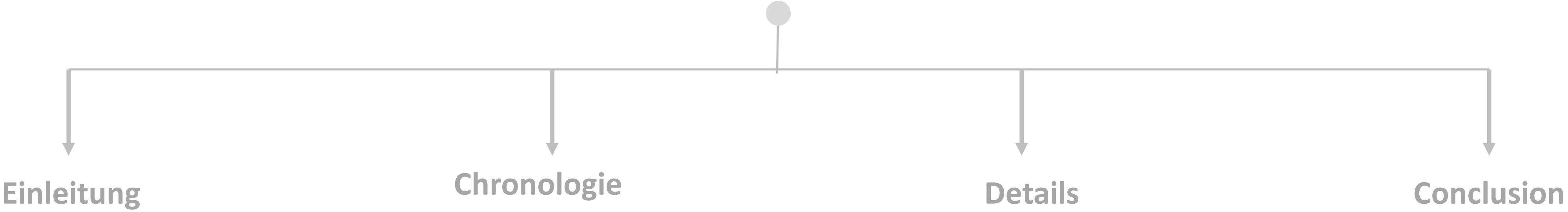
osm solutions

Objective Security Management

Hacking während der US Präsidentschaftswahl

Agenda

Hacking während dem US Präsidentschaftswahlkampf



Einleitung

Chronologie

Details

Conclusion

Our Services

The main **Service Areas**

Compliance

Want to enter a new market or know what requirements your IT will need to fulfil to comply to GDPR or PCI DSS? Our experienced professionals will help you overcome these hurdles for your business.

IT Security

From assessing your IT landscape to advisory on security best practice, we support you in identifying threats and establishing information security measures to protect your valuable assets.

Solutions

We maintain and operate your IT Security. From outsourced firewall operation to security management. Our experts have long experience in deploying and operating IT security solutions.

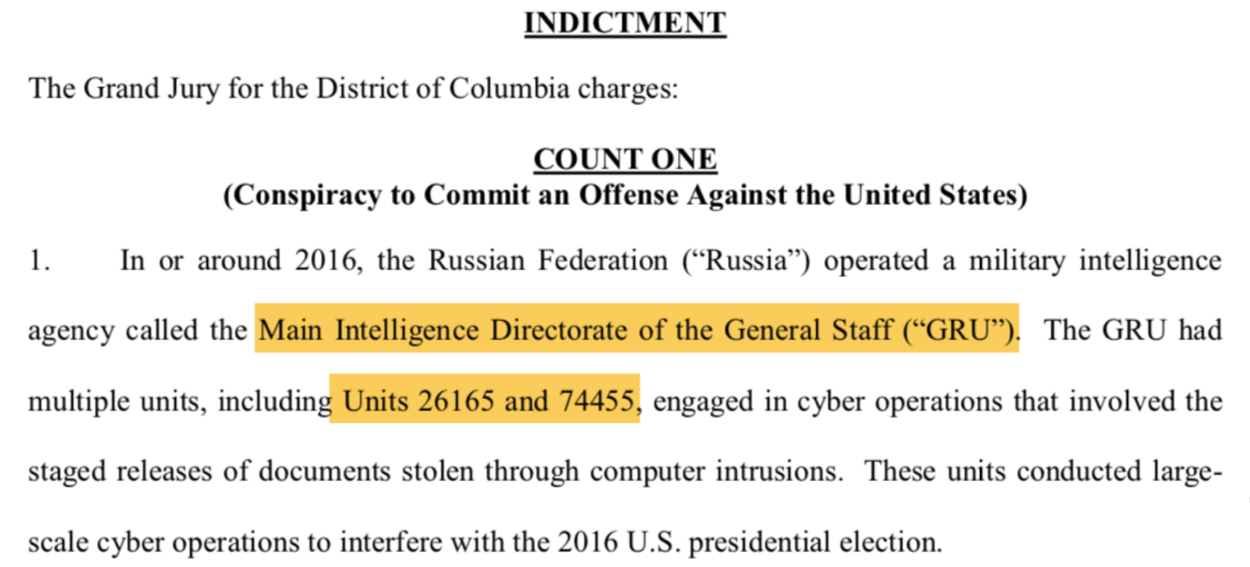
Einleitung

Übersicht und Motivation

- Leak von sensitiven Inhalten des DNC im Sommer 2016
  - Wikileaks
  - Guccifer 2.0
  - DCLeaks.com
- Informationen über ‘undemokratische Vorgänge’ innerhalb der Partei, z.B. Favorisierung von H. Clinton gegenüber B. Sanders
- Anklage von 12 namentlich genannten Russen, eingegangen am 13.7.2018

Anklage

Viele Details

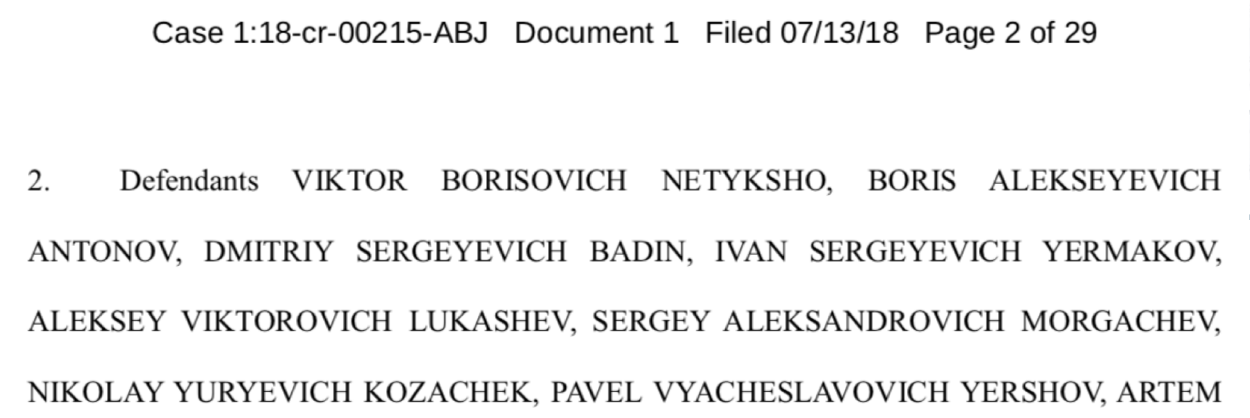


INDICTMENT

The Grand Jury for the District of Columbia charges:

COUNT ONE
(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.



Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 2 of 29

2. Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM

Rechtliches

Rechtliche Perspektive

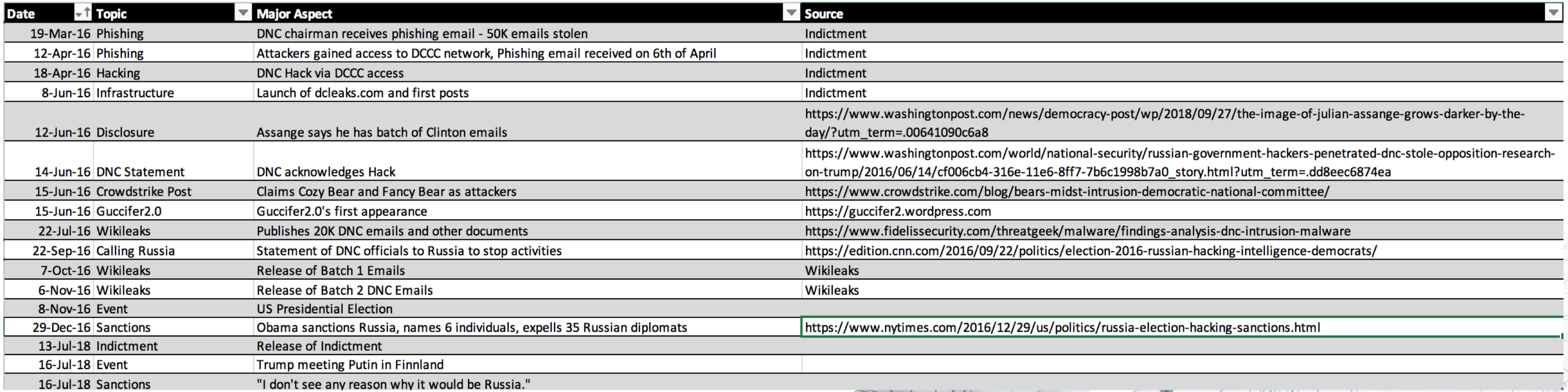
- Anklage ‘nur’ nach US Recht
  - Conspiracy to Commit an Offense Against the United States
  - Aggravated Identity Theft
  - Conspiracy to Launder Money
- Souveränitätsverletzung umstritten - Cyberspionage als Verletzung des Interventionsverbots?
  - Tendenz nicht erkennbar mit Ausnahme von Andeutungen durch USA
- Kein Auslieferungsvertrag auf eigene Bürger

Details aus der Anklage

Woher wissen die das?

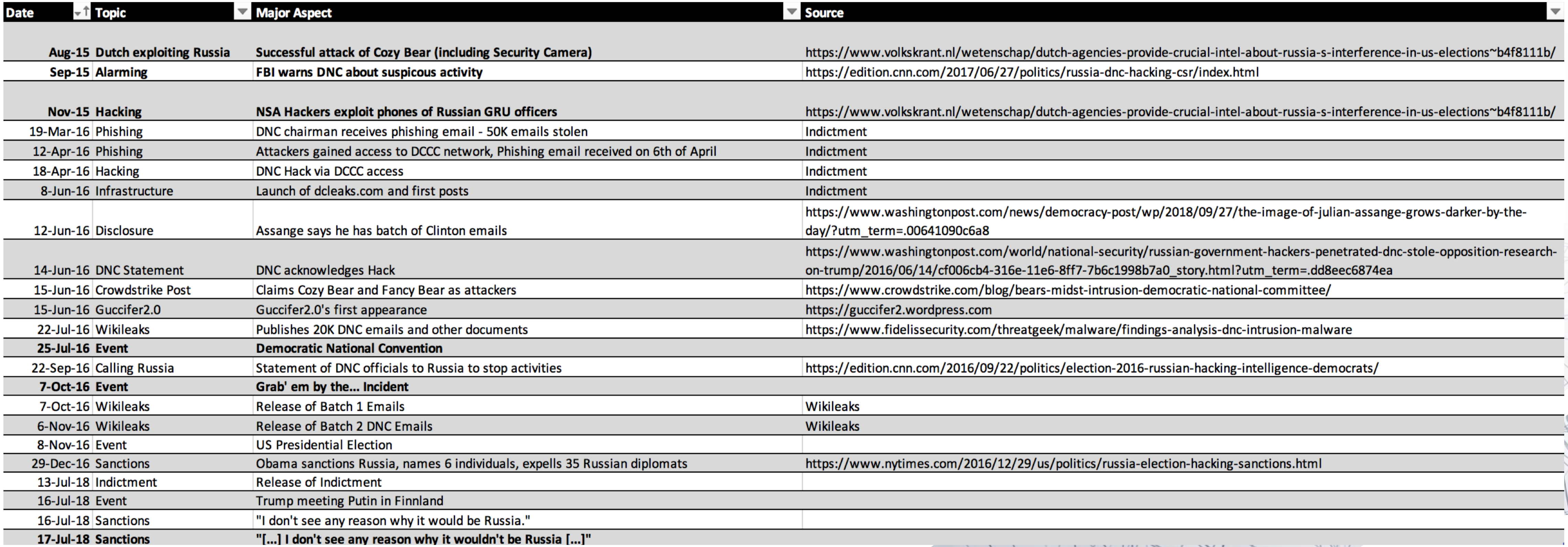
- **Units 26165 and 74455** conducted large- scale cyber operations to interfere with the 2016 U.S. presidential election.
- …used the **same john356gh account** to mask additional links included in spearphishing emails …
- … funds used to pay for the dcleaks.com domain originated from an account at an online cryptocurrency service that the Conspirators **also used** to fund the lease of a virtual private server …
- The Conspirators operated the @dcleaks_ Twitter account **from the same computer** used for other efforts to interfere with the 2016 U.S. presidential election.
- … **researched** PowerShell commands related to accessing and managing the Microsoft Exchange Server
- … Conspirators **logged into** a Moscow-based server used and managed by Unit 74455 and, between 4:19 PM and 4:56 PM Moscow Standard Time, **searched for certain words and phrases** …
- … **ran a technical query** for the DNC’s internet protocol configurations to identify connected devices …

Zeitlicher Ablauf



Date	Topic	Major Aspect	Source
19-Mar-16	Phishing	DNC chairman receives phishing email - 50K emails stolen	Indictment
12-Apr-16	Phishing	Attackers gained access to DCCC network, Phishing email received on 6th of April	Indictment
18-Apr-16	Hacking	DNC Hack via DCCC access	Indictment
8-Jun-16	Infrastructure	Launch of dcleaks.com and first posts	Indictment
12-Jun-16	Disclosure	Assange says he has batch of Clinton emails	https://www.washingtonpost.com/news/democracy-post/wp/2018/09/27/the-image-of-julian-assange-grows-darker-by-the-day/?utm_term=.00641090c6a8
14-Jun-16	DNC Statement	DNC acknowledges Hack	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?utm_term=.dd8eec6874ea
15-Jun-16	Crowdstrike Post	Claims Cozy Bear and Fancy Bear as attackers	https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
15-Jun-16	Guccifer2.0	Guccifer2.0's first appearance	https://guccifer2.wordpress.com
22-Jul-16	Wikileaks	Publishes 20K DNC emails and other documents	https://www.fidelissecurity.com/threatgeek/malware/findings-analysis-dnc-intrusion-malware
22-Sep-16	Calling Russia	Statement of DNC officials to Russia to stop activities	https://edition.cnn.com/2016/09/22/politics/election-2016-russian-hacking-intelligence-democrats/
7-Oct-16	Wikileaks	Release of Batch 1 Emails	Wikileaks
6-Nov-16	Wikileaks	Release of Batch 2 DNC Emails	Wikileaks
8-Nov-16	Event	US Presidential Election	
29-Dec-16	Sanctions	Obama sanctions Russia, names 6 individuals, expells 35 Russian diplomats	https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html
13-Jul-18	Indictment	Release of Indictment	
16-Jul-18	Event	Trump meeting Putin in Finnland	
16-Jul-18	Sanctions	"I don't see any reason why it would be Russia."	

Zeitlicher Ablauf (extended)

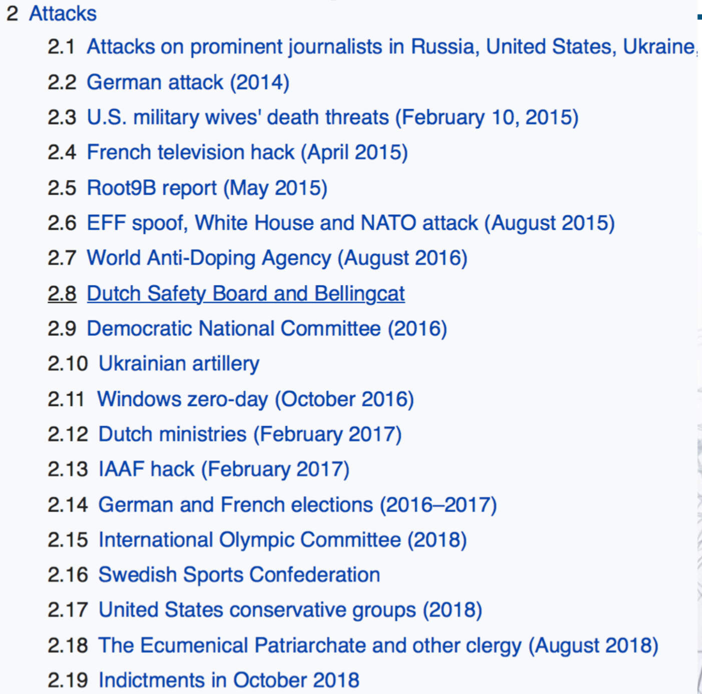


Date	Topic	Major Aspect	Source
Aug-15	**Dutch exploiting Russia**	**Successful attack of Cozy Bear (including Security Camera)**	https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/
Sep-15	**Alarming**	**FBI warns DNC about suspicous activity**	https://edition.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html
Nov-15	**Hacking**	**NSA Hackers exploit phones of Russian GRU officers**	https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/
19-Mar-16	Phishing	DNC chairman receives phishing email - 50K emails stolen	Indictment
12-Apr-16	Phishing	Attackers gained access to DCCC network, Phishing email received on 6th of April	Indictment
18-Apr-16	Hacking	DNC Hack via DCCC access	Indictment
8-Jun-16	Infrastructure	Launch of dcleaks.com and first posts	Indictment
12-Jun-16	Disclosure	Assange says he has batch of Clinton emails	https://www.washingtonpost.com/news/democracy-post/wp/2018/09/27/the-image-of-julian-assange-grows-darker-by-the-day/?utm_term=.00641090c6a8
14-Jun-16	DNC Statement	DNC acknowledges Hack	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?utm_term=.dd8eec6874ea
15-Jun-16	Crowdstrike Post	Claims Cozy Bear and Fancy Bear as attackers	https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
15-Jun-16	Guccifer2.0	Guccifer2.0's first appearance	https://guccifer2.wordpress.com
22-Jul-16	Wikileaks	Publishes 20K DNC emails and other documents	https://www.fidelissecurity.com/threatgeek/malware/findings-analysis-dnc-intrusion-malware
25-Jul-16	**Event**	**Democratic National Convention**	
22-Sep-16	Calling Russia	Statement of DNC officials to Russia to stop activities	https://edition.cnn.com/2016/09/22/politics/election-2016-russian-hacking-intelligence-democrats/
7-Oct-16	**Event**	**Grab' em by the... Incident**	
7-Oct-16	Wikileaks	Release of Batch 1 Emails	Wikileaks
6-Nov-16	Wikileaks	Release of Batch 2 DNC Emails	Wikileaks
8-Nov-16	Event	US Presidential Election	
29-Dec-16	Sanctions	Obama sanctions Russia, names 6 individuals, expells 35 Russian diplomats	https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html
13-Jul-18	Indictment	Release of Indictment	
16-Jul-18	Event	Trump meeting Putin in Finnland	
16-Jul-18	Sanctions	"I don't see any reason why it would be Russia."	
17-Jul-18	**Sanctions**	**"[...] I don't see any reason why it wouldn't be Russia [...]"**	

Analyse durch Crowdstrike

Verbindung mit Russland und den Bären

- 15. Juni 2016
- Identifizierung von
  - Cozy Bear (APT29, seit 2015)
    - Auslandsnachrichtendienst
  - Fancy Bear (APT28, GRU, seit April 2016)
    - Militärischer Geheimdienst
- Bestätigt durch andere Analysen (Fidelis, Mandiant)



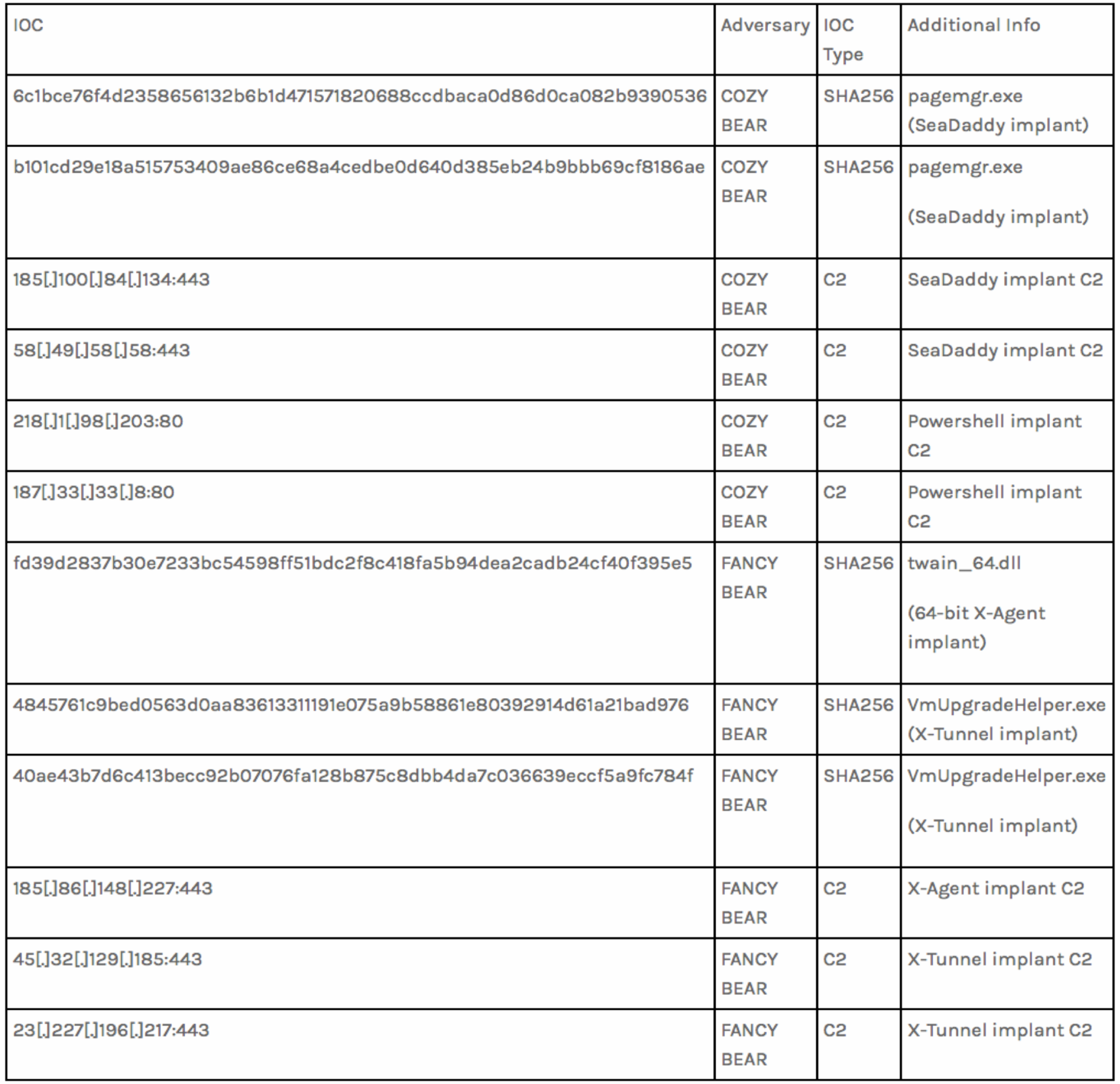
2 Attacks

- 2.1 Attacks on prominent journalists in Russia, United States, Ukraine,
- 2.2 German attack (2014)
- 2.3 U.S. military wives' death threats (February 10, 2015)
- 2.4 French television hack (April 2015)
- 2.5 Root9B report (May 2015)
- 2.6 EFF spoof, White House and NATO attack (August 2015)
- 2.7 World Anti-Doping Agency (August 2016)
- 2.8 Dutch Safety Board and Bellingcat
- 2.9 Democratic National Committee (2016)
- 2.10 Ukrainian artillery
- 2.11 Windows zero-day (October 2016)
- 2.12 Dutch ministries (February 2017)
- 2.13 IAAF hack (February 2017)
- 2.14 German and French elections (2016–2017)
- 2.15 International Olympic Committee (2018)
- 2.16 Swedish Sports Confederation
- 2.17 United States conservative groups (2018)
- 2.18 The Ecumenical Patriarchate and other clergy (August 2018)
- 2.19 Indictments in October 2018

Analyse durch Crowdstrike

IOCs

- Keine Zusammenarbeit zwischen Cozy Bear und Fancy Bear
- Overlapping responsibilities, rarely exchange intel and even steal from each other…
- Portfolio an Toolset
  - X-Agent -> RAT
  - X-Tunnel -> Exfiltration
  - Powershell und Python Tools

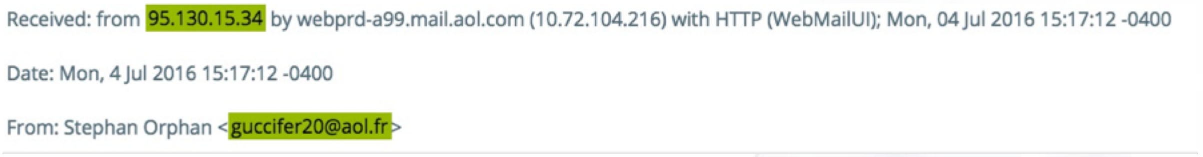


IOC	Adversary	IOC Type	Additional Info
6c1bce76f4d2358656132b6b1d471571820688ccdbaca0d86d0ca082b9390536	COZY BEAR	SHA256	pagemgr.exe (SeaDaddy implant)
b101cd29e18a515753409ae86ce68a4cedbe0d640d385eb24b9bbb69cf8186ae	COZY BEAR	SHA256	pagemgr.exe (SeaDaddy implant)
185[.]100[.]84[.]134:443	COZY BEAR	C2	SeaDaddy implant C2
58[.]49[.]58[.]58:443	COZY BEAR	C2	SeaDaddy implant C2
218[.]1[.]98[.]203:80	COZY BEAR	C2	Powershell implant C2
187[.]33[.]33[.]8:80	COZY BEAR	C2	Powershell implant C2
fd39d2837b30e7233bc54598ff51bdc2f8c418fa5b94dea2cadb24cf40f395e5	FANCY BEAR	SHA256	twain_64.dll (64-bit X-Agent implant)
4845761c9bed0563d0aa83613311191e075a9b58861e80392914d61a21bad976	FANCY BEAR	SHA256	VmUpgradeHelper.exe (X-Tunnel implant)
40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f	FANCY BEAR	SHA256	VmUpgradeHelper.exe (X-Tunnel implant)
185[.]86[.]148[.]227:443	FANCY BEAR	C2	X-Agent implant C2
45[.]32[.]129[.]185:443	FANCY BEAR	C2	X-Tunnel implant C2
23[.]227[.]196[.]217:443	FANCY BEAR	C2	X-Tunnel implant C2

Noch mehr Spuren nach Russland

Guccifer2.0 ein Franzose? ThreatConnect says no!

- Analyse von E-Mails zwischen Guccifer 2.0 und TSG -> französischer AOL Account

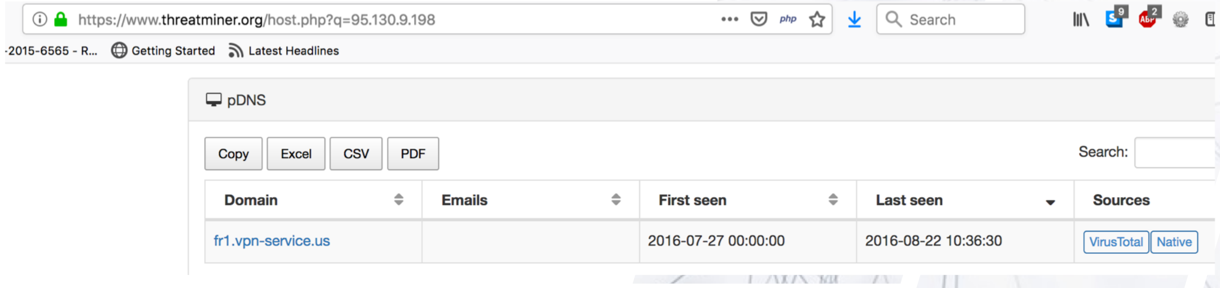


Received: from 95.130.15.34 by webprd-a99.mail.aol.com (10.72.104.216) with HTTP (WebMailUI); Mon, 04 Jul 2016 15:17:12 -0400

Date: Mon, 4 Jul 2016 15:17:12 -0400

From: Stephan Orphan <guccifer20@aol.fr>

- Ähnlicher Host (mit gleichem SSH fingerprint) hat fr1.vpn-service.us gehostet

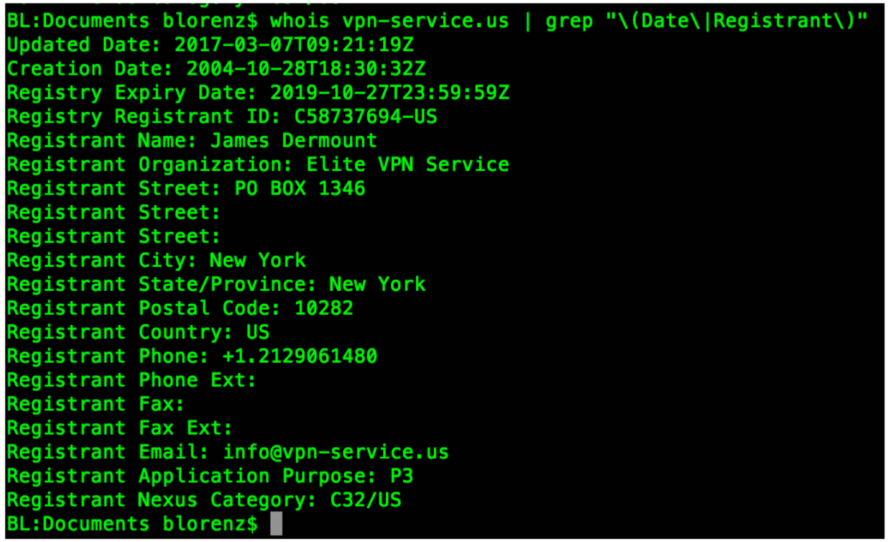


Domain	Emails	First seen	Last seen	Sources
fr1.vpn-service.us		2016-07-27 00:00:00	2016-08-22 10:36:30	VirusTotal Native

Noch mehr Spuren nach Russland

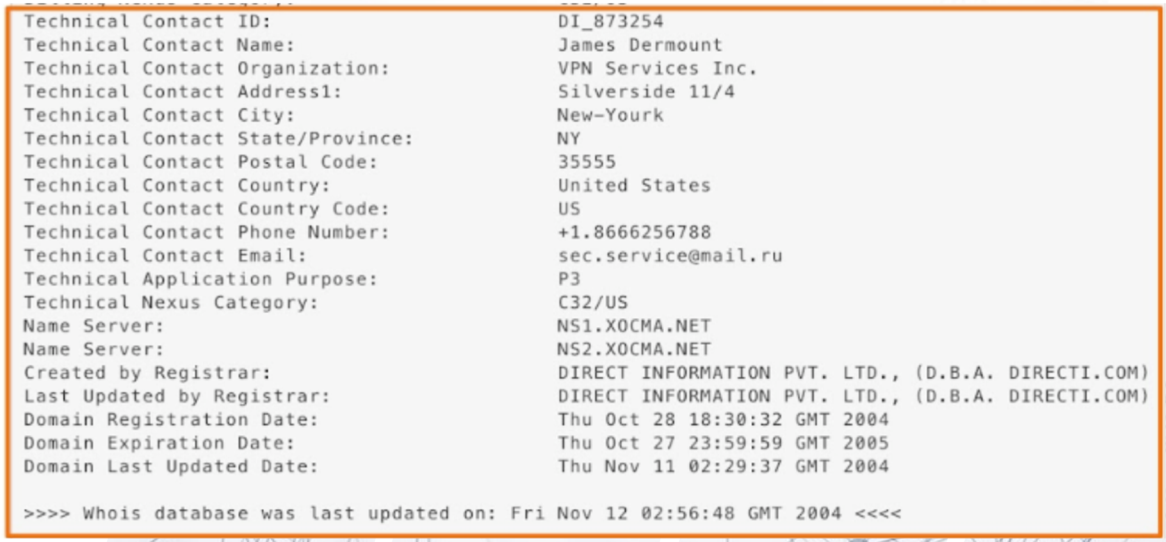
Guccifer2.0 ein Franzose? ThreatConnect says no!

- heute



```
BL:Documents blorenz$ whois vpn-service.us | grep "\(Date\|Registrant\)"
Updated Date: 2017-03-07T09:21:19Z
Creation Date: 2004-10-28T18:30:32Z
Registry Expiry Date: 2019-10-27T23:59:59Z
Registry Registrant ID: C58737694-US
Registrant Name: James Dermount
Registrant Organization: Elite VPN Service
Registrant Street: PO BOX 1346
Registrant Street:
Registrant Street:
Registrant City: New York
Registrant State/Province: New York
Registrant Postal Code: 10282
Registrant Country: US
Registrant Phone: +1.2129061480
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: info@vpn-service.us
Registrant Application Purpose: P3
Registrant Nexus Category: C32/US
BL:Documents blorenz$
```

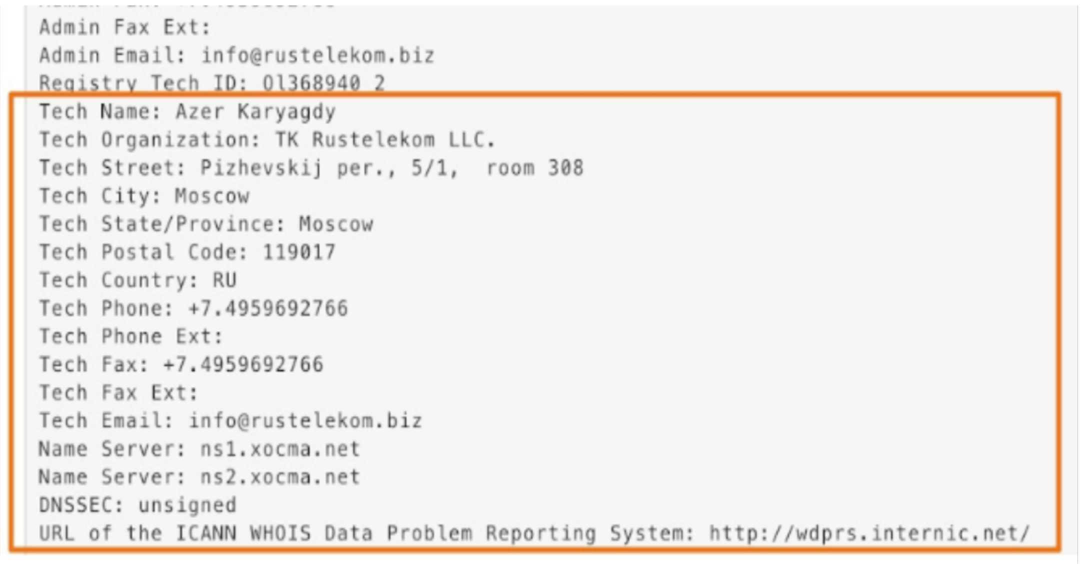
- 2004



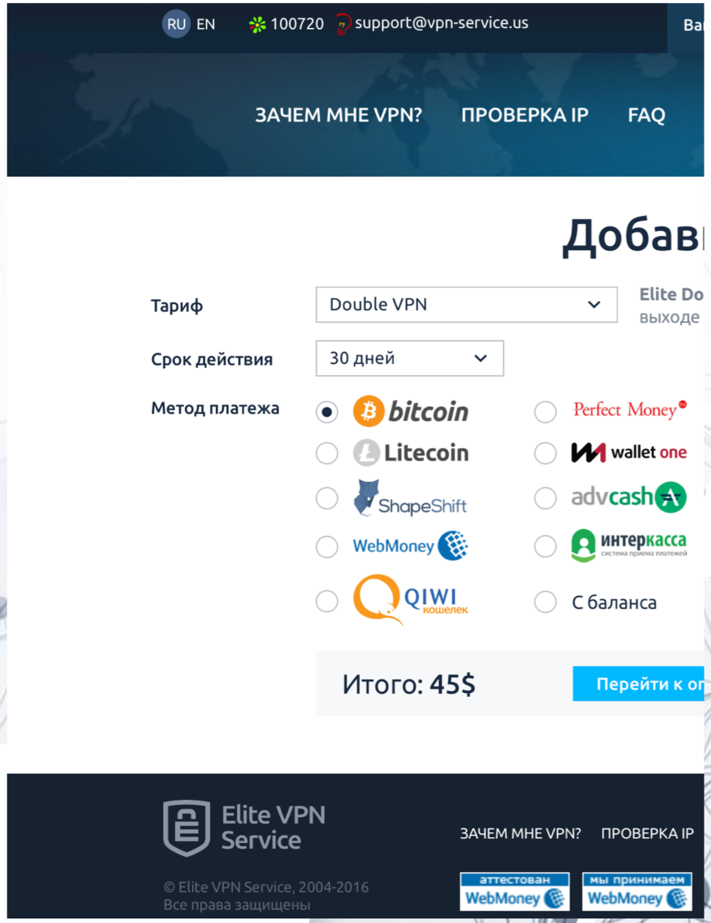
```
Technical Contact ID:                      DI_873254
Technical Contact Name:                    James Dermount
Technical Contact Organization:            VPN Services Inc.
Technical Contact Address1:                Silverside 11/4
Technical Contact City:                    New-Yourk
Technical Contact State/Province:          NY
Technical Contact Postal Code:             35555
Technical Contact Country:                 United States
Technical Contact Country Code:            US
Technical Contact Phone Number:            +1.8666256788
Technical Contact Email:                   sec.service@mail.ru
Technical Application Purpose:             P3
Technical Nexus Category:                  C32/US
Name Server:                               NS1.XOCMA.NET
Name Server:                               NS2.XOCMA.NET
Created by Registrar:                      DIRECT INFORMATION PVT. LTD., (D.B.A. DIRECTI.COM)
Last Updated by Registrar:                 DIRECT INFORMATION PVT. LTD., (D.B.A. DIRECTI.COM)
Domain Registration Date:                  Thu Oct 28 18:30:32 GMT 2004
Domain Expiration Date:                    Thu Oct 27 23:59:59 GMT 2005
Domain Last Updated Date:                  Thu Nov 11 02:29:37 GMT 2004

>>>> Whois database was last updated on: Fri Nov 12 02:56:48 GMT 2004 <<<<
```

Noch mehr Spuren nach Russland

Guccifer2.0 ein Franzose? ThreatConnect says no!



```
Admin Fax Ext:
Admin Email: info@rustelekom.biz
Registry Tech ID: 01368940 2
Tech Name: Azer Karyagdy
Tech Organization: TK Rustelekom LLC.
Tech Street: Pizhevskij per., 5/1,  room 308
Tech City: Moscow
Tech State/Province: Moscow
Tech Postal Code: 119017
Tech Country: RU
Tech Phone: +7.4959692766
Tech Phone Ext:
Tech Fax: +7.4959692766
Tech Fax Ext:
Tech Email: info@rustelekom.biz
Name Server: ns1.xocma.net
Name Server: ns2.xocma.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```



Добав

Тариф: Double VPN

Elite Do
выходе

Срок действия: 30 дней

Метод платежа:
● bitcoin ○ Perfect Money
○ Litecoin ○ wallet one
○ ShapeShift ○ advcash
○ WebMoney ○ интеркасса
○ QIWI кошелек ○ С баланса

Итого: 45$

Перейти к о

© Elite VPN Service, 2004-2016
Все права защищены

Noch mehr Spuren nach Russland

Guccifer2.0 ein Franzose?

- Fehler der Angreifer
  - Guccifer2.0 Story wird zunehmend unglaubwürdig
  - Verwendung eines Providers, der viele Metadaten ausgibt

Podesta Phishing

Der Mensch das schwächste Glied!

- Vorsitzende der Hillary Clinton Kampagne
- Einer der ersten Angriffe
- 50K E-Mails gestohlen

- **Demo vom Spearphishing** E-Mail

Podesta Phishing

Der Mensch das schwächste Glied?

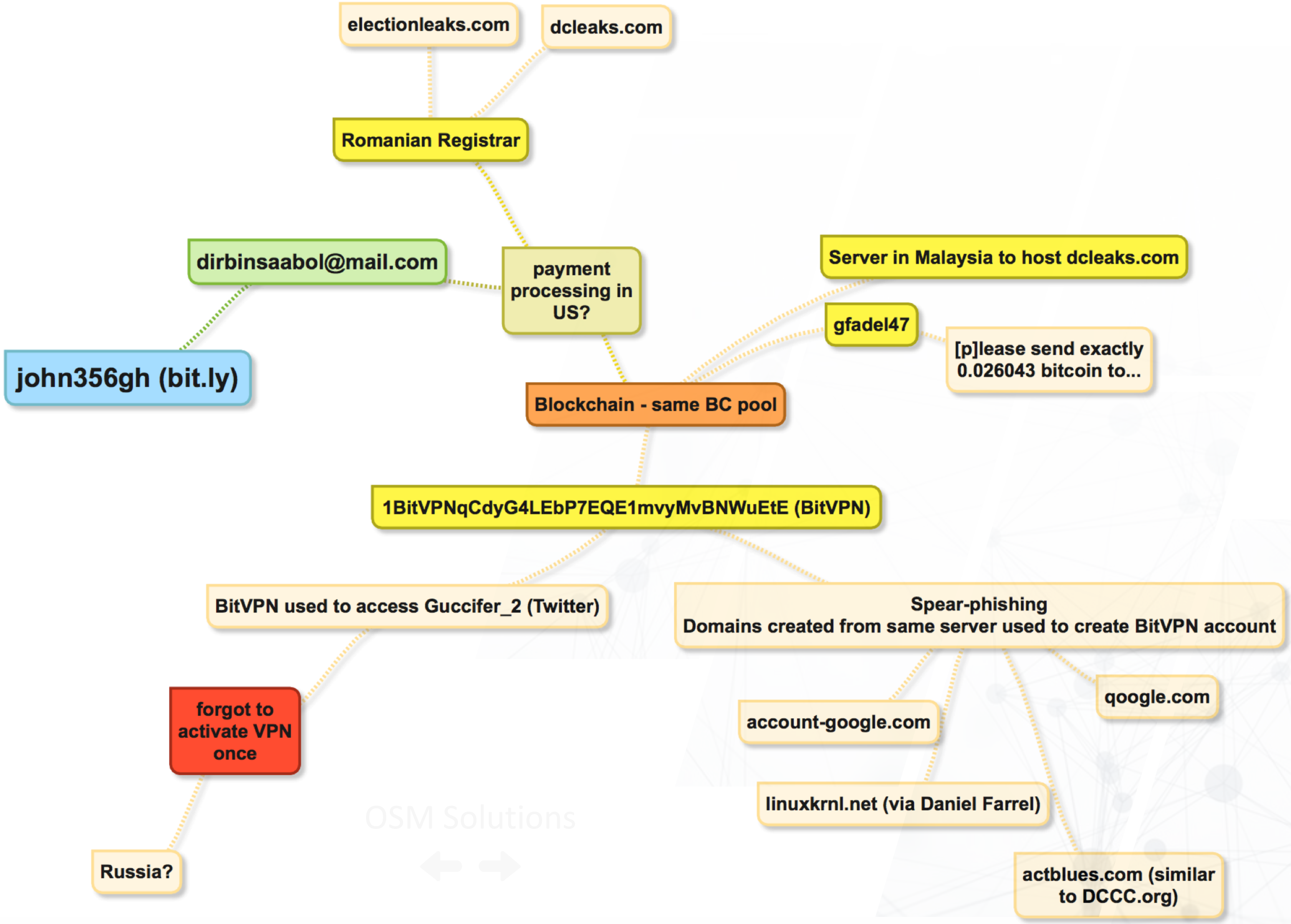
- Triviale Aufarbeitung durch Behörden
  - Bit.ly ein US-Unternehmen -> Patriot Act und Cloud Act ziehen -> Einsicht der US Behörden
  - Angreifer war angemeldet (?) -> john356gh

- Fehler der Opfer
  - MFA
  - Awareness
  - Privater Account?

Follow the money (and user accounts)

Spielverderber Blockchain

- Wiederverwendung von
  - Bitcoin Pools
  - Benutzerkonten
  - Infrastruktur
  - E-Mail Adressen
- Bitcoin =! Anonymität
- Ein Fehler deckt das ganze Netzwerk auf



electionleaks.com

dcleaks.com

Romanian Registrar

dirbinsaabol@mail.com

payment processing in US?

Server in Malaysia to host dcleaks.com

gfadel47

[p]lease send exactly 0.026043 bitcoin to...

john356gh (bit.ly)

Blockchain - same BC pool

1BitVPNqCdyG4LEbP7EQE1mvyMvBNWuEtE (BitVPN)

BitVPN used to access Guccifer_2 (Twitter)

Spear-phishing
Domains created from same server used to create BitVPN account

forgot to activate VPN once

qoogle.com

account-google.com

linuxkrnl.net (via Daniel Farrel)

Russia?

actblues.com (similar to DCCC.org)

Allgemeine Fehler!(?)

Viel Raum für Verschwörungstheorien

- Wiederverwendung von Benutzerkonten und Infrastruktur
- C2-Server aus Arizona and Illinois (Gut und schlecht)
  - Erst Tage später einen weiteren Hop eingefügt, vorher direkt mit C2-server kommuniziert
- Bekannte Malware verwendet (X-Tunnel und X-Agent deuten auf Fancy Bear hin)
- Metadata in Dokumenten vergessen -> Russland
- Sprachkenntnisse und Stil (über die Zeit verändert)
- Financial tracing (Bitcoin garantiert nicht Anonymität)
- Schlechtes timing
- OPSEC Fail – VPN nicht aktiviert

Conclusion

Was wissen wir

- Manche Zusammenhänge erklärbar, viele vermutbar, das Meiste aber nicht bewiesen
- Raum für sehr viele Verschwörungstheorien
- Ev. herkömmliche Spionage?
  - Ganze Reihe von Verhaftungen von rahnghohen Geheimdienstmitarbeitern
- Fehler der Angreifer?

- Krieg in der Cyberwelt!

Quellen

Zum selbst Nachlesen

- https://www.justice.gov/file/1080281/download
- https://threatconnect.com/blog/tapping-into-democratic-national-committee/
- https://threatconnect.com/blog/guccifer-2-all-roads-lead-russia/
- https://www.elliptic.co/our-thinking/doj-indictment-russian-hackers-blockchain-analysis
- https://www.fidelissecurity.com/threatgeek/malware/findings-analysis-dnc-intrusion-malware
- https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/
- https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer
- https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
- https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/
- 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?utm_term=.dd8eec6874ea

Danke sehr!

OSM Solutions GmbH
Praterstraße 48/4
1020 Wien

office@osm-s.com
www.osm-s.com