Subject: [ICC-L] DHCP Log searches
Date: Tuesday, January 27, 2015 at 1:04:04 PM Eastern Standard Time
From: Hyde,Wayne J (sent by IFAS Computer Coordinators List <ICC-L@LISTS.IFAS.UFL.EDU>)
To: . IFAS-ICC-L

There are two ways for OU admins to search the IFAS DHCP logs to associate a UFIRT incident with a computer name – or to simply search the logs to find one of your hosts. Both of these methods use the same log file sources and will work depending on your skill set and I will try to explain both in detail below. (The solution to the limitation Dennis brought up is at the bottom.) The two methods (both require your ADMN credentials) are:

- Scan the DHCP logs directly via our DFS share using **find** or **findstr**
- Use Chris' DHCPSearch webapp

The log location we use to archive DHCP logs is:

\\AD.UFL.EDU\IFAS\LOGS\DHCP\YYYY\MM\

The on-campus DHCP logs are named:

YYYY-MM-DD_IFAS-DHCP-SITE.LOG

WAN site logs are saved in the following filename format:

YYYY-MM-DD_IFAS-SITENAME-SITE.log

The first method of associating MAC/IP/HOSTNAME information with DHCP log entries involves using either **find** or **findstr** from a command line using your ADMN credentials. To see what the various options are for the utilities, run them with a "/?" as the parameter to see the help information.

The following 3 commands will search today's on-campus DHCP log for an IP address, computer name and finally MAC address:

```
C:\>findstr "10.242.34.80" \\AD.UFL.EDU\IFAS\LOGS\DHCP\2015\01\2015-01-27_ifas-
dhcp-Site.log
30,01/27/15,09:43:15,DNS Update Request,10.242.34.80,IF-ITSA-
C74B5V1.ad.ufl.edu,,,0,6,,,
11,01/27/15,09:43:15,Renew,10.242.34.80,IF-ITSA-
C74B5V1.ad.ufl.edu,5CF9DD7775AE,,2110426391,0,,,
32,01/27/15,09:43:27,DNS Update Successful,10.242.34.80,IF-ITSA-
C74B5V1.ad.ufl.edu,,,0,6,,,

C:\>findstr /i "IF-ITSA-C74B5V1" \\AD.UFL.EDU\IFAS\LOGS\DHCP\2015\01\2015-01-
27_ifas-dhcp-Site.log
30,01/27/15,09:43:15,DNS Update Request,10.242.34.80,IF-ITSA-
C74B5V1.ad.ufl.edu,,,0,6,,,
11,01/27/15,09:43:15,Renew,10.242.34.80,IF-ITSA-
C74B5V1.ad.ufl.edu,5CF9DD7775AE,,2110426391,0,,,
32,01/27/15,09:43:27,DNS Update Successful,10.242.34.80,IF-ITSA-
C74B5V1.ad.ufl.edu,,,0,6,,,

C:\>findstr /i "5CF9DD7775AE" \\AD.UFL.EDU\IFAS\LOGS\DHCP\2015\01\2015-01-
27_ifas-dhcp-Site.log
```

```
11,01/27/15,09:43:15,Renew,10.242.34.80,IF-ITSA-
C74B5V1.ad.ufl.edu,5CF9DD7775AE,,2110426391,0,,,
```

You can use the output of one command to expand your search. For example, if you only had the IP address information you could search for the IP address to get the hostname and then search the logs again based on the hostname to find additional entries in case the computer changed IP addresses.

To use **find**, substitute find for findstr with the same syntax. When searching multiple files using a wildcard in the filename to search, some people may like the output of **find** easier to read. Try the following two commands to see the difference:

```
find /i "5CF9DD7775AE" \\AD.UFL.EDU\IFAS\LOGS\DHCP\2015\01\2015-01-2?_ifas-
dhcp-Site.log
findstr /i "5CF9DD7775AE" \\AD.UFL.EDU\IFAS\LOGS\DHCP\2015\01\2015-01-2?_ifas-
dhcp-Site.log
```

The two commands search 2015 January 20-27 logs (if they exist; obviously the 28th and 29th logs don't because I don't drive a Delorean) for the MAC address as shown.

Be warned, **findstr** is capable of using more powerful regular expression syntax and is easier to get incorrect or unexpected return values if you don't know what you are doing.

Also, please be sure to check incident timestamps with the DHCP timestamps. If you use the "Create-date" of the UFIRT ticket may find the wrong machine using DHCP logs as tickets can be created hours or days after the actual incident.

To use Chris' DHCPSearch webapp, simply browse to the following URL and login with your ADMN credentials:

http://itsa.ifas.ufl.edu/dhcpsearch/

Use the application the same as you have in the past -- enter in the date to search in the first box, which site in the second, and the search criteria in the third. If you want to find out the manufacturer for a NIC, enter the MAC address, check the "Display NIC Manufacturer" option and then click "MAC Mask". This can help you determine if the computer is a Dell, Apple, etc.

Here is how ITSA will address the limitation brought up by Dennis yesterday. We currently have a scheduled task on each of our DHCP servers to archive the previous day's logs to our DFS share. This script will be modified to also archive the current in-use log multiple times a day. On-campus will be first as bandwidth won't be a factor. We will need to examine the size of logs and site bandwidth before modifying the WAN site job to get a good balance of frequency vs log size.

--
Wayne J. Hyde, RHCE
Information Security Manager
University of Florida, IFAS
(352) 846-2565

From: IFAS Computer Coordinators List [mailto:ICC-L@LISTS.IFAS.UFL.EDU] **On Behalf Of** Hyde,Wayne J
Sent: Monday, January 26, 2015 5:35 PM
To: . IFAS-ICC-L
Subject: Re: [ICC-L] UFIRT alerts for "Upatre" -- infected hosts from today's email malware

Good point and we'll get a solution for that problem.

-Wayne

From: Brown, Dennis G
Sent: Monday, January 26, 2015 5:09 PM
To: Hyde,Wayne J; . IFAS-ICC-L
Subject: RE: [ICC-L] UFIRT alerts for "Upatre" -- infected hosts from today's email malware

This brings up this problem. We can't use the DHCP Search until the next day. We can look at DHCP but there is no guarantee that the computer that had the ip number in question at 10am this morning is the same one that has it now at 5pm. Is there another way to confirm same day which computer is the one in the IRT report?

Thanks.

Dennis

From: IFAS Computer Coordinators List [mailto:ICC-L@LISTS.IFAS.UFL.EDU] **On Behalf Of** Hyde,Wayne J
Sent: Monday, January 26, 2015 4:50 PM
To: . IFAS-ICC-L
Subject: [ICC-L] UFIRT alerts for "Upatre" -- infected hosts from today's email malware

FYI,

It appears that today's malware is designated as "Upatre Infection" in UFIRT alerts.

--
Wayne J. Hyde, RHCE
Information Security Manager
University of Florida, IFAS
(352) 846-2565