

URL

4.0.1236 NETAMS 4.0 - .

:

- RemoteAgentDataSource
- UNIX-
- (), "", "" ()

(, PCAP) . , - (TCP- SRC DST 80, 81, 8000, 8080, 3128) URL (-).

: IP- -?

: .- URL (), .-, IP- () . , , .-, www.someserver.ru 210.172.56.8, - ip8-pool56.clients.megahosting.com. , HTTP/1.1 , IP- () -. IP-, "Host:" . "".

, .-, UNIX- NETAMS 4.0. URL:

Источник данных: 3

Ключ	Наименование	Значение
ds_name	Data-source friendly name	RemoteAgentDataSource
listen_at	Listen for remote agents at given local IP address	0.0.0.0
port	Listen for agent signalling at given local UDP port	20002
accept_from	Accept flows from given remote source IP address(es)	0.0.0.0
password	Secure communication with password, 5 to 20 symbols	password
interface	Source will capture packets at following interface	eth0
rule	Source will apply following filter rule	ip
url_detect	Enable URL detection in flows	☒
enable_dpi	Enable deep packet inspection (DPI)	☐

Применить

Обновить

Закрыть

- (URL) . Wireshark TCP- (HTTP-) - www.lenta.ru (IP- 81.19.85.116):

4 0.001859 93. 81.19.85.116 HTTP GET / HTTP/1.1

Frame 4: 821 bytes on wire (6568 bits), 821 bytes captured (6568 bits)

Ethernet II, Src: Dell_5f:7f:50 (00:1e:c9:5f:7f:50), Dst: Cisco_d6:8c:00 (00:1e:13:d6:8c:00)

Internet Protocol, Src: , Dst: 81.19.85.116 (81.19.85.116)

Transmission Control Protocol, Src Port: sybasesrvmon (4950), Dst Port: http (80), Seq: 1, Ac

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

[truncated] Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/vnd.ms-exe

Accept-Language: ru\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; GTB7.2; .NET CL

Accept-Encoding: gzip, deflate\r\n

Host: www.lenta.ru\r\n

Connection: Keep-Alive\r\n

Cookie: __utma=33679038.1141911010.1297170806.1325149949.1325161639.138; __utmz=33679038.12

\r\n

```

(www.lenta.ru) URL (GET /) HTTP/1.1 :
0000 00 1e 13 d6 8c 00 00 1e c9 5f 7f 50 08 00 45 00 ..... ..P..E.
0010 03 27 27 d4 40 00 80 06 c5 31 5d b4 06 90 51 13 .'.@... .1]...Q.
0020 55 74 13 56 00 50 10 cf 8e 12 41 4c 00 9d 50 18 Ut.V.P.. ..AL..P.
0030 ff ff 0d e5 00 00 47 45 54 20 2f 20 48 54 54 50 .....GE T / HTTP
0040 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d /1.1..Ac cept: im
0050 61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 6a age/gif, image/j
0060 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65 67 peg, ima ge/pjpeg
0070 2c 20 69 6d 61 67 65 2f 70 6a 70 65 67 2c 20 61 , image/ pjpeg, a
0080 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e 64 2e 6d pplicati on/vnd.m
0090 73 2d 65 78 63 65 6c 2c 20 61 70 70 6c 69 63 61 s-excel, applica
00a0 74 69 6f 6e 2f 76 6e 64 2e 6d 73 2d 70 6f 77 65 tion/vnd .ms-powe
00b0 72 70 6f 69 6e 74 2c 20 61 70 70 6c 69 63 61 74 rpoint, applicat
00c0 69 6f 6e 2f 6d 73 77 6f 72 64 2c 20 61 70 70 6c ion/mswo rd, appl
00d0 69 63 61 74 69 6f 6e 2f 78 61 6d 6c 2b 78 6d 6c ication/ xaml+xml
00e0 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e , applic ation/vn
00f0 64 2e 6d 73 2d 78 70 73 64 6f 63 75 6d 65 6e 74 d.ms-xps document
0100 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d , applic ation/x-
0110 6d 73 2d 78 62 61 70 2c 20 61 70 70 6c 69 63 61 ms-xbap, applica
0120 74 69 6f 6e 2f 78 2d 6d 73 2d 61 70 70 6c 69 63 tion/x-m s-applic
0130 61 74 69 6f 6e 2c 20 61 70 70 6c 69 63 61 74 69 ation, a pplicati
0140 6f 6e 2f 78 2d 73 68 6f 63 6b 77 61 76 65 2d 66 on/x-sho ckwave-f
0150 6c 61 73 68 2c 20 2a 2f 2a 0d 0a 41 63 63 65 70 lash, */ *.Accep
0160 74 2d 4c 61 6e 67 75 61 67 65 3a 20 72 75 0d 0a t-Langua ge: ru..
0170 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
0180 6c 6c 61 2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 lla/4.0 (compati
0190 62 6c 65 3b 20 4d 53 49 45 20 38 2e 30 3b 20 57 ble; MSI E 8.0; w
01a0 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 54 indows NT 5.1; T
01b0 72 69 64 65 6e 74 2f 34 2e 30 3b 20 47 54 42 37 rident/4 .0; GTB7
01c0 2e 32 3b 20 2e 4e 45 54 20 43 4c 52 20 31 2e 31 .2; .NET CLR 1.1
01d0 2e 34 33 32 32 3b 20 2e 4e 45 54 20 43 4c 52 20 .4322; . NET CLR
01e0 32 2e 30 2e 35 30 37 32 37 3b 20 2e 4e 45 54 20 2.0.5072 7; .NET
01f0 43 4c 52 20 33 2e 30 2e 30 34 35 30 36 2e 33 30 CLR 3.0. 04506.30
0200 3b 20 2e 4e 45 54 20 43 4c 52 20 33 2e 30 2e 34 ; .NET C LR 3.0.4
0210 35 30 36 2e 32 31 35 32 3b 20 2e 4e 45 54 20 43 506.2152 ; .NET C
0220 4c 52 20 33 2e 35 2e 33 30 37 32 39 3b 20 4d 53 LR 3.5.3 0729; MS
0230 2d 52 54 43 20 4c 4d 20 38 3b 20 2e 4e 45 54 34 -RTC LM 8; .NET4
0240 2e 30 43 3b 20 2e 4e 45 54 34 2e 30 45 29 0d 0a .0C; .NE T4.0E)..
0250 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Accept-E ncoding:
0260 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a gzip, d eflate..
0270 48 6f 73 74 3a 20 77 77 77 2e 6c 65 6e 74 61 2e Host: ww w.lenta.
0280 72 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 ru..Conn ection:
0290 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b Keep-Ali ve..Cook
02a0 69 65 3a 20 5f 5f 75 74 6d 61 3d 33 33 36 37 39 ie' ut ma=33679

```

```

, ( ), URL ( ).
, :
• , ( HTTP-), (" ") ,
• (.), . " "
• -, , HTTP-.
, UriIsReport . , , :
•
•
•
• URL
, ( ) URL:

```

Обработка UrIsReport [Посещенные сайты]

Наименование: ☐ Доступен абоненту

Период:

Группа контрактов: Контракт:

Услуга:

☒ Группировать по путям ☐ Группировать по домену ☐ Внутренние сайты Количество записей:

Исключение:

По заданному URL:

Формат: Выводить отчет:

Посещенные сайты

за период с 10.01.2012 0:00:00 по 10.01.2012 23:59:59

Контракт: FNM_C_144

URL	Посещений
notify16.dropbox.com	325
ad.rambler.ru	14
wirelessccle.blogspot.com	9
expertwireless2be.blogspot.com	8
www.my80211.com	8
img.lenta.ru	4
blakekrone.com	3
mc.yandex.ru	2

, -, " " (URL, -) :

Обработка UrIsReport [Посещенные сайты]

Наименование: ☐ Доступен абоненту

Период:

Группа контрактов: Контракт:

Услуга:

☐ Группировать по путям ☐ Группировать по домену ☒ Внутренние сайты Количество записей:

Исключение:

По заданному URL:

Формат: Выводить отчет:

Посещенные сайты

за период с 10.01.2012 0:00:00 по 10.01.2012 23:59:59

Контракт: NM

URL	Посещений
url: www.nanometer.ru/fig/forms.css	690
url: www.nanometer.ru/fig/common.js	677
url: www.nanometer.ru/fig/cal_conf2.js	544
url: www.nanometer.ru/fig/cal2.js	508
url: www.nanometer.ru/fig/nm.css	483
url: www.nanometer.ru/2007/12/24/ovij_qod_5503/PROP_IMG_images	385
url: www.nanometer.ru/fig/linkedselect.js	339
url: www.nanometer.ru/favicon.ico	321