Kaspersky®

SECURITY
ANALYST
SUMMIT

DON'T PUSH THE BUTTON OR I WILL YARA YOU DOWN

Markus Neis

Swisscom

WHAT IS YARA?

Pattern matching engine

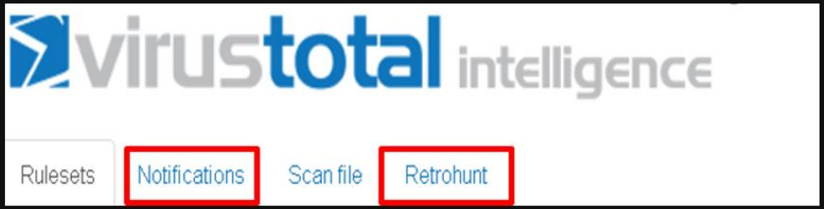
Patterns are defined inside of rules

Patterns are either Text, Hex or Regex

```
rule patterns:
{
        strings:
                $text_pattern = "mypattern"
                $hex_pattern = { E2 34 A1 C8 23 FB }
                $reg_pattern  = /[0-9a-zA-Z]{32}/

        condition:
                $text_pattern or $hex_pattern or $reg_pattern
}
```

YARA AND VIRUSTOTAL

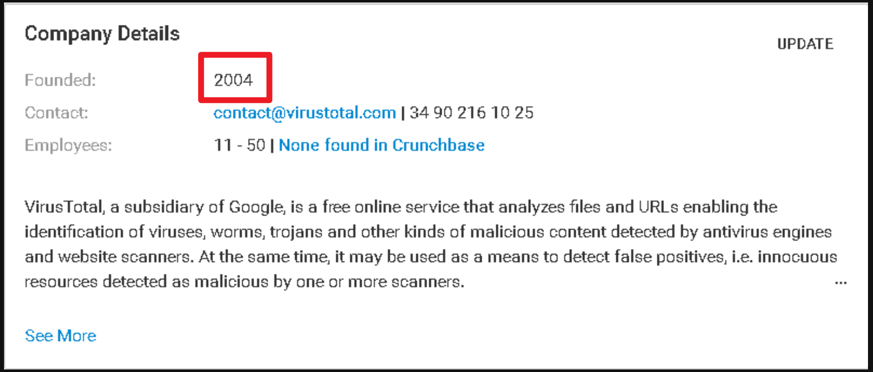


Notifications

- Realtime notification if file matches rule
- Up to 25 YARA rules

Retrohunt

- Goes back 3 months in time
- Maximum of 10.000 results



Company Details

UPDATE

Founded: 2004

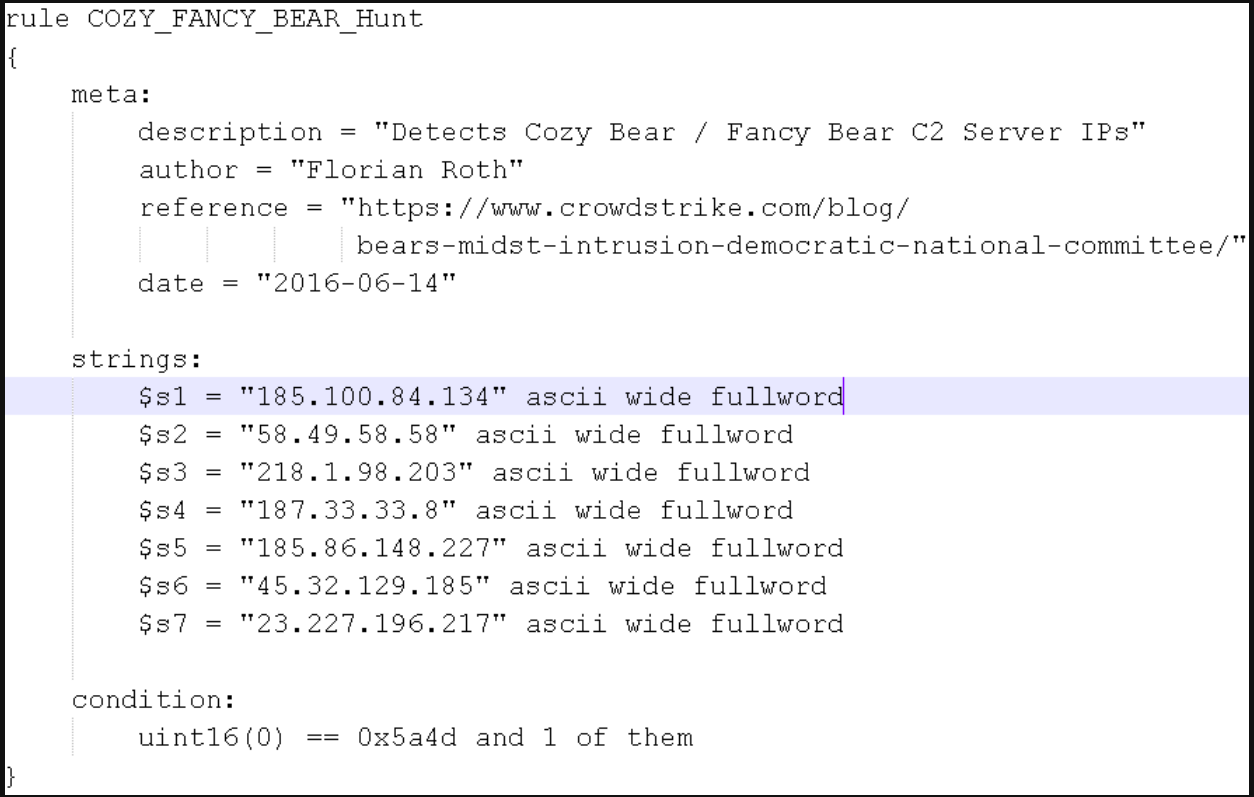
Contact: contact@virustotal.com | 34 90 216 10 25

Employees: 11 - 50 | None found in Crunchbase

VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. At the same time, it may be used as a means to detect false positives, i.e. innocuous resources detected as malicious by one or more scanners. ...

See More

YARA AND VIRUSTOTAL



```
rule COZY_FANCY_BEAR_Hunt
{
    meta:
        description = "Detects Cozy Bear / Fancy Bear C2 Server IPs"
        author = "Florian Roth"
        reference = "https://www.crowdstrike.com/blog/
                    bears-midst-intrusion-democratic-national-committee/"
        date = "2016-06-14"

    strings:
        $s1 = "185.100.84.134" ascii wide fullword
        $s2 = "58.49.58.58" ascii wide fullword
        $s3 = "218.1.98.203" ascii wide fullword
        $s4 = "187.33.33.8" ascii wide fullword
        $s5 = "185.86.148.227" ascii wide fullword
        $s6 = "45.32.129.185" ascii wide fullword
        $s7 = "23.227.196.217" ascii wide fullword

    condition:
        uint16(0) == 0x5a4d and 1 of them
}
```

Track

Malware Family

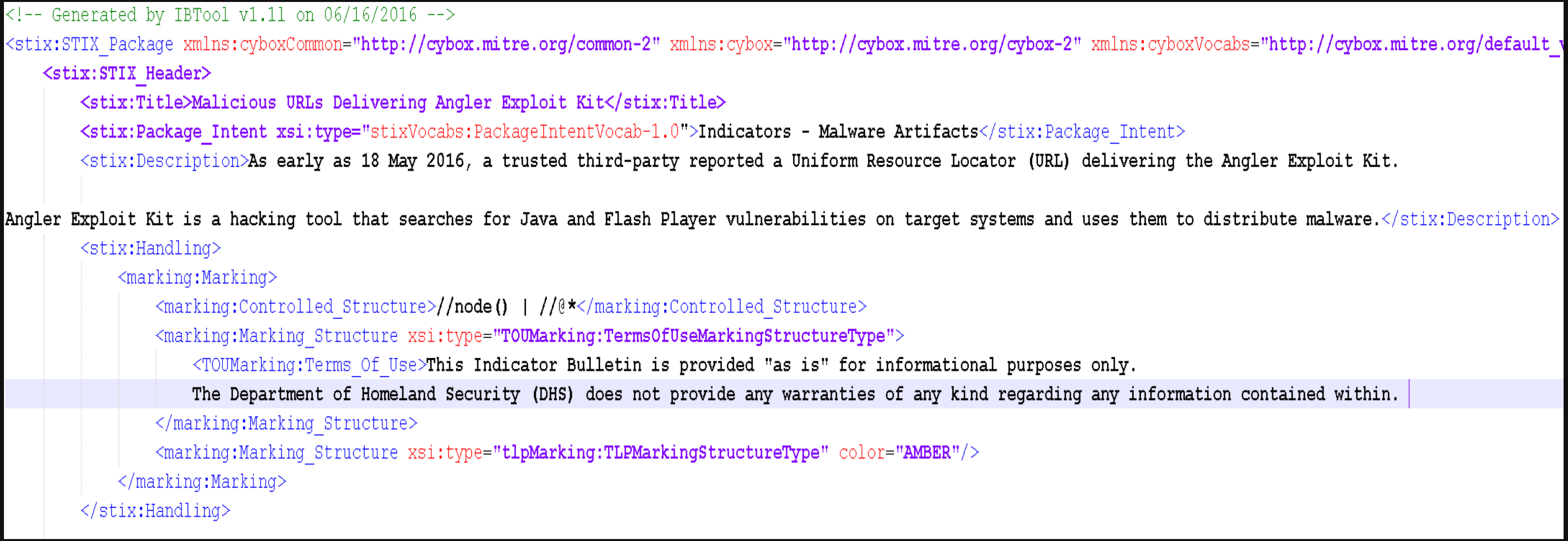
Threat Actors

GIVE ME INTEL

STIX

```
rule stix
{
    strings:
        $tlp = /TLP(\s*|:) (RED|AMBER|GREEN|WHITE)/ nocase ascii wide
        $stix = "tlpMarking:TLPMarkingStructureType" nocase ascii wide
    condition:
        $tlp and $stix
}
```

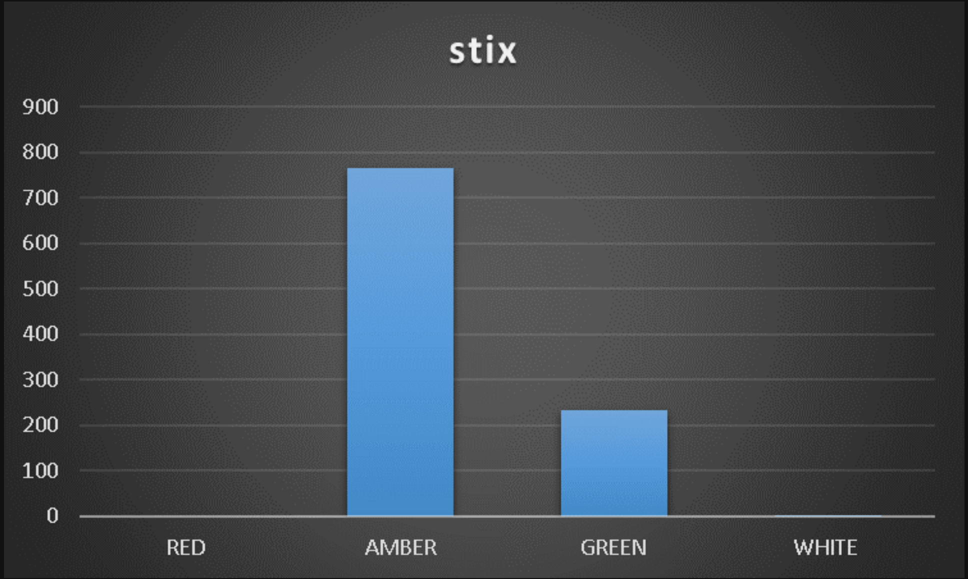
GIVE ME INTEL



```
<!-- Generated by IBTool v1.11 on 06/16/2016 -->
<stix:STIX_Package xmlns:cyboxCommon="http://cybox.mitre.org/common-2" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:cyboxVocabs="http://cybox.mitre.org/default_
    <stix:STIX_Header>
        <stix:Title>Malicious URLs Delivering Angler Exploit Kit</stix:Title>
        <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Malware Artifacts</stix:Package_Intent>
        <stix:Description>As early as 18 May 2016, a trusted third-party reported a Uniform Resource Locator (URL) delivering the Angler Exploit Kit.

Angler Exploit Kit is a hacking tool that searches for Java and Flash Player vulnerabilities on target systems and uses them to distribute malware.</stix:Description>
        <stix:Handling>
            <marking:Marking>
                <marking:Controlled_Structure>//node() | //@*</marking:Controlled_Structure>
                <marking:Marking_Structure xsi:type="TOUMarking:TermsOfUseMarkingStructureType">
                    <TOUMarking:Terms_Of_Use>This Indicator Bulletin is provided "as is" for informational purposes only.
                    The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within.
                </marking:Marking_Structure>
                <marking:Marking_Structure xsi:type="tlpMarking:TLPMarkingStructureType" color="AMBER"/>
            </marking:Marking>
        </stix:Handling>
```

GIVE ME INTEL



Retrohunt stix

~ 800 TLP Amber

~ 250 TLP Green

Almost all from DHL

Great for defensive purposes ☺

Attackers benefit too ☹

GIVE ME INTEL

Mandiant Schema

```
rule mandiant {
        strings:
                $schema = "schemas.mandiant.com" ascii nocase
        condition:
                $schema
}
```

Retrohunt mandiant

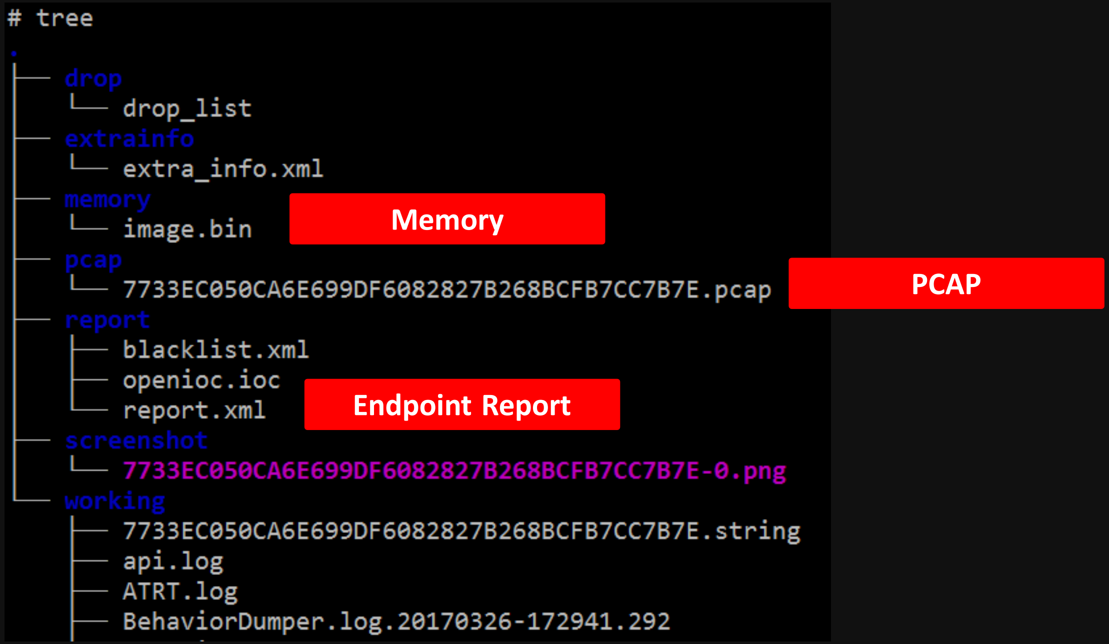
- 63 MIR Reports

MIR endpoint agent

- All the data from the endpoint

GIVE ME INTEL

Mandiant Intelligence Response (MIR) Namespace



```
# tree
.
├── drop
│   └── drop_list
├── extrainfo
│   └── extra_info.xml
├── memory
│   └── image.bin
├── pcap
│   └── 7733EC050CA6E699DF6082827B268BCFB7CC7B7E.pcap
├── report
│   ├── blacklist.xml
│   ├── openioc.ioc
│   └── report.xml
├── screenshot
│   └── 7733EC050CA6E699DF6082827B268BCFB7CC7B7E-0.png
└── working
    ├── 7733EC050CA6E699DF6082827B268BCFB7CC7B7E.string
    ├── api.log
    ├── ATRT.log
    ├── BehaviorDumper.log.20170326-172941.292
```

Retrohunt mandiant

Full Memory Dump

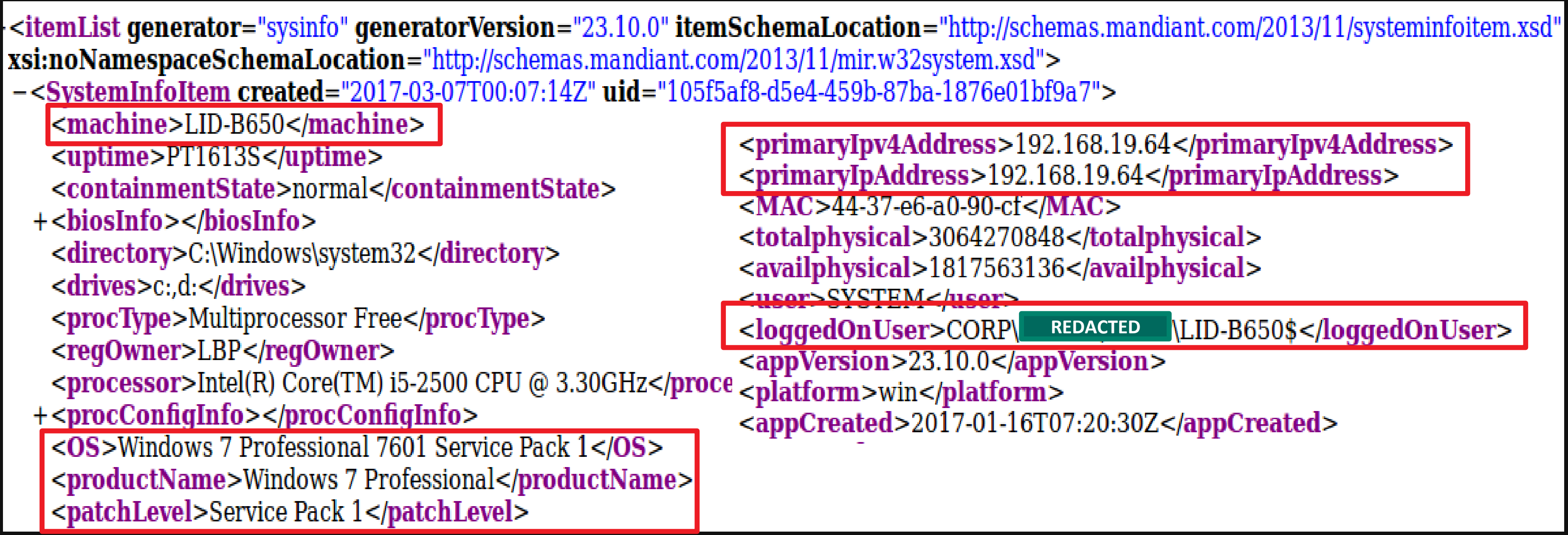
Network Traffic

Comprehensive Endpoint Report

GIVE ME INTEL

Mandiant Intelligence Response (MIR) Namespace

Retrohunt mandiant

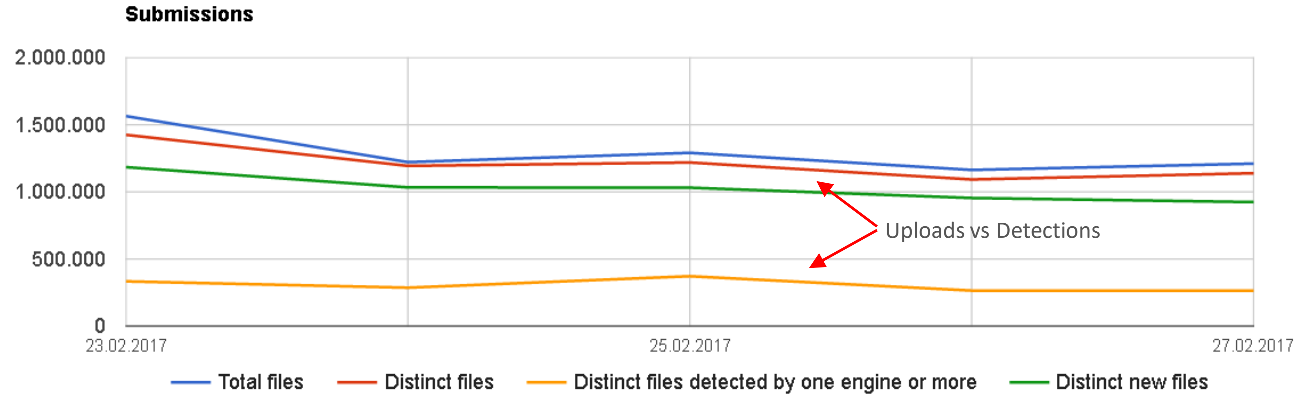


```
<itemList generator="sysinfo" generatorVersion="23.10.0" itemSchemaLocation="http://schemas.mandiant.com/2013/11/systeminfoitem.xsd"
xsi:noNamespaceSchemaLocation="http://schemas.mandiant.com/2013/11/mir.w32system.xsd">
 -<SystemInfoItem created="2017-03-07T00:07:14Z" uid="105f5af8-d5e4-459b-87ba-1876e01bf9a7">
    <machine>LID-B650</machine>
    <uptime>PT1613S</uptime>
    <containmentState>normal</containmentState>
  +<biosInfo></biosInfo>
    <directory>C:\Windows\system32</directory>
    <drives>c:,d:</drives>
    <procType>Multiprocessor Free</procType>
    <regOwner>LBP</regOwner>
    <processor>Intel(R) Core(TM) i5-2500 CPU @ 3.30GHz</proce
  +<procConfigInfo></procConfigInfo>
    <OS>Windows 7 Professional 7601 Service Pack 1</OS>
    <productName>Windows 7 Professional</productName>
    <patchLevel>Service Pack 1</patchLevel>

    <primaryIpv4Address>192.168.19.64</primaryIpv4Address>
    <primaryIpAddress>192.168.19.64</primaryIpAddress>
    <MAC>44-37-e6-a0-90-cf</MAC>
    <totalphysical>3064270848</totalphysical>
    <availphysical>1817563136</availphysical>
    <user>SYSTEM</user>
    <loggedOnUser>CORP\ REDACTED \LID-B650$</loggedOnUser>
    <appVersion>23.10.0</appVersion>
    <platform>win</platform>
    <appCreated>2017-01-16T07:20:30Z</appCreated>
```

WHAT ELSE IS THERE?

Huge Asymmetry between Uploads vs Detections



Uploads vs Detections

WHAT ELSE IS THERE?

Is there other data that is a threat to my organisation?

How do we transmit critical data ?

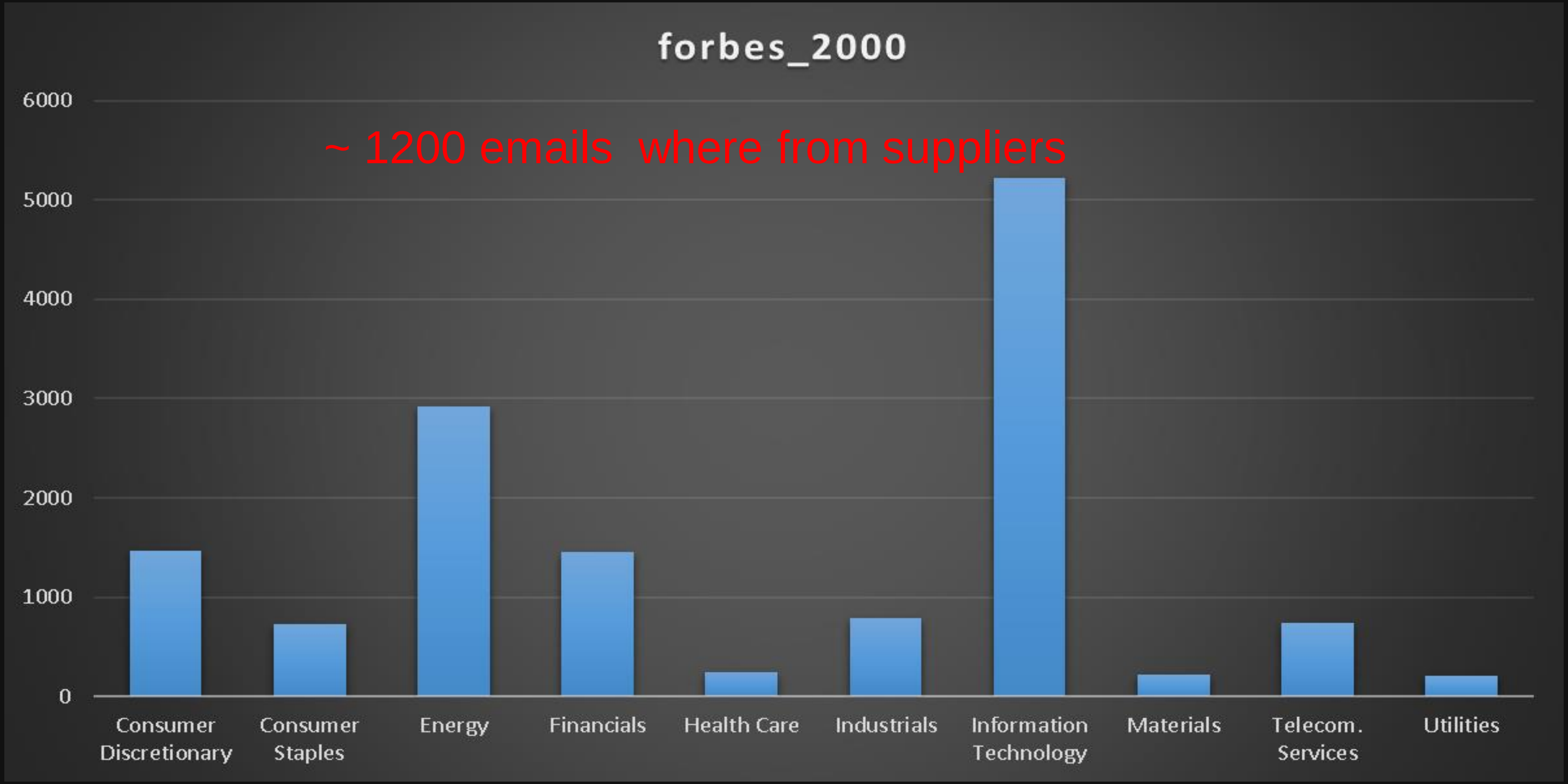
EMAIL

Forbes 2000 aka the worlds biggest companies

```
rule forbes_2000
{
strings:
        $from =   "From:" ascii wide nocase
        $subject = "Subject:" ascii wide nocase
        $forbes1 = "@americanexpress." ascii wide nocase
        $forbes2 = "@capitalone." ascii wide nocase
                                        ....
condition:
        $from and $subject and ( 1 of ($forbes*))

}
```

FORBES 2000 RETROHUNT BY SECTOR



~ 1200 emails where from suppliers

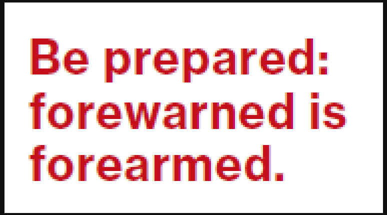
CREATIVITY IS THE LIMIT

```
rule email
{
        strings:
                $from =    "From:" ascii wide nocase
                $subject =  "Subject:" ascii wide nocase
                $domain1 = "<WHATEVER>" ascii wide nocase
                $domain2 = "<WHATEVER>" asciii wide nocase

        condition:
                $from and $subject and ( 1 of ($domain*))
}
```

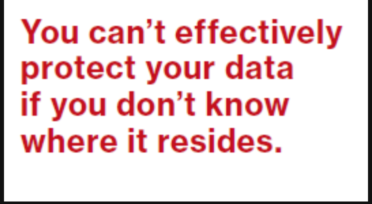
USE CASES FROM VERIZON DBIR 2016

Predicting Attacks



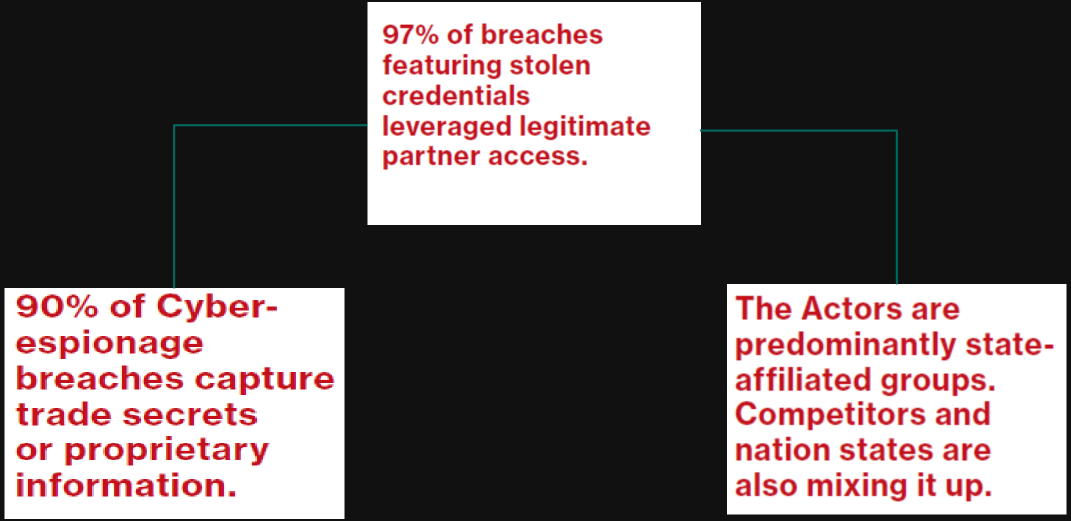
Be prepared: forewarned is forearmed.

Data Leakages



You can't effectively protect your data if you don't know where it resides.

Supply Chain and Espionage

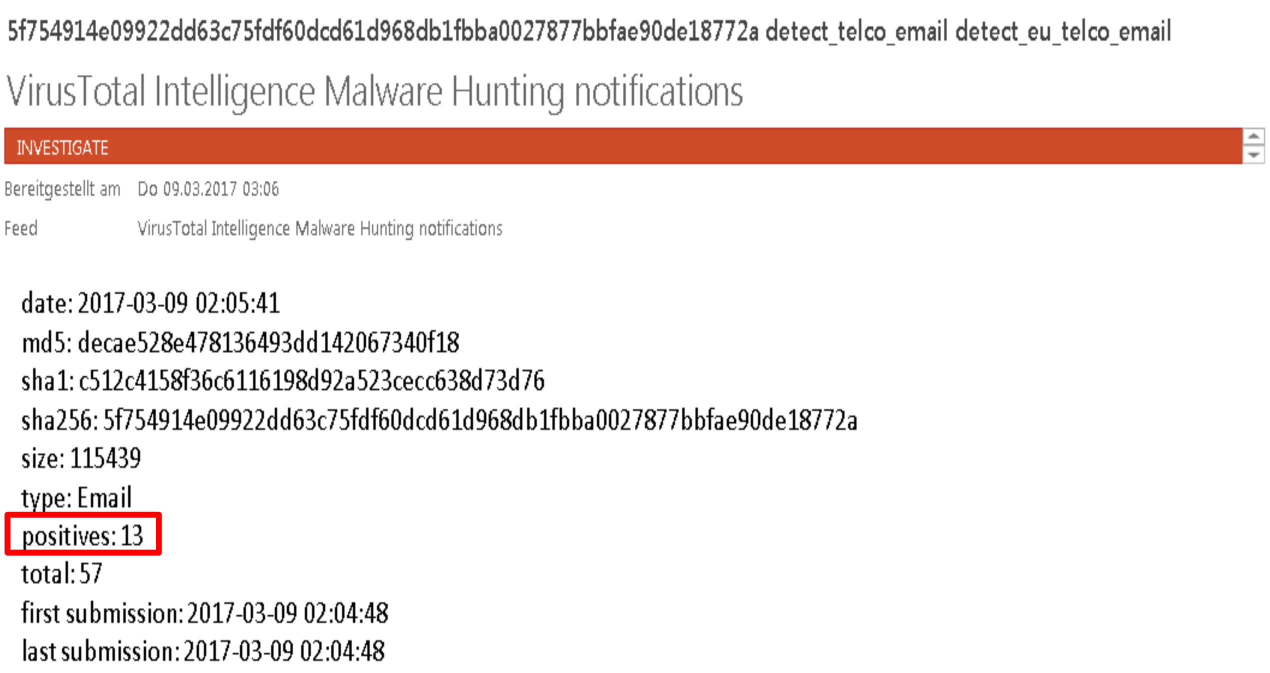


97% of breaches featuring stolen credentials leveraged legitimate partner access.

90% of Cyber-espionage breaches capture trade secrets or proprietary information.

The Actors are predominantly state-affiliated groups. Competitors and nation states are also mixing it up.

PREDICTING ATTACKS



5f754914e09922dd63c75fdf60dcd61d968db1fbba0027877bbfae90de18772a detect_telco_email detect_eu_telco_email

VirusTotal Intelligence Malware Hunting notifications

Bereitgestellt am Do 09.03.2017 03:06

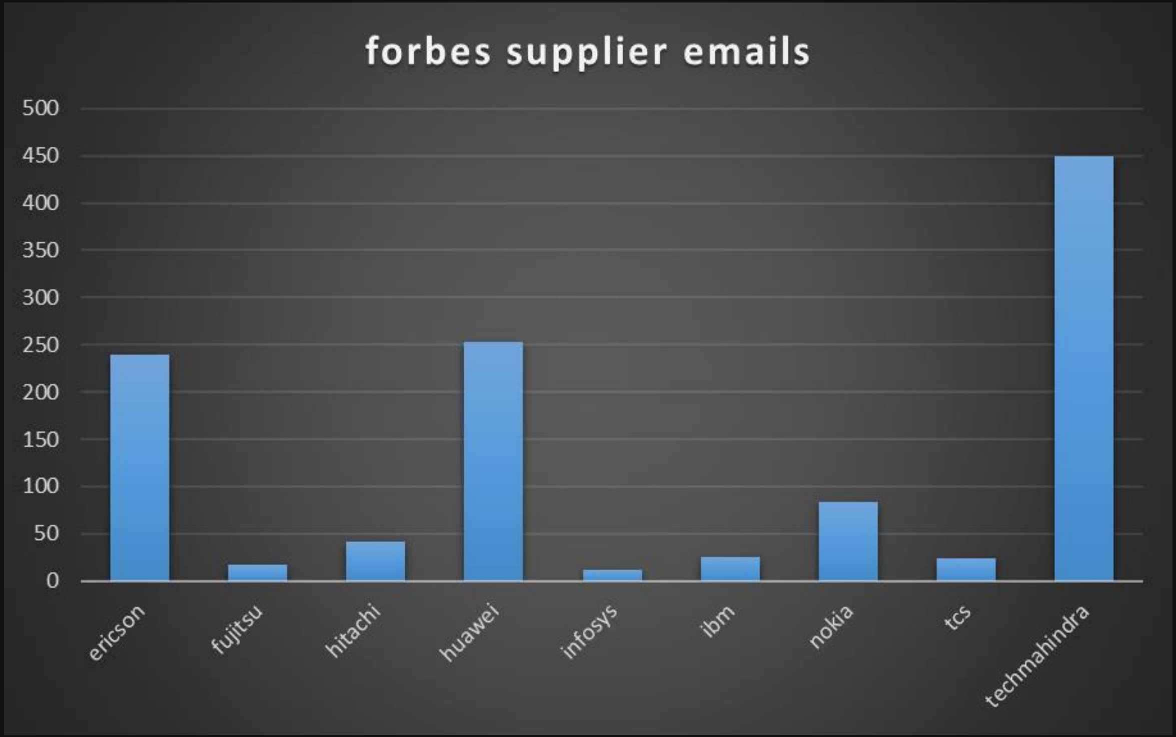
Feed VirusTotal Intelligence Malware Hunting notifications

```
date: 2017-03-09 02:05:41
md5: decae528e478136493dd142067340f18
sha1: c512c4158f36c6116198d92a523cecc638d73d76
sha256: 5f754914e09922dd63c75fdf60dcd61d968db1fbba0027877bbfae90de18772a
size: 115439
type: Email
positives: 13
total: 57
first submission: 2017-03-09 02:04:48
last submission: 2017-03-09 02:04:48
```

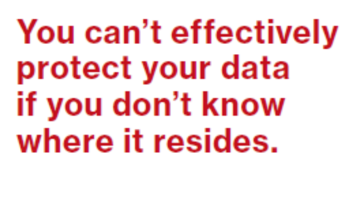
What affects our industry?

Be prepared: forewarned is forearmed.

SUPPLY CHAIN INTELLIGENCE

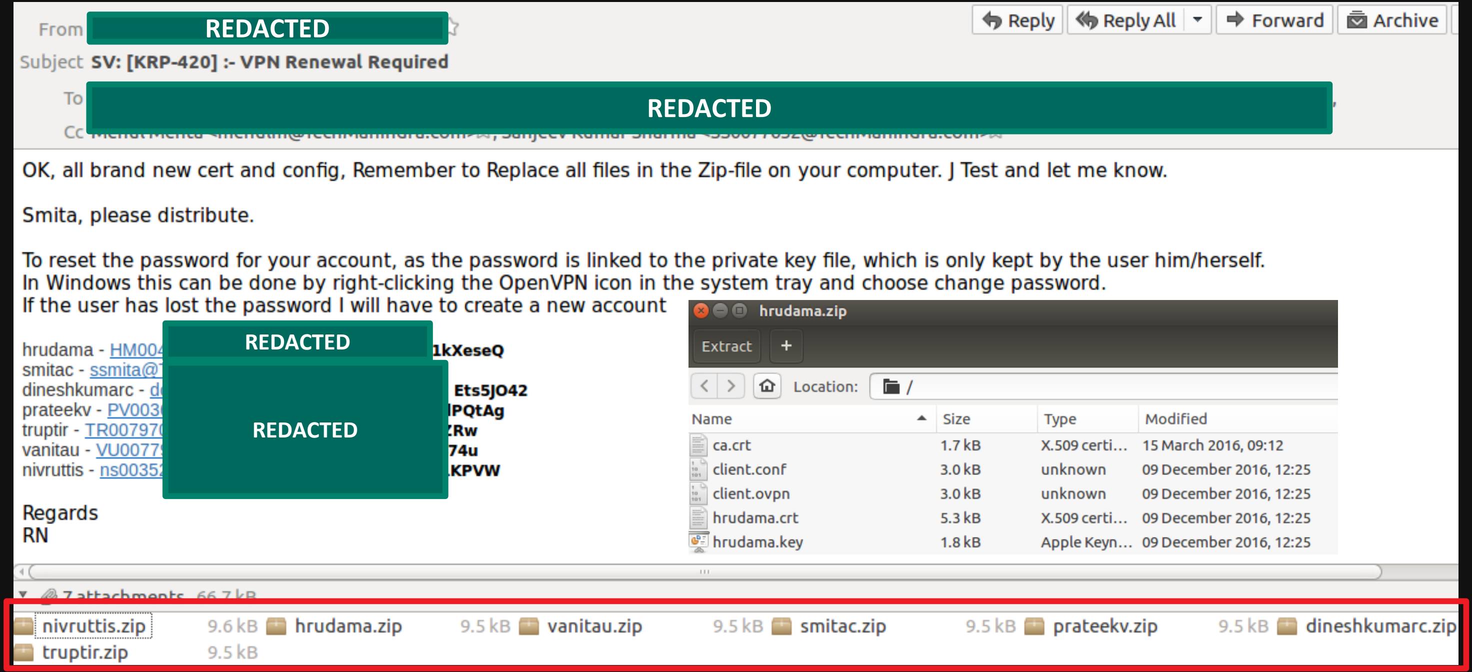


Is your Supplier an outsourced attack surface?



You can't effectively protect your data if you don't know where it resides.

SUPPLY CHAIN LEAKS YOUR CREDENTIALS



From REDACTED

Subject **SV: [KRP-420] :- VPN Renewal Required**

To REDACTED

Cc

OK, all brand new cert and config, Remember to Replace all files in the Zip-file on your computer. J Test and let me know.

Smita, please distribute.

To reset the password for your account, as the password is linked to the private key file, which is only kept by the user him/herself.
In Windows this can be done by right-clicking the OpenVPN icon in the system tray and choose change password.
If the user has lost the password I will have to create a new account

hrudama - REDACTED
smitac -
dineshkumarc -
prateekv -
truptir -
vanitau -
nivruttis - REDACTED

Regards
RN

hrudama.zip

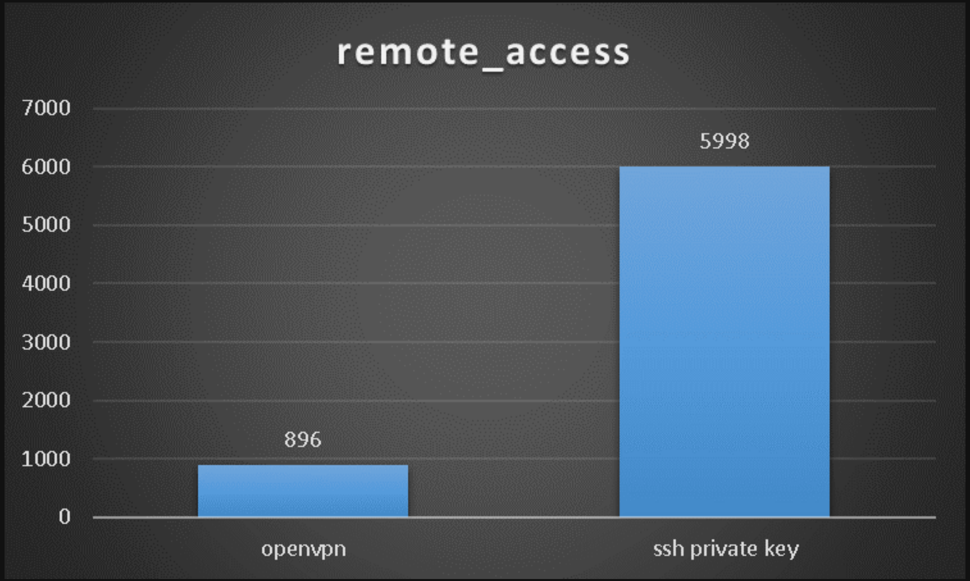
Name	Size	Type	Modified
ca.crt	1.7 kB	X.509 certi…	15 March 2016, 09:12
client.conf	3.0 kB	unknown	09 December 2016, 12:25
client.ovpn	3.0 kB	unknown	09 December 2016, 12:25
hrudama.crt	5.3 kB	X.509 certi…	09 December 2016, 12:25
hrudama.key	1.8 kB	Apple Keyn…	09 December 2016, 12:25

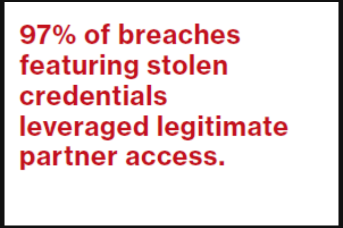
7 attachments 66.7 kB

nivruttis.zip	9.6 kB	hrudama.zip	9.5 kB	vanitau.zip	9.5 kB	smitac.zip	9.5 kB	prateekv.zip	9.5 kB	dineshkumarc.zip	
truptir.zip	9.5 kB										

97% of breaches featuring stolen credentials leveraged legitimate partner access.

SUPPLY CHAIN LEAKS YOUR CREDENTIALS





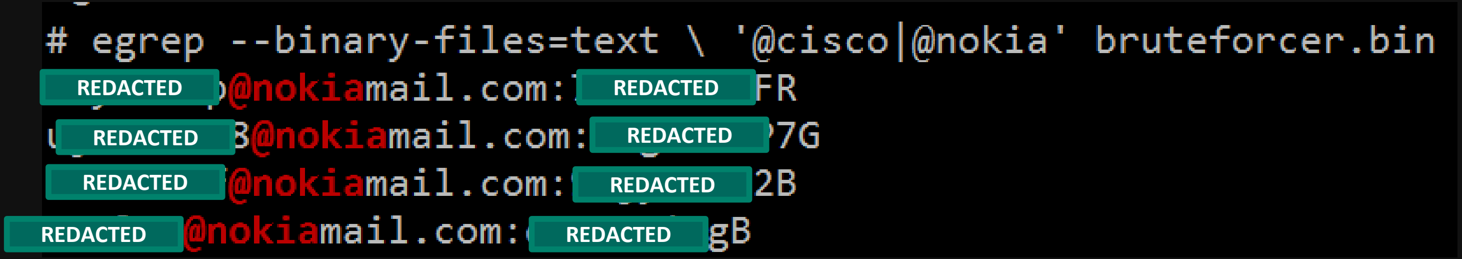
97% of breaches featuring stolen credentials leveraged legitimate partner access.

~ 900 openvpn configs

~ 6000 ssh private keys

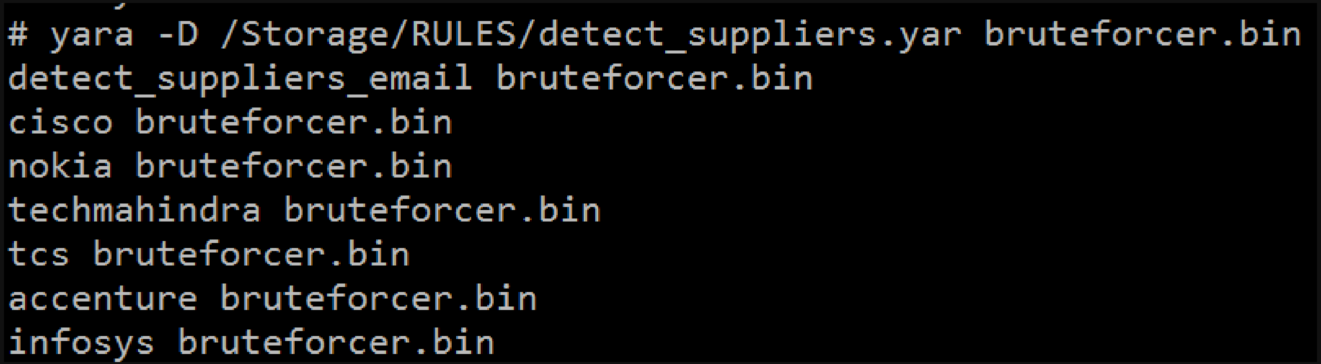
Direct access into networks

SUPPLY CHAIN TARGETED



```
# egrep --binary-files=text \ '@cisco|@nokia' bruteforcer.bin
REDACTED@nokiamail.com:REDACTEDFR
REDACTED@nokiamail.com:REDACTED7G
REDACTED@nokiamail.com:REDACTED2B
REDACTED@nokiamail.com:REDACTEDgB
```

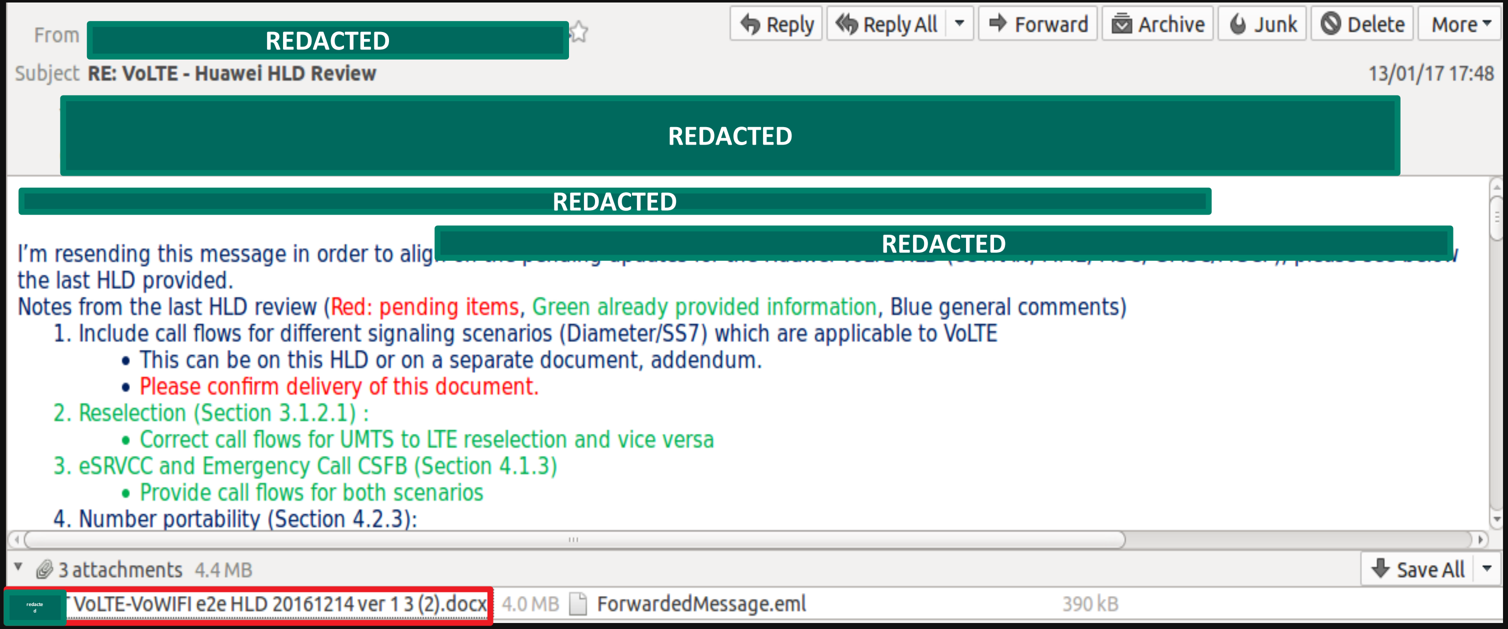
97% of breaches featuring stolen credentials leveraged legitimate partner access.



```
# yara -D /Storage/RULES/detect_suppliers.yar bruteforcer.bin
detect_suppliers_email bruteforcer.bin
cisco bruteforcer.bin
nokia bruteforcer.bin
techmahindra bruteforcer.bin
tcs bruteforcer.bin
accenture bruteforcer.bin
infosys bruteforcer.bin
```

Creds found in Attack Tools

SUPPLY CHAIN AND ESPIONAGE



From REDACTED

Subject **RE: VoLTE - Huawei HLD Review**

13/01/17 17:48

REDACTED

REDACTED

I'm resending this message in order to alig REDACTED
the last HLD provided.

Notes from the last HLD review (Red: pending items, Green already provided information, Blue general comments)

1. Include call flows for different signaling scenarios (Diameter/SS7) which are applicable to VoLTE
   - This can be on this HLD or on a separate document, addendum.
   - Please confirm delivery of this document.
2. Reselection (Section 3.1.2.1) :
   - Correct call flows for UMTS to LTE reselection and vice versa
3. eSRVCC and Emergency Call CSFB (Section 4.1.3)
   - Provide call flows for both scenarios
4. Number portability (Section 4.2.3):

3 attachments 4.4 MB

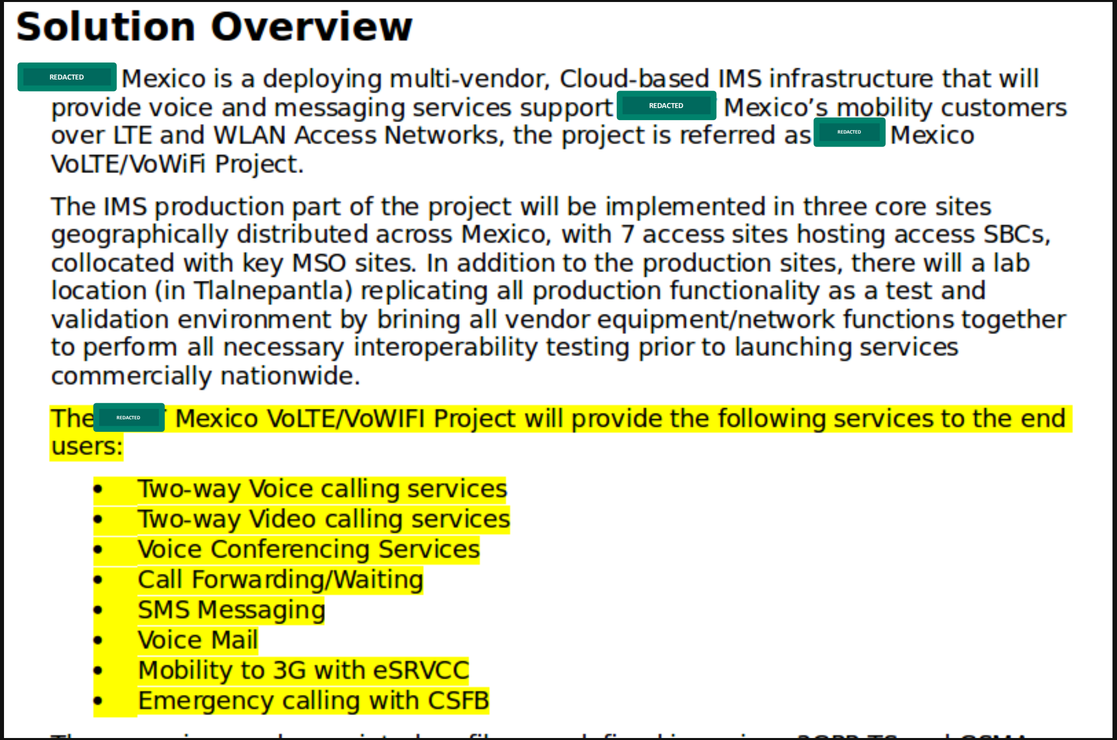
redacted VoLTE-VoWIFI e2e HLD 20161214 ver 1 3 (2).docx 4.0 MB

ForwardedMessage.eml 390 kB

90% of Cyber-espionage breaches capture trade secrets or proprietary information.

The Actors are predominantly state-affiliated groups. Competitors and nation states are also mixing it up.

SUPPLY CHAIN AND ESPIONAGE



Solution Overview

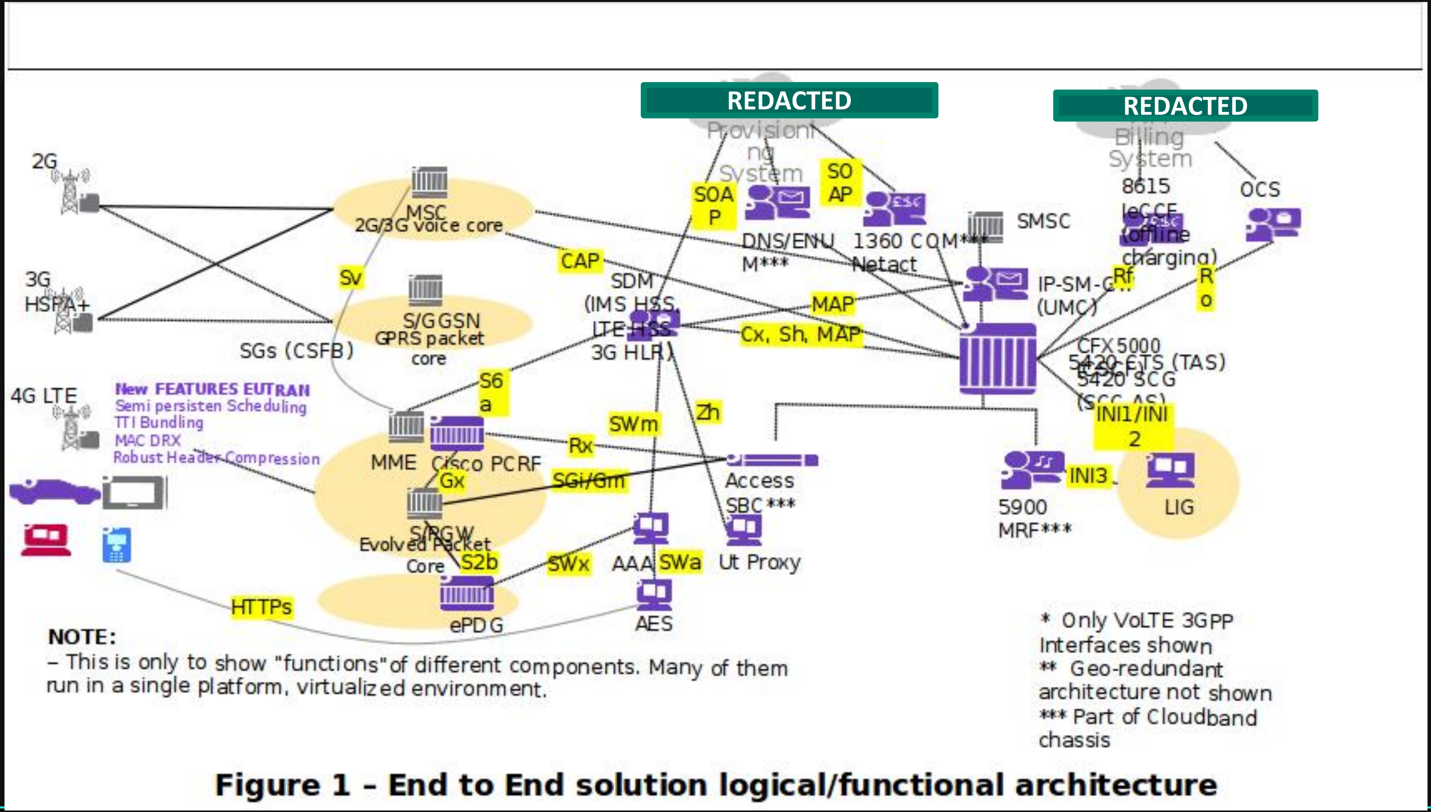
REDACTED Mexico is a deploying multi-vendor, Cloud-based IMS infrastructure that will provide voice and messaging services support REDACTED Mexico's mobility customers over LTE and WLAN Access Networks, the project is referred as REDACTED Mexico VoLTE/VoWiFi Project.

The IMS production part of the project will be implemented in three core sites geographically distributed across Mexico, with 7 access sites hosting access SBCs, collocated with key MSO sites. In addition to the production sites, there will a lab location (in Tlalnepantla) replicating all production functionality as a test and validation environment by brining all vendor equipment/network functions together to perform all necessary interoperability testing prior to launching services commercially nationwide.

The REDACTED Mexico VoLTE/VoWIFI Project will provide the following services to the end users:

- Two-way Voice calling services
- Two-way Video calling services
- Voice Conferencing Services
- Call Forwarding/Waiting
- SMS Messaging
- Voice Mail
- Mobility to 3G with eSRVCC
- Emergency calling with CSFB

ESPIONAGE - COMPETITIVE ADVANTAGE



NOTE:
– This is only to show "functions" of different components. Many of them run in a single platform, virtualized environment.

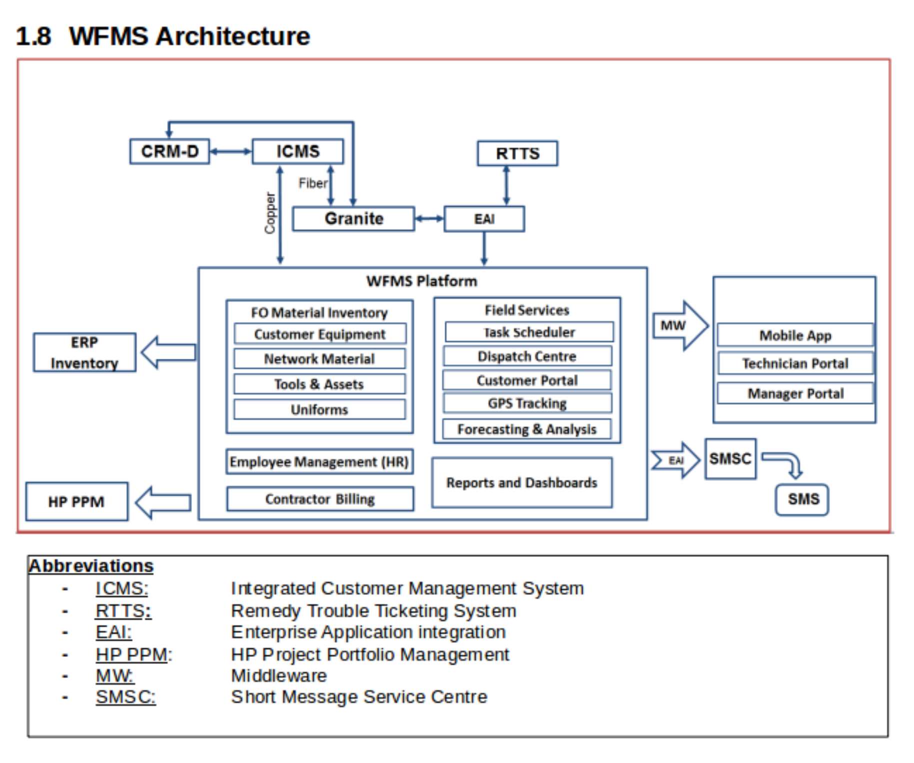
* Only VoLTE 3GPP Interfaces shown
** Geo-redundant architecture not shown
*** Part of Cloudband chassis

Figure 1 - End to End solution logical/functional architecture

90% of Cyber-espionage breaches capture trade secrets or proprietary information.

The Actors are predominantly state-affiliated groups. Competitors and nation states are also mixing it up.

SUPPLY CHAIN AND ESPIONAGE

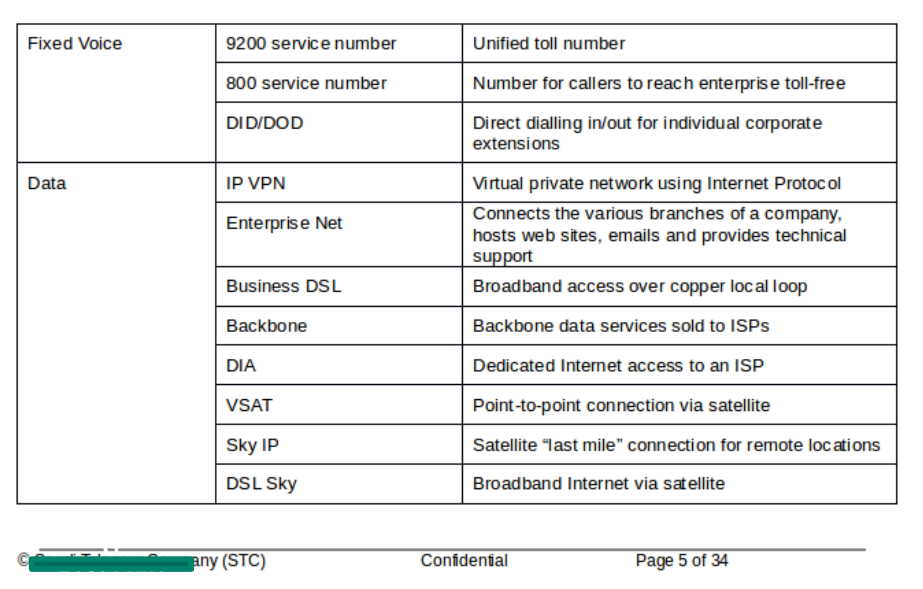


1.8 WFMS Architecture

Abbreviations

- ICMS: Integrated Customer Management System
- RTTS: Remedy Trouble Ticketing System
- EAI: Enterprise Application integration
- HP PPM: HP Project Portfolio Management
- MW: Middleware
- SMSC: Short Message Service Centre

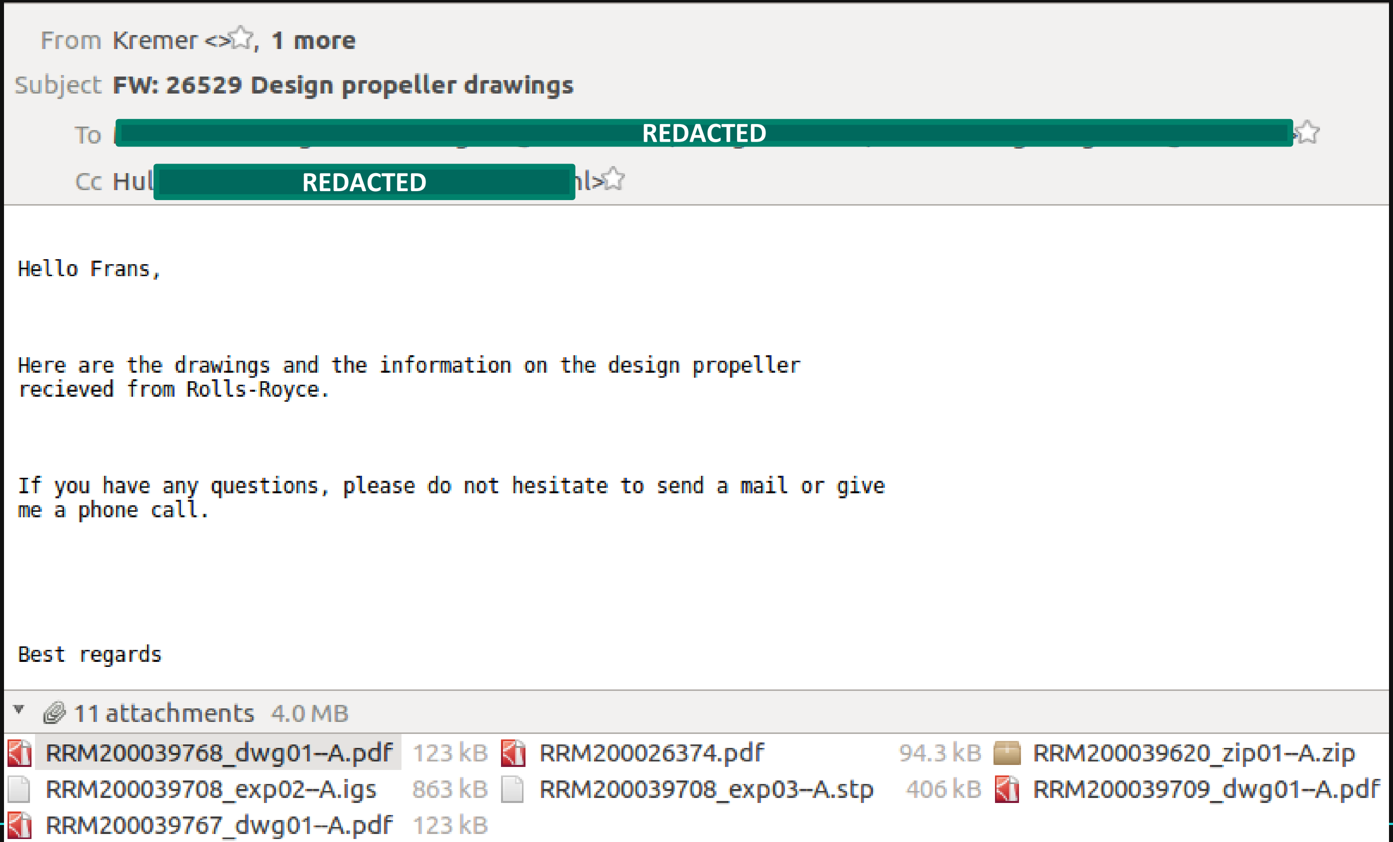
Rolls Royce



Fixed Voice	9200 service number	Unified toll number
	800 service number	Number for callers to reach enterprise toll-free
	DID/DOD	Direct dialling in/out for individual corporate extensions
Data	IP VPN	Virtual private network using Internet Protocol
	Enterprise Net	Connects the various branches of a company, hosts web sites, emails and provides technical support
	Business DSL	Broadband access over copper local loop
	Backbone	Backbone data services sold to ISPs
	DIA	Dedicated Internet access to an ISP
	VSAT	Point-to-point connection via satellite
	Sky IP	Satellite "last mile" connection for remote locations
	DSL Sky	Broadband Internet via satellite

© [redacted]any (STC) Confidential Page 5 of 34

SUPPLY CHAIN AND ESPIONAGE



From Kremer <>☆, **1 more**

Subject **FW: 26529 Design propeller drawings**

To REDACTED ☆

Cc Hul REDACTED nl>☆

Hello Frans,

Here are the drawings and the information on the design propeller recieved from Rolls-Royce.

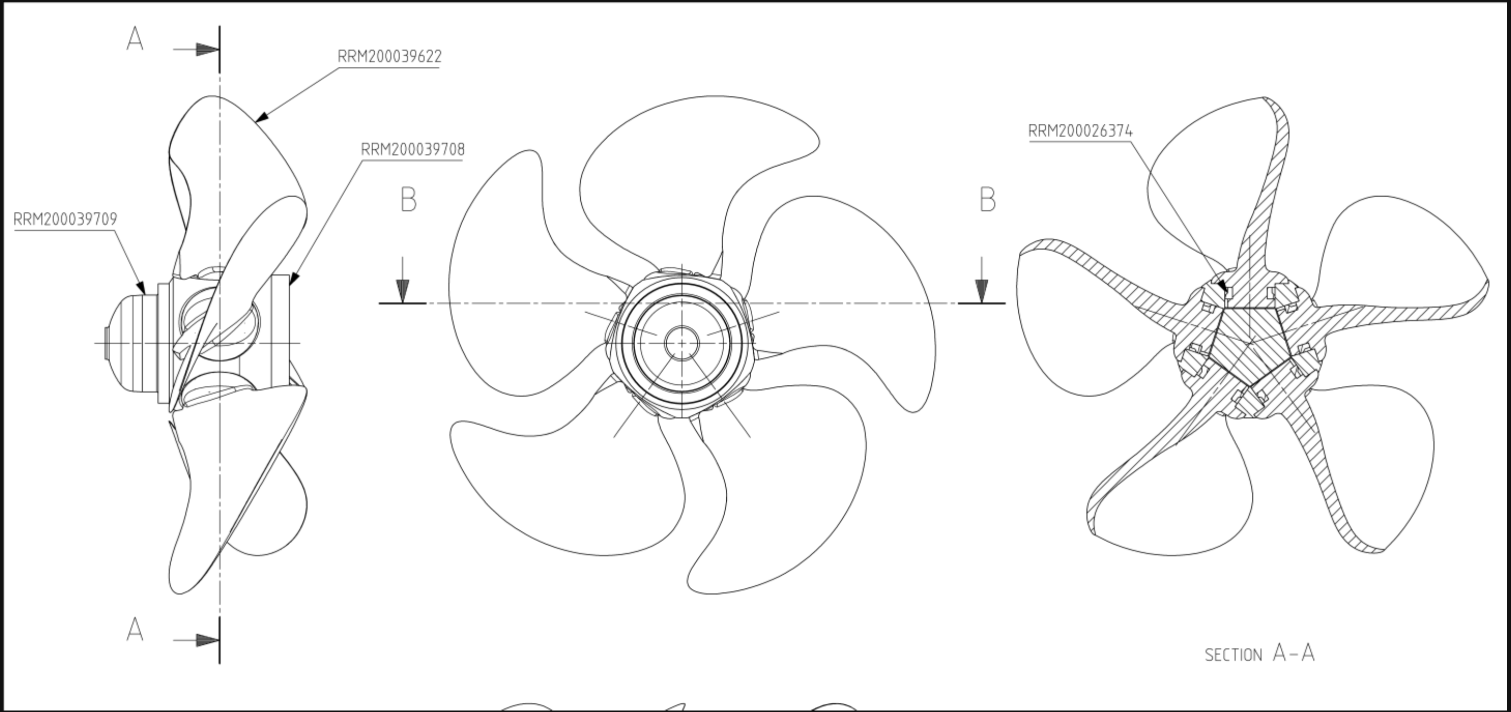
If you have any questions, please do not hesitate to send a mail or give me a phone call.

Best regards

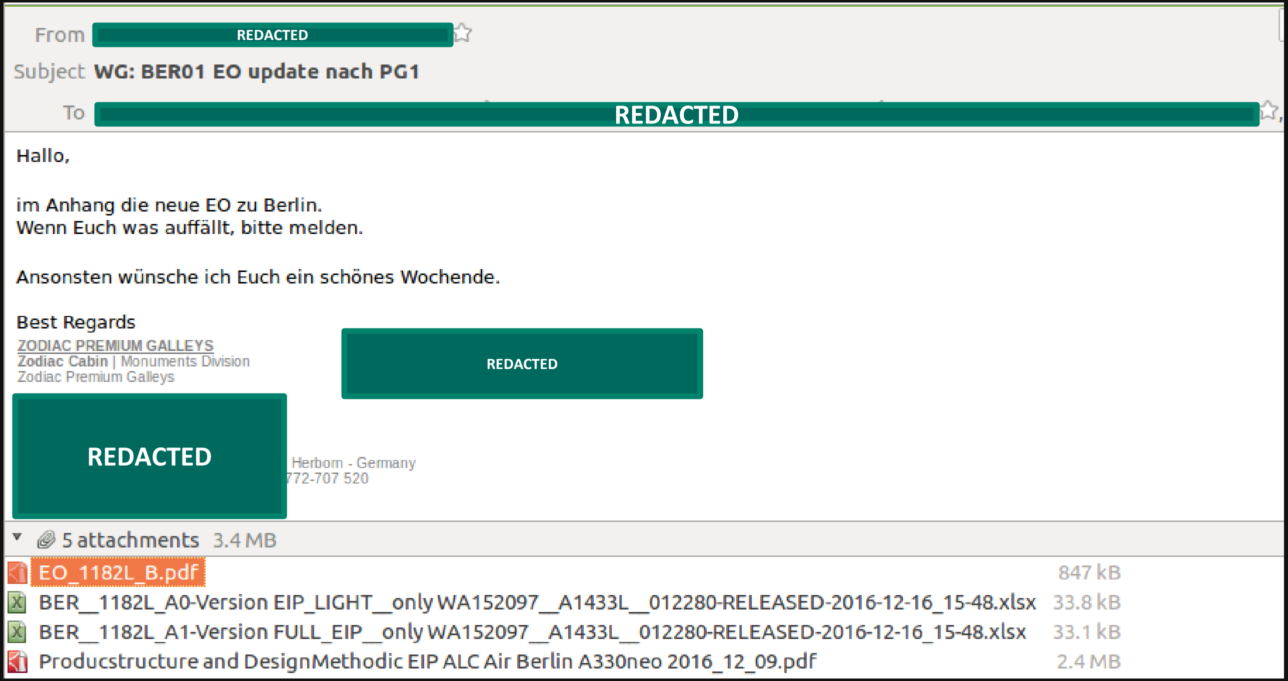
▾ 11 attachments 4.0 MB

RRM200039768_dwg01–A.pdf	123 kB	RRM200026374.pdf	94.3 kB	RRM200039620_zip01–A.zip
RRM200039708_exp02–A.igs	863 kB	RRM200039708_exp03–A.stp	406 kB	RRM200039709_dwg01–A.pdf
RRM200039767_dwg01–A.pdf	123 kB			

SUPPLY CHAIN AND ESPIONAGE



ESPIONAGE - COMPETITIVE ADVANTAGE



From REDACTED

Subject **WG: BER01 EO update nach PG1**

To REDACTED

Hallo,

im Anhang die neue EO zu Berlin.
Wenn Euch was auffällt, bitte melden.

Ansonsten wünsche ich Euch ein schönes Wochende.

Best Regards
ZODIAC PREMIUM GALLEYS
Zodiac Cabin | Monuments Division
Zodiac Premium Galleys

REDACTED

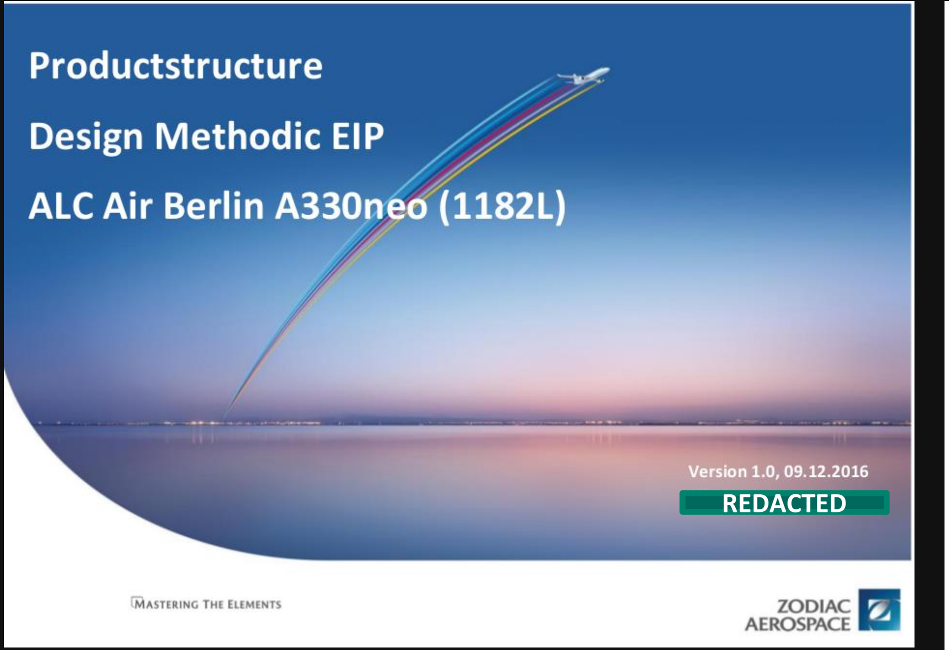
REDACTED

Herborn - Germany
772-707 520

5 attachments 3.4 MB

EO_1182L_B.pdf	847 kB
BER__1182L_A0-Version EIP_LIGHT__only WA152097__A1433L__012280-RELEASED-2016-12-16_15-48.xlsx	33.8 kB
BER__1182L_A1-Version FULL_EIP__only WA152097__A1433L__012280-RELEASED-2016-12-16_15-48.xlsx	33.1 kB
Producstructure and DesignMethodic EIP ALC Air Berlin A330neo 2016_12_09.pdf	2.4 MB

SUPPLY CHAIN AND ESPIONAGE



Productstructure

Design Methodic EIP

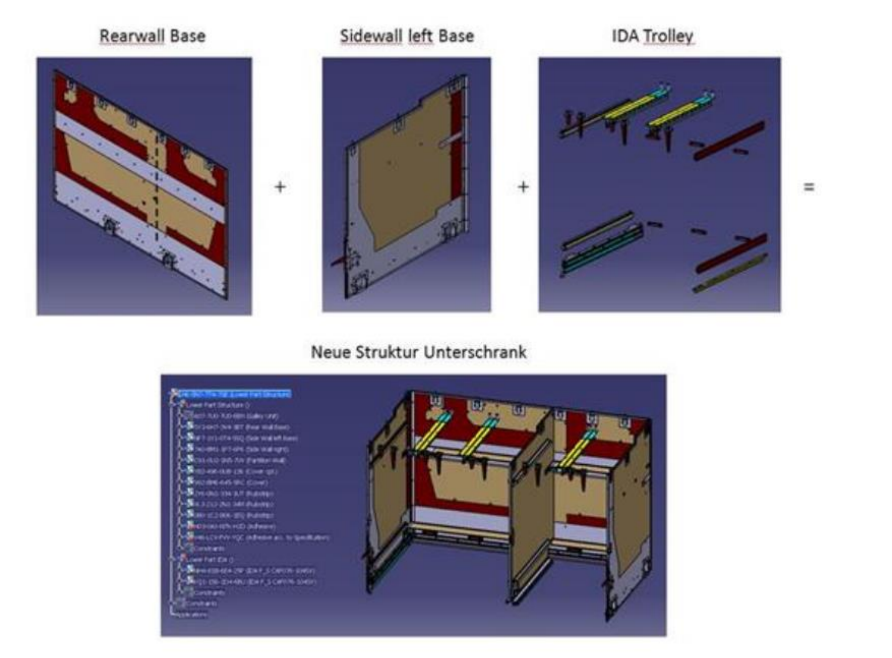
ALC Air Berlin A330neo (1182L)

Version 1.0, 09.12.2016

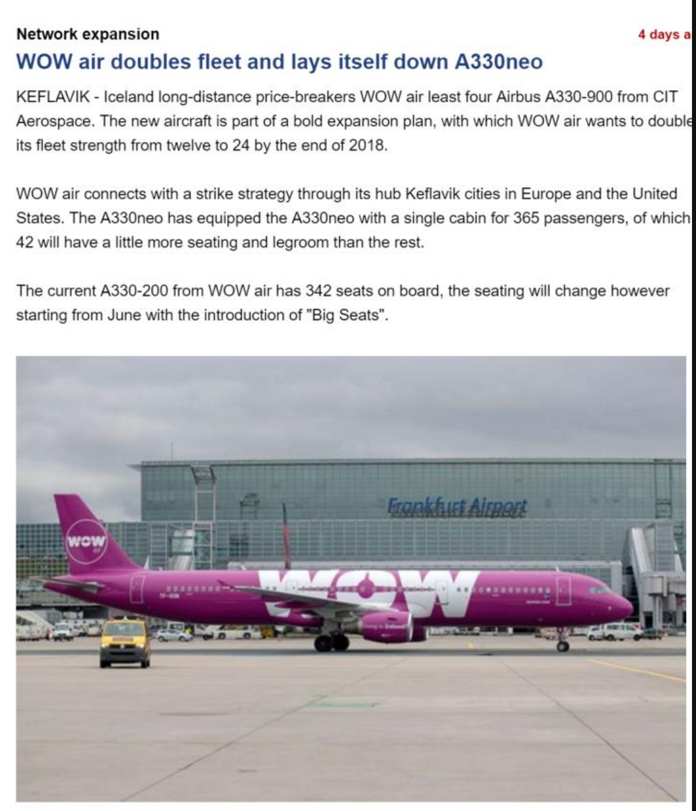
REDACTED

MASTERING THE ELEMENTS

ZODIAC AEROSPACE



SUPPLY CHAIN AND ESPIONAGE



Network expansion 4 days a

WOW air doubles fleet and lays itself down A330neo

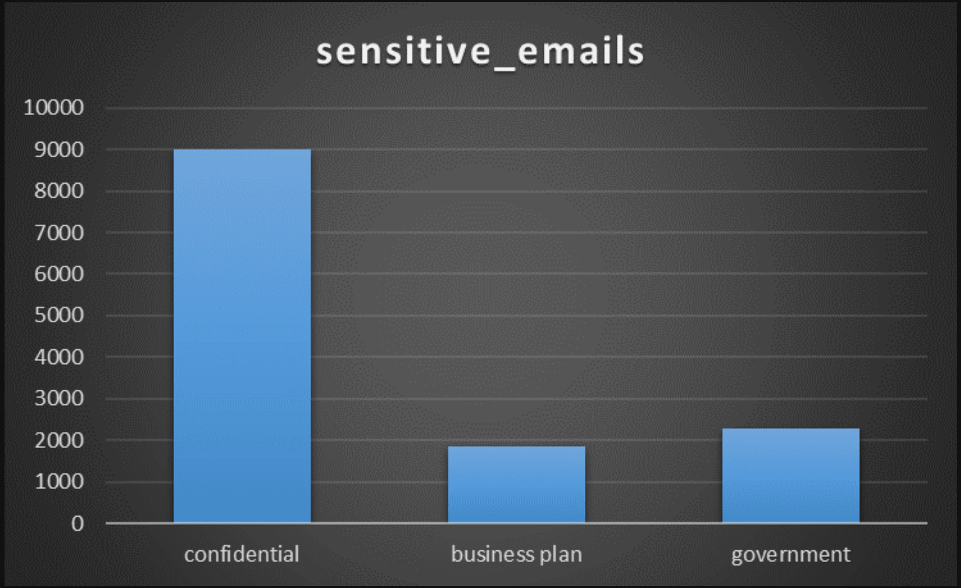
KEFLAVIK - Iceland long-distance price-breakers WOW air least four Airbus A330-900 from CIT Aerospace. The new aircraft is part of a bold expansion plan, with which WOW air wants to double its fleet strength from twelve to 24 by the end of 2018.

WOW air connects with a strike strategy through its hub Keflavik cities in Europe and the United States. The A330neo has equipped the A330neo with a single cabin for 365 passengers, of which 42 will have a little more seating and legroom than the rest.

The current A330-200 from WOW air has 342 seats on board, the seating will change however starting from June with the introduction of "Big Seats".

- Anounced 4 days ago
- Plans obtained in December 2016

SUPPLY CHAIN AND ESPIONAGE

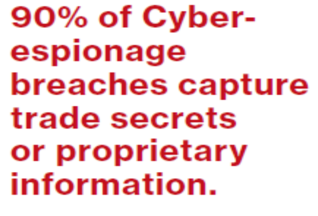


Various Retrohunts Found

- 9000 emails marked as confidential

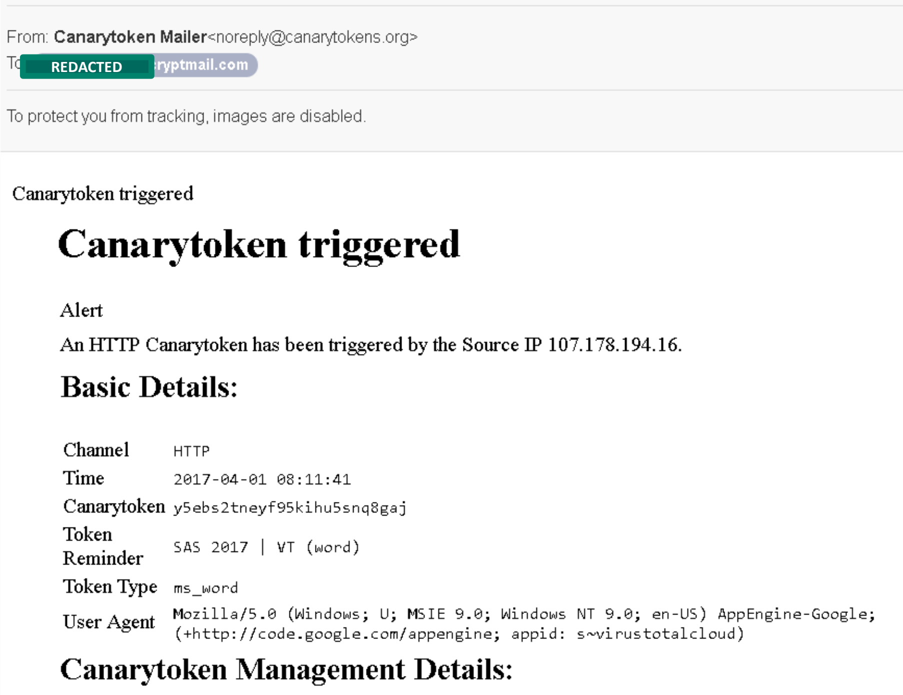
~ 1900 emails containing business plan

~ 2200 emails from governments



90% of Cyber-espionage breaches capture trade secrets or proprietary information.

WHERE IS YOUR FILE GOING?



From: **Canarytoken Mailer**<noreply@canarytokens.org>
To REDACTED ryptmail.com

To protect you from tracking, images are disabled.

Canarytoken triggered

Canarytoken triggered

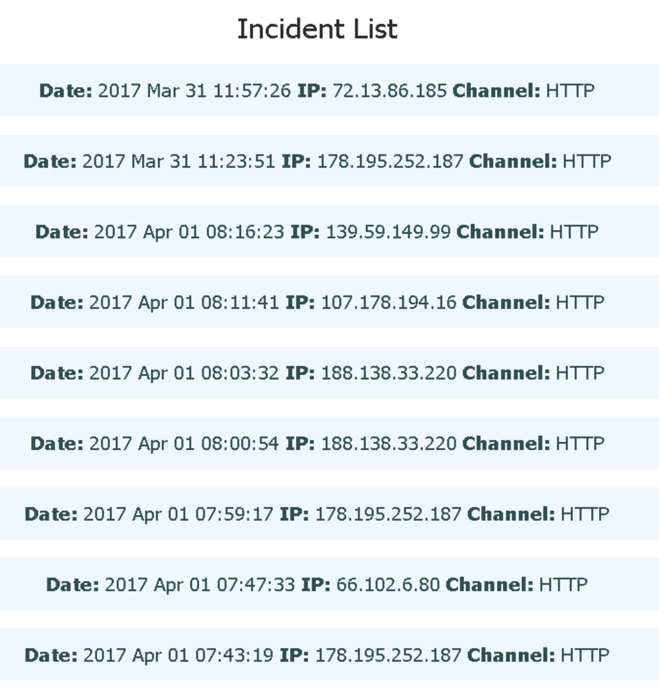
Alert

An HTTP Canarytoken has been triggered by the Source IP 107.178.194.16.

Basic Details:

Channel	HTTP
Time	2017-04-01 08:11:41
Canarytoken	y5ebs2tneyf95kihu5snq8gaj
Token Reminder	SAS 2017 | VT (word)
Token Type	ms_word
User Agent	Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US) AppEngine-Google; (+http://code.google.com/appengine; appid: s~virustotalcloud)

Canarytoken Management Details:



Incident List

Date: 2017 Mar 31 11:57:26 **IP:** 72.13.86.185 **Channel:** HTTP

Date: 2017 Mar 31 11:23:51 **IP:** 178.195.252.187 **Channel:** HTTP

Date: 2017 Apr 01 08:16:23 **IP:** 139.59.149.99 **Channel:** HTTP

Date: 2017 Apr 01 08:11:41 **IP:** 107.178.194.16 **Channel:** HTTP

Date: 2017 Apr 01 08:03:32 **IP:** 188.138.33.220 **Channel:** HTTP

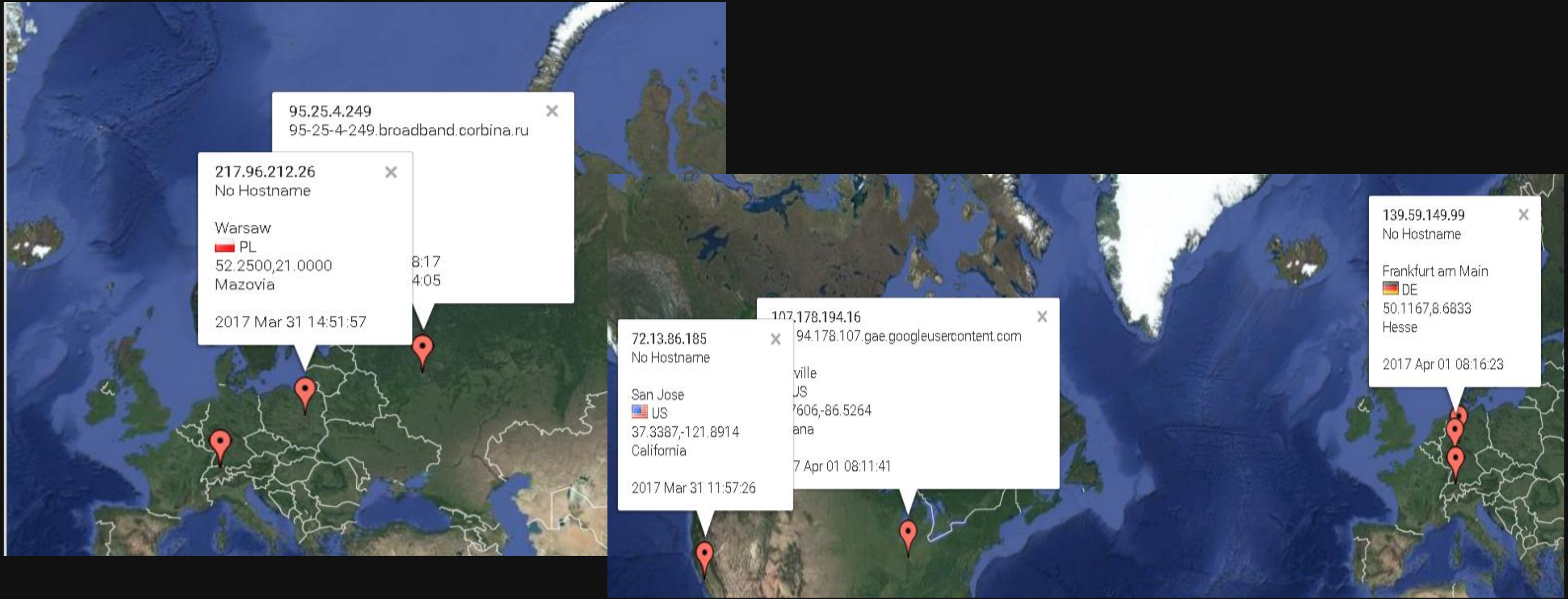
Date: 2017 Apr 01 08:00:54 **IP:** 188.138.33.220 **Channel:** HTTP

Date: 2017 Apr 01 07:59:17 **IP:** 178.195.252.187 **Channel:** HTTP

Date: 2017 Apr 01 07:47:33 **IP:** 66.102.6.80 **Channel:** HTTP

Date: 2017 Apr 01 07:43:19 **IP:** 178.195.252.187 **Channel:** HTTP

WHERE IS YOUR FILE GOING?



95.25.4.249
95-25-4-249.broadband.corbina.ru

8:17
4:05

217.96.212.26
No Hostname

Warsaw
PL
52.2500,21.0000
Mazovia

2017 Mar 31 14:51:57

107.178.194.16
94.178.107.gae.googleusercontent.com

ville
JS
7606,-86.5264
ana

7 Apr 01 08:11:41

72.13.86.185
No Hostname

San Jose
US
37.3387,-121.8914
California

2017 Mar 31 11:57:26

139.59.149.99
No Hostname

Frankfurt am Main
DE
50.1167,8.6833
Hesse

2017 Apr 01 08:16:23

THANK YOU

My Recommendation slide is missing because I have only one recommendation, go and hunt yourself because others might be doing it already.