Finding malicious activity and malware in the network.

Thursday, January 22, 2015

User-agent Strings

A user-agent string is a value used by an application that identifies itself to the server. There are many sites that go into this a bit deeper, so I won't harp on it here. The purpose here is to identify malware that uses unique user-agent string values, which makes it terribly easy to find malicious traffic being generated by certain malware.

The best place to find these values are proxy logs, so you will need to know the field name that your proxy server uses to identify the user-agent string: I believe the field in BlueCoat proxy logs is *cs(User-Agent)* but yours may be different. Below is a list of user-agent strings that I have seen in our logs and have confirmed that they have been used by malware; there are many other out there, but I will not include those. I have also included a line that you can use to dig through old logs in order to locate past infections.

Malware: Houdini / Iniduoh / njRAT
This one should pop right out in your logs. It uses the below characters as a field separator, so there will be several of these in the user-agent field.

- User-agent contains: <|>
- Regex: <\|>
- Regex: ((\w+)|(\W+))((<\|>)|(\\))((\w+)|(\W+))((<\|>)|(\\))((\w+)|(\W+))((<\|>)|(\\))[^<|\\]+((<\|>)|(\\))((\w+)|(\W+))[^<|\\]+((<\|>)|(\\))[^<|\\]+((\w+)|(\W+))((\w+)|(\W+))+
  - I did not write the above regex for this one and I cannot remember where I found it, so I am unable to give credit. If it's yours then please let me know.

Malware: Zero Access

- User-agent: nsis_inetc (mozilla)
- Regex: nsis_inetc\s\(mozilla\)

Malware: Generic Trojan

- User-agent: Mozilla/5.0 WinInet
- Regex: Mozilla\/5\.0\sWinInet

Malware: Dyre / Upatre
The following string was found on a Windows machine.

- User-agent: Wget/1.9+cvs-stable (Red Hat modified)
- Regex: Wget\/1\.9\+cvs-stable\s\(Red\sHat\smodified\)

Malware: Generic password stealing Trojan

- User-agent: RookIE/1.0
- Regex: RookIE\/1\.0

The following two user-agent strings will require the use of Log Parser. Attempting to do a regex search with these will return a large amount of results.

Malware: Tupym
Although AutoIt is legitemate, finding this user-agent may be malicious. Make sure you investigate this a bit further if you find it in your log files.

- User-agent: AutoIt
- SQL: SELECT [user-agent column name] FROM [file path] WHERE [user-agent column name] = 'AutoIt'

Malware: HkMain
Yes, this was actually found in proxy logs.

- User-agent: M

Indicator Pages

User-agent Strings
Houdini Tracker
Geodo Indicators
Indicators

Blog Archive

Labels

about dridex dyre geodo houdini indicators insecure malware mudrop predictions regex review spyware sql tools tracking trojan updates user-agent welcome zbot zeus

Favorite Blogs

Blaze's Security Blog
Dynamoo's Blog
Malware Battle
Malware Analysis: The Final Frontier

- User-agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
- Regex: Mozilla\/4\.0\s\(compatible;\sMSIE\s8\.0;\sWindows\sNT\s5\.1;\sTrident\/4\.0\)

Malware: Botnet / Adware
This was found in a known botnet as well as some adware.

- User-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
- Regex: Mozilla\/4\.0\s\(compatible;\sMSIE\s6\.0;\sWindows\sNT\s5\.1;\sSV1\)

Malware: Yakes
Notice the lack of spacing within the parantheses.

- User-agent: Mozilla/4.0 (compatible;MSIE 7.0;Windows NT 6.0)
- Regex: Mozilla\/4\.0\s\(compatible;MSIE\s7\.0;Windows\sNT\s6\.0\)

That is it for now. I will add a separate page for these in the future as I continue to find more malicious user-agent strings.

Further reading:

- Deepend Security - great repository of malicious traffic values.
- Malware Traffic Patterns - more indicators and analysis than you can handle.
- 2013 User-agent Blacklist - old but it still contains useful data.

Posted by Justin at 09:31

Labels: indicators, malware, user-agent

No comments:

Post a Comment

Please feel free to leave a comment that is relevant to the post.

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

Malware-Traffic-Analysis.net

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)