DATA BREACH IN GERMANY, 2018

INVESTIGATION REPORT

WHAT HAPPENED

- On January 3, 2019, German media, including newspaper Bild and broadcasting company RBB Inforadio, reported a data breach in German Parliament. Personal data and documents of more than 100 German politicians, including German Chancellor Angela Merkel, German president Frank-Walter Steinmeier and Brandenburg's prime minister Dietmar Woidke, along with some German artists, journalists, and YouTube celebrities was leaked on Twitter. Journalists from public broadcasters ARD and ZDF as well as TV satirist Jan Böhmermann, rapper Marteria and rap group K.I.Z were among the ones affected. In total, about 1,000 people were affected in the data leak scandal. That is the point from which public and police interest rose quickly.

- The data looked initially to largely be from private cloud storage and social media accounts than a particular official server. Private information was stolen for the purposes of publishing online, known in the tech world as "doxxing". Along with Twitter, Outlook and Facebook accounts were also hacked. According to security experts who've seen portions of the data, the hacker spread the stolen information across several sites and mirrors, making it "really hard to take down." It was reported that the hacker may have obtained passwords using social engineering or possibly phishing techniques to access social media accounts. Often, hackers do this by tricking a phone company into "porting out" a person's phone number to another SIM card, allowing them to password reset accounts or obtain two-factor codes.

- The leaks showed extensive data about some politicians, including photos, chat logs and private letters, but little on others except private addresses, phone numbers, Skype and e-mail addresses as well as semi-public information (e.g. names of relatives); much apparently all this was painstakingly compiled. German media said a fax number and two email addresses used by Angela Merkel had been published. According to a government spokesperson, there was no "sensitive" data from the chancellor's office, but other lawmakers had more personal data stolen. The hacked material included private chats by Greens leader Robert Habeck with family members and the identity cards of his children.

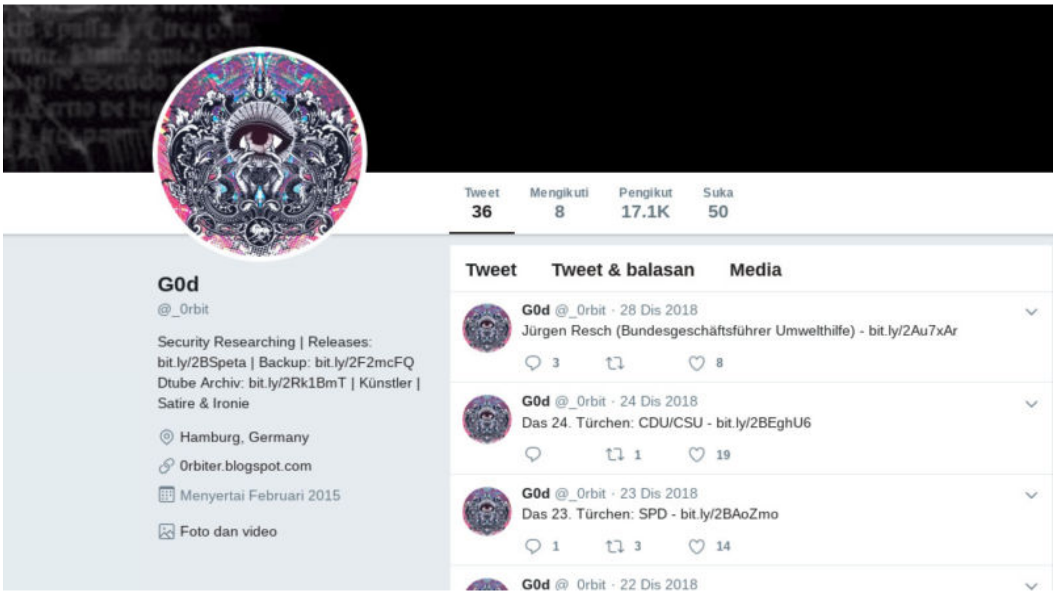
- The hacker leaked data on senior lawmakers across the political spectrum, but noticeably absent were accounts for the country's far-right Alternative for Germany (AfD) party, as per the statement from Germany's Federal Office for Information Security (BSI). It believed there was no attack on the government's networks. Die Welt newspaper reported that published lists included names of 410 members of Merkel’s conservatives, 230 Social Democrats, 106 Greens party members, 91 members of the radical Left party and 28 Free Democrats. The Defence Ministry said the armed forces were not affected.

- Justice Minister Katarina Barley described the incident as a “serious attack” and added: “The perpetrators wanted to damage our trust in democracy and our institutions.”

HOW IT HAPPENED

- According to German newspaper Die Zeit, the leak itself started on December 1, 2018, when a username named G0d (Twitter handle “@_orbit”) started to tweet sensitive details and links to download sites containing sensitive data regarding German celebrities and parliament members. These tweets continued on a daily basis and went mostly unnoticed until the 24th of December 2018. In parallel, these links were also published on a Word press blog bearing the same name (G0d / @_orbit).

- The Twitter account, which existed for four years and reportedly had more than 18,000 followers, released the data as a sort of ‘Advent calendar’ throughout December. On each day of Advent, a “door” leading to a cache of stolen data was released. G0d took great care to make it difficult to take down the files, creating numerous mirror locations and using servers outside Germany. The account, which has since been suspended, had been tagged with the terms "security researching", "artist" and "satire and irony" and as being based in Hamburg.



G0d
@_0rbit

Security Researching | Releases: bit.ly/2BSpeta | Backup: bit.ly/2F2mcFQ Dtube Archiv: bit.ly/2Rk1BmT | Künstler | Satire & Ironie

Hamburg, Germany
0rbiter.blogspot.com
Menyertai Februari 2015
Foto dan video

G0d @_0rbit · 28 Dis 2018
Jürgen Resch (Bundesgeschäftsführer Umwelthilfe) - bit.ly/2Au7xAr
3 8

G0d @_0rbit · 24 Dis 2018
Das 24. Türchen: CDU/CSU - bit.ly/2BEghU6
1 19

G0d @_0rbit · 23 Dis 2018
Das 23. Türchen: SPD - bit.ly/2BAoZmo
1 3 14

G0d @_0rbit · 22 Dis 2018

- Interior Minister, Horst Seehoferm said that a preliminary analysis showed the data had been obtained through “wrongful use of log-in information for cloud services, email accounts or social networks”. He said the hacker would not have been able to gather as much data as he had, if his victims had created more sophisticated passwords. He said Bad passwords were one of the reasons he had it so easy. He was shocked at how simple most passwords were like a whole array of really simple things.

- It was discovered that the data leak was done by a 20-year-old man named Johannes S., living in the western state of Hesse, who is considered having “considerable IT skills”. The German police arrested the suspected hacker on Sunday, January 6, 2019, at which point it systematically started removing the links the hacker posted. On January 4th, a friend of the hacker named Jan Schürlein (Twitter handle @janomine), published an email correspondence with the hacker in which he told him that he is going to close his telegram account and destroy his computer.

- Later, Johannes S. made a "comprehensive" confession that he was behind a data breach that some blamed on foreign intelligence services. He was accused of spying and unauthorised publication of data. He insisted that he used no malware or other spy software but simple password-cracking software. Investigators, quoted by DPA, said he had taught himself the skills he needed using online resources, and had no training in computer science. He took advantage of passwords as weak as “Iloveyou” and “1234” to hack into online accounts. He used relatively simple techniques to hack into successive accounts in peoples’ smartphones. He "exploited several vulnerabilities", investigators said, adding that several such security gaps have since been fixed. While the German police responded slowly to the case, the hacker moved quickly to upload the data to as many media outlets as he could, thus ensuring that the breached data will be available for download even if he were arrested. There were over 70 mirrors of the initial download link alone, while each of the 40 download links has another 3-5 mirrors each. Each of the tens of thousands of files uploaded appeared to have its own or indeed multiple mirrors; something that would have taken a huge amount of manpower. He used the following aliases in his different publications: G0d@_0rbit, 'r00t OF 0rbit', nullr0uter, r00taccess, NFOr00t, Ther00t, Jitachi, dennis567 and p0wer.

- The initial publications from police investigation showed that he acted alone and was motivated by a right wing political agenda (advent by the lack of leaked “AfD” documents). He stated that he leaked the information of figures that “annoyed him.” Investigators say it is likely he acted alone but are still searching for clues of third-party involvement on his computers, hard drives and other technical equipment.

- Before leaking the private details of German government officials, Johannes S. was known for doxxing several YouTubers in 2016 with his NFOr00t alias.The Email correspondence with Janomine also exposes his alias "Ther00t" as it points to another email address: Ther00t@portonmail.com. This address is also associated with prior doxing operations

- The leaked data is a composition of freely obtainable materials, including personal email correspondence and personal photos and documents most likely obtained directly from phone hacks/malware (SMS correspondence) or cloud backup hacks (cloud backup storage). As the documents were collected across many years and from various sources, it cannot be attributed to one specific source. It is highly likely that it came from multiple different hacks that were initiated across the years by different threat actors, and aggregated to this database by Johannes S. For example, some folders in the breach came from smartphone galleries or cloud accounts that date back to circa 2013. The private information seemed to have been acquired over a substantial period of time in 2018 in what officials called a "sophisticated" operation, and added to publicly available information.

IMPACT AND REPERCUSSIONS

Initial impact:

- German magazine reporter Julian Ropcke, of the BILD, reported that German MPs had begun to receive threatening messages saying their pornography choices were also stolen and they should "come clean" about their sexual preferences. He added that perusal of "3 percent" of the data had already revealed "cases of corruption and bad political scandals". 4chan users were already revelling in some of the scandals, from sexual proclivities to Wikipedia edits by politicians.

- The German government and security agencies were accused of not taking internet security seriously, as this huge data breach affected hundreds of politicians and celebrities.

- The hack is likely to increase Germans' comparatively high degree of scepticism towards social media, experts say.

- The incident shocked the establishment and prompted calls for security agencies to clarify whether any security deficiencies they were aware of had been exploited, and if they could have acted sooner to head off the breach.

- The BSI, federal office for information security in Germany, said in a statement that it was contacted by a lawmaker in early December about suspicious activity on their private email and social media accounts. “Only by becoming aware of the release of the data sets via the Twitter account ‘G0d’ on January 3rd, 2019, could the BSI in a further analysis on January 4th, 2019 connect this case and four other cases that the BSI became aware of during 2018,” it said.

- The city-state of Hamburg was working with Irish data protection authorities to stop the data being spread via Twitter, but said the company had not been responsive.

- Twitter intervened and suspended the account distributing links to the leaked data, based on a new rule it set in place last October that banned the distribution of hacked materials on its site.

- The leak caused panic among Germany's political class, many fearing they'll be subject to online fraud or identity theft attacks, due to the very sensitive nature of the exposed documents.

- The attack raised new questions about whether the government had structures in place to adequately help users safeguard their computers and sensitive personal information.

- Katarina Barley, the justice minister, said her office was looking into whether it made sense to further tighten the country’s already strict privacy laws, or those requiring software providers and companies running internet platforms to respond more swiftly to requests for data to be taken down. She and Mr. Seehofer encouraged Germans to use strong passwords, avoid using the same password for multiple accounts and two-step verification to access to their online accounts as their best.

Political repercussions:

- The fallout created widespread alarm politically. Robert Habeck, leader of the Greens, deleted both his Twitter and Facebook accounts on Monday after being affected by the data breach. He described the panic he felt on realising that large amounts of data from his accounts, including family photographs, had been hacked, but said he also regretted the manner in which he had frequently adopted a polemical style to further his arguments.

- The scandal prompted calls for action to improve cyber-security practices. German government officials are tightening up data security laws.

- German Interior Minister Horst Seehofer pledged to provide clarity on a massive data breach that had shaken Germany's political establishment. Seehofer told Süddeutsche Zeitung that he would meet the heads of the Criminal Police Office (BKA) and cyberdefense agency (BSI) to find out what they knew about the cyberattack and how they dealt with it. The interior minister said he would share his findings with the public by the middle of the next week at the latest. "The public will know everything I know," Seehofer said.

- The interior committee of the German parliament's lower house, the Bundestag, also met for a special session to discuss the breach. Angela Merkel's junior coalition partner, the Social Democrats (SPD), demanded that the government provide more clarity on the data breach.

- Lars Klingbeil, the general secretary of the party, told the Funke media group that the government must quickly shed light on "which agencies knew what exactly when, and how that was dealt with”. "This should be a priority for Horst Seehofer. It's about protecting our democracy," Klingbeil said.

- Political parties criticized the BSI for its handling of the data breach. The BSI clarified that it only became aware of the full extent of this week's breach on 5th of January — a day after BSI chief Arne Schönbohm said the agency had known about isolated breaches in early December.

- The Greens' parliamentary leader, Anton Hofreiter, demanded that Schönbohm explain himself urgently to an extraordinary parliamentary committee meeting.

- The deputy leader of the Free Democrats (FDP), Wolfgang Kubicki, suggested that Schönbohm should quit. "A president who first says he's known about the breach since the beginning of December and then backtracks to say he's only known about it since January 3 must ask himself if he's the right man for the job," he said.

- Joachim Herrmann, interior minister for the southern state of Bavaria, said he was appalled at the way the federal government and information security agency, the BSI, was handling the scandal, the biggest data leak in German history, after it was revealed it had dismissed a breach in December as one-off incident. “I was astonished at the way they communicated this, it was bewildering,” he told the tabloid Bild. Herrmann said he believed the perpetrator behind the hack was an individual and not a foreign government, as was initially feared, with many pointing the finger at Russia. Herrmann insisted the BSI should be forced to reveal what it knew when, and why it failed to crack down on the breach at the earliest opportunity.

- Germany’s BSI cyberdefense agency then defended its role in responding to a far-reaching data breach, saying it could not have connected individual cases it was aware of last year until the entire data release became public.

Breakthrough in investigation:

- On January 4, a 19-year-old German man was questioned by police, over his alleged involvement with the hacker believed to be responsible. Police raided the teenager’s house in the town of Heilbronn in south-west Germany on 6th of January and took away the contents of rubbish bins and computer equipment. Identified only as Jan S, he denied being the main perpetrator behind the leaks but claimed to know “Orbit”, the hacker who had claimed responsibility via Twitter. Jan S, who works in the IT industry, told the state broadcaster ARD he had been questioned “for several hours”. He was being treated only as a witness to the security breach, having allegedly been in communication with Orbit. On his Twitter account, Jan S said he had been in touch with the hacker known as Orbit for years via an encrypted messenger service. He said Orbit had sent him an email shortly after the publication of the hacked data, telling him he was planning to destroy his computer so he could not be traced. Jan S said the alleged hacker had since deleted his account with the messenger service.

- On 6th of January, German police arrested a man responsible for the data-breach. The 20-year-old man from the western state of Hesse, who lived at home with his parents and calls himself ‘G0d’ on Twitter, confessed to releasing the information in early December, though news of the leak only became public on January 3rd.

References:

https://www.reuters.com/article/us-germany-politics-cyber/german-politicians-data-published-online-in-massive-breach-idUSKCN1OY0IW

https://www.siliconrepublic.com/enterprise/german-data-leak-merkel

https://abcnews.go.com/International/german-politicians-personal-information-leaked-twitter-mass-cyberattack/story?id=60160048

https://www.bbc.com/news/world-europe-46793116

https://www.nytimes.com/2019/01/08/world/europe/germany-hacking-arrest.html

https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

https://www.nexsesolutions.com/single-post/2019/01/09/Hackers-Leak-Personal-Data-from-Hundreds-of-German-Politicians-On-Twitter

https://www.bloomberg.com/opinion/articles/2019-01-07/why-germany-s-god-hack-wasn-t-such-a-scandal

https://blog.prilock.com/2019/01/07/german-politicians-leaked-twitter-hack/

https://www.intsights.com/blog/who-was-the-hacker-behind-the-german-data-breach

https://www.irishtimes.com/news/world/europe/german-data-hacker-says-he-was-annoyed-by-politicians-1.3751332

https://www.thelocal.de/20190108/suspect-20-arrested-over-massive-german-politician-data-hack

https://techcrunch.com/2019/01/04/germany-data-breach-lawmakers-leak/
Jan 4

https://www.dw.com/en/germanys-horst-seehofer-promises-clarity-after-hack-attack/a-46974976
Jan 6

https://www.japantimes.co.jp/news/2019/01/06/world/german-cyberdefence-agency-defends-handling-data-breach/#.XIxQzC-cZQI
Jan 6

https://www.theguardian.com/world/2019/jan/07/germany-data-breach-teenager-being-questioned-by-police
Jan 7

http://time.com/5496579/arrest-german-data-leak/
Jan 8

https://gdpr.report/news/2019/01/08/man-arrested-over-major-data-breach-in-germany/
Jan 8