qualifiers="0">1033</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
```

```
    <Keywords>0x80000000000000</Keywords>
    <TimeCreated SystemTime="2017-05-10T16:46:59.000000000Z" />
    EventRecordID>6653</EventRecordID>
    <Correlation />
    <Execution ProcessID="0" ThreadID="0" />
    <Channel>System</Channel>
    <Computer>dc1.lab.internal</Computer>
    <Security />
    </System>
    <EventData>
    <Data>Der Vorgang wurde erfolgreich beendet.</Data>
    <Binary>00000000</Binary>
    </EventData>
    </Event>
```

attachment #2

```
    <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    <System>
    <Provider Name="Microsoft-Windows-DHCP-Server"
    Guid="{6D64F02C-A125-4DAC-9A01-F0555B41CA84}" EventSourceName="DhcpServer" />
    <EventID Qualifiers="0">1034</EventID>
    <Version>0</Version>
    <Level>3</Level>
    <Task>0</Task>
    <Opcode>0</Opcode>
    <Keywords>0x80000000000000</Keywords>
    <TimeCreated SystemTime="2017-05-10T17:30:35.000000000Z" />
    <EventRecordID>6659</EventRecordID>
    <Correlation />
    <Execution ProcessID="0" ThreadID="0" />
    <Channel>System</Channel>
    <Computer>dc1.lab.internal</Computer>
    <Security />
    </System>
    - <EventData>
    <Data>%1 ist keine zulässige Win32-Anwendung.</Data>
```

attachment #3

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFBD9}" />
<EventID>13</EventID>
<Version>2</Version>
<Level>4</Level>
<Task>13</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<TimeCreated SystemTime="2017-05-11T11:12:46.430391500Z" />
<EventRecordID>16483</EventRecordID>
<Correlation />
<Execution ProcessID="1264" ThreadID="2980" />
<Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>dc1.lab.internal</Computer>
<Security UserID="S-1-5-18" />
</System>
- <EventData>
<Data Name="EventType">SetValue</Data>
<Data Name="UtcTime">2017-05-11 11:12:46.429</Data>
<Data Name="ProcessGuid">{85D1CFA0-8027-5911-0000-0010B5836E00}</Data>
<Data Name="ProcessId">3804</Data>
<Data Name="Image">C:\Windows\regedit.exe</Data>
<Data Name="TargetObject">\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\DHCPServer\Parameters\CalloutDlls</Data>
<Data Name="Details">Binary Data</Data>
```

```
</EventData>
</Event>
```

attachment #4

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFBD9}" />
<EventID>13</EventID>
<Version>2</Version>
<Level>4</Level>
<Task>13</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<TimeCreated SystemTime="2017-05-11T11:12:40.404721300Z" />
<EventRecordID>16482</EventRecordID>
<Correlation />
<Execution ProcessID="1264" ThreadID="2980" />
<Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>dc1.lab.internal</Computer>
<Security UserID="S-1-5-18" />
</System>
- <EventData>
<Data Name="EventType">SetValue</Data>
<Data Name="UtcTime">2017-05-11 11:12:40.403</Data>
<Data Name="ProcessGuid">{85D1CFA0-8027-5911-0000-0010B5836E00}</Data>
<Data Name="ProcessId">3804</Data>
<Data Name="Image">C:\Windows\regedit.exe</Data>
<Data Name="TargetObject">\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\DHCPServer\Parameters\CalloutEnabled</Data>
<Data Name="Details">DWORD (0x00000001)</Data>
</EventData>
</Event>
```

By @dimi in [Threat Hunting] Thu 11 May 2017
Tags : #Threat Hunting, #sysmon, #DNS, #Windows, #Microsoft, #DHCP, #mimilib, #mimikatz,