Club de la sécurité de l'information français

Panorama de la cybercriminalité année 2016

Paris, 11 janvier 2017

Evénement organisé avec le soutien de nos sponsors

Club de la sécurité de l'information français

CLUSIF

Élection, géopolitique et cybersécurité

Loïc GUEZO
Stratégiste CyberSécurité pour Trend Micro France – Trend Micro Inc.

@lguezo

Panorama Cybercriminalité, année 2015

Panorama Cybercriminalité, année 2015

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Et la Russie ?

- Un pacte sino-russe de non agression, signé 4 mois avant les rencontres avec les USA
- Ne signifie pas pour autant l'arrêt des opérations entre eux
- Volonté russe de suivre la Chine dans son activité de Gouvernance de l'Internet ? Surement car entre Ouverture et Souveraineté, Russie et Chine sont largement alignés sur l'idée de Souveraineté.

- De l' actualité en Ukraine (et en Crimée comme vers l'Ouest), principalement autour des systèmes ICS/SCADA, Energie …

2016, année présidentielle, à risque

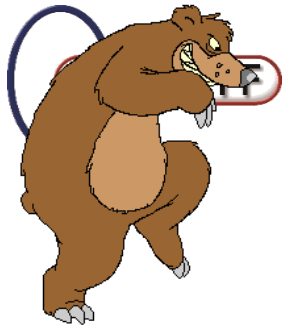
National intelligence director: Hackers have targeted 2016 presidential campaigns

Director of National Intelligence James Clapper speaks on Capitol Hill on Feb. 9. (Alex Brandon/AP)

Chronologie simplifiée – Elections le 8/11

- Juin – **intrusion DNC publique** ; BEARS versus Guccifer 2.0
- Juillet – Wikileaks publie 20000 mails ; FBI ouvre une enquête
- Août – publication de données personnelles (GSM) Démocrates
- Septembre – V.POUTINE déclare n'avoir rien à voir avec le hacking mais que les données révélées sont importantes.
- 7 octobre – DHS et ONI sont "confident that the Russian Government directed the recent compromises of emails from US persons and institutions."
- 10 octobre – Podesta emails part 1 …
- 8 novembre – **Election de D.Trump**
- 29 novembre – demande de déclassification d'informations ; il apparaitrait la volonté de favoriser les votes Trump
- 9 décembre – FBI et CIA non alignés ; Obama demande un travail de fonds (depuis 2008) dont le compte-rendu est à rendre avantle 20 janvier
- 12 décembre – Intérêts Républicains piratés ; pas de diffusion
- 29 décembre – **Executive order** de Obama avec 35 diplomates expulsés

Parfum de guerre froide



Story highlights

Experts say Russian hackers breached the DNC files on Donald Trump

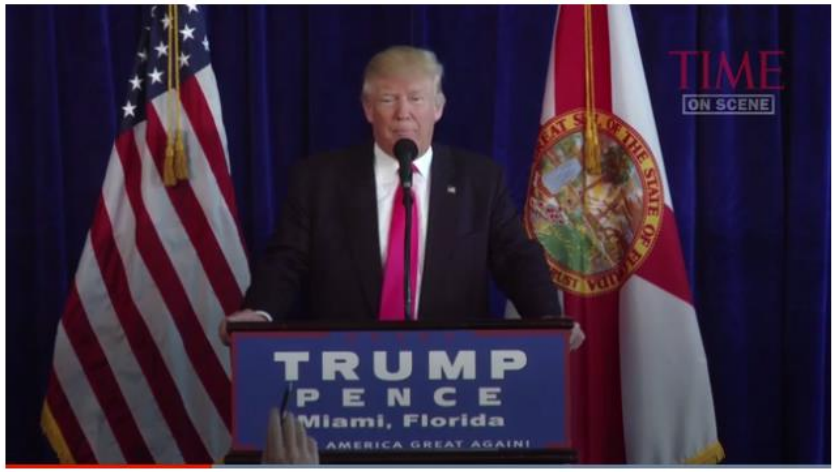
CrowdStrike was enlisted by the DNC early last month

Washington (CNN) — Hackers connected to the Russian government broke into the servers of the Democratic National Committee and stole opposition research on Donald Trump, the cybersecurity experts responding to the intrusion said Tuesday.

Two separate Russian intelligence-linked cyberattack groups were both in the DNC's networks, Dmitri Alperovitch, co-founder and chief technology officer of CrowdStrike, which responded to the breach, told CNN. They likely didn't even know the other was in the systems, he added.

The U.S. government, however, has not yet determined that the hackers who breached the server are connected to the Russian government, a U.S. official told CNN.

Wikileaks - DNC



Donald Trump encouraged Russia to commit a cybercrime against Hillary Clinton, saying he hoped the foreign nation could recover some of her deleted emails.

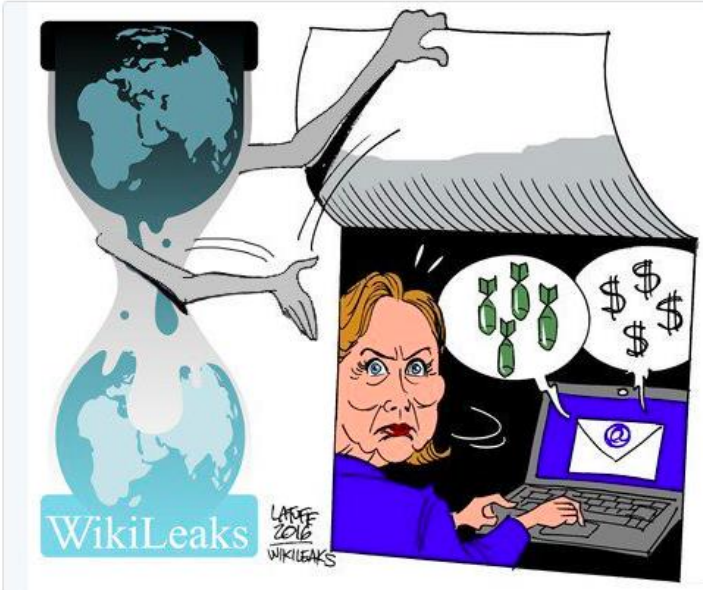
"Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing," Trump said at a press conference in Doral, Florida, Wednesday morning after the second night of the Democratic convention. "I think you will probably be rewarded mightily by our press. Let's see if that happens."

WikiLeaks @wikileaks — Suivre

RELEASE: 8,034 US DNC attachmentments including thousands of images, 891 documents & 175 spreadsheets wikileaks.org/dnc-emails/?fi…

17:11 - 22 Juil 2016

1 783 1 455



WikiLeaks @wikileaks — Suivre

RELEASE: 19,252 emails from the US Democratic National Committee wikileaks.org/dnc-emails/ #Hillary2016 #FeelTheBern

16:50 - 22 Juil 2016

15 925 13 853

Wikileaks – John Podesta

- Publication de 60 000 courriels échangés par le staff de la candidate :
  - Dessous de la campagne,
  - Pratiques de la fondation Clinton,
  - Liens intimes avec certains journalistes …

- « Un enfant de 14 ans aurait pu pirater les emails de Podesta », affirme Julian Assange.

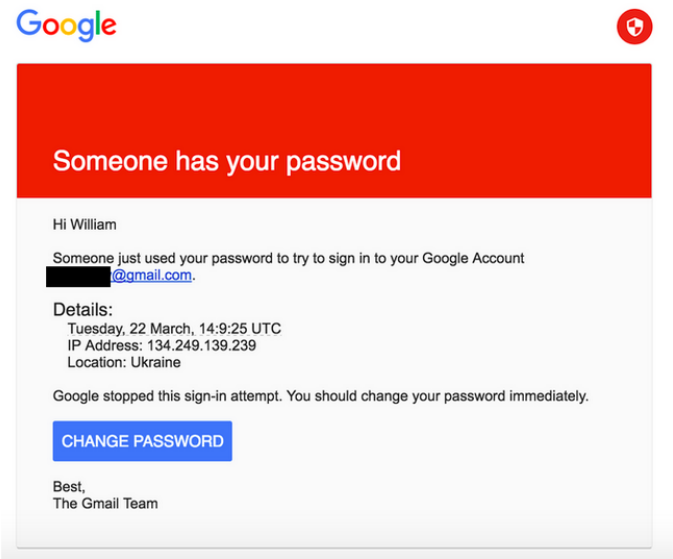
- Podesta's password is …

P@ssw0rd

- "La source est le gouvernement russe, et il y a d'autres informations, non divulguées.", ou pas …

Parasitage de la campagne !

- A NOTER pour RSSI les signes avant-coureurs ignorés, l'absence de réaction ad-hoc, (il)legitimate …
- Faible réaction de la Maison Blanche dans les premiers mois



Incrimination officielle de la Russie …

Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security

Release Date: October 7, 2016

For Immediate Release
DHS Press Office
Contact: 202-282-8010

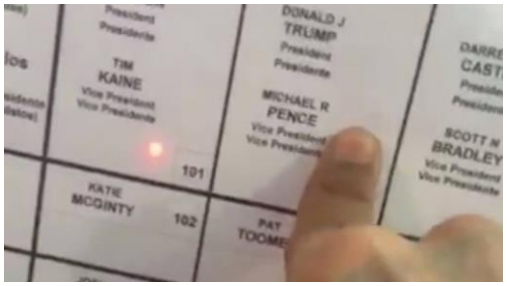
The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

… mais rassurant sur piratage du vote ?

Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government. The USIC and the Department of Homeland Security (DHS) assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyber attack or intrusion. This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place. States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process.

Théorie du possible

50+ modèles, petites structures de maintenance
Pas de connexion, mais paramétrage, comptages…
Logs papier (dans 70% des cas) ; inutilisable.
Le 1% qui swingue …



In fine : ATTENTION pour 2020 !

15.12 Piratage par RASPUTIN de l'Election Assistance Commission, autorité de certification …

Rapport officiel

Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity

Release Date: December 29, 2016

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

On October 7, 2016, Secretary Johnson and Director Clapper issued a joint statement that the intelligence community is confident the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations, and that the disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks are consistent with the Russian-directed efforts. The statement also noted that the Russians have used similar tactics and techniques across Europe and Eurasia to influence public opinion there.

Today, DHS and FBI released a Joint Analysis Report (JAR) which further expands on that statement by providing details of the tools and infrastructure used by Russian intelligence services to compromise and exploit networks and infrastructure associated with the recent U.S. election, as well as a range of U.S. government, political and private sector entities.

This activity by Russian intelligence services is part of a decade-long campaign of cyber-enabled operations directed at the U.S. Government and its citizens. These cyber operations have included spearphishing, campaigns targeting government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations; theft

Preuves ?

TLP:WHITE

NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

*DISCLAIMER: This report 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. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as **TLP:WHITE:** Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296 **December 29, 2016**

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

RT
@RT_com

Suivre

No real proof in 'Russian hacking' report, as it lacks crucial details – ex-NSA tech director

À l'origine en anglais

No real proof in 'Russian hacking' report, as it lacks crucial details – ex-NSA t...

The FBI report supposedly bursting with evidence that Russian hackers breached US servers contains no real proof, computer experts say – among them former N...

rt.com

RETWEETS 301 J'AIME 291

13:02 - 1 janv. 2017

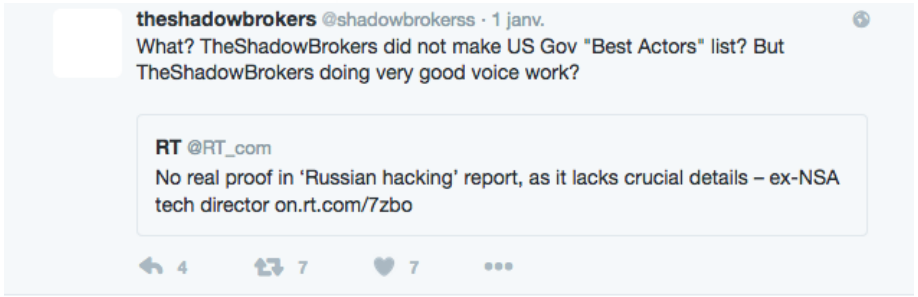
28 301 291

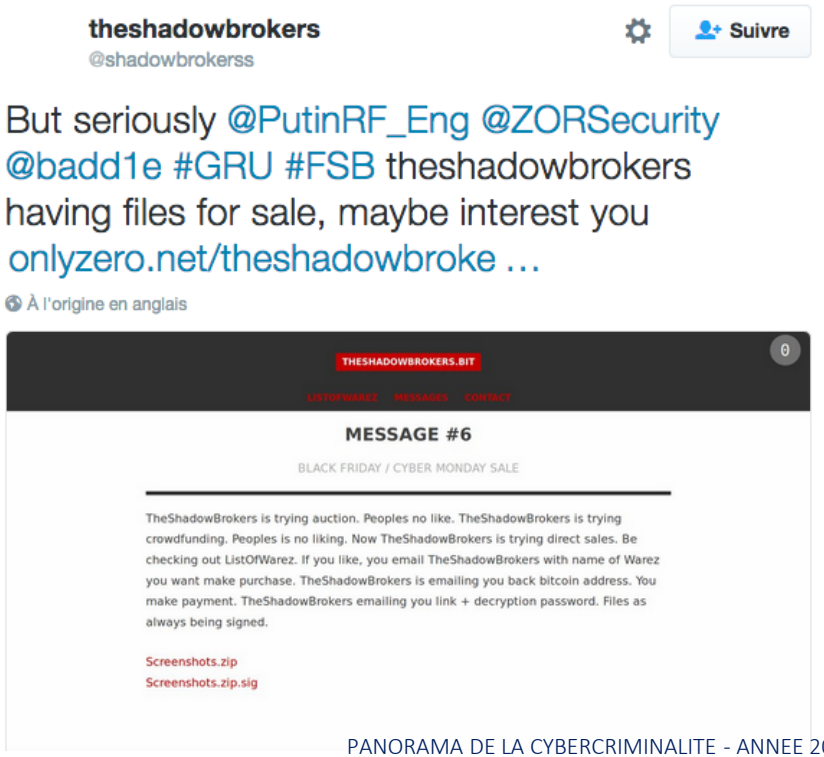
V.PUTIN, @realDonaldTrump et @POTUS

Trente-cinq diplomates russes expulsés

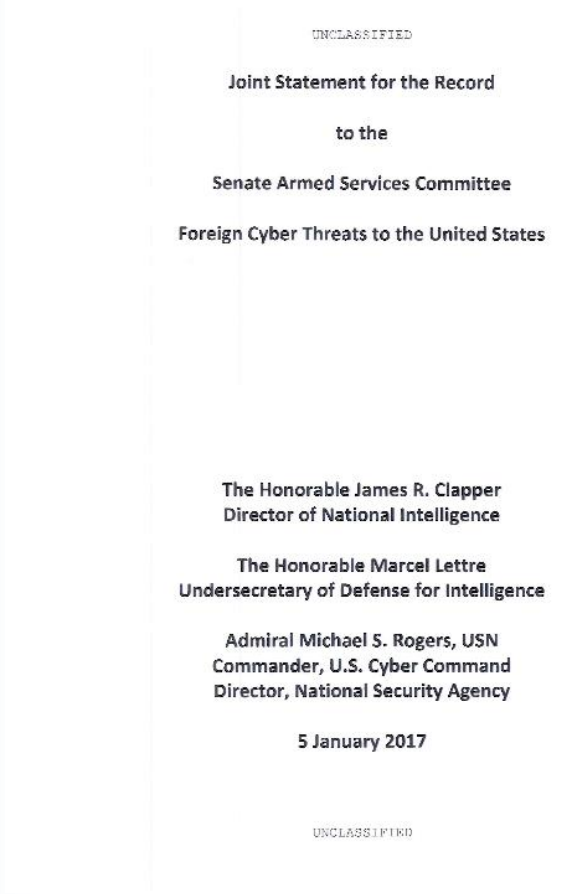
« Nous n'allons expulser personne », a assuré Vladimir Poutine, vendredi, alors que son chef de la diplomatie, Sergueï Lavrov, avait proposé d'expulser trente-cinq diplomates américains. La Russie se réserve toutefois *« le droit de prendre des mesures de rétorsion »*, et *« restaurera les relations russo-américaines au vu de ce que sera la politique du président américain élu Donald Trump »*, a précisé le président russe.

Cyber dissémination en cours …





Vers un “Bras de fer” annoncé ?



UNCLASSIFIED

Joint Statement for the Record

to the

Senate Armed Services Committee

Foreign Cyber Threats to the United States

The Honorable James R. Clapper
Director of National Intelligence

The Honorable Marcel Lettre
Undersecretary of Defense for Intelligence

Admiral Michael S. Rogers, USN
Commander, U.S. Cyber Command
Director, National Security Agency

5 January 2017

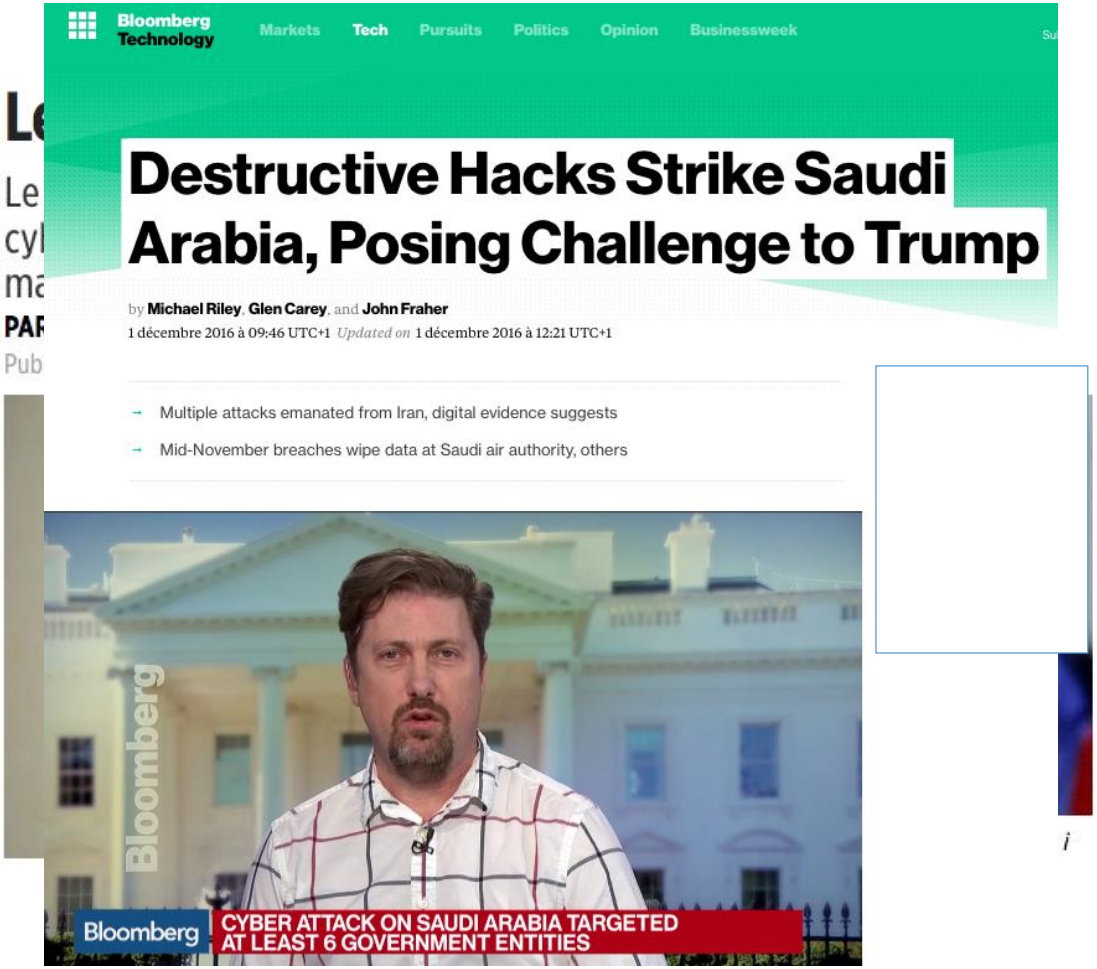
UNCLASSIFIED

Cyber Threat Actors

Russia. Russia is a full-scope cyber actor that poses a major threat to U.S. Government, military, diplomatic, commercial, and critical infrastructure and key resource networks because of its highly advanced offensive cyber program and sophisticated tactics, techniques, and procedures. In recent years, we have observed the Kremlin assume a more aggressive cyber posture. Russian cyber operations targeted government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations often using spearphishing campaigns. In foreign countries, Russian actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases Russian intelligence actors have masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. We assess that only Russia's senior-most officials could have authorized the recent election-focused data thefts and disclosures, based on the scope and sensitivity of the targets. Russia also has used cyber tactics and techniques to seek to influence public opinion across Europe and Eurasia. Looking forward, Russian cyber operations will likely target the United States to gather intelligence, support Russian decisionmaking, conduct influence operations to support Russian military and political objectives, and prepare the cyber environment for future contingencies.

China. Beijing continues to conduct cyber espionage against the U.S. Government, our allies, and U.S. companies. Since the China-U.S. cyber commitments in September 2015, private-sector security experts continue to detect cyber activity from China, although at reduced levels and without confirmation that stolen data was used for commercial gain. Beijing has also

L’actualité semble le démontrer …



Mais pas forcément celui attendu !

Russia hacking: US intelligence chief hits back at Trump's 'disparagement'

James Clapper tells Congress he will release more evidence of Russian interference in US election and describes 'multifaceted' cyber assault

Clapper made clear that Russia did not alter vote tallies but said that US intelligence agencies 'stand more resolutely' behind their findings of cyber-attacks during the election campaign. Photograph: Chip Somodevilla/Getty Images

2017, année d'élections en Europe

L'Allemagne accuse la Russie de cyberattaques

Berlin voit dans la multiplication de récents piratages informatiques la volonté de Moscou de perturber le jeu politique à moins d'un an des législatives allemandes.

Le Monde.fr avec AFP | 29.11.2016 à 14h21 • Mis à jour le 30.11.2016 à 19h20

Bruno Kahl, le patron des services secrets allemands, et la chancelière Angela Merkel, le 28 novembre, à Berlin. HANNIBAL HANSCHKE / AFP

L'Agence nationale de la sécurité des systèmes d'information (Anssi) prévient que les partis politiques peuvent être visés par des piratages. PATRICK KOVARIK / AFP

L'élection présidentielle française risque-t-elle d'être perturbée par des attaques informatiques ? Le risque est très concret, ont prévenu lors d'une conférence de presse, mercredi 21 décembre, l'Agence nationale de la sécurité des systèmes d'information (Anssi) et le secrétariat général de la défense et de la sécurité nationale (SGDSN), auquel la première est rattachée.

Sources consultées (images et contenus)

- 2016, année à risque
https://www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html
- DNC hack
http://edition.cnn.com/2016/06/14/politics/democratic-national-committee-breach-russians-donald-trump/
- Incrimination par le DHS, 7 octobre
https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national
- Résumé des faits
http://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/
- Rapport officiel pour l'executive order
https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
- Piratage des machines à voter ?
http://www.lemonde.fr/pixels/article/2016/12/30/il-est-facile-de-pirater-l-election-americaine-assurent-des-specialistes-du-vote-electronique_5055823_4408996.html
- Vidéo de D.TRUMP sur sa position versus le piratage de l'élection US
https://www.youtube.com/watch?v=gRMlkSK5eGs
- EAC piratée par Rasputin
https://www.engadget.com/2016/12/15/hacker-breaches-the-us-agency-that-certifies-voting-machines/
- Rapport Cyber Threat US du 5 janvier 2017
http://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf
- Alarmes de l'Allemagne et de la France sur élections de 2017
http://www.lemonde.fr/europe/article/2016/11/29/l-allemagne-accuse-la-russie-de-cyberattaques_5040241_3214.html
http://www.lemonde.fr/pixels/article/2016/12/21/des-attaques-informatiques-a-visee-politique-envisageables-en-france_5052650_4408996.html
- Le rôle de WikiLeaks, selon WikiLeaks
http://www.lefigaro.fr/flash-actu/2017/01/05/97001-20170105FILWWW00075-assange-un-ado-de-14-ans-aurait-pu-pirater-podesta.php