

ThreatFactor NSIA - Feature #59

ThreatPattern Extensions

04/08/2010 11:37 PM - Luke Murphey

Status:	New	Start date:	04/08/2010
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:	Scan Engine	Estimated time:	0.00 hour
Target version:			

Description

ThreatSignatures could have more power if they supported extensions that could be used inside of definitions. These extensions could be used to perform operations not typically available within ThreatSignatures. Below is an example of the syntax that may be used:

```
Extension.HTTP.Header["Server"] = "/Apache.*i";  
Extension.HTTP.Cookie("auth", true) != "[A-F0-9]{,32}i";
```

The actual function to process the extension would include the following function prototype:

```
boolean matchedExtension(  
    String extensionName, // "Extension.HTTP.Cookie"  
    String[] arguments, // "auth", "true"  
    boolean notFlagSet, // true  
    String operand ); // "[A-F0-9]{,32}i"
```

History

#1 - 11/02/2010 01:14 PM - Luke Murphey

- Category set to Scan Engine