NATO
OTAN

CYBER DEFENCE
@EMERGING SECURITY
CHALLENGES DIVISION

INTERNATIONAL STAFF
EMERGING SECURITY CHALLENGES

SECRÉTARIAT INTERNATIONAL
DÉFIS DE SÉCURITÉ ÉMERGENTS

# Data Analytics applied to Spear Phishing correlation

7-May-2015

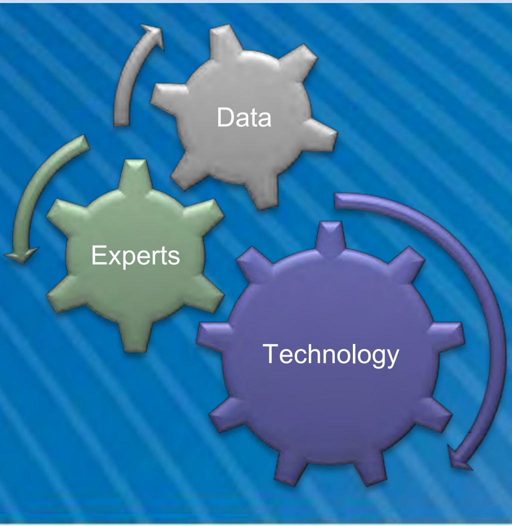
Virginia Aguilar
NCIRC Coordination Centre

# What is this presentation about?

DO WE HAVE ANY ACTIONABLE ANALYTICS FROM OUR BIG DATA IN THE CLOUD?
YES, THE DATA SHOWS THAT MY PRODUCTIVITY PLUNGES WHENEVER YOU LEARN NEW JARGON.
MAYBE IN-MEMORY COMPUTING WILL ACCEL-ERATE YOUR APPLICA-TIONS.
PLUNGE. PLUNGE. PLUNGE.
Dilbert.com DilbertCartoonist@gmail.com
1-9-13 ©2013 Scott Adams, Inc./Dist. by Universal Uclick

# Why did we start this project?

| What we want to achieve | The challenges |
|---|---|
| Comprehensive analysis of incidents targeting NATO networks | • Volume and diversity of data sources<br>• Difficulties correlating information (with internal and external sources)<br>• Difficulties tracking activity over time |
| Identify the "threat landscape" targeting NATO Networks | |
| Search for threat actors that "should" be targeting NATO not identified (yet) | |



**DATA ANALYTICS**

# Benefits of data analytics

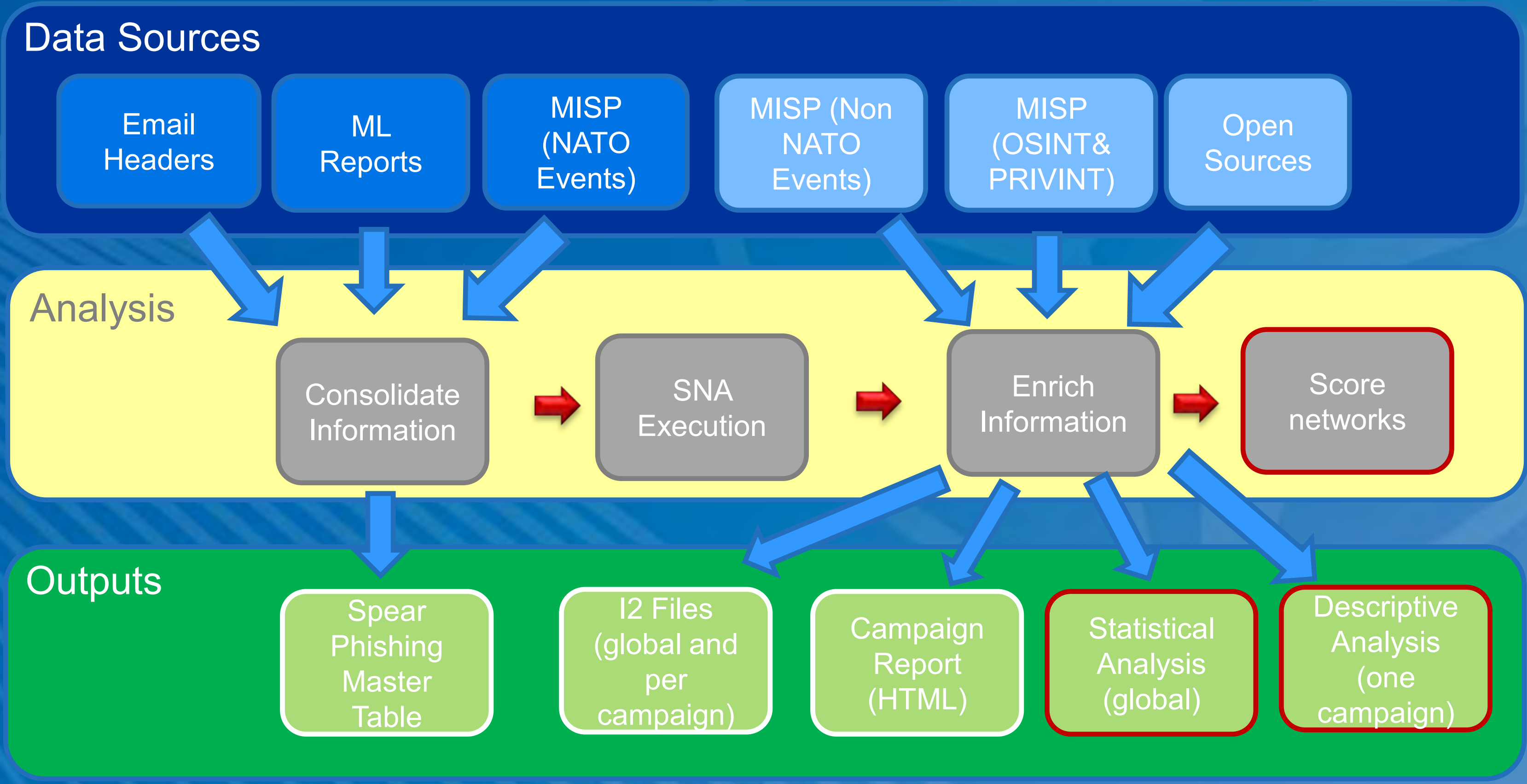
- “Know your enemy”: analyse and track activity overtime
- Automatic correlation affiliates the new events with past activities and correlates together new events for a bigger picture
- Helps in prioritisation: how to distinguish a targeted from a non targeted activity
- Reduces the time of analysis and helps the analyst to focus on the most relevant incidents

GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.
SLANE

CYBER DEFENCE
@EMERGING SECURITY
CHALLENGES DIVISION

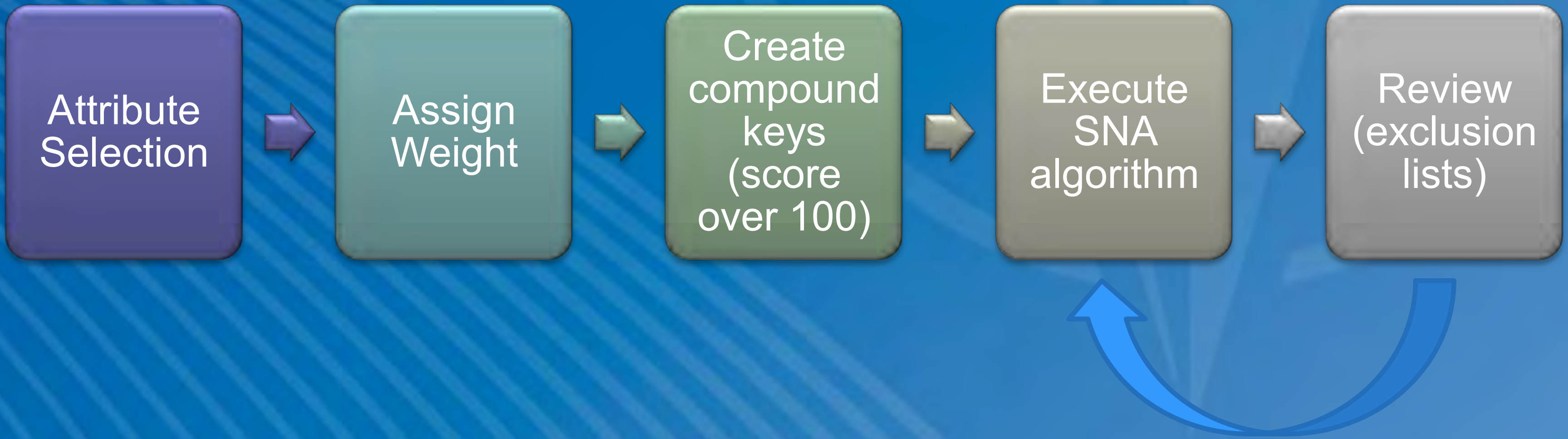
NATO
OTAN

# How do we do it?



# What is the logic?

- Two events are related when they share “enough similarities”
- Need to find the balance to avoid false positive and false negatives
- Examples: same malware family sent in an email with the same subject line and the same mailer, same C&C used in the same day in an email that belongs to the same “anomaly cluster”, etc.



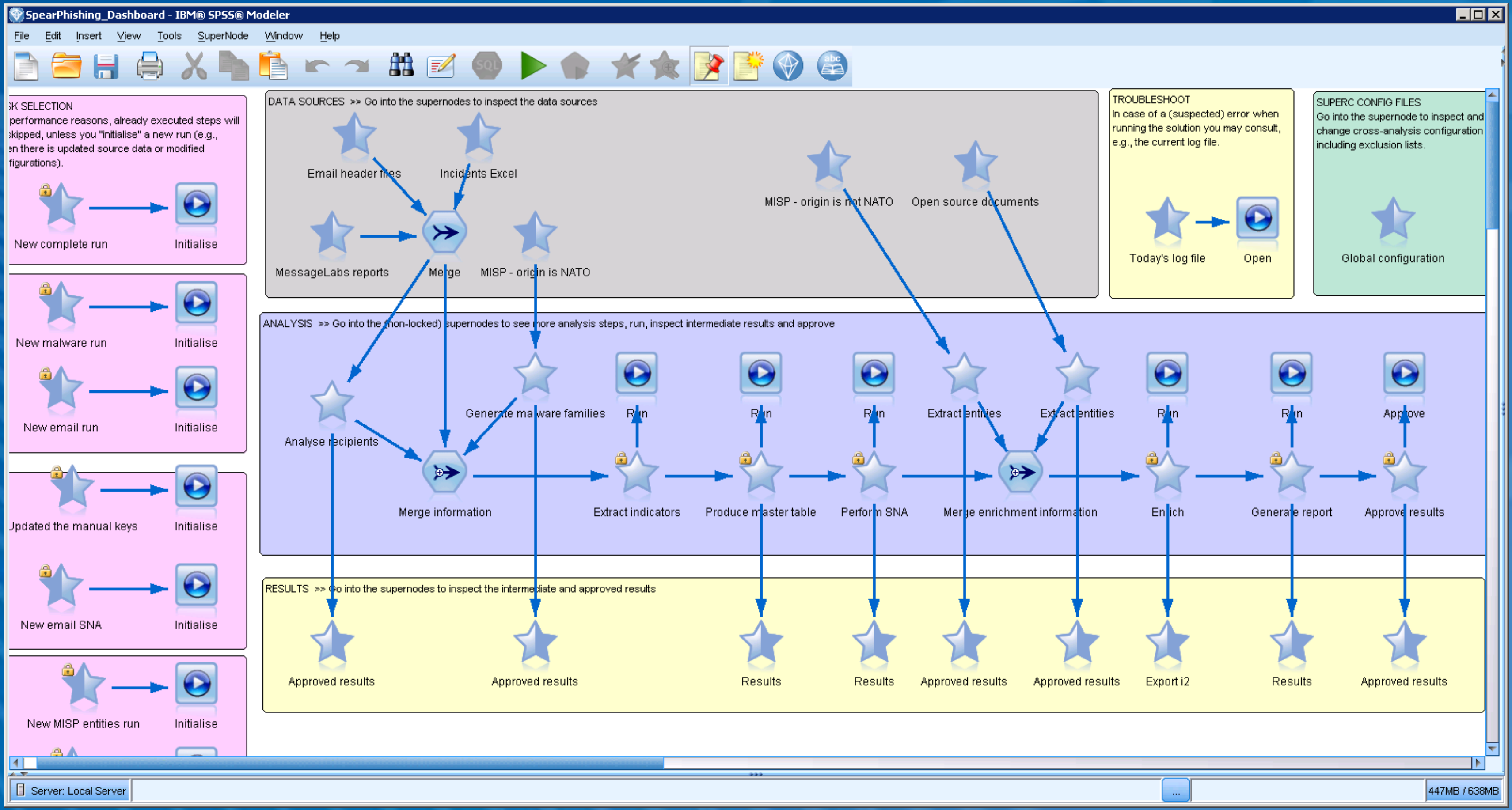
Attribute Selection → Assign Weight → Create compound keys (score over 100) → Execute SNA algorithm → Review (exclusion lists)

# Enrich information for affiliation

- Loose connection with open sources and other MISP tickets
- Text analytics that extracts IP addresses, domains and hashes from documents for correlation
- Need of an analyst that validates and affiliates the activity when unknown or validates the new connection made

SOMEONE SENT ME ANOTHER ANONYMOUS EMAIL WITH A LINK TO AN ARTICLE ABOUT THE WORLD'S WORST BOSSES.
Dilbert.com DilbertCartoonist@gmail.com
I GET ONE OF THOSE EMAILS EVERY TIME I LEAVE YOUR CUBICLE. DID YOU THINK I WOULDN'T NOTICE THE CORRELATION?
11-28-11 ©2011 Scott Adams, Inc./Dist. by Universal Uclick
CORRELATION DOES NOT IMPLY CAUSATION.
SLURP

# The implementation in SPSS



K SELECTION
performance reasons, already executed steps will kipped, unless you "initialise" a new run (e.g., en there is updated source data or modified figurations).

DATA SOURCES >> Go into the supernodes to inspect the data sources

TROUBLESHOOT
In case of a (suspected) error when running the solution you may consult, e.g., the current log file.

SUPERC CONFIG FILES
Go into the supernode to inspect and change cross-analysis configuration including exclusion lists.

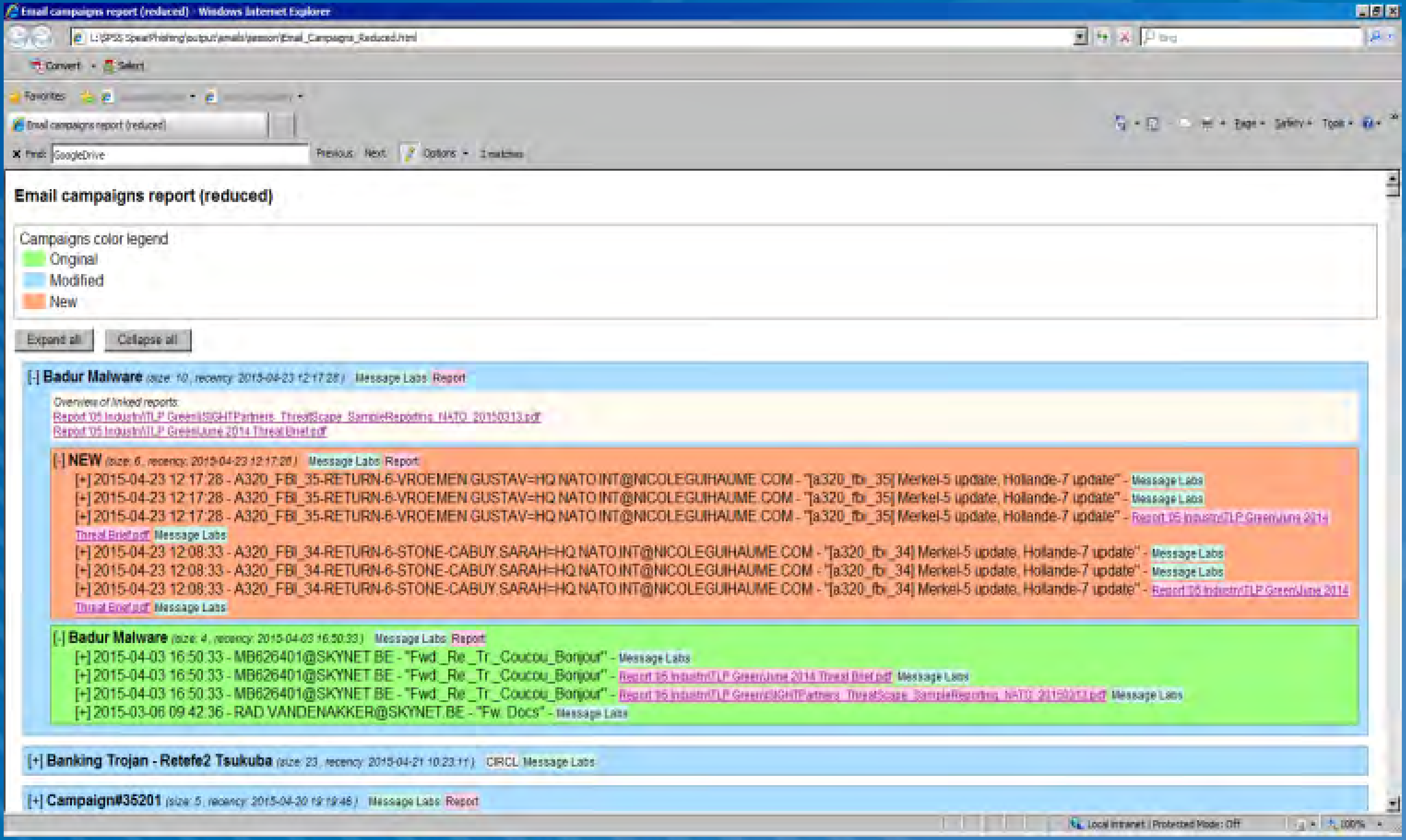
ANALYSIS >> Go into the (non-locked) supernodes to see more analysis steps, run, inspect intermediate results and approve

RESULTS >> Go into the supernodes to inspect the intermediate and approved results

Server: Local Server

447MB / 638MB

# Output Examples


Email campaigns report (reduced) - Windows Internet Explorer
L:\SPSS\SpearPhishing\output\emails\session\Email_Campaigns_Reduced.html
Convert
Select
Favorites
Email campaigns report (reduced)
Page
Safety
Tools
Find: GoogleDrive
Previous
Next
Options
1 matches
Local intranet | Protected Mode: Off
100%

## Email campaigns report (reduced)

Campaigns color legend
🟩 Original
🟦 Modified
🟧 New

Expand all | Collapse all

[-] **Badur Malware** *(size: 10 , recency: 2015-04-23 12:17:28 )* Message Labs Report

*Overview of linked reports:*
Report '05 Industry\TLP Green\iSIGHTPartners_ThreatScape_SampleReporting_NATO_20150313.pdf
Report '05 Industry\TLP Green\June 2014 Threat Brief.pdf

[-] **NEW** *(size: 6 , recency: 2015-04-23 12:17:28 )* Message Labs Report

[+] 2015-04-23 12:17:28 - A320_FBI_35-RETURN-6-VROEMEN.GUSTAV=HQ.NATO.INT@NICOLEGUIHAUME.COM - "[a320_fbi_35] Merkel-5 update, Hollande-7 update" - Message Labs
[+] 2015-04-23 12:17:28 - A320_FBI_35-RETURN-6-VROEMEN.GUSTAV=HQ.NATO.INT@NICOLEGUIHAUME.COM - "[a320_fbi_35] Merkel-5 update, Hollande-7 update" - Message Labs
[+] 2015-04-23 12:17:28 - A320_FBI_35-RETURN-6-VROEMEN.GUSTAV=HQ.NATO.INT@NICOLEGUIHAUME.COM - "[a320_fbi_35] Merkel-5 update, Hollande-7 update" - Report '05 Industry\TLP Green\June 2014 Threat Brief.pdf Message Labs
[+] 2015-04-23 12:08:33 - A320_FBI_34-RETURN-6-STONE-CABUY.SARAH=HQ.NATO.INT@NICOLEGUIHAUME.COM - "[a320_fbi_34] Merkel-5 update, Hollande-7 update" - Message Labs
[+] 2015-04-23 12:08:33 - A320_FBI_34-RETURN-6-STONE-CABUY.SARAH=HQ.NATO.INT@NICOLEGUIHAUME.COM - "[a320_fbi_34] Merkel-5 update, Hollande-7 update" - Message Labs
[+] 2015-04-23 12:08:33 - A320_FBI_34-RETURN-6-STONE-CABUY.SARAH=HQ.NATO.INT@NICOLEGUIHAUME.COM - "[a320_fbi_34] Merkel-5 update, Hollande-7 update" - Report '05 Industry\TLP Green\June 2014 Threat Brief.pdf Message Labs

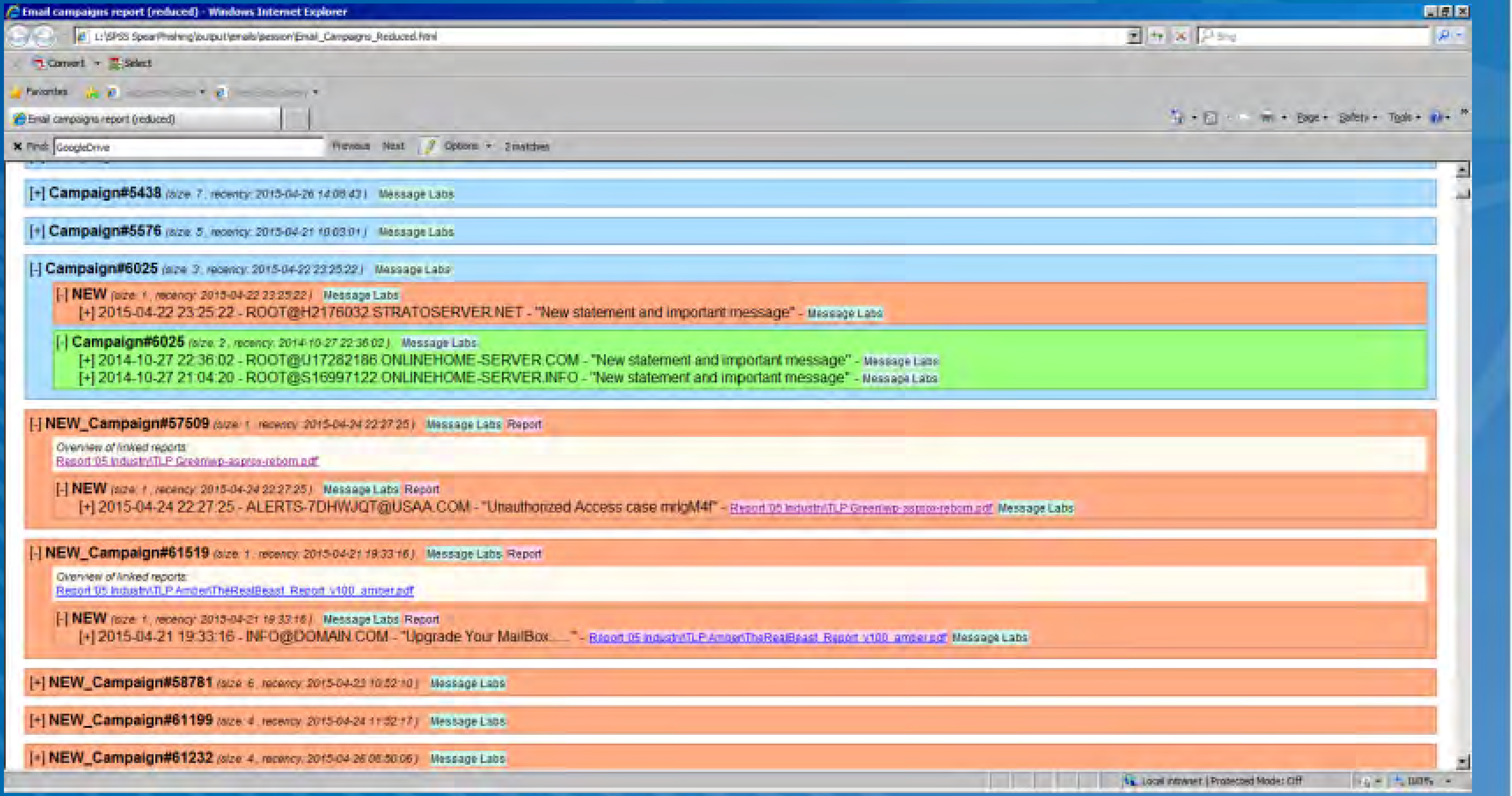
[-] **Badur Malware** *(size: 4 , recency: 2015-04-03 16:50:33 )* Message Labs Report

[+] 2015-04-03 16:50:33 - MB626401@SKYNET.BE - "Fwd_Re_Tr_Coucou_Bonjour" - Message Labs
[+] 2015-04-03 16:50:33 - MB626401@SKYNET.BE - "Fwd_Re_Tr_Coucou_Bonjour" - Report '05 Industry\TLP Green\June 2014 Threat Brief.pdf Message Labs
[+] 2015-04-03 16:50:33 - MB626401@SKYNET.BE - "Fwd_Re_Tr_Coucou_Bonjour" - Report '05 Industry\TLP Green\iSIGHTPartners_ThreatScape_SampleReporting_NATO_20150313.pdf Message Labs
[+] 2015-03-06 09:42:36 - RAD.VANDENAKKER@SKYNET.BE - "Fw: Docs" - Message Labs

[+] **Banking Trojan - Retefe2 Tsukuba** *(size: 23 , recency: 2015-04-21 10:23:11 )* CIRCL Message Labs

[+] **Campaign#35201** *(size: 5 , recency: 2015-04-20 19:19:46 )* Message Labs Report

# Output Examples



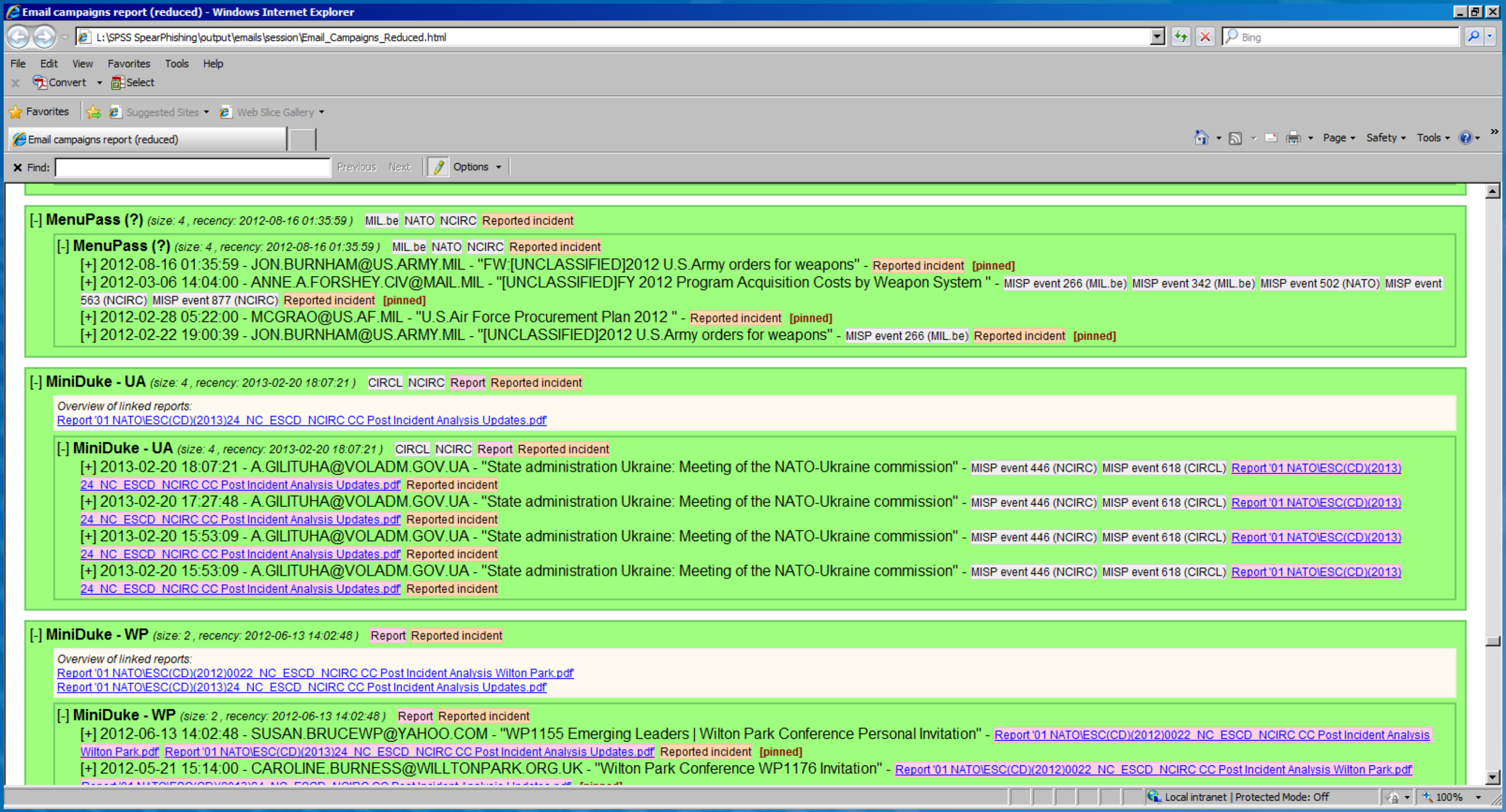
Email campaigns report (reduced) - Windows Internet Explorer

L:\SPSS SpearPhishing\output\emails\session\Email_Campaigns_Reduced.html

Find: GoogleDrive 2 matches

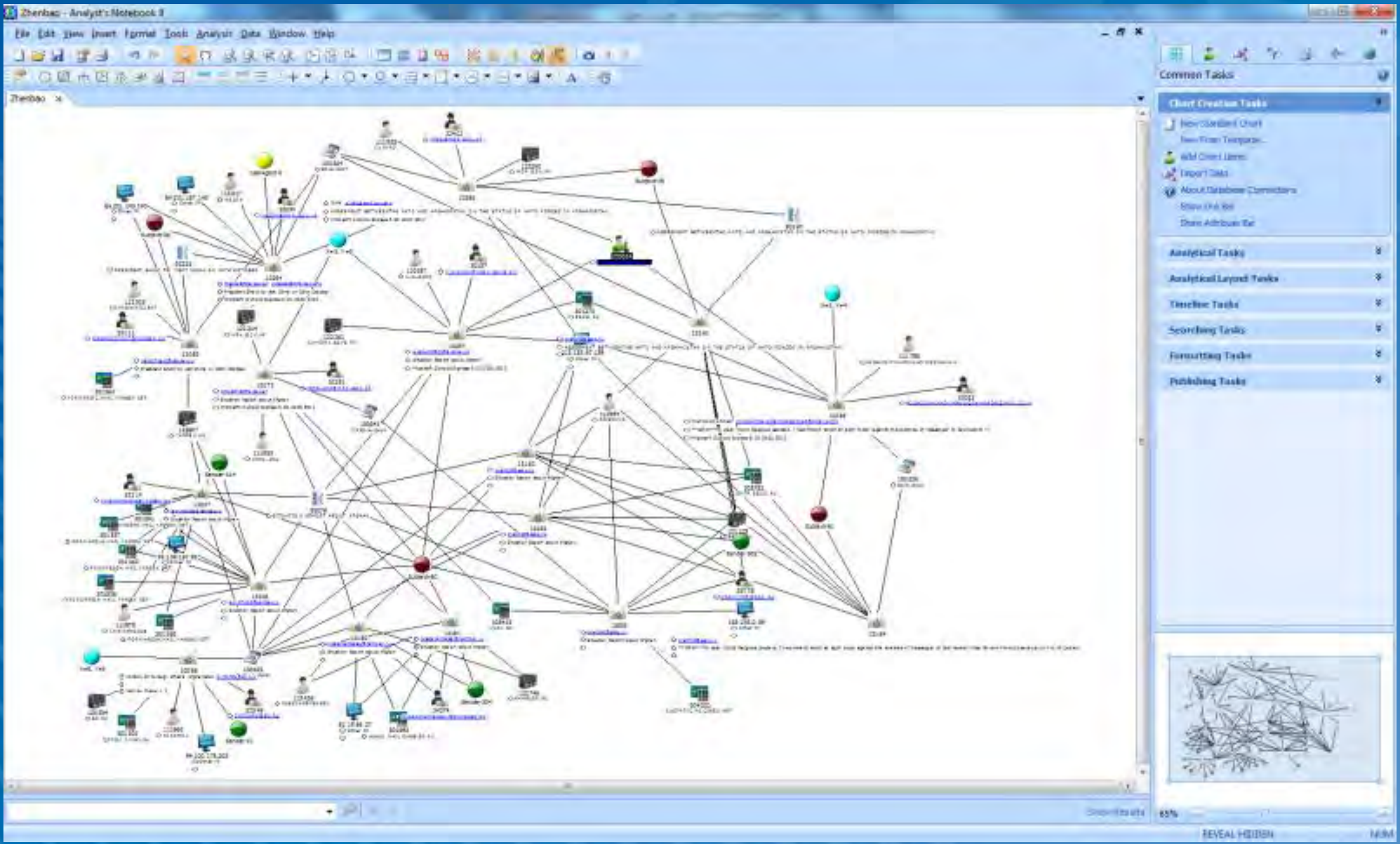
```
[+] Campaign#5438 (size: 7 , recency: 2015-04-26 14:08:43 )  Message Labs

[+] Campaign#5576 (size: 5 , recency: 2015-04-21 10:03:01 )  Message Labs

[-] Campaign#6025 (size: 3 , recency: 2015-04-22 23:25:22 )  Message Labs
    [-] NEW (size: 1 , recency: 2015-04-22 23:25:22 )  Message Labs
        [+] 2015-04-22 23:25:22 - ROOT@H2176032.STRATOSERVER.NET - "New statement and important message" - Message Labs
    [-] Campaign#6025 (size: 2 , recency: 2014-10-27 22:36:02 )  Message Labs
        [+] 2014-10-27 22:36:02 - ROOT@U17282186.ONLINEHOME-SERVER.COM - "New statement and important message" - Message Labs
        [+] 2014-10-27 21:04:20 - ROOT@S16997122.ONLINEHOME-SERVER.INFO - "New statement and important message" - Message Labs

[-] NEW_Campaign#57509 (size: 1 , recency: 2015-04-24 22:27:25 )  Message Labs Report
    Overview of linked reports:
    Report 05 Industry\TLP Green\wp-aspros-reborn.pdf
    [-] NEW (size: 1 , recency: 2015-04-24 22:27:25 )  Message Labs Report
        [+] 2015-04-24 22:27:25 - ALERTS-7DHWJQT@USAA.COM - "Unauthorized Access case mrlgM4f" - Report 05 Industry\TLP Green\wp-aspros-reborn.pdf Message Labs

[-] NEW_Campaign#61519 (size: 1 , recency: 2015-04-21 19:33:16 )  Message Labs Report
    Overview of linked reports:
    Report 05 Industry\TLP Amber\TheRealBeast_Report_v100_amber.pdf
    [-] NEW (size: 1 , recency: 2015-04-21 19:33:16 )  Message Labs Report
        [+] 2015-04-21 19:33:16 - INFO@DOMAIN.COM - "Upgrade Your MailBox......" - Report 05 Industry\TLP Amber\TheRealBeast_Report_v100_amber.pdf Message Labs

[+] NEW_Campaign#58781 (size: 6 , recency: 2015-04-23 10:52:10 )  Message Labs

[+] NEW_Campaign#61199 (size: 4 , recency: 2015-04-24 11:52:17 )  Message Labs

[+] NEW_Campaign#61232 (size: 4 , recency: 2015-04-26 06:50:06 )  Message Labs
```

# Output Examples

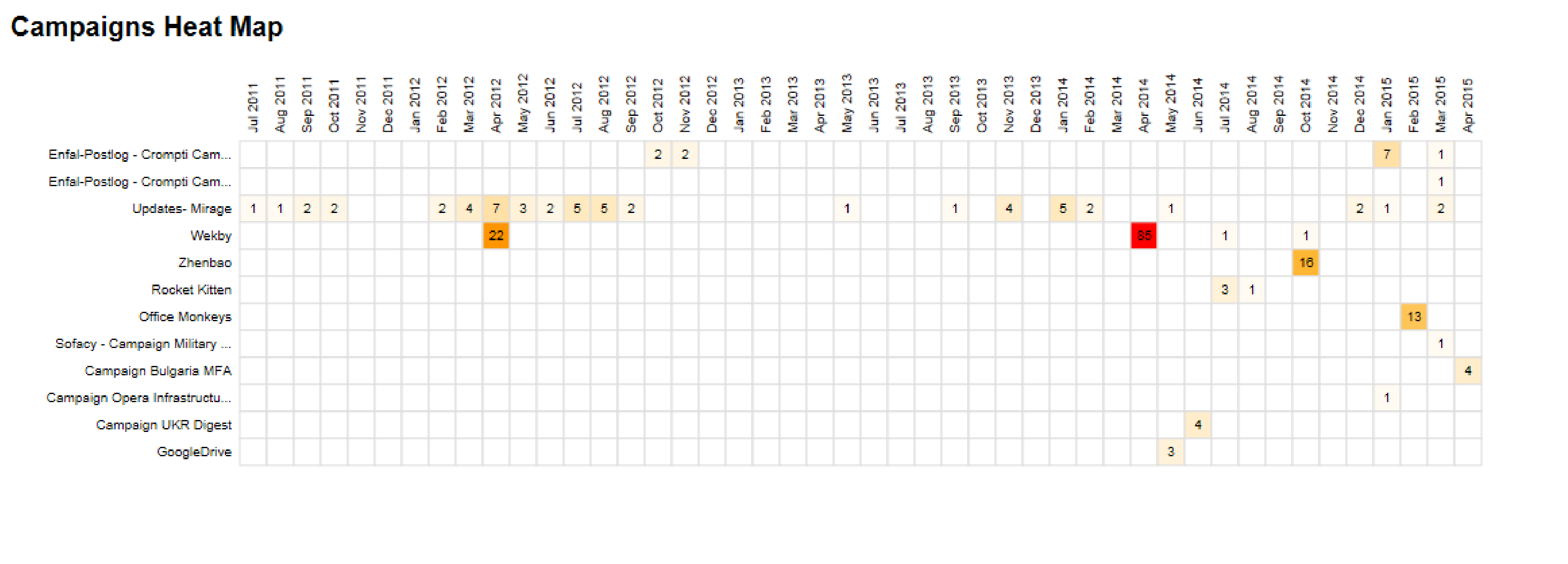

Email campaigns report (reduced) - Windows Internet Explorer
L:\SPSS SpearPhishing\output\emails\session\Email_Campaigns_Reduced.html
Bing
File Edit View Favorites Tools Help
Convert Select
Favorites Suggested Sites Web Slice Gallery
Email campaigns report (reduced)
Page Safety Tools
Find: Previous Next Options
Local intranet | Protected Mode: Off
100%

```
[-] MenuPass (?) (size: 4 , recency: 2012-08-16 01:35:59 )  MIL.be NATO NCIRC Reported incident
    [-] MenuPass (?) (size: 4 , recency: 2012-08-16 01:35:59 )  MIL.be NATO NCIRC Reported incident
        [+] 2012-08-16 01:35:59 - JON.BURNHAM@US.ARMY.MIL - "FW:[UNCLASSIFIED]2012 U.S.Army orders for weapons" - Reported incident [pinned]
        [+] 2012-03-06 14:04:00 - ANNE.A.FORSHEY.CIV@MAIL.MIL - "[UNCLASSIFIED]FY 2012 Program Acquisition Costs by Weapon System " - MISP event 266 (MIL.be) MISP event 342 (MIL.be) MISP event 502 (NATO) MISP event
        563 (NCIRC) MISP event 877 (NCIRC) Reported incident [pinned]
        [+] 2012-02-28 05:22:00 - MCGRAO@US.AF.MIL - "U.S.Air Force Procurement Plan 2012 " - Reported incident [pinned]
        [+] 2012-02-22 19:00:39 - JON.BURNHAM@US.ARMY.MIL - "[UNCLASSIFIED]2012 U.S.Army orders for weapons" - MISP event 266 (MIL.be) Reported incident [pinned]

[-] MiniDuke - UA (size: 4 , recency: 2013-02-20 18:07:21 )  CIRCL NCIRC Report Reported incident
    Overview of linked reports:
    Report '01 NATO\ESC(CD)(2013)24_NC_ESCD_NCIRC CC Post Incident Analysis Updates.pdf
    [-] MiniDuke - UA (size: 4 , recency: 2013-02-20 18:07:21 )  CIRCL NCIRC Report Reported incident
        [+] 2013-02-20 18:07:21 - A.GILITUHA@VOLADM.GOV.UA - "State administration Ukraine: Meeting of the NATO-Ukraine commission" - MISP event 446 (NCIRC) MISP event 618 (CIRCL) Report '01 NATO\ESC(CD)(2013)
        24_NC_ESCD_NCIRC CC Post Incident Analysis Updates.pdf Reported incident
        [+] 2013-02-20 17:27:48 - A.GILITUHA@VOLADM.GOV.UA - "State administration Ukraine: Meeting of the NATO-Ukraine commission" - MISP event 446 (NCIRC) MISP event 618 (CIRCL) Report '01 NATO\ESC(CD)(2013)
        24_NC_ESCD_NCIRC CC Post Incident Analysis Updates.pdf Reported incident
        [+] 2013-02-20 15:53:09 - A.GILITUHA@VOLADM.GOV.UA - "State administration Ukraine: Meeting of the NATO-Ukraine commission" - MISP event 446 (NCIRC) MISP event 618 (CIRCL) Report '01 NATO\ESC(CD)(2013)
        24_NC_ESCD_NCIRC CC Post Incident Analysis Updates.pdf Reported incident
        [+] 2013-02-20 15:53:09 - A.GILITUHA@VOLADM.GOV.UA - "State administration Ukraine: Meeting of the NATO-Ukraine commission" - MISP event 446 (NCIRC) MISP event 618 (CIRCL) Report '01 NATO\ESC(CD)(2013)
        24_NC_ESCD_NCIRC CC Post Incident Analysis Updates.pdf Reported incident

[-] MiniDuke - WP (size: 2 , recency: 2012-06-13 14:02:48 )  Report Reported incident
    Overview of linked reports:
    Report '01 NATO\ESC(CD)(2012)0022_NC_ESCD_NCIRC CC Post Incident Analysis Wilton Park.pdf
    Report '01 NATO\ESC(CD)(2013)24_NC_ESCD_NCIRC CC Post Incident Analysis Updates.pdf
    [-] MiniDuke - WP (size: 2 , recency: 2012-06-13 14:02:48 )  Report Reported incident
        [+] 2012-06-13 14:02:48 - SUSAN.BRUCEWP@YAHOO.COM - "WP1155 Emerging Leaders | Wilton Park Conference Personal Invitation" - Report '01 NATO\ESC(CD)(2012)0022_NC_ESCD_NCIRC CC Post Incident Analysis
        Wilton Park.pdf Report '01 NATO\ESC(CD)(2013)24_NC_ESCD_NCIRC CC Post Incident Analysis Updates.pdf Reported incident [pinned]
        [+] 2012-05-21 15:14:00 - CAROLINE.BURNESS@WILLTONPARK.ORG.UK - "Wilton Park Conference WP1176 Invitation" - Report '01 NATO\ESC(CD)(2012)0022_NC_ESCD_NCIRC CC Post Incident Analysis Wilton Park.pdf
```

# Output Examples



# Heatmaps 2014-2015

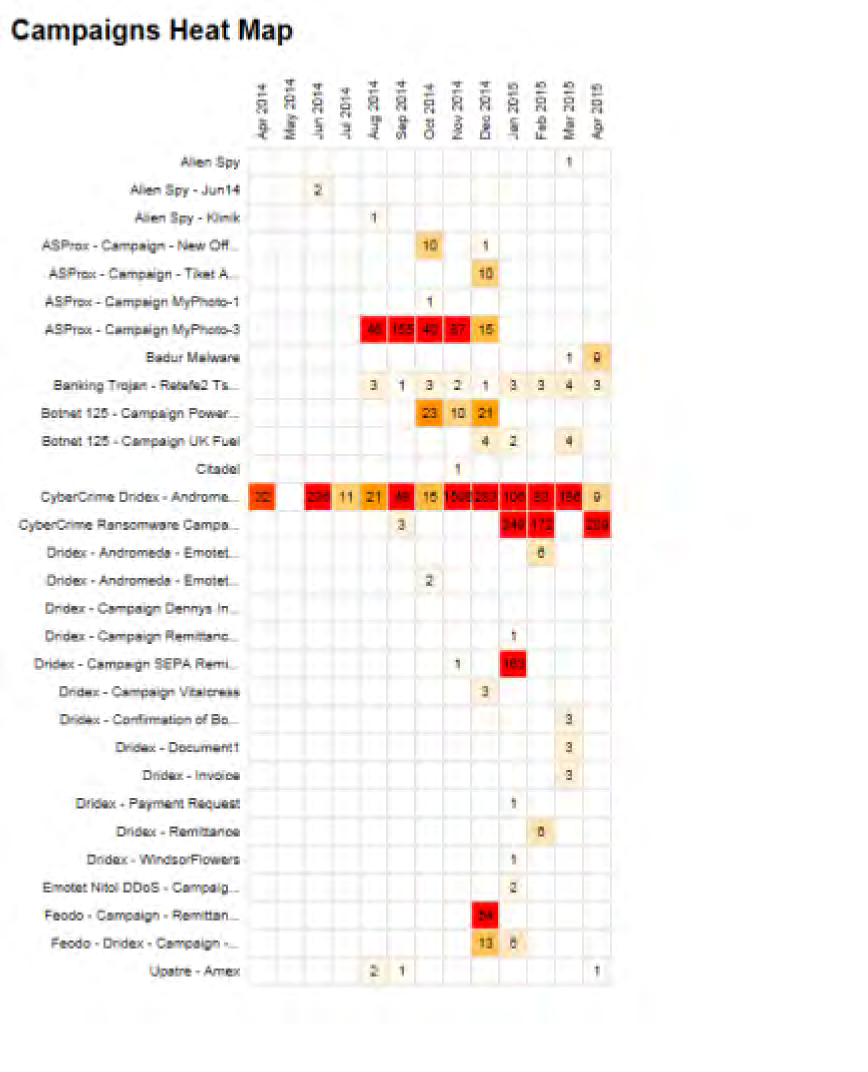


## Campaigns Heat Map

| | Jul 2011 | Aug 2011 | Sep 2011 | Oct 2011 | Nov 2011 | Dec 2011 | Jan 2012 | Feb 2012 | Mar 2012 | Apr 2012 | May 2012 | Jun 2012 | Jul 2012 | Aug 2012 | Sep 2012 | Oct 2012 | Nov 2012 | Dec 2012 | Jan 2013 | Feb 2013 | Mar 2013 | Apr 2013 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Enfal-Postlog - Crompti Cam... | | | | | | | | | | | | | | | | 2 | 2 | | | | | |
| Enfal-Postlog - Crompti Cam... | | | | | | | | | | | | | | | | | | | | | | |
| Updates- Mirage | 1 | 1 | 2 | 2 | | | | 2 | 4 | 7 | 3 | 2 | 5 | 5 | 2 | | | | | | | |
| Wekby | | | | | | | | | | 22 | | | | | | | | | | | | |
| Zhenbao | | | | | | | | | | | | | | | | | | | | | | |
| Rocket Kitten | | | | | | | | | | | | | | | | | | | | | | |
| Office Monkeys | | | | | | | | | | | | | | | | | | | | | | |
| Sofacy - Campaign Military ... | | | | | | | | | | | | | | | | | | | | | | |
| Campaign Bulgaria MFA | | | | | | | | | | | | | | | | | | | | | | |
| Campaign Opera Infrastructu... | | | | | | | | | | | | | | | | | | | | | | |
| Campaign UKR Digest | | | | | | | | | | | | | | | | | | | | | | |
| GoogleDrive | | | | | | | | | | | | | | | | | | | | | | |

| | May 2013 | Jun 2013 | Jul 2013 | Aug 2013 | Sep 2013 | Oct 2013 | Nov 2013 | Dec 2013 | Jan 2014 | Feb 2014 | Mar 2014 | Apr 2014 | May 2014 | Jun 2014 | Jul 2014 | Aug 2014 | Sep 2014 | Oct 2014 | Nov 2014 | Dec 2014 | Jan 2015 | Feb 2015 | Mar 2015 | Apr 2015 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Enfal-Postlog - Crompti Cam... | | | | | | | | | | | | | | | | | | | | | 7 | | 1 | |
| Enfal-Postlog - Crompti Cam... | | | | | | | | | | | | | | | | | | | | | | | 1 | |
| Updates- Mirage | 1 | | | | 1 | | 4 | | 5 | 2 | | | 1 | | | | | | | 2 | 1 | | 2 | |
| Wekby | | | | | | | | | | | | 85 | | | 1 | | | 1 | | | | | | |
| Zhenbao | | | | | | | | | | | | | | | | | | 16 | | | | | | |
| Rocket Kitten | | | | | | | | | | | | | | | 3 | 1 | | | | | | | | |
| Office Monkeys | | | | | | | | | | | | | | | | | | | | | | 13 | | |
| Sofacy - Campaign Military ... | | | | | | | | | | | | | | | | | | | | | | | 1 | |
| Campaign Bulgaria MFA | | | | | | | | | | | | | | | | | | | | | | | | 4 |
| Campaign Opera Infrastructu... | | | | | | | | | | | | | | | | | | | | | 1 | | | |
| Campaign UKR Digest | | | | | | | | | | | | | | 4 | | | | | | | | | | |
| GoogleDrive | | | | | | | | | | | | | 3 | | | | | | | | | | | |

# Heatmaps 2014-2015

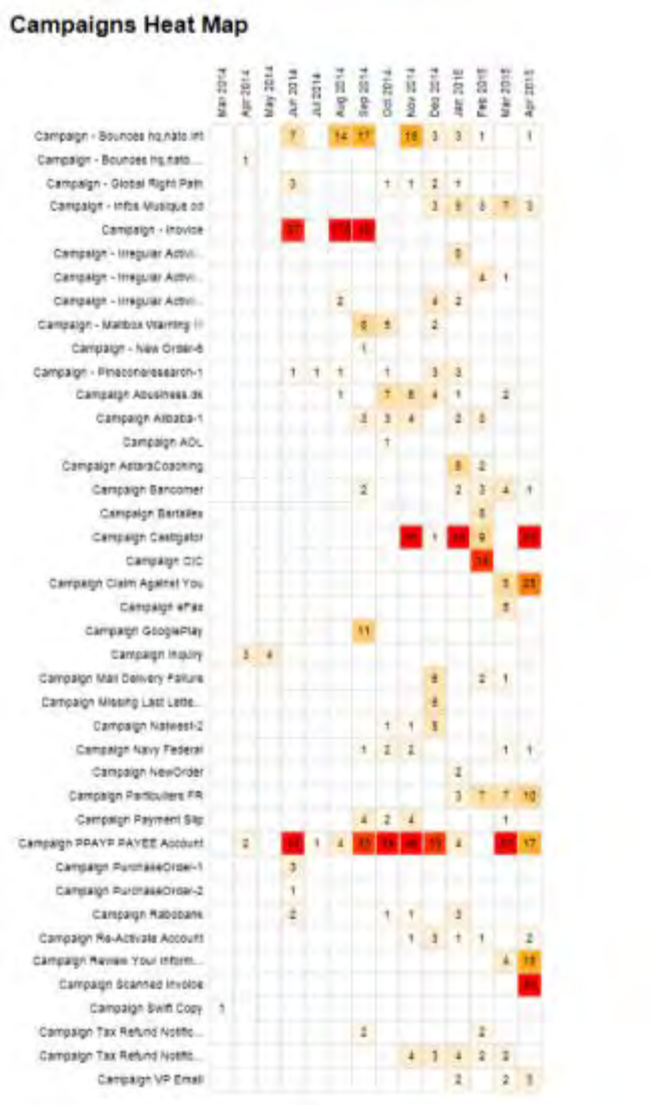


## Campaigns Heat Map

| | Apr 2014 | May 2014 | Jun 2014 | Jul 2014 | Aug 2014 | Sep 2014 | Oct 2014 | Nov 2014 | Dec 2014 | Jan 2015 | Feb 2015 | Mar 2015 | Apr 2015 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alien Spy | | | | | | | | | | | | 1 | |
| Alien Spy - Jun14 | | | 2 | | | | | | | | | | |
| Alien Spy - Klinik | | | | | 1 | | | | | | | | |
| ASProx - Campaign - New Off... | | | | | | | 10 | | 1 | | | | |
| ASProx - Campaign - Tiket A... | | | | | | | | | 10 | | | | |
| ASProx - Campaign MyPhoto-1 | | | | | | | 1 | | | | | | |
| ASProx - Campaign MyPhoto-3 | | | | | 46 | 155 | 40 | 87 | 15 | | | | |
| Badur Malware | | | | | | | | | | | | 1 | 9 |
| Banking Trojan - Retefe2 Ts... | | | | | 3 | 1 | 3 | 2 | 1 | 3 | 3 | 4 | 3 |
| Botnet 125 - Campaign Power... | | | | | | | 23 | 10 | 21 | | | | |
| Botnet 125 - Campaign UK Fuel | | | | | | | | | 4 | 2 | | 4 | |
| Citadel | | | | | | | | 1 | | | | | |
| CyberCrime Dridex - Androme... | 32 | | 226 | 11 | 21 | 48 | 15 | 1508 | 283 | 106 | 83 | 186 | 9 |
| CyberCrime Ransomware Campa... | | | | | | 3 | | | | 249 | 172 | | 229 |
| Dridex - Andromeda - Emotet... | | | | | | | | | | | 6 | | |
| Dridex - Andromeda - Emotet... | | | | | | | 2 | | | | | | |
| Dridex - Campaign Dennys In... | | | | | | | | | | | | | |
| Dridex - Campaign Remittanc... | | | | | | | | | | 1 | | | |
| Dridex - Campaign SEPA Remi... | | | | | | | | 1 | | 163 | | | |
| Dridex - Campaign Vitalcress | | | | | | | | | 3 | | | | |
| Dridex - Confirmation of Bo... | | | | | | | | | | | | 3 | |
| Dridex - Document1 | | | | | | | | | | | | 3 | |
| Dridex - Invoice | | | | | | | | | | | | 3 | |
| Dridex - Payment Request | | | | | | | | | | 1 | | | |
| Dridex - Remittance | | | | | | | | | | | 6 | | |
| Dridex - WindsorFlowers | | | | | | | | | | 1 | | | |
| Emotet Nitol DDoS - Campaig... | | | | | | | | | | 2 | | | |
| Feodo - Campaign - Remittan... | | | | | | | | | 58 | | | | |
| Feodo - Dridex - Campaign -... | | | | | | | | | 13 | 6 | | | |
| Upatre - Amex | | | | | 2 | 1 | | | | | | | 1 |

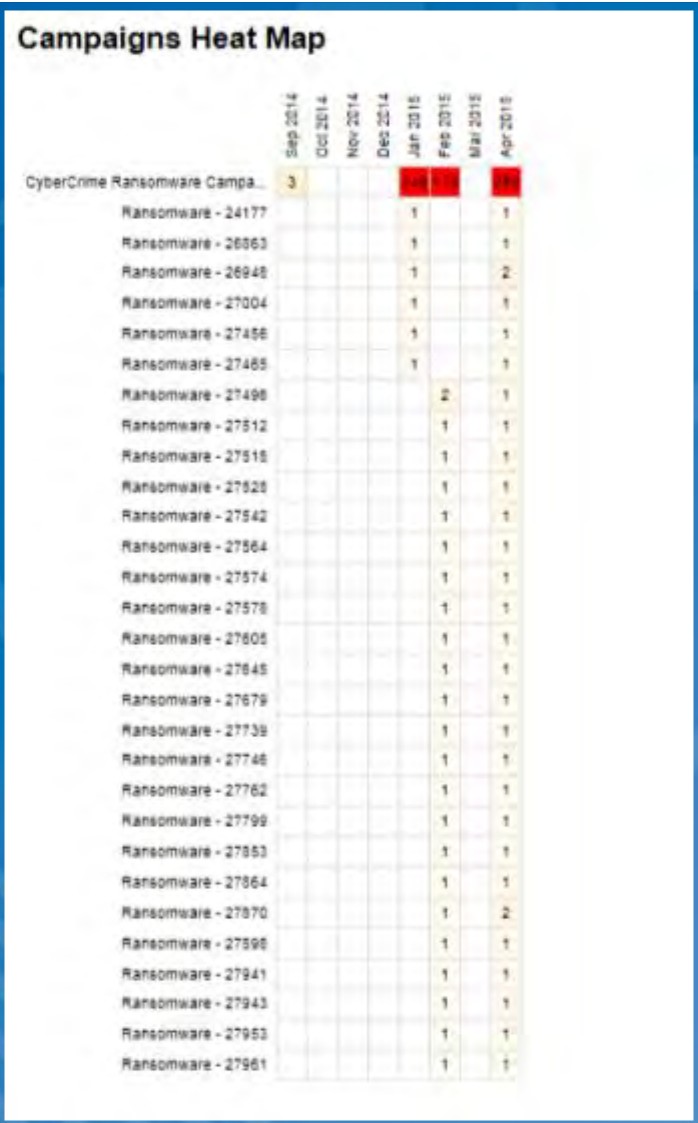
]

# Heatmaps 2014-2015



## Campaigns Heat Map

| | Mar 2014 | Apr 2014 | May 2014 | Jun 2014 | Jul 2014 | Aug 2014 | Sep 2014 | Oct 2014 | Nov 2014 | Dec 2014 | Jan 2015 | Feb 2015 | Mar 2015 | Apr 2015 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Campaign - Bounces hq.nato.int | | | | 7 | | 14 | 17 | | 18 | 3 | 3 | 1 | | 1 |
| Campaign - Bounces hq.nato.... | | 1 | | | | | | | | | | | | |
| Campaign - Global Right Path | | | | 3 | | | | 1 | 1 | 2 | 1 | | | |
| Campaign - Infos Musique.od | | | | | | | | | | 3 | 9 | 5 | 7 | 3 |
| Campaign - Invoice | | | | [illegible] | | [illegible] | [illegible] | | | | | | | |
| Campaign - Irregular Activi... | | | | | | | | | | | 5 | | | |
| Campaign - Irregular Activi... | | | | | | | | | | | | 4 | 1 | |
| Campaign - Irregular Activi... | | | | | | 2 | | | | 4 | 2 | | | |
| Campaign - Mailbox Warning !! | | | | | | | 6 | 5 | | 2 | | | | |
| Campaign - New Order-6 | | | | | | | 1 | | | | | | | |
| Campaign - Pineconeresearch-1 | | | | 1 | 1 | 1 | | 1 | | 3 | 3 | | | |
| Campaign Abusiness.dk | | | | | | 1 | | 7 | 8 | 4 | 1 | | 2 | |
| Campaign Alibaba-1 | | | | | | | 3 | 3 | 4 | | 2 | 3 | | |
| Campaign AOL | | | | | | | | 1 | | | | | | |
| Campaign AstaraCoaching | | | | | | | | | | | 8 | 2 | | |
| Campaign Bancomer | | | | | | | 2 | | | | 2 | 3 | 4 | 1 |
| Campaign Bertalles | | | | | | | | | | | | 5 | | |
| Campaign Castigator | | | | | | | | | [illegible] | 1 | [illegible] | 9 | | [illegible] |
| Campaign CIC | | | | | | | | | | | | 14 | | |
| Campaign Claim Against You | | | | | | | | | | | | | 3 | 25 |
| Campaign eFax | | | | | | | | | | | | | 5 | |
| Campaign GooglePlay | | | | | | | 11 | | | | | | | |
| Campaign Inquiry | | 3 | 4 | | | | | | | | | | | |
| Campaign Mail Delivery Failure | | | | | | | | | | 8 | | 2 | 1 | |
| Campaign Missing Last Lette... | | | | | | | | | | 6 | | | | |
| Campaign Natwest-2 | | | | | | | | 1 | 1 | 5 | | | | |
| Campaign Navy Federal | | | | | | | 1 | 2 | 2 | | | | 1 | 1 |
| Campaign NewOrder | | | | | | | | | | | 2 | | | |
| Campaign Particuliers FR | | | | | | | | | | | 3 | 7 | 7 | 10 |
| Campaign Payment Slip | | | | | | | 4 | 2 | 4 | | | | 1 | |
| Campaign PRAYP PAYEE Account | | 2 | | [illegible] | 1 | 4 | [illegible] | [illegible] | [illegible] | [illegible] | 4 | | [illegible] | 17 |
| Campaign PurchaseOrder-1 | | | | 3 | | | | | | | | | | |
| Campaign PurchaseOrder-2 | | | | 1 | | | | | | | | | | |
| Campaign Rabobank | | | | 2 | | | | 1 | 1 | | 3 | | | |
| Campaign Re-Activate Account | | | | | | | | | 1 | 3 | 1 | 1 | | 2 |
| Campaign Review Your Inform... | | | | | | | | | | | | | 4 | 11 |
| Campaign Scanned Invoice | | | | | | | | | | | | | | [illegible] |
| Campaign Swift Copy | 1 | | | | | | | | | | | | | |
| Campaign Tax Refund Notific... | | | | | | | 2 | | | | | 2 | | |
| Campaign Tax Refund Notific... | | | | | | | | | 4 | 1 | 4 | 2 | 3 | |
| Campaign VP Email | | | | | | | | | | | 2 | | 2 | 3 |



## Campaigns Heat Map

| | Sep 2014 | Oct 2014 | Nov 2014 | Dec 2014 | Jan 2015 | Feb 2015 | Mar 2015 | Apr 2015 |
|---|---|---|---|---|---|---|---|---|
| CyberCrime Ransomware Campa... | 3 | | | | [illegible] | [illegible] | | [illegible] |
| Ransomware - 24177 | | | | | 1 | | | 1 |
| Ransomware - 26863 | | | | | 1 | | | 1 |
| Ransomware - 26948 | | | | | 1 | | | 2 |
| Ransomware - 27004 | | | | | 1 | | | 1 |
| Ransomware - 27456 | | | | | 1 | | | 1 |
| Ransomware - 27465 | | | | | 1 | | | 1 |
| Ransomware - 27498 | | | | | | 2 | | 1 |
| Ransomware - 27512 | | | | | | 1 | | 1 |
| Ransomware - 27515 | | | | | | 1 | | 1 |
| Ransomware - 27528 | | | | | | 1 | | 1 |
| Ransomware - 27542 | | | | | | 1 | | 1 |
| Ransomware - 27564 | | | | | | 1 | | 1 |
| Ransomware - 27574 | | | | | | 1 | | 1 |
| Ransomware - 27578 | | | | | | 1 | | 1 |
| Ransomware - 27605 | | | | | | 1 | | 1 |
| Ransomware - 27645 | | | | | | 1 | | 1 |
| Ransomware - 27679 | | | | | | 1 | | 1 |
| Ransomware - 27739 | | | | | | 1 | | 1 |
| Ransomware - 27746 | | | | | | 1 | | 1 |
| Ransomware - 27762 | | | | | | 1 | | 1 |
| Ransomware - 27799 | | | | | | 1 | | 1 |
| Ransomware - 27853 | | | | | | 1 | | 1 |
| Ransomware - 27864 | | | | | | 1 | | 1 |
| Ransomware - 27870 | | | | | | 1 | | 2 |
| Ransomware - 27898 | | | | | | 1 | | 1 |
| Ransomware - 27941 | | | | | | 1 | | 1 |
| Ransomware - 27943 | | | | | | 1 | | 1 |
| Ransomware - 27953 | | | | | | 1 | | 1 |
| Ransomware - 27961 | | | | | | 1 | | 1 |

# Future developments

- Prioritise which campaigns we should analyse
- Visualisation techniques
- Add non spear phishing events
- On-line service to query the campaigns
- Threat actors knowledge base

# Questions & Comments

**Thank you!!**