ROCKET KITTEN

Tillmann Werner, Director of Technical Analysis

tillmann@crowdstrike.com

ROCKET KITTEN

TIMEFRAME

Spring 2014 - Present

RECENT TARGETING

Defense and Space

Western Governments

OBJECTIVES

Intellectual Property

Information about Diplomatic Strategies

TOOLS

Office Documents with Macros

Core Impact Pro

Custom MPK RAT

Custom Keylogger

Custom Credential Stealer

SPEAR PHISHING EMAIL

From: [redacted]
Date: Wed, Apr 23, 2014 10:08 AM
Subject: Message
To: [redacted]

Dear all,
Enclosed is some information that I hope you will find it useful.
Hag Sameah.

--
[redacted]
CEO, [redacted]

[redacted]

SPEAR PHISHING EMAIL

From: [redacted]
Date: Wed, Apr 23, 2014 10:12 AM
Subject: File
To: [redacted]

Sorry,
here is the file.

--
[redacted]
CEO, [redacted]

[redacted]

SPEAR PHISHING EMAIL

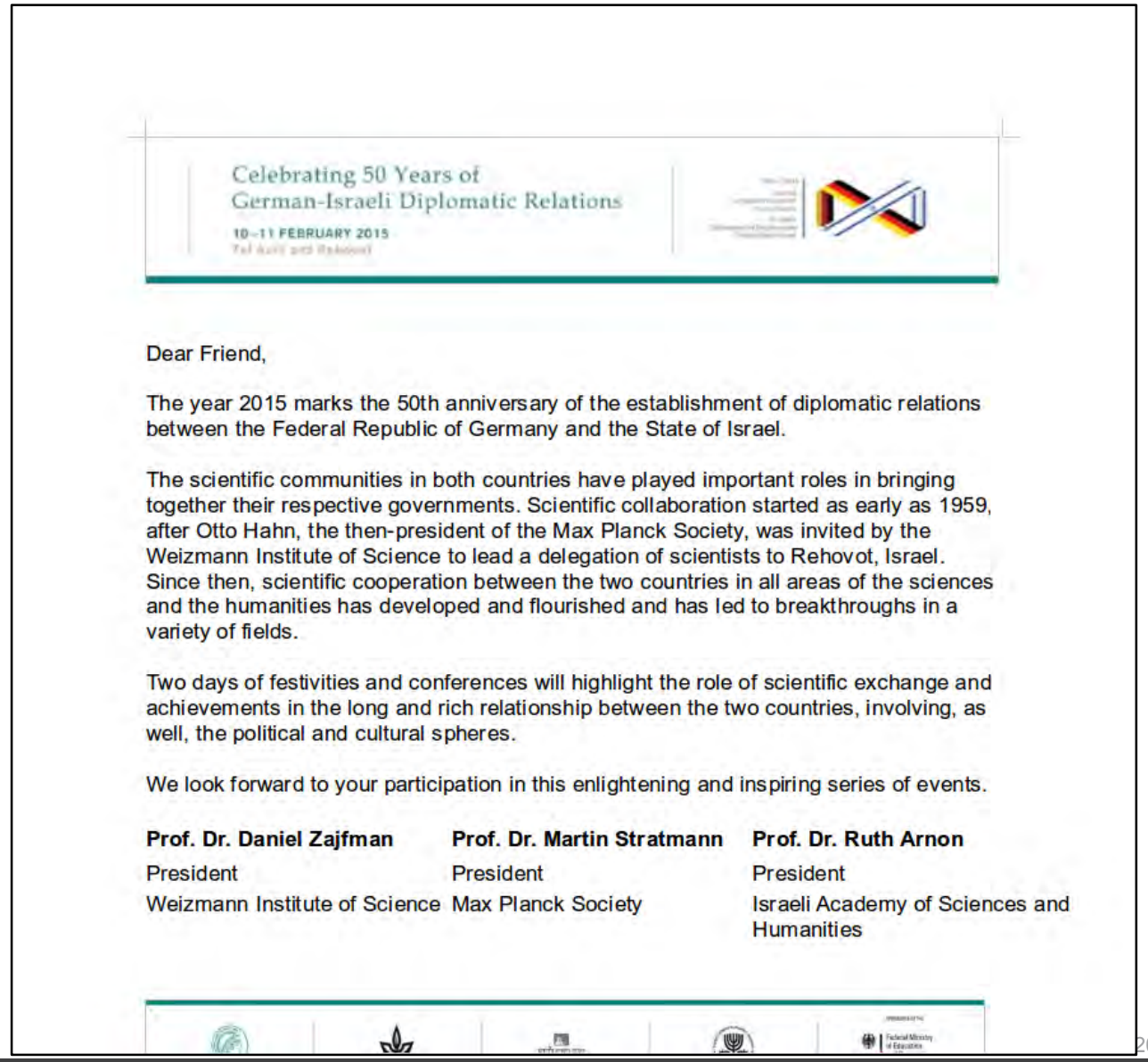
From: [redacted]
Date: Wed, Apr 23, 2014 at 10:13 AM
Subject: again I am sorry
To: [redacted]

I forgot to attach the file again.
here it is.

--
[redacted]
CEO, [redacted]

[redacted]

LURE DOCUMENT EXAMPLE



Celebrating 50 Years of
German-Israeli Diplomatic Relations

10–11 FEBRUARY 2015

Dear Friend,

The year 2015 marks the 50th anniversary of the establishment of diplomatic relations between the Federal Republic of Germany and the State of Israel.

The scientific communities in both countries have played important roles in bringing together their respective governments. Scientific collaboration started as early as 1959, after Otto Hahn, the then-president of the Max Planck Society, was invited by the Weizmann Institute of Science to lead a delegation of scientists to Rehovot, Israel. Since then, scientific cooperation between the two countries in all areas of the sciences and the humanities has developed and flourished and has led to breakthroughs in a variety of fields.

Two days of festivities and conferences will highlight the role of scientific exchange and achievements in the long and rich relationship between the two countries, involving, as well, the political and cultural spheres.

We look forward to your participation in this enlightening and inspiring series of events.

Prof. Dr. Daniel Zajfman	**Prof. Dr. Martin Stratmann**	**Prof. Dr. Ruth Arnon**
President	President	President
Weizmann Institute of Science	Max Planck Society	Israeli Academy of Sciences and Humanities

LURE DOCUMENT METADATA

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties"
xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/"
xmlns:dcmitype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<cp:coreProperties><dc:creator>
        Wool3n.H4t
    </dc:creator>
    <cp:lastModifiedBy>
        Wool3n.H4t
    </cp:lastModifiedBy>
    <dcterms:created xsi:type="dcterms:W3CDTF">
        2014-04-23T04:03:01Z
    </dcterms:created>
    <dcterms:modified xsi:type="dcterms:W3CDTF">
        2014-04-23T06:12:00Z
    </dcterms:modified>
</cp:coreProperties>
```

DEBUG DIRECTORIES

```
Debug Table (1 directories)
Directory 01
  Characteristics:    00000000
  TimeDateStamp:      547D5C31 Tue Dec  2 06:29:05 2014
  Version             0.00
  Type:               2 (CODEVIEW)
  SizeOfData:         118
  AddressOfRawData:   0000F5B0
  PointerToRawData:   0000DDB0
    CodeView Data
      Signature:          RSDS
      Guid:               {79065b62-5496-4d7f-8c5c-fb86f730b610}
      Age:                0000000C
      Filename:           C:\Users\Wool3n.H4t\Documents\Visual Studio 2010\Projects\
                          C-CPP\CWoolger\Release\CWoolger.pdb
```

STRING ARTIFACTS IN PAYLOADS

- Custom keylogger contains a hardcoded decryption key

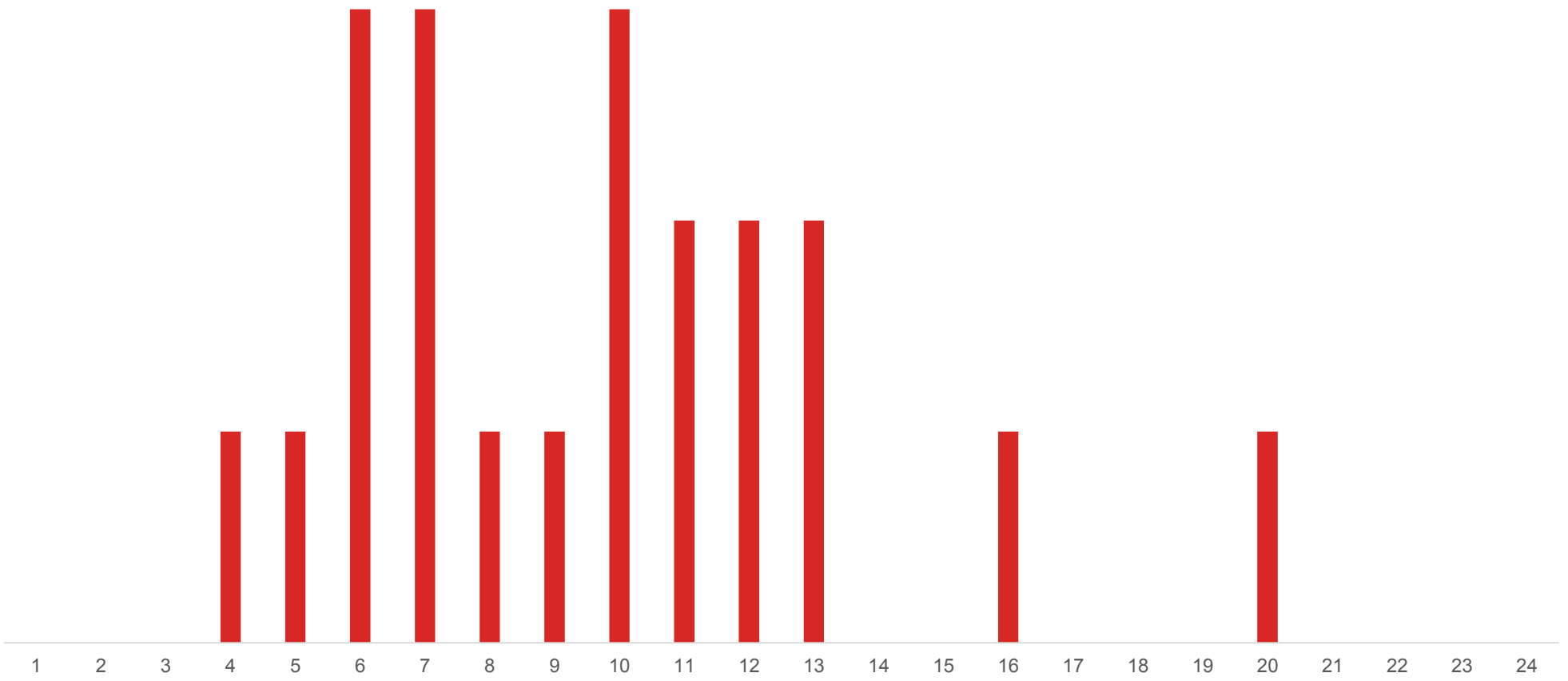
  `salamaaaaaaaaaaaaaaaaaaaaaaaaa`

- Dropper uses a marker string for memory scanning

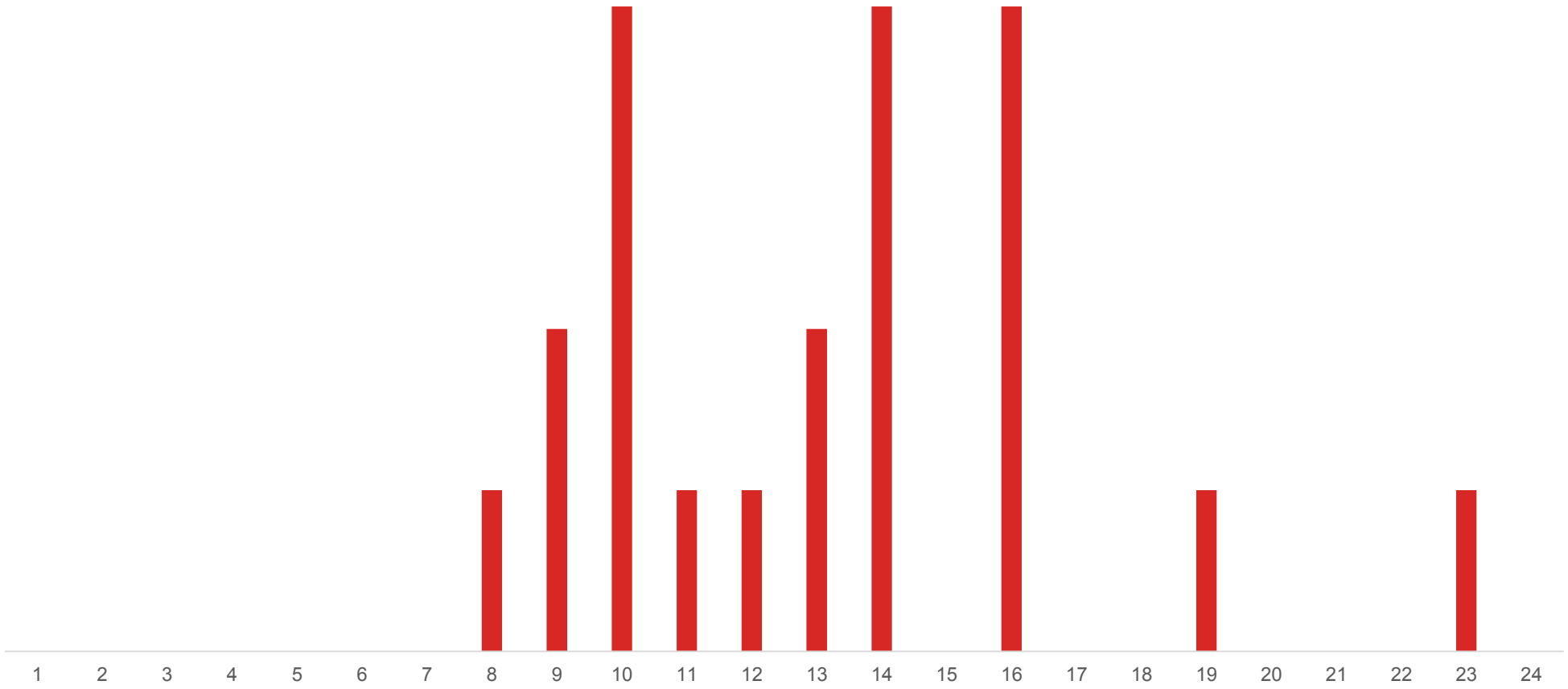
  `aallaamoot` (إلموت *Alamūt*)

Source of images: Wikipedia, Google Maps

BUILD TIMES IN UTC



BUILD TIMES IN IRAN STANDARD TIME (UTC+3:30)



EXCEPTIONS

```
Debug Table (1 directories)
Directory 01
  Characteristics:    00000000
  TimeDateStamp:      542B1EF5 Tue Sep 30 23:21:57 2014
  Version             0.00
  Type:               2 (CODEVIEW)
  SizeOfData:         162
  AddressOfRawData:   000382D8
  PointerToRawData:   000382D8
    CodeView Data
      Signature:          RSDS
      Guid:               {37ea7d58-0356-4010-abfc-3c87c2d7b81b}
      Age:                00000001
      Filename:           d:\nightly\sandbox_avg10_vc9_SP1_2011\source\avg10\avg9_all_vs90\
                          bin\Release_Unicode_vs90\Win32\avgam.pdb
```

CAMPAIGN-SPECIFIC CONFIGURATION

```
   Unknown value 1: 1
Socket timeout (s): 30
    Time delta (s): 86400
     String length: 8
       Campaign ID: MArM1Jy8
              IPv6: 0
     C2 IP address: 83.170.33.37
       C2 TCP Port: 3442
    RSA Public Key: cb8d37e09d0251918b7cb3e4bb65fc659ae9a36ddad1b3f7a86b02c9b261fb711bc5af
                    a60d7625e8f6cddca4eb941d2768380d05c3e53aebcbb2cfc476b2452b92e893de3f28
                    c0ae8131958cdca9ea50a4248e859c97c8764aafdf4bc266a63ada91fdb7e8eab2b783
                    979164b4f9cb45a88cc4b968b24bdd4f0151ad75f2c5b7
```

IDENTIFIED CAMPAIGNS

Document modified	C2 IP Address	Campaign	RSA Public Key
2014-04-23 05:55:46	83.170.43.67	HRMsCllz	ed5115960971a38906115b30a37d69eb3fe83a76ed41ee4a54d45b17a4732847b43b...
2014-04-23 06:12:00	83.170.43.67	HRMsCllz	ed5115960971a38906115b30a37d69eb3fe83a76ed41ee4a54d45b17a4732847b43b...
n/a	83.170.33.37	MArM1Jy8	cb8d37e09d0251918b7cb3e4bb65fc659ae9a36ddad1b3f7a86b02c9b261fb711bc5...
2014-07-02 15:22:55	84.11.75.220	Gh8ntaAi	ab041292478652394a79c09b073a745baee252250621c34548ccbc6651e342a0ebe2...
2014-07-07 05:24:57	84.11.75.220	Gh8ntaAi	ab041292478652394a79c09b073a745baee252250621c34548ccbc6651e342a0ebe2...
2014-07-13 06:47:15	84.11.75.220	Gh8ntaAi	ab041292478652394a79c09b073a745baee252250621c34548ccbc6651e342a0ebe2...
2014-07-15 07:54:32	84.11.75.220	Gh8ntaAi	ab041292478652394a79c09b073a745baee252250621c34548ccbc6651e342a0ebe2...
2014-07-24 10:19:50	84.11.75.220	Gh8ntaAi	ab041292478652394a79c09b073a745baee252250621c34548ccbc6651e342a0ebe2...
2014-07-27 11:57:21	84.11.75.220	Gh8ntaAi	ab041292478652394a79c09b073a745baee252250621c34548ccbc6651e342a0ebe2...
2014-07-27 09:40:32	84.11.75.220	Gh8ntaAi	ab041292478652394a79c09b073a745baee252250621c34548ccbc6651e342a0ebe2...
2014-07-30 04:31:52	84.11.75.220	Gh8ntaAi	ab041292478652394a79c09b073a745baee252250621c34548ccbc6651e342a0ebe2...
2014-08-07 06:20:22	83.170.33.60	abcdef12	d0e8f95447c85cefa13840090881e573fc5f4b3de4711be30ab8d219c43cc24419dd...
2014-11-11 07:48:11	83.170.33.80	2ERujijF	be158a49a856268ab4f4a45902895d2b7e06c2d64f90f6ac66033c3ffd2641d1be6a...
2014-12-01 04:55:19	83.170.33.80	2ERujijF	be158a49a856268ab4f4a45902895d2b7e06c2d64f90f6ac66033c3ffd2641d1be6a...

C2 IP ADDRESSES

- IP addresses belong to network ranges owned by IABG
- German satellite services provider

```
83.170.33.37
83.170.33.60
83.170.33.80
83.170.43.67
84.11.26.230
84.11.75.220
84.11.146.55
```

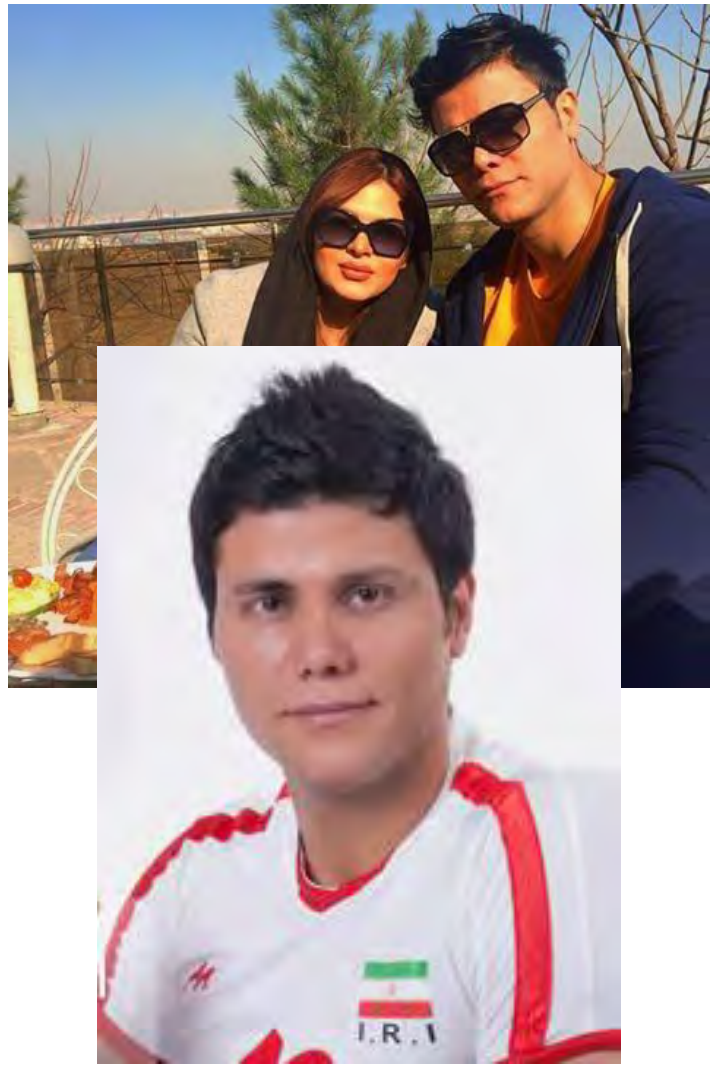
WHOIS RECORDS

```
inetnum:        83.170.33.32 - 83.170.33.63
netname:        DE-IABG-TELEPORT-MAHDAVI_8
descr:          IABG - Teleport customer Mehdi Mahdavi
country:        DE
remarks:        TT # 17986
status:         ASSIGNED PA
mnt-by:         IABG-MNT
source:         RIPE # Filtered
```

WHOIS RECORDS

```
Inetnum :      83.170.33.32 - 83.170.33.63
Netname :      DE-IABG-TELEPORT-MAHDAVI_8
Descr :IABG - Teleport customer Mehdi Mahdavi
Country :      IR
Status :       ASSIGNED PA
Mnt-by :       IABG-MNT

Person :       Mehdi Mahdavi
Address :      No 83 - Baharestan st
Address :      Isfahan
Address :      IR
Phone :       +98 913 115 8009
Nic-hdl :      MM39703-RIPE
Mnt-by :       IABG-MNT
```

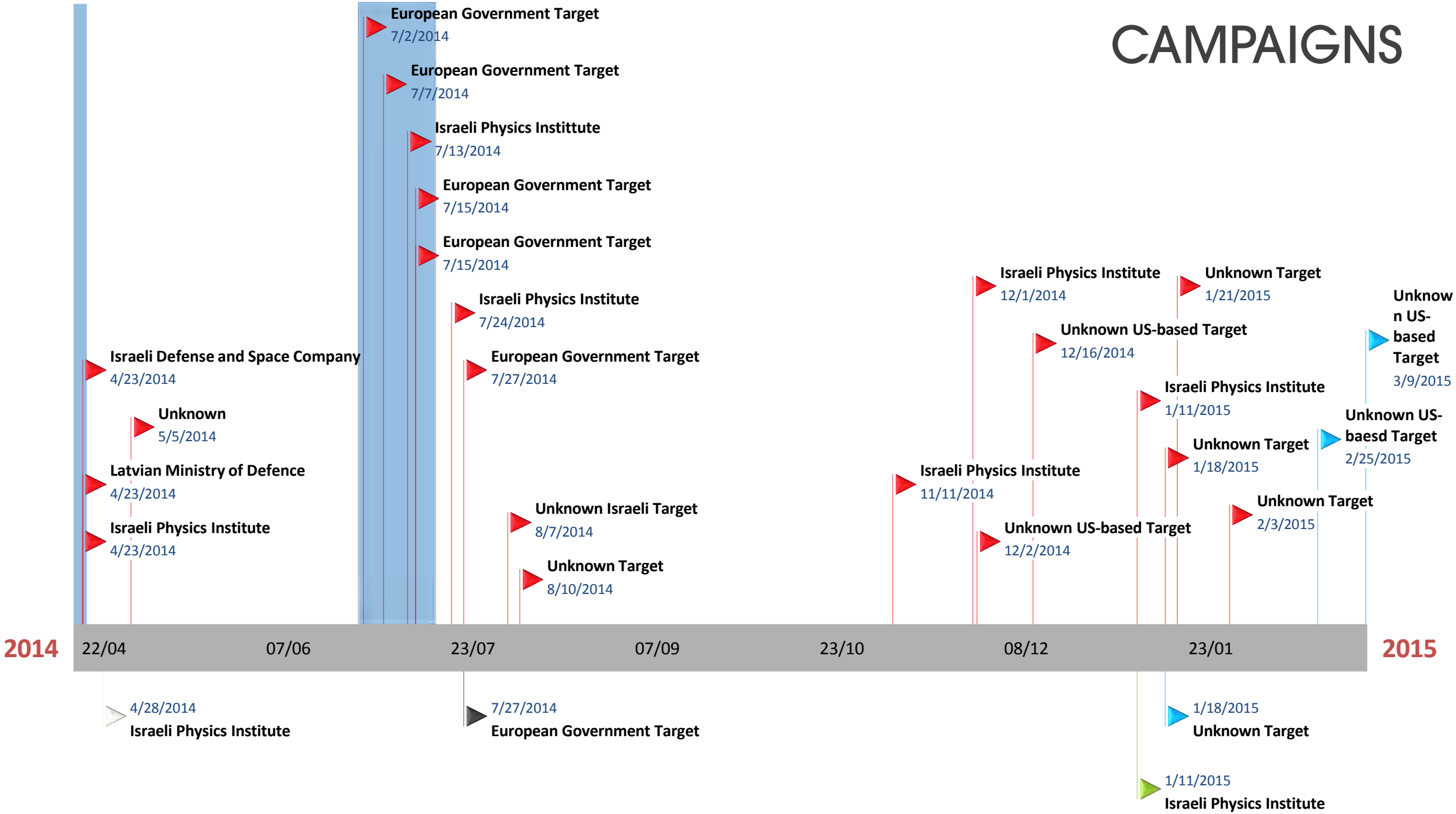


MEHDI MAHDAVI, ASSOCIATE PROFESSOR AT ISFAHAN UNI

Isfahan University of Technology

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

CAMPAIGNS


European Government Target
7/2/2014
European Government Target
7/7/2014
Israeli Physics Insttitute
7/13/2014
European Government Target
7/15/2014
European Government Target
7/15/2014
Israeli Physics Institute
7/24/2014
European Government Target
7/27/2014
Israeli Defense and Space Company
4/23/2014
Unknown
5/5/2014
Latvian Ministry of Defence
4/23/2014
Israeli Physics Institute
4/23/2014
Unknown Israeli Target
8/7/2014
Unknown Target
8/10/2014
Israeli Physics Institute
12/1/2014
Unknown Target
1/21/2015
Unknown US-based Target
12/16/2014
Israeli Physics Institute
1/11/2015
Unknown US-based Target
3/9/2015
Unknown US-baesd Target
2/25/2015
Unknown Target
1/18/2015
Israeli Physics Institute
11/11/2014
Unknown Target
2/3/2015
Unknown US-based Target
12/2/2014
2014
22/04
07/06
23/07
07/09
23/10
08/12
23/01
2015
4/28/2014
Israeli Physics Institute
7/27/2014
European Government Target
1/18/2015
Unknown Target
1/11/2015
Israeli Physics Institute

RECENT WAVE OF ATTACKS

THANK YOU.