2/1/2006

CME-24 (Blackworm)

Analysis and Identification using the Cisco MARS

Overview

Common Malware Enumeration (CME) – 24 referred to in this document as "Blackworm" can also be identified using the following aliases:
Authentium: W32/Kapser.A@mm
AVIRA: Worm/KillAV.GR
CA: Win32/Blackmal.F
Fortinet: W32/Grew.A!wm
F-Secure: Nyxem.E
Grisoft: Worm/Generic.FX
H+BEDV: Worm/KillAV.GR
Kaspersky: Email-Worm.Win32.Nyxem.e
McAfee: W32/MyWife.d@MM
Norman: W32/Small.KI
Panda: W32/Tearec.A.worm
Sophos: W32/Nyxem-D
Symantec: W32.Blackmal.E@mm
TrendMicro: WORM_GREW.A

This mass mailing worm had already been identified and analyzed by the major AntiVirus vendors. This document illustrates how to identify and analyze the worm using basic network events collected and correlated by the Cisco Security Monitoring, Analysis and Response System (MARS) from a single egress (Internet) firewall.

For detailed information on the Cisco MARS:
http://www.cisco.com/en/US/products/ps6241/index.html

For additional detailed information on Blackworm:
http://isc.sans.org/blackworm
http://cme.mitre.org/data/list.html
http://www.priveon.com/

For similar research, documents and information on Priveon's network and security services:
http://www.priveon.com/

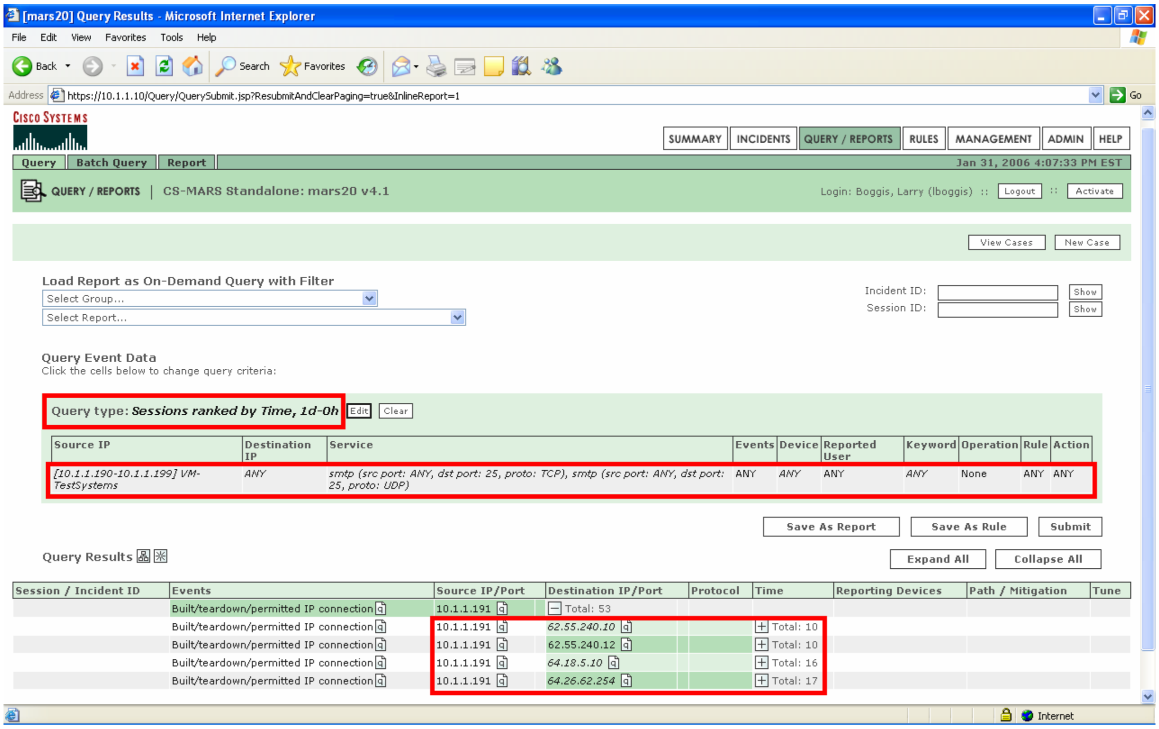
High-Level Network Analysis

Often, one of the easiest ways to identify infected systems on a network is to simply look at the logs from the egress (Internet) firewall. Specifically, a security analyst would look at any system trying to use an external DNS or SMTP server or service. Of course, there are many more attack and propagation vectors than those basic services listed, but it's always easier to target the obvious and work down from there. Furthermore, it is important to stress the importance of egress filtering. It's always a good idea, and Priveon's recommendation, to apply egress (outbound) filters to your perimeter firewalls. There is rarely a good reason to have a 'permit all' policy for egress traffic. (…but, that's a topic for another paper)

Let's start by taking a look at internal systems trying to send email using "external" [or non-corporate] email servers. If you think about it, why would a system try to use a non-corporate email server to send email? To name a few:

- To bypass corporate policy
- Recreational email (users accessing personal email)
- To hide content leaving the network
- To evade AntiVirus email servers
- To spread malware without detection

Figure 1 illustrates an extremely simple query on the Cisco MARS to report on the internal systems accessing external SMTP services:


[mars20] Query Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.1.1.10/Query/QuerySubmit.jsp?ResubmitAndClearPaging=true&InlineReport=1
Go
Cisco Systems
SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP
Query Batch Query Report
Jan 31, 2006 4:07:33 PM EST
QUERY / REPORTS | CS-MARS Standalone: mars20 v4.1
Login: Boggis, Larry (lboggis) :: Logout :: Activate
View Cases New Case
Load Report as On-Demand Query with Filter
Select Group...
Select Report...
Incident ID: Show
Session ID: Show
Edit Clear
Save As Report Save As Rule Submit
Expand All Collapse All
Internet

Query Event Data
Click the cells below to change query criteria:

Query type: *Sessions ranked by Time, 1d-0h*

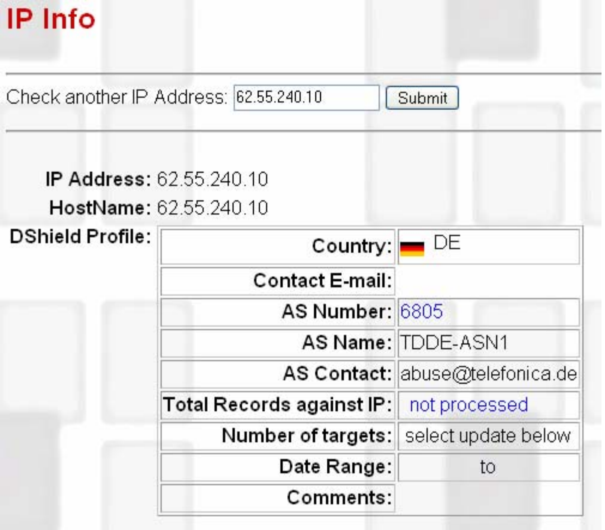
Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
[10.1.1.190-10.1.1.199] VM-TestSystems	*ANY*	*smtp (src port: ANY, dst port: 25, proto: TCP), smtp (src port: ANY, dst port: 25, proto: UDP)*	ANY	*ANY*	ANY	*ANY*	None	ANY	ANY

Query Results

Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Devices	Path / Mitigation	Tune
	Built/teardown/permitted IP connection	10.1.1.191	⊟ Total: 53					
	Built/teardown/permitted IP connection	10.1.1.191	*62.55.240.10*		⊞ Total: 10			
	Built/teardown/permitted IP connection	10.1.1.191	62.55.240.12		⊞ Total: 10			
	Built/teardown/permitted IP connection	10.1.1.191	*64.18.5.10*		⊞ Total: 16			
	Built/teardown/permitted IP connection	10.1.1.191	*64.26.62.254*		⊞ Total: 17			

FIGURE 1: Simple External SMTP Query

From this query, we identify an inside system "10.1.1.191" accessing several external SMTP servers. If we do some basic investigation and look at the first external server listed (62.55.240.10), we see that it's registered in Germany – see Figure 2. That's funny … I don't remember opening up an office in Germany:



IP Info

Check another IP Address: 62.55.240.10 Submit

IP Address: 62.55.240.10
HostName: 62.55.240.10
DShield Profile:

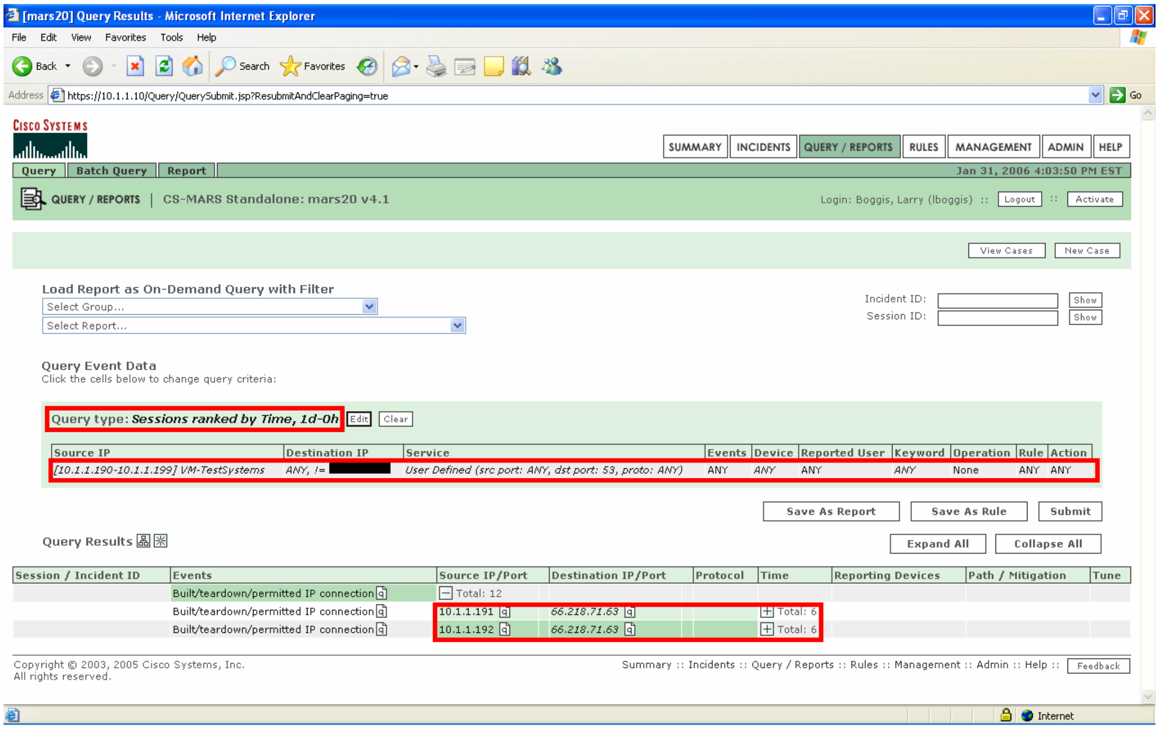
Country:	DE
Contact E-mail:	
AS Number:	6805
AS Name:	TDDE-ASN1
AS Contact:	abuse@telefonica.de
Total Records against IP:	not processed
Number of targets:	select update below
Date Range:	to
Comments:	

FIGURE 2: Dshield IP Lookup

The way the Cisco MARS displays the query data makes it extremely easy to identify and view patterns. These patterns help us to identify infected systems and malicious activity.

NOTE: *It is important to understand that the steps in this document prove the MARS ability to locate possible worm infections in a network using only a single egress firewall as the sole data source. Other data sources such as Router logs, NetFlow, and Network and Host IPS would only enhance the results and accuracy.*

Another eye-opening query, as displayed in Figure 3, is to look for internal systems (non-DNS servers) accessing external DNS servers for name resolution. Let's take a look:


[mars20] Query Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.1.1.10/Query/QuerySubmit.jsp?ResubmitAndClearPaging=true
Go
Cisco Systems
SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP
Query Batch Query Report
Jan 31, 2006 4:03:50 PM EST
QUERY / REPORTS | CS-MARS Standalone: mars20 v4.1
Login: Boggis, Larry (lboggis) :: Logout :: Activate
View Cases
New Case
Incident ID: Show
Session ID: Show
Internet

Load Report as On-Demand Query with Filter

Select Group...

Select Report...

Query Event Data

Click the cells below to change query criteria:

Query type: ***Sessions ranked by Time, 1d-0h*** Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
[10.1.1.190-10.1.1.199] VM-TestSystems	*ANY, !=* [redacted]	*User Defined (src port: ANY, dst port: 53, proto: ANY)*	ANY	*ANY*	ANY	*ANY*	None	ANY	ANY

Save As Report Save As Rule Submit

Query Results

Expand All Collapse All

Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Devices	Path / Mitigation	Tune
	Built/teardown/permitted IP connection	⊟ Total: 12						
	Built/teardown/permitted IP connection	10.1.1.191	*66.218.71.63*		⊞ Total: 6			
	Built/teardown/permitted IP connection	10.1.1.192	*66.218.71.63*		⊞ Total: 6			

Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback

FIGURE 3: Simple External DNS Server Query

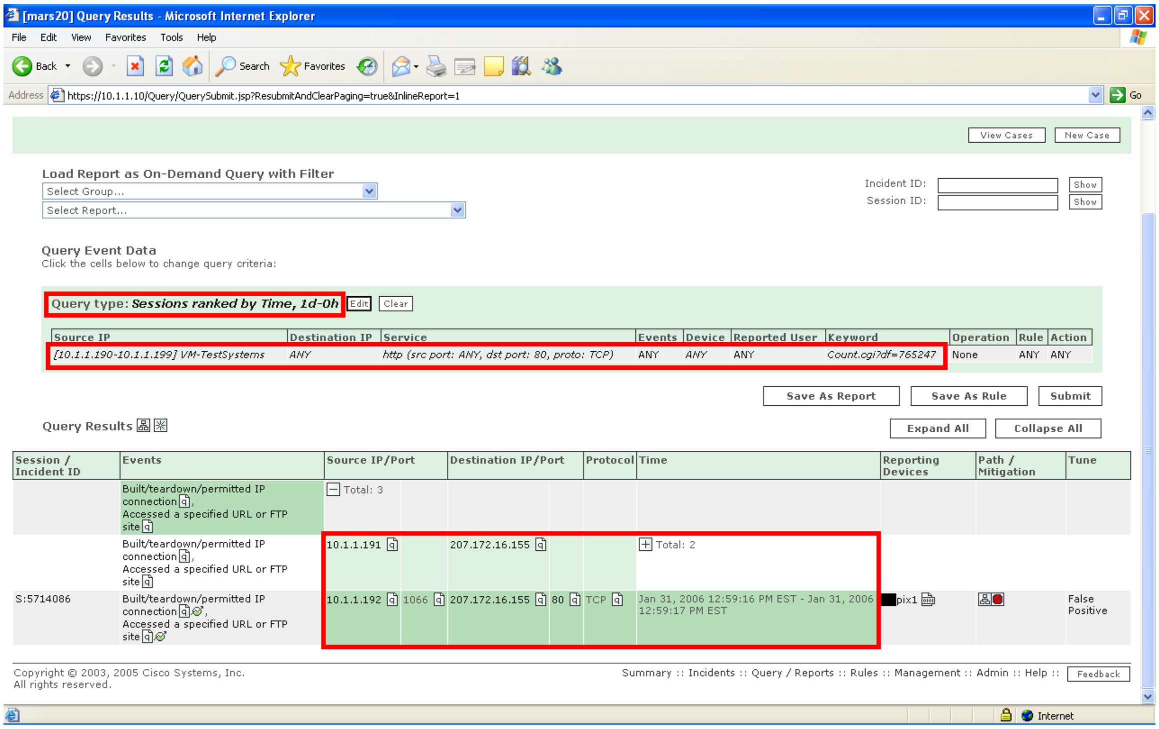
Here, we see two systems (10.1.1.191 and 10.1.1.192) accessing the same outside server (66.218.71.63) for name resolution.

Unfortunately, the data we get from the FW logs does not give us any detailed DNS query information, however, just the fact that outside servers are being accessed for DNS queries gives us room for suspicion.

Targeted Analysis

We know from previous research that one "signature" of Blackworm is for it to access a certain URL to update an online counter. The assumption is that this is a counter of the number of machines currently infected by the worm. We can narrow our query criteria to include this URL [or part of the URL] to identify infected systems on the internalnetwork.

Figure 4 displays a sample query looking for a keyword "Count.cgi?df=765247" in HTTP (TCP/80) traffic:



[mars20] Query Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.1.1.10/Query/QuerySubmit.jsp?ResubmitAndClearPaging=true&InlineReport=1
Go
View Cases
New Case
Show
Show
Edit
Clear
Save As Report
Save As Rule
Submit
Expand All
Collapse All
Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help ::
Feedback
Internet

Load Report as On-Demand Query with Filter

Select Group...

Select Report...

Incident ID:

Session ID:

Query Event Data

Click the cells below to change query criteria:

Query type: *Sessions ranked by Time, 1d-0h*

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
[10.1.1.190-10.1.1.199] VM-TestSystems	*ANY*	*http (src port: ANY, dst port: 80, proto: TCP)*	ANY	*ANY*	ANY	*Count.cgi?df=765247*	None	ANY	ANY

Query Results

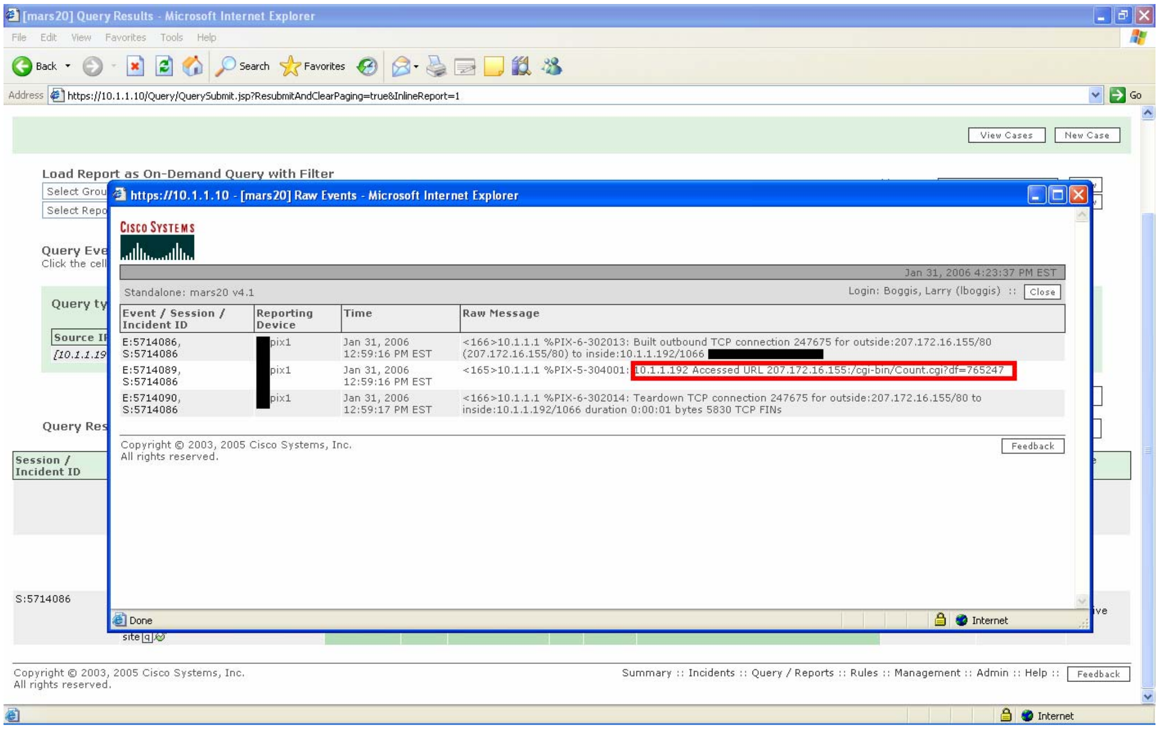
Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Devices	Path / Mitigation	Tune
	Built/teardown/permitted IP connection, Accessed a specified URL or FTP site	Total: 3								
	Built/teardown/permitted IP connection, Accessed a specified URL or FTP site	10.1.1.191		207.172.16.155			Total: 2			
S:5714086	Built/teardown/permitted IP connection, Accessed a specified URL or FTP site	10.1.1.192	1066	207.172.16.155	80	TCP	Jan 31, 2006 12:59:16 PM EST - Jan 31, 2006 12:59:17 PM EST	[redacted] pix1		False Positive

Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.

FIGURE 4: Keyword Query

From this query we see that we have two systems (10.1.1.191 and 10.1.1.192) that accessed a URL with the specified keyword. One system, in fact, had multiple entries.

Drilling down a little deeper, as in Figure 5, we can see the event details:



[mars20] Query Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.1.1.10/Query/QuerySubmit.jsp?ResubmitAndClearPaging=true&InlineReport=1
Go
View Cases
New Case
https://10.1.1.10 - [mars20] Raw Events - Microsoft Internet Explorer
CISCO SYSTEMS
Close
Feedback
Done
Internet
Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help ::
Feedback
Internet

Load Report as On-Demand Query with Filter

Jan 31, 2006 4:23:37 PM EST

Standalone: mars20 v4.1

Login: Boggis, Larry (lboggis) ::

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:5714086, S:5714086	[redacted] pix1	Jan 31, 2006 12:59:16 PM EST	<166>10.1.1.1 %PIX-6-302013: Built outbound TCP connection 247675 for outside:207.172.16.155/80 (207.172.16.155/80) to inside:10.1.1.192/1066 [redacted]
E:5714089, S:5714086	pix1	Jan 31, 2006 12:59:16 PM EST	<165>10.1.1.1 %PIX-5-304001: 10.1.1.192 Accessed URL 207.172.16.155:/cgi-bin/Count.cgi?df=765247
E:5714090, S:5714086	pix1	Jan 31, 2006 12:59:17 PM EST	<166>10.1.1.1 %PIX-6-302014: Teardown TCP connection 247675 for outside:207.172.16.155/80 to inside:10.1.1.192/1066 duration 0:00:01 bytes 5830 TCP FINs

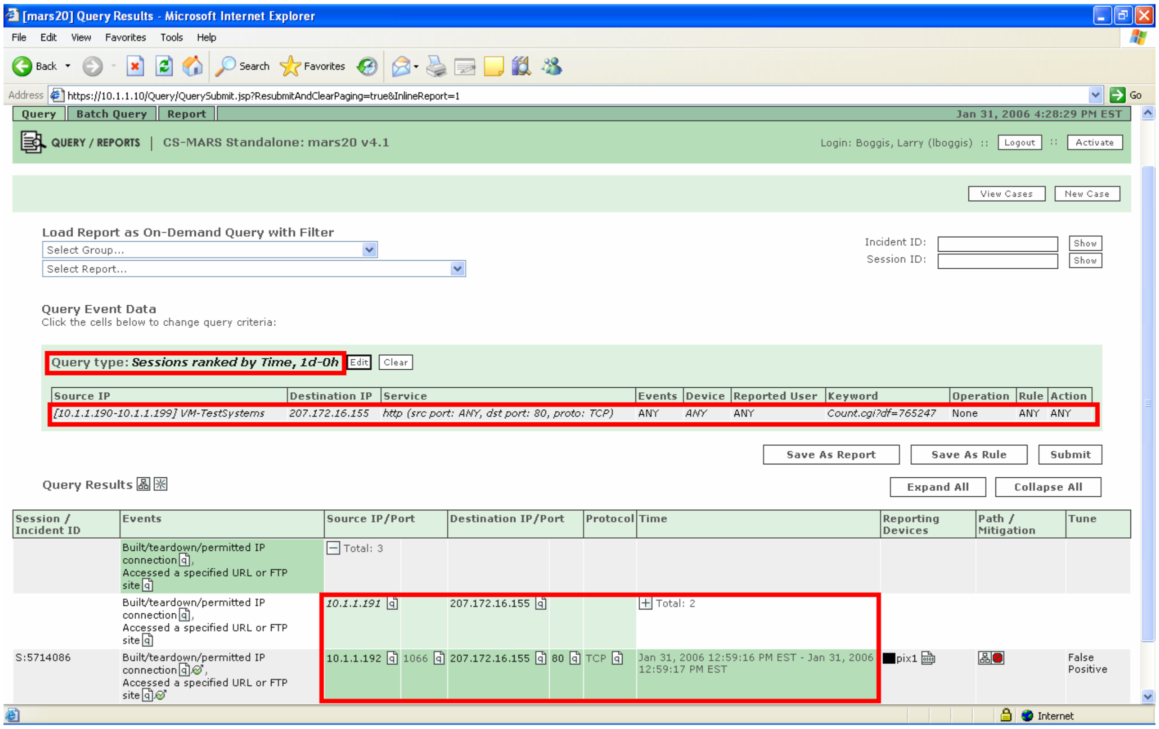
Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.

S:5714086

Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.

FIGURE 5: Raw Message Reveals URL Detail

We can further refine our search to make sure that we get as specific as possible by including the destination IP address as well. According to previous Blackworm research, the destination host should be "webstats.mrf.va.web.rcn.net" (207.172.16.155), which is exactly what Figure 6 displays.



https://10.1.1.10/Query/QuerySubmit.jsp?ResubmitAndClearPaging=true&InlineReport=1

Jan 31, 2006 4:28:29 PM EST

CS-MARS Standalone: mars20 v4.1

Login: Boggis, Larry (lboggis) :: Logout :: Activate

Load Report as On-Demand Query with Filter

Select Group...

Select Report...

Incident ID:

Session ID:

Query Event Data

Click the cells below to change query criteria:

Query type: *Sessions ranked by Time, 1d-0h*

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
[10.1.1.190-10.1.1.199] VM-TestSystems	*207.172.16.155*	*http (src port: ANY, dst port: 80, proto: TCP)*	ANY	*ANY*	ANY	*Count.cgi?df=765247*	None	ANY	ANY

Query Results

Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Devices	Path / Mitigation	Tune
	Built/teardown/permitted IP connection, Accessed a specified URL or FTP site	Total: 3						
	Built/teardown/permitted IP connection, Accessed a specified URL or FTP site	*10.1.1.191*	207.172.16.155		Total: 2			
S:5714086	Built/teardown/permitted IP connection, Accessed a specified URL or FTP site	10.1.1.192 1066	207.172.16.155 80	TCP	Jan 31, 2006 12:59:16 PM EST - Jan 31, 2006 12:59:17 PM EST	pix1		False Positive

FIGURE 6: Worm Confirmation using DST IP and URL keyword

The Cisco MARS has the capability of drilling even deeper by identifying exactly where on you network the infected systems reside—down to the router interface, subnet and switch port. In addition the MARS can show the exact attack path traversed and also provide the network/security device command syntax which could be used to mitigate the attack and/or infection from spreading.

Summary

In summary, the use of network log data is extremely helpful in identifying systems infected by both known and unknown malware. The "network behavior" can be identified rather easily using the event correlation and reporting functions of the Cisco MARS. The example above used event data from a single Internet firewall alone to demonstrate that a tool like the Cisco MARS can be beneficial in any environment when identifying "anomalies" and malware activity. Our message is that event correlation and visibility into security and network event data is important for any size environment.

Some organizations use basic syslog servers to archive FW and network log data. Imagine trying to parse through days, weeks and months of log data given that most environments generate millions of events on a daily basis.

The Cisco MARS is an invaluable tool to help identify traffic (sessions), network "behavior" (events) and statistical anomalies, to correlate data from both network and security devices on your network and to identify when and where events occur on your network.