Network traffic surveillance – effective means to analyse network security incidents

Raitis Misa

October 6th, 2016

ugunssiena IT

Data for analysis

To monitor network traffic and gather data to analyse, solution developed by Ugunssiena IT was used. Main components of the solution are:

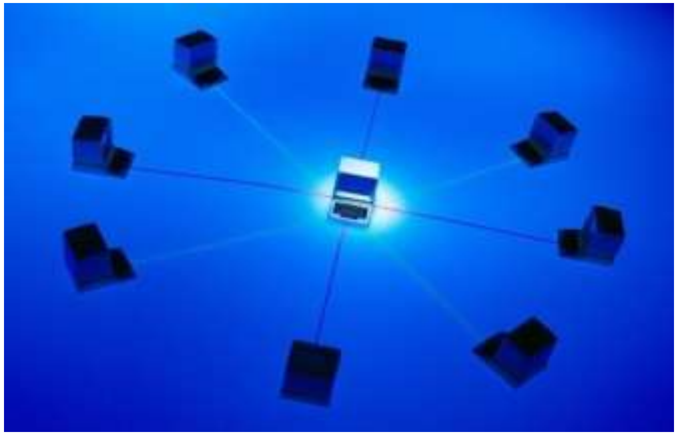
- Firewall
- Router
- Email security
- **Network traffic surveillance system**
- SSL proxy

How NTSS works

Similar to CCTV in physical world, NTSS gathers data about network activity

WEB

EMAIL



DOWNLOADS

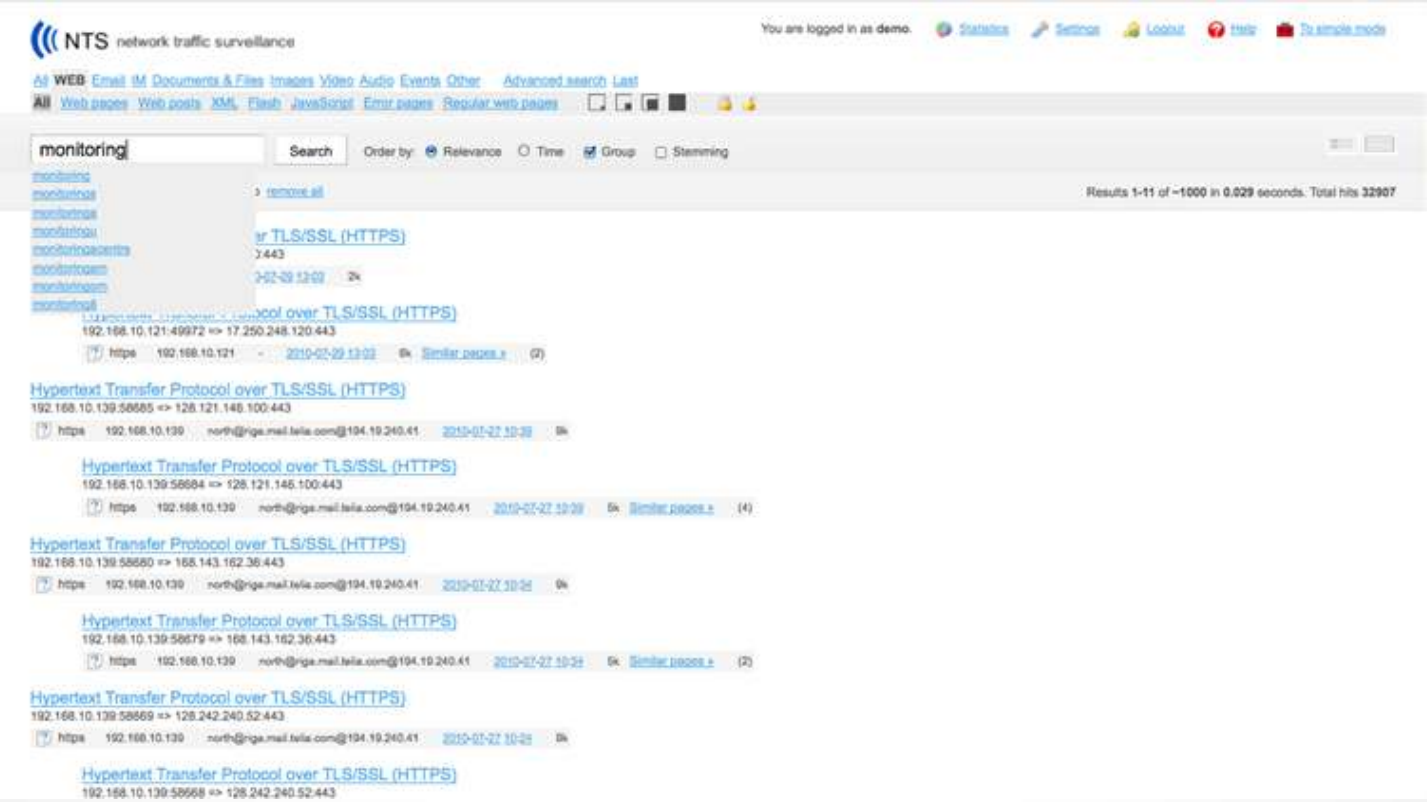
CHAT

How NTSS works

- NTSS records ALL network traffic - TCP and UDP packets
- Traffic is stored in pcap (packet capture) format and restored to the application level – into web pages, e-mails, documents sent etc.
- All data recorded are fully indexed and available for fast search

How NTSS works

Full-text search allows to access all data objects recorded



NTS network traffic surveillance

You are logged in as **demo**. Statistics Settings Logout Help To simple mode

All **WEB** Email IM Documents & Files Images Video Audio Events Other   Advanced search Last

All Web pages Web posts XML Flash JavaScript Error pages Regular web pages

monitoring | Search | Order by: ● Relevance ○ Time ☑ Group □ Stemming

monitoring
monitorings
monitoringa
monitoringu
monitoringacentrs
monitoringam
monitoringom
monitoringā

› remove all

Results **1-11** of **~1000** in **0.029** seconds. Total hits **32907**

r TLS/SSL (HTTPS)
:443
-07-29 13:03   2k

col over TLS/SSL (HTTPS)
192.168.10.121:49972 => 17.250.248.120:443
https   192.168.10.121   -   2010-07-29 13:03   6k   Similar pages »   (2)

Hypertext Transfer Protocol over TLS/SSL (HTTPS)
192.168.10.139:58685 => 128.121.146.100:443
https   192.168.10.139   north@riga.mail.telia.com@194.19.240.41   2010-07-27 10:39   9k

Hypertext Transfer Protocol over TLS/SSL (HTTPS)
192.168.10.139:58684 => 128.121.146.100:443
https   192.168.10.139   north@riga.mail.telia.com@194.19.240.41   2010-07-27 10:39   5k   Similar pages »   (4)

Hypertext Transfer Protocol over TLS/SSL (HTTPS)
192.168.10.139:58680 => 168.143.162.36:443
https   192.168.10.139   north@riga.mail.telia.com@194.19.240.41   2010-07-27 10:34   9k

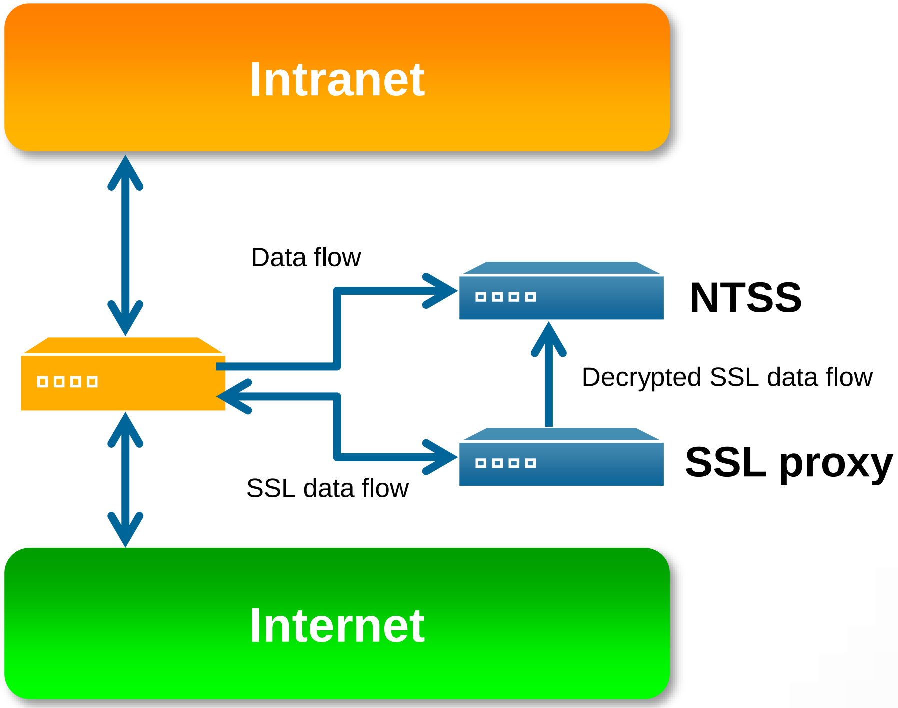
Hypertext Transfer Protocol over TLS/SSL (HTTPS)
192.168.10.139:58679 => 168.143.162.36:443
https   192.168.10.139   north@riga.mail.telia.com@194.19.240.41   2010-07-27 10:34   5k   Similar pages »   (2)

Hypertext Transfer Protocol over TLS/SSL (HTTPS)
192.168.10.139:58669 => 128.242.240.52:443
https   192.168.10.139   north@riga.mail.telia.com@194.19.240.41   2010-07-27 10:24   8k

Hypertext Transfer Protocol over TLS/SSL (HTTPS)
192.168.10.139:58668 => 128.242.240.52:443

How NTSS works

SSL traffic is recorded by using SSL proxy



Why NTSS

NTSS allows to be in control of **Unpredictable**:

- Anti-virus software
- Port filters
- Proxies
- Firewalls
- Application firewalls

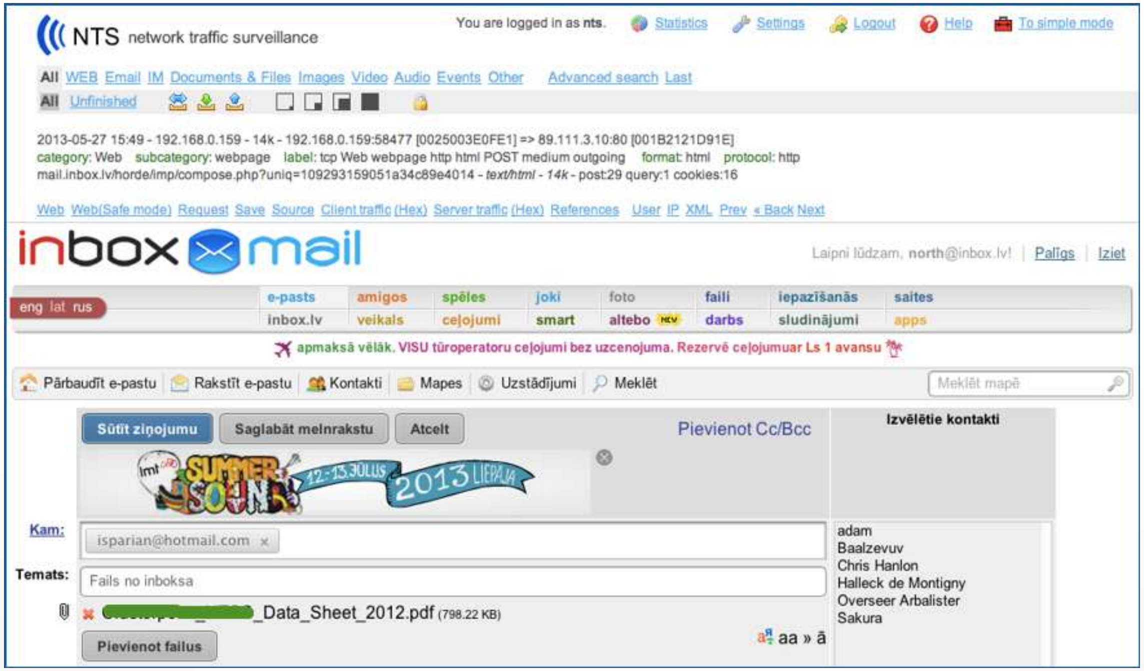
... they all mostly deal with **predictable**, **pre-defined**, already known threats or anomalies and patterns.

NTSS collects all traffic data regardless of predefined assumptions, and therefore helps to pinpoint and discover **unforeseen** security threats.

Why NTSS

Control Acceptable Use Policy

Easily point out Acceptable Use Policy violations, either by manually locating the incidents, or setting up automated Alerts.



You are logged in as **nts**.

2013-05-27 15:49 - 192.168.0.159 - 14k - 192.168.0.159:58477 [0025003E0FE1] => 89.111.3.10:80 [001B2121D91E]
category: Web subcategory: webpage label: tcp Web webpage http html POST medium outgoing format: html protocol: http
mail.inbox.lv/horde/imp/compose.php?uniq=109293159051a34c89e4014 - *text/html* - *14k* - post:29 query:1 cookies:16

Laipni lūdzam, **north**@inbox.lv!

apmaksā vēlāk. VISU tūroperatoru ceļojumi bez uzcenojuma. Rezervē ceļojumuar Ls 1 avansu

Kam: isparian@hotmail.com ×

Temats: Fails no inboksa

[redacted]_Data_Sheet_2012.pdf (798.22 KB)

Izvēlētie kontakti

adam
Baalzevuv
Chris Hanlon
Halleck de Montigny
Overseer Arbalister
Sakura

NTS network traffic surveillance
Statistics
Settings
Logout
Help
To simple mode
All WEB Email IM Documents & Files Images Video Audio Events Other
Advanced search Last
All Unfinished
Web Web(Safe mode) Request Save Source Client traffic (Hex) Server traffic (Hex) References User IP XML Prev « Back Next
inbox mail
Palīgs
Iziet
eng lat rus
e-pasts amigos spēles joki foto faili iepazīšanās saites
inbox.lv veikals ceļojumi smart altebo NEW darbs sludinājumi apps
Pārbaudīt e-pastu
Rakstīt e-pastu
Kontakti
Mapes
Uzstādījumi
Meklēt
Meklēt mapē
Sūtīt ziņojumu
Saglabāt melnrakstu
Atcelt
Pievienot Cc/Bcc
lmt SUMMER SOUND 12-13.JŪLIJS 2013 LIEPĀJA
Pievienot failus
aa » ā

Why NTSS

Discover long standing data security threats.

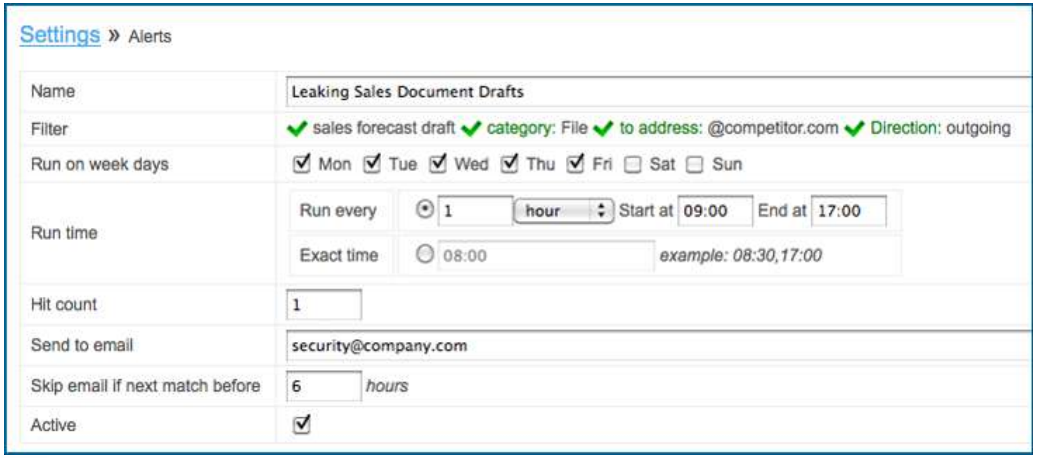
Some security breaches are not obvious in real-time using short term monitoring strategies.

Having access to transaction data over several months can help to pinpoint planned long-term attacks.

Why NTSS

“Insider” Information Theft Monitoring

Setup alerts to warn IT security when documents with specific contents are sent out to a specific or any destination on the Internet.



Settings » Alerts

Name	Leaking Sales Document Drafts	
Filter	✓ sales forecast draft ✓ category: File ✓ to address: @competitor.com ✓ Direction: outgoing	
Run on week days	☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun	
Run time	Run every	● 1 hour Start at 09:00 End at 17:00
	Exact time	○ 08:00 *example: 08:30,17:00*
Hit count	1	
Send to email	security@company.com	
Skip email if next match before	6 *hours*	
Active	☑	

Receive alert when documents containing specific keyword(s) or metadata are sent to external e-mails or web-mail accounts.

Why NTSS

Have a complete, reliable and searchable backup of all e-mail traffic from the company, including web-mails.

Ugunssiena NTSS stores and makes fully searchable all inbound and outbound e-mail communications of your company. Full-text search possible in:

- e-mail contents or metadata
- attached documents
- webmail

Real life examples

Acceptable Use Policy violation detection

During NTSS demo at customers site in less than a minute violation of the Acceptable Use Policy was detected. It turned out that users had access to the *draugiem.lv* social networking portal not allowed by Acceptable Use Policy.

Still, network administrators were sure that everything was fine as all network traffic access rules were in place... with one exception – the use of IP addresses was not forbidden.

NTSS not only detected the violation but was even able to show the picture of the employee from his profile on the social network in question.

Real life examples

Protection of personal data

Personal Data Protection Law restricts the use of personal data like Personal identification codes. NTSS can monitor traffic for Personal identification codes being sent over network and trigger alert.

Using NTSS to monitor traffic of public sector organisation unintentional violation of Personal Data Protection Law was detected. Personal identification codes were sent by e-mail in Word file attachments.

Real life examples

Long term (slow) threat detection

Today users are smart and know that after 3+ failed login attempts alerts will be triggered, access denied and questions asked.

But if intrusion attempts are made only 1-2 times a day, most likely no alerts will go off.

In situations like this, when suspicions arise, it is only possible to eventually catch the bad guy if you have recorded several months of activity.

Some analysis

With information gathered we can make analysis like:

- What is the share of SSL traffic
- From firewall data we can see how persistent are various scanners searching for vulnerabilities
- Windows 10 activities

Encrypted vs open traffic

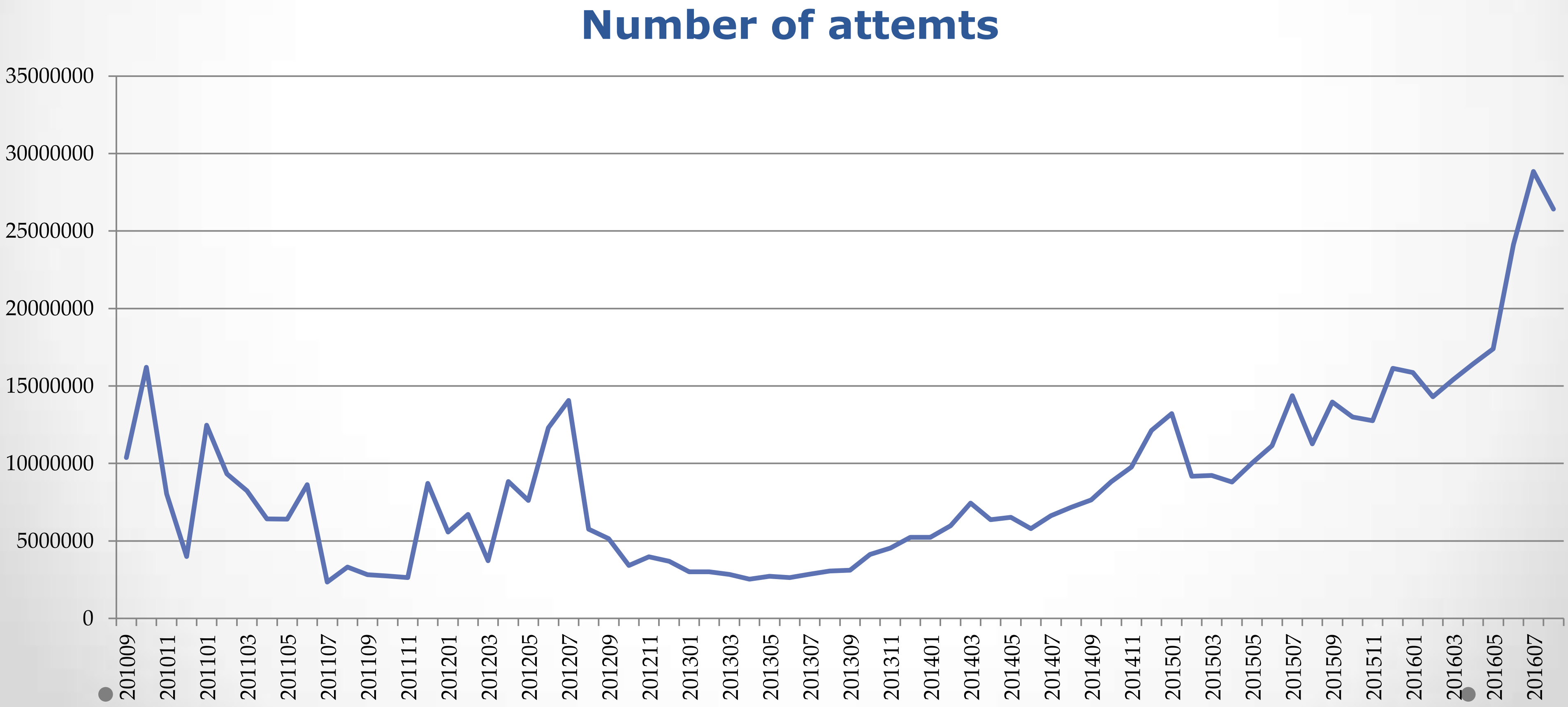
Today many internet resources accept HTTPS connections. According to a claim by Google, more than 80% of all it’s traffic is encrypted. Facebook and Twitter also encrypt it’s traffic by default with others following.

But how about our everyday traffic?

As it turns out, on average, depending on a user, about 1/3 to 1/2 of traffic is encrypted.

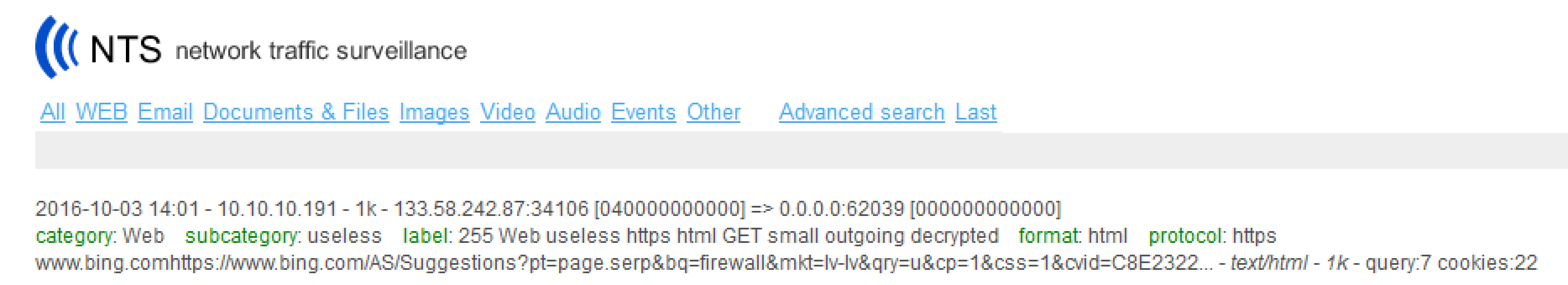
Attack attempts

How many attack attempts a month are made on your network and what is dynamics? We gathered data from the network with about 200 outside IP address for more than five years.



Bing search suggestions

Search dynamic suggestions (600-700 bytes each)



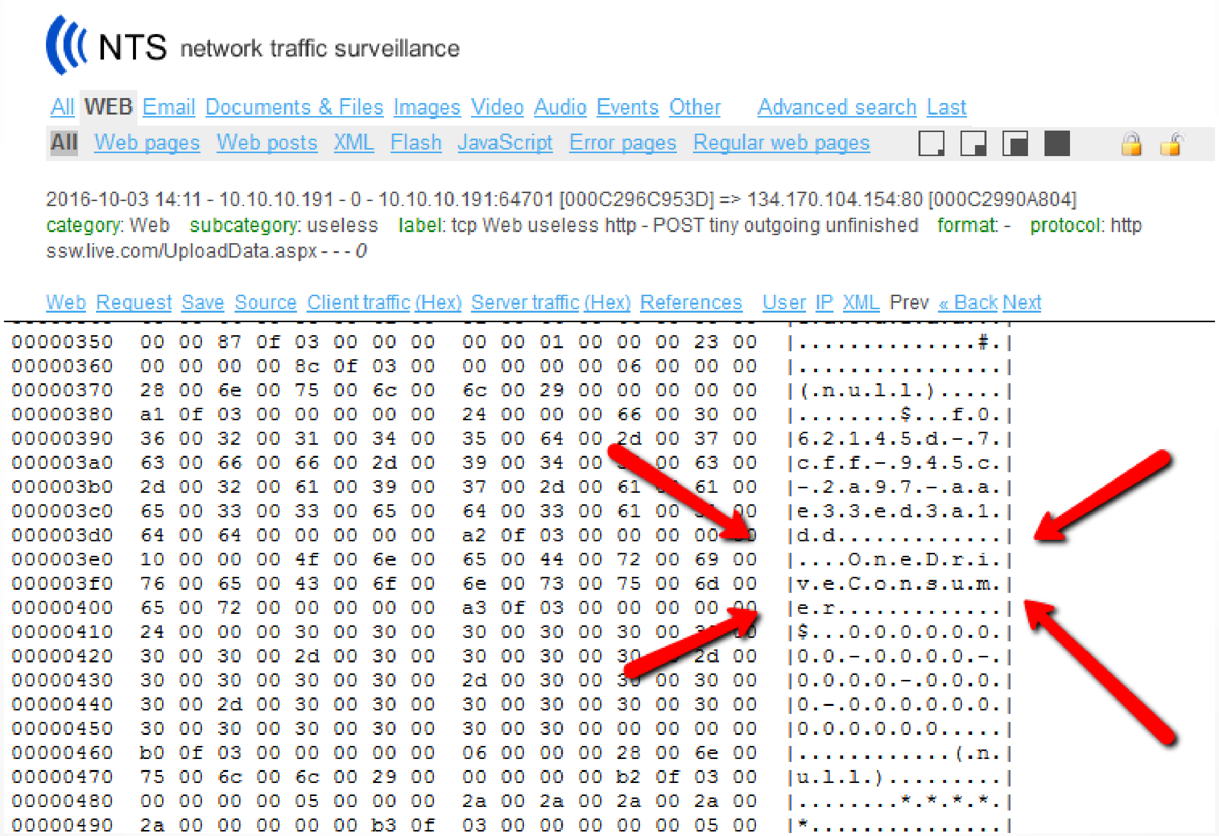
NTS network traffic surveillance
All WEB Email Documents & Files Images Video Audio Events Other Advanced search Last

```
2016-10-03 14:01 - 10.10.10.191 - 1k - 133.58.242.87:34106 [040000000000] => 0.0.0.0:62039 [000000000000]
category: Web    subcategory: useless    label: 255 Web useless https html GET small outgoing decrypted    format: html    protocol: https
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=u&cp=1&css=1&cvid=C8E2322... - text/html - 1k - query:7 cookies:22
```

```
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=ug&cp=2&cvid=C8E2322ABC19... -
text/html - 640 - query:6 cookies:22
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=ugu&cp=3&cvid=C8E2322ABC1... -
text/html - 660 - query:6 cookies:22
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=ugun&cp=4&cvid=C8E2322ABC... -
text/html - 646 - query:6 cookies:22
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=uguns&cp=5&cvid=C8E2322AB... -
text/html - 638 - query:6 cookies:22
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=ugunss&cp=6&cvid=C8E2322A... -
text/html - 670 - query:6 cookies:22
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=ugunssi&cp=7&cvid=C8E2322... -
text/html - 648 - query:6 cookies:22
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=ugunssie&cp=8&cvid=C8E232... -
text/html - 664 - query:6 cookies:22
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=ugunssien&cp=9&cvid=C8E23... -
text/html - 361 - query:6 cookies:22
www.bing.comhttps://www.bing.com/AS/Suggestions?pt=page.serp&bq=firewall&mkt=lv-lv&qry=ugunssiena&cp=10&cvid=C8E... -
text/html - 32 - query:6 cookies:22
```

OneDrive

Even with OneDrive not set up, it checks for updates and status.



NTS network traffic surveillance

All WEB Email Documents & Files Images Video Audio Events Other Advanced search Last
All Web pages Web posts XML Flash JavaScript Error pages Regular web pages

2016-10-03 14:11 - 10.10.10.191 - 0 - 10.10.10.191:64701 [000C296C953D] => 134.170.104.154:80 [000C2990A804]
category: Web subcategory: useless label: tcp Web useless http - POST tiny outgoing unfinished format: - protocol: http
ssw.live.com/UploadData.aspx - - - *0*

Web Request Save Source Client traffic (Hex) Server traffic (Hex) References User IP XML Prev « Back Next

```
00000350  00 00 87 0f 03 00 00 00  00 00 01 00 00 00 23 00  |..............#.|
00000360  00 00 00 00 8c 0f 03 00  00 00 00 00 06 00 00 00  |................|
00000370  28 00 6e 00 75 00 6c 00  6c 00 29 00 00 00 00 00  |(.n.u.l.l.).....|
00000380  a1 0f 03 00 00 00 00 00  24 00 00 00 66 00 30 00  |........$...f.0.|
00000390  36 00 32 00 31 00 34 00  35 00 64 00 2d 00 37 00  |6.2.1.4.5.d.-.7.|
000003a0  63 00 66 00 66 00 2d 00  39 00 34 00 35 00 63 00  |c.f.f.-.9.4.5.c.|
000003b0  2d 00 32 00 61 00 39 00  37 00 2d 00 61 00 61 00  |-.2.a.9.7.-.a.a.|
000003c0  65 00 33 00 33 00 65 00  64 00 33 00 61 00 31 00  |e.3.3.e.d.3.a.1.|
000003d0  64 00 64 00 00 00 00 00  a2 0f 03 00 00 00 00 00  |d.d.............|
000003e0  10 00 00 00 4f 00 6e 00  65 00 44 00 72 00 69 00  |....O.n.e.D.r.i.|
000003f0  76 00 65 00 43 00 6f 00  6e 00 73 00 75 00 6d 00  |v.e.C.o.n.s.u.m.|
00000400  65 00 72 00 00 00 00 00  a3 0f 03 00 00 00 00 00  |e.r.............|
00000410  24 00 00 00 30 00 30 00  30 00 30 00 30 00 30 00  |$...0.0.0.0.0.0.|
00000420  30 00 30 00 2d 00 30 00  30 00 30 00 30 00 2d 00  |0.0.-.0.0.0.0.-.|
00000430  30 00 30 00 30 00 30 00  2d 00 30 00 30 00 30 00  |0.0.0.0.-.0.0.0.|
00000440  30 00 2d 00 30 00 30 00  30 00 30 00 30 00 30 00  |0.-.0.0.0.0.0.0.|
00000450  30 00 30 00 30 00 30 00  30 00 30 00 00 00 00 00  |0.0.0.0.0.0.....|
00000460  b0 0f 03 00 00 00 00 00  06 00 00 00 28 00 6e 00  |............(.n.|
00000470  75 00 6c 00 6c 00 29 00  00 00 00 00 b2 0f 03 00  |u.l.l.).........|
00000480  00 00 00 00 05 00 00 00  2a 00 2a 00 2a 00 2a 00  |........*.*.*.*.|
00000490  2a 00 00 00 00 00 b3 0f  03 00 00 00 00 00 05 00  |*...............|
```

Windows 10

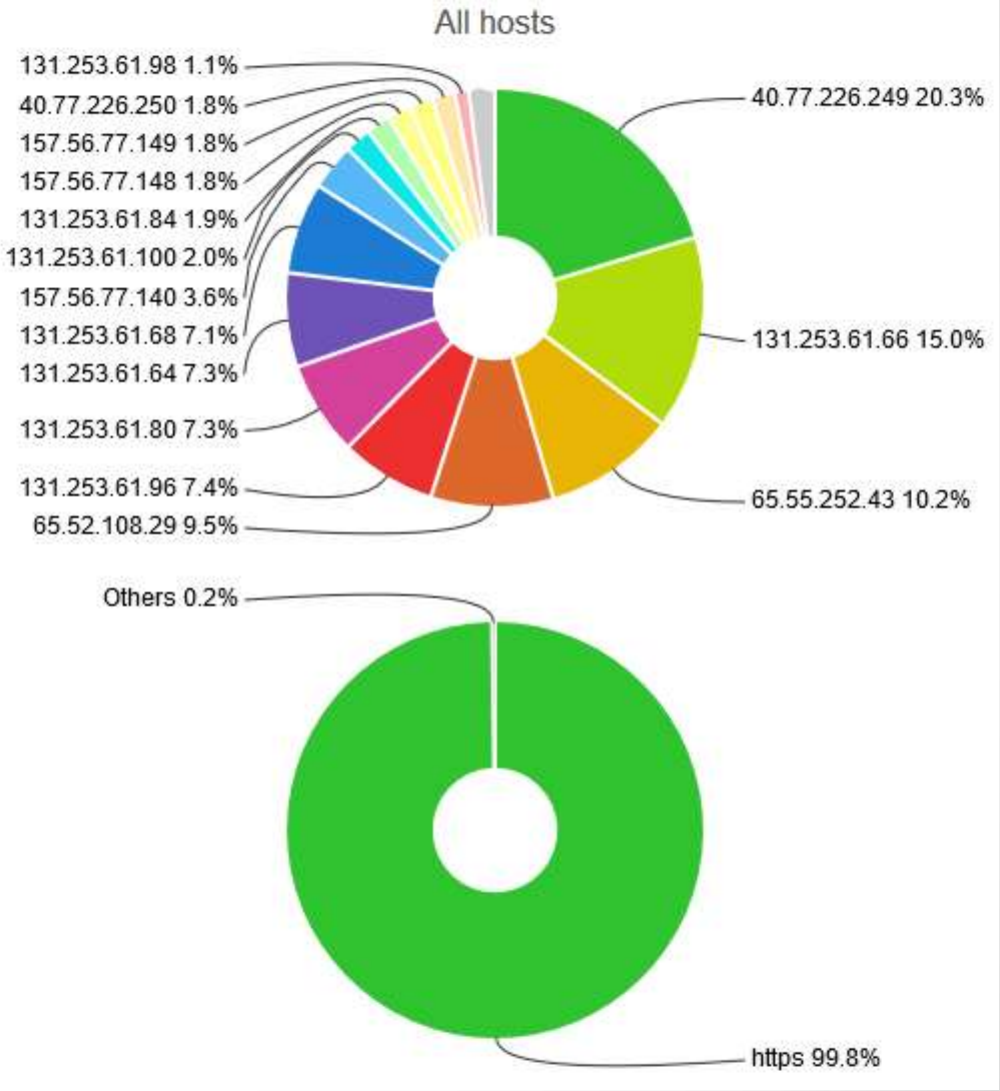
Windows 10 is reporting on your activity and it is no big news. But what kind of information is being sent *home*?

Note that most of the communication done by Windows 10, just like by various services of Google and others, is in SSL.

Windows 10 opens many connections and sends same information, but one thing is for sure – Windows don't send *home* all your information.

Windows 10

Windows 10, even when left alone, makes many connections, all to Microsoft itself and all in SSL.



Thank you!

Web:	http://firewall.lv/
Email:	info@firewall.lv
Phone:	+371 6780 7099