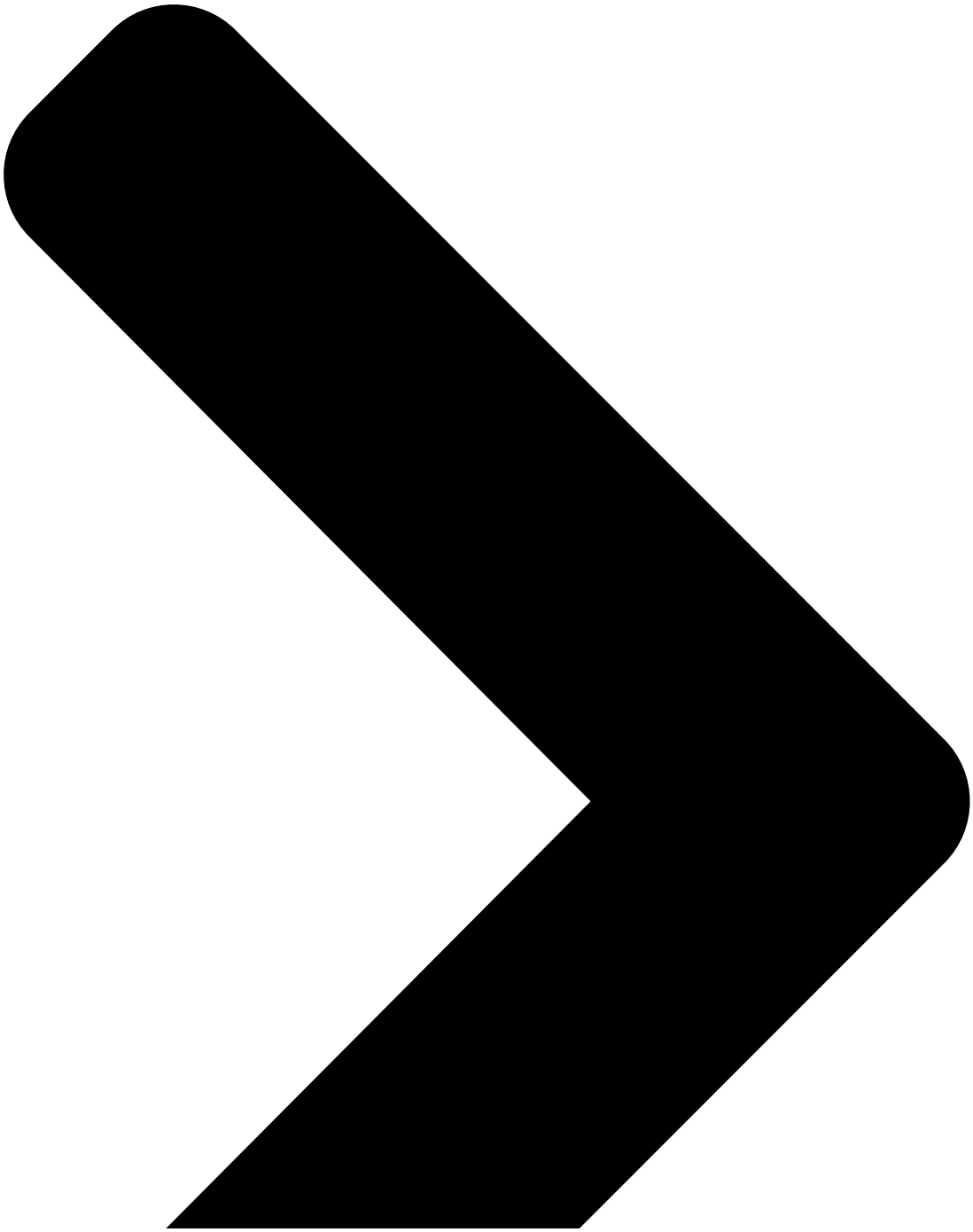
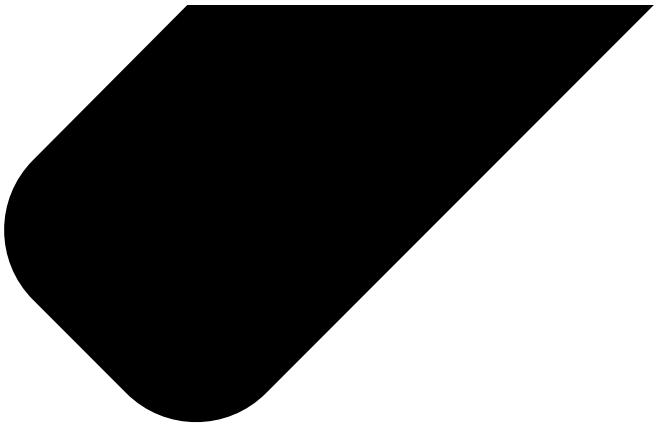
From Pearl to Pegasus Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits

citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/

August 24, 2021

Research





Targeted Threats

By Bill Marczak, Ali Abdulemam, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, John Scott-Railton, and Ron Deibert

[1] Red Line for Gulf

August 24, 2021

Summary & Key Findings

- We identified nine Bahraini activists whose iPhones were successfully hacked with NSO Group's Pegasus spyware between June 2020 and February 2021. Some of the activists were hacked using two zero-click iMessage exploits: the 2020 ***KISMET*** exploit and a 2021 exploit that we call ***FORCEDENTRY***.
- The hacked activists included three members of Waad (a secular Bahraini political society), three members of the Bahrain Center for Human Rights, two exiled Bahraini dissidents, and one member of Al Wefaq (a Shiite Bahraini political society).
- At least four of the activists were hacked by ***LULU***, a Pegasus operator that we attribute with high confidence to the government of Bahrain, a well-known abuser of spyware. One of the activists was hacked in 2020 several hours after they revealed during an interview that their phone was hacked with Pegasus in 2019.
- Two of the hacked activists now reside in London, and at least one was in London when they were hacked. In our research, we have only ever seen the Bahrain government spying in Bahrain and Qatar using Pegasus; never in Europe. Thus, the Bahraini activist in London may have been hacked by a Pegasus operator associated with a different government.
- We shared a list of the targeted phone numbers we identified with Forbidden Stories. They confirmed that numbers associated with five of the hacked devices were contained on the Pegasus Project's list of potential targets of NSO Group's customers, data that Forbidden Stories and Amnesty International describe as dating from 2016 up to several years ago.

1. Human Rights in Bahrain: A History of Brutal Repression

- *Bahrain is a constitutional monarchy on paper*, though in practice, all key power is concentrated in the hands of the ruling Al-Khalifa family. Bahrain's legislature consists of an upper house (Shura Council) appointed by the king, and a lower house (National Assembly) elected from districts of unequal population, drawn to ensure the opposition cannot attain a majority. Bahrain has a long history of political movements seeking greater democratic political reform. More details.
- *Bahrain has a history of brutal repression of dissent.* After King Hamad came to power as Emir in 1999, the political and human rights situation briefly improved. The king allowed the formation of civil society organizations, including human rights groups, independent newspapers, and political parties. However, these reforms were gradually undone, and by 2010, Bahrain had reverted to its long pattern of arrests, torture, and aggressive silencing of political opposition. Little vestige of Bahraini civil society remains today. More details.
- *Bahrain employs a number of methods to block or suppress Internet content.* Bahrain's government implements Internet censorship using website-blocking technology from a Canadian company, Netsweeper, and also employs targeted Internet disruptions in order to stymie protests. Bahrainis who have posted critical content online have been pursued by the Ministry of Interior's Cyber Crime Unit and arrested. More details.
- *Bahrain surveils human rights activists, dissidents, and members of the political opposition.* The government increasingly uses Internet controls and spyware, targeting individuals inside Bahrain and outside the country. Since 2010, Bahrain has purchased spyware from FinFisher, Hacking Team, and NSO Group. More details.

2. Pegasus Hacking of Bahraini Activists

The government of Bahrain appears to have purchased NSO Group's Pegasus spyware in 2017. Our Hide and Seek report identified a Pegasus operator spying entirely in Bahrain and Qatar that we referred to as ***PEARL***, which had been active since July 2017.

We observed a massive global spike in Pegasus activity in July 2020, and began conducting research in a number of country contexts, including Bahrain. We hunted for Pegasus in Bahrain by instructing targets to forward us their phone logs for analysis, and by setting up VPNs for key targets to monitor their Internet traffic. We analyzed the phone logs using our forensic process, and found that nine devices belonging to nine Bahraini activists had been hacked. In three cases, our forensic analysis concluded that the phones were hacked, but we were unable to establish an approximate date of the hacking. Analysis is ongoing in these cases to see if a more precise date can be identified. In the remaining six cases, our analysis established some precise dates when Pegasus was active on the phones.

The two targets we identified in London consented to be named, though all of the targets in Bahrain wished to be referred to by their affiliations only.

Target	Description	Date(s) of Hacking
Moosa Abd-Ali *	Activist	(Sometime before September 2020)
Yusuf Al-Jamri	Blogger	(Sometime before September 2019)
Activist A	Member of Waad	September 16, 2020
Activist B *	Member of Waad, Labor Law Researcher	June 3, 2020 July 12, 2020 July 19, 2020 July 24, 2020 August 6, 2020 September 15, 2020
Activist C	Member of Waad	September 14, 2020
Activist D *	Member of BCHR	September 14, 2020
Activist E	Member of BCHR	February 10, 2021
Activist F *	Member of BCHR	July 11, 2020 July 15, 2020 July 22, 2020 October 13, 2020
Activist G *	Member of Al Wefaq	(Sometime before October 2019)

(*) = Forbidden Stories confirmed that the phone number currently associated with the device is on the Pegasus Project list, indicating that it was previously a potential target of NSO Group's customers.

Bahraini Targets

This section describes the Bahraini targets hacked with Pegasus that we identified.

Waad

Three targets are members of Waad, a center-left secular political society in Bahrain. Political parties are illegal in Bahrain, but "political societies," which perform many of the functions of political parties, have been allowed since 2001.

Figure 1: The logo of Bahrain's Waad political society.

The Bahraini government banned Waad and seized its assets amidst a wave of repression in early 2017. The government claimed that Waad had "support[ed] terrorism and sanction[ed] violence," despite the fact that Waad has never used violence, and has always committed itself to peaceful methods. Before it was banned, Waad's headquarters was twice subjected to arson, and was defaced by pro-government protesters in 2011 who wrote "Down with Iran" and slogans against Bahrain's Shia muslims.

Bahrain Center for Human Rights

Three targets are members of the Bahrain Center for Human Rights, a Bahraini NGO formed in 2002, and banned since 2004, when the Center's then-President blamed Bahrain's Prime Minister for failing to address citizens' economic concerns. Nevertheless, the organization has continued to operate without government approval, and was awarded the 2013 Rafto Prize.

Figure 2: The logo of the Bahrain Center for Human Rights.

Al Wefaq

One target is a member of Al Wefaq, Bahrain's largest opposition political society. All of the Al Wefaq members of Bahrain's National Assembly resigned en masse in 2011 in protest of the government's violent repression of peaceful protesters. A Bahrain-based news channel *Al-Arab* was shut down less than 24 hours after it was launched in February 2015 because the channel aired an interview with the Secretary General of Al Wefaq. In July 2016, the Bahraini government dissolved Al Wefaq and seized its assets. Also in 2016, the Bahraini government revoked the citizenship of Al Wefaq's de-facto spiritual leader Sheikh Isa Qassim, a Bahraini by birth.

Figure 3: The logo of Bahrain's Al-Wefaq political society.

The Bahrain government has clumsily attempted to link Al Wefaq to terrorism and violence for a number of years. During the height of the protests in Bahrain in 2011, state television aired a forced confession read by a detainee who had earlier died under torture. In the forced confession, the detainee said that Matar Matar, a moderate member of Al Wefaq, had ordered him to murder policemen. Matar had earlier called for the establishment of a secular democracy in Bahrain, and had condemned the arrest of doctors that had treated protesters.

London Targets

Two of the targets, Moosa Abd-Ali and Yusuf Al-Jamri, are Bahrainis currently living in exile in London.

Figure 4: Bahraini blogger Yusuf Al-Jamri.

Al-Jamri was granted asylum by the UK Home Office in 2018, based on his reports that he was tortured in 2017 while in the custody of Bahrain's main intelligence agency, the National Security Apparatus (جهاز الأمن الوطني). Bahrain's National Security Apparatus (NSA) is infamous for torturing to death journalist Karim Fakhrawi in 2011, according to the findings of an independent inquiry (para. 877) that Bahrain's king ordered under international pressure. After recommendations from the same commission of inquiry, Bahrain's king in 2012 revoked the NSA's law enforcement powers, though he restored these powers in a January 2017 Royal Decree. A Royal Decree in 2020 changed the name of the NSA to the National Intelligence Service (جهاز المخابرات الوطني).

Al-Jamri's iPhone 7 appears to have been hacked with Pegasus at some point prior to September 2019. We were unable to determine whether he was hacked while in Bahrain or London. Further forensic analysis may be able to establish a more precise date of hacking.

Figure 5: Bahraini activist Moosa Abd-Ali protesting in front of the Bahraini Embassy in London.

Moosa Abd-Ali is a Bahraini activist living in exile in London. He sued FinFisher, another spyware company, for supplying the Bahraini government with spyware that was used to hack his personal computer in 2011. The spying against Moosa's computer was first revealed in data leaked from FinFisher. Abd-Ali's iPhone 8 appears to have been hacked with Pegasus at some point prior to September 2020. Further forensic analysis may be able to establish a more precise date of the hacking.

***LULU*: A Bahrain Government Operator**

We attributed the hacking of Activists A-D (three members of Waad, and one member of BCHR) to a Bahrain government operator of Pegasus that we call ***LULU***. Like ***PEARL***, ***LULU*** appeared to be spying exclusively in Bahrain and Qatar. The ***LULU*** operator may in fact be the same operator as ***PEARL***, which we identified in 2017 and 2018. While we did not identify any IP addresses or domain names in common between ***LULU*** and ***PEARL***, we would not necessarily expect to identify any infrastructure in common, as NSO Group registered servers with new domain names and new IP addresses for all its clients following 2018 reports by Citizen Lab and Amnesty Tech. We have never observed more than one Bahrain government operator active at a time.

The Pegasus spyware installed on the phones of Activists A-D used four IP addresses for command-and-control. Each IP address returned a TLS certificate for *hooklevel[.]com*, though no DNS lookups were performed for this domain, and the spyware's TLS *Client Hello* message did not contain an SNI. The infection server used was **.api1r3f4.redirectweburl[.]com*.

IPs	CN in TLS Certificate
172.105.89.243	****.api1r3f4.redirectweburl[.]com***
64.227.121.213 **206.189.31.108**	
195.181.213.122	
80.211.231.5	***hooklevel[.]com***

Table 1: Servers that *LULU* used to spy on Bahraini activists.

Our forensic analysis has not yet established which Pegasus operator hacked the remaining five devices. Because we have never observed the Bahrain government successfully hack a target outside of Bahrain or Qatar with Pegasus, we suspect that Moosa Abd-Ali was hacked by a second Pegasus operator. That a foreign government may have been responsible for the hacking does not preclude the possibility that the ultimate recipient of the hacked data was the Bahraini government.

Mechanisms of Hacking

This section provides a high-level overview of the mechanisms by which the Bahraini targets were hacked. This section involves synthesis of data from multiple phones, including phones belonging to non-Bahraini targets.

July – September 2020: *KISMET* iMessage Zero-Click

When the ***KISMET*** exploit was being fired at one of the devices running iOS 13.5.1, the log showed crashes associated with *IMTranscoderAgent*, which is responsible for transcoding and previewing images in iMessages. Specifically, the crashes were segfaults in the *com.apple.IMTranscoderPreviewGenerationQueue* thread while apparently parsing ICC color profile data in a JPEG image received via iMessage. Unfortunately, we were only able to locate crash summaries with abbreviated stack traces in the system logs.

```
Thread 1 name: Dispatch queue: com.apple.IMTranscoderPreviewGenerationQueue
Thread 1 Crashed:
  0: CoreFoundation 0x1803a6b48 _CFDataGetLength + 16
  1: ColorSync      0x1871e13c4 _copy_description_from_DSCMTag + 44
  2: ColorSync      0x1871e1ca4 _ColorSyncProfileCopyASCIIDescriptionString + 636
  3: ColorSync      0x1871e3ab4 _ColorSyncVerifyAdobeRGBData + 284
  4: CoreGraphics   0x1873d95a8 _CGColorSpaceCreateWithICCData + 344
  5: ImageIO        0x180de1fa0 _CGColorSpaceCreateWithCopyOfData + 56
  6: ImageIO        0x180db93b8 __ZN19AppleJPEGReadPlugin10initializeEP13IIODictionary + 5844
  7: ImageIO        0x180cf0908 __ZN13IIOReadPlugin14callInitializeEv + 220
  8: ImageIO        0x180d58a1c __ZN20IIO_Reader_AppleJPEG17initImageAtOffsetEP13CGImagePluginmmm + 172
  9: ImageIO        0x180c62390 __ZN14IIOImageSource13makeImagePlusEmP13IIODictionary + 936
 10: ImageIO        0x180c61bcc __ZN14IIOImageSource28getPropertiesAtIndexInternalEmP13IIODictionary + 68
 11: ImageIO        0x180c61b44 __ZN14IIOImageSource21copyPropertiesAtIndexEmP13IIODictionary + 16
```

Figure 6: A symbolicated crash summary for KISMET on an iPhone Xs running iOS 13.5.1. After the crashes, IMTranscoderAgent then invoked WebKit to download and render items from the Pegasus infection server. The rendering triggered a memory pressure warning in *JavaScriptCore*, and also triggered a *Metal* shader compilation.

We believe that KISMET was used as a zero-day exploit against at least iOS 13.5.1 and 13.7.

September 2020: Back to One-Click Exploits

Shortly after **Activist B** upgraded to iOS 14 in September 2020, they received an SMS link to Pegasus from “MailExpress,” indicating that the ***KISMET*** exploit was not supported on iOS 14.

Figure 7: Pegasus SMS message that Activist B received in September 2020 after updating to iOS 14.

The message was a fake DHL package tracking notification. The target may have accidentally previewed the link in the message while attempting to copy the message to send it to us. The target’s VPN recorded that the link in the message was opened, and redirected to a unique subdomain of *api1r3f4.redirectweburl[.]com*, confirming that it was a Pegasus link

connected to the Bahraini government operator of Pegasus, ***LULU***. This action did not result in the infection of the phone; it is possible that the target closed the preview before the exploit ran.

NSO Group may have temporarily switched back to one-click iOS exploits due to the new *BlastDoor* security feature implemented by Apple. The *BlastDoor* feature was designed to make zero-click exploitation via iMessage harder.

February – July 2021: *FORCEDENTRY* iMessage Zero-Click

Starting in February 2021, we began to observe NSO Group deploying a new zero-click iMessage exploit that circumvented Apple's *BlastDoor* feature. We refer to the exploit as ***FORCEDENTRY***, because of its ability to circumvent *BlastDoor*. Amnesty Tech also observed zero-click iMessage exploitation activity around the same time, and referred to the activity they observed as "Megalodon." We confirmed with Amnesty Tech that the "Megalodon" activity they observed matches the characteristics of the ***FORCEDENTRY*** exploit that we observed.

When the ***FORCEDENTRY*** exploit was being fired at a device, the device logs showed crashes associated with *IMTranscoderAgent*. The crashes appeared to be segfaults generated by invoking the *copyGifFromPath:toDestinationPath:error* function on files received via iMessage.

The crashes appeared to be of two types. Type one crashes indicate that the chain of events set off by invoking *copyGifFromPath:toDestinationPath:error* ultimately crashed while apparently invoking ImageIO's functionality for rendering Adobe Photoshop PSD data.

```
Thread 1 name: Dispatch queue: com.apple.root.default-qos
Thread 1 Crashed:
  0: ImageIO                0x181b326f0 __ZN13PSDReadPlugin12GetRangeInfoEP9LayerInfoP19IIOImageReadSessionRK13PSDPluginDatat + 244
  1: ImageIO                0x181b326ec __ZN13PSDReadPlugin12GetRangeInfoEP9LayerInfoP19IIOImageReadSessionRK13PSDPluginDatat + 240
  2: ImageIO                0x181b32abc __ZN13PSDReadPlugin11DecodeLayerEP9LayerInfoRK6CGRectP19IIOImageReadSessionRK14ReadPluginDataRK13PSDPluginData + 448
  3: ImageIO                0x181b32d40 __ZN13PSDReadPlugin11MergeLayersEP19IIOImageReadSessionR20IIODecodeFrameParamsRK14ReadPluginDataRK13PSDPluginData + 276
  4: ImageIO                0x181b33248 __ZN13PSDReadPlugin11DecodeBlockEP19IIOImageReadSessionR20IIODecodeFrameParamsRK14ReadPluginDataRK13PSDPluginDatajj + 232
  5: ImageIO                0x181b34c4c ____ZN13PSDReadPlugin12DecodeBlocksEP12IIOImageReadRK14ReadPluginDataRK13PSDPluginDataRNSt3__16vectorI20IIODecodeFrameParamsNS8_9allocatorISA_EEEE_block_invoke + 116
  6: libdispatch.dylib      0x18004b860 __dispatch_client_callout2 + 20
  7: libdispatch.dylib      0x18005f988 __dispatch_apply_serial + 120
  8: libdispatch.dylib      0x18004b81c __dispatch_client_callout + 20
  9: libdispatch.dylib      0x180050c7c __dispatch_sync_function_invoke + 56
 10: libdispatch.dylib      0x18005f844 _dispatch_apply_f + 908
 11: ImageIO                0x181b34bcc __ZN13PSDReadPlugin12DecodeBlocksEP12IIOImageReadRK14ReadPluginDataRK13PSDPluginDataRNSt3__16vectorI20IIODecodeFrameParamsNS8_9allocatorISA_EEEE + 140
 12: ImageIO                0x181b34364 __ZN13PSDReadPlugin17copyImageBlockSetEP7InfoRecP15CGImageProvider6CGRect6CGSizePK14__CFDictionary + 1028
 13: ImageIO                0x181a28388 __ZN10IIO_Reader21CopyImageBlockSetProcEPvP15CGImageProvider6CGRect6CGSizePK14__CFDictionary + 152
 14: ImageIO                0x181a36510 __ZN20IIOImageProviderInfo28copyImageBlockSetWithOptionsEP15CGImageProvider6CGRect6CGSizePK14__CFDictionary + 756
 15: ImageIO                0x181a33e74 __ZN20IIOImageProviderInfo28CopyImageBlockSetWithOptionsEPvP15CGImageProvider6CGRect6CGSizePK14__CFDictionary + 584
 16: CoreGraphics           0x182004c68 _imageProvider_retain_data + 92
 17: CoreGraphics           0x181decaa8 _CGDataProviderRetainData + 80
 18: CoreGraphics           0x181ff1e04 _CGAccessSessionCreate + 108
 19: CoreGraphics           0x181e21bc8 _CGDataProviderCopyData + 168
 20: CoreGraphics           0x181d95230 _CGImageGetDataProviderInternal + 268
 21: CoreGraphics           0x181eccc10 _img_image + 600
 22: CoreGraphics           0x181ecc6e8 _CGSImageDataLock + 1004
 23: CoreGraphics           0x181ceb2bc _ripc_AcquireRIPImageData + 716
 24: CoreGraphics           0x181eed25c _ripc_DrawImage + 1152
 25: CoreGraphics           0x181ed3b40 _CGContextDrawImageWithOptions + 1216
 26: ImageIO                0x181ae2730 __ZN14GIFWritePlugin16writeSingleFrameEv + 1016
 27: ImageIO                0x181ae3890 __ZN14GIFWritePlugin8writeAllEv + 580
 28: ImageIO                0x181a6d76c __ZN14IIO_Writer_GIF5writeEPvS0_ + 36
 29: ImageIO                0x181aae554 __ZN19IIOImageDestination19finalizeDestinationEv + 548
 30: ImageIO                0x181aaffd4 _CGImageDestinationFinalize + 132
 31: IMSharedUtilities      0x18f77c9b4 writeNewFileAtPath:withProperties:fromImageSource:error: + 236
 32: IMSharedUtilities      0x18f77cd88 copyGifFromPath:toDestinationPath:error: + 348
 33: IMTranscoderAgent      0xf08e58c8
```

Figure 8: A Symbolicated Type One crash for FORCEDENTRY on an iPhone 12 Pro Max running iOS 14.6.

Type two crashes indicate that the chain of events set off by invoking *copyGifFromPath:toDestinationPath:error* ultimately crashed while invoking CoreGraphics' functionality for decoding JBIG2-encoded data in a PDF file.

```
Thread 2 name: Dispatch queue: IMTranscoderNormalPriorityQueue
Thread 2 Crashed:
  0: CoreGraphics            0x181d6e228 __ZN11JBIG2Stream17readTextRegionSegEjiijPjj + 900
  1: CoreGraphics            0x181d6e20c __ZN11JBIG2Stream17readTextRegionSegEjiijPjj + 872
  2: CoreGraphics            0x181d6c67c __ZN11JBIG2Stream12readSegmentsEv + 1988
  3: CoreGraphics            0x181d6be70 __ZN11JBIG2Stream5resetEv + 260
  4: CoreGraphics            0x181cf9f9c __ZL10read_bytesPvS_m + 1024
  5: CoreGraphics            0x181d1e324 _jbig2_filter_refill + 128
  6: CoreGraphics            0x181d8d098 _CGPDFSourceRefill + 196
  7: CoreGraphics            0x181d8cfa4 _CGPDFSourceGetc + 36
  8: CoreGraphics            0x181d63088 _xref_stream_read_section + 188
  9: CoreGraphics            0x181d62e60 _xref_stream_create + 828
 10: CoreGraphics            0x181d62a54 _CGPDFXRefStreamCreate + 112
 11: CoreGraphics            0x181e26694 _pdf_xref_create + 1748
 12: CoreGraphics            0x181d06eb0 _CGPDFDocumentCreateWithProvider + 280
 13: ImageIO                 0x181b0fdd4 __Z19CreateSessionPDFRefP10IIOScannerPb + 112
 14: ImageIO                 0x181a92404 __ZN4IIO_Reader_PDF22updateSourcePropertiesEP19IIOImageReadSessionP13IIODictionaryS3_S3_P19CGImageSourceStatus + 84
 15: ImageIO                 0x181a138fc __ZN14IIOImageSource13getPropertiesEP13IIODictionary + 408
 16: ImageIO                 0x181a139a4 __ZN14IIOImageSource14copyPropertiesEP13IIODictionary + 16
 17: ImageIO                 0x181a17f00 _CGImageSourceCopyProperties + 244
 18: IMSharedUtilities       0x18f77b974 readFileProperties:fromImageSource:error: + 48
 19: IMSharedUtilities       0x18f77c740 readFileProperties:fromImageSource:withUpdatedLoopCount:error: + 84
 20: IMSharedUtilities       0x18f77cd34 copyGifFromPath:toDestinationPath:error: + 264
 21: IMTranscoderAgent       0xecc258c8
```

Figure 9: A Symbolicated Type Two crash for FORCEDENTRY on an iPhone 12 Pro Max running iOS 14.6.

After the *IMTranscoderAgent* crashes, we noticed that the Apple thermal monitoring daemon, *thermalmonitord*, returned a series of errors:

Exception caught during decoding of reply to message 'propertiesOfPath:handler:', dropping incoming message and calling failure block.

Then, *thermalmonitord* invoked the *tailspin* process three times. The *tailspin* process caused two segfaults, but we ultimately found an invocation of *tailspin* running alongside the spyware:

/usr/bin/tailspin test-symbolicate 1234567

Phone logs indicated that the "responsible process" for the spyware was *amfid*, the Apple mobile file integrity daemon.

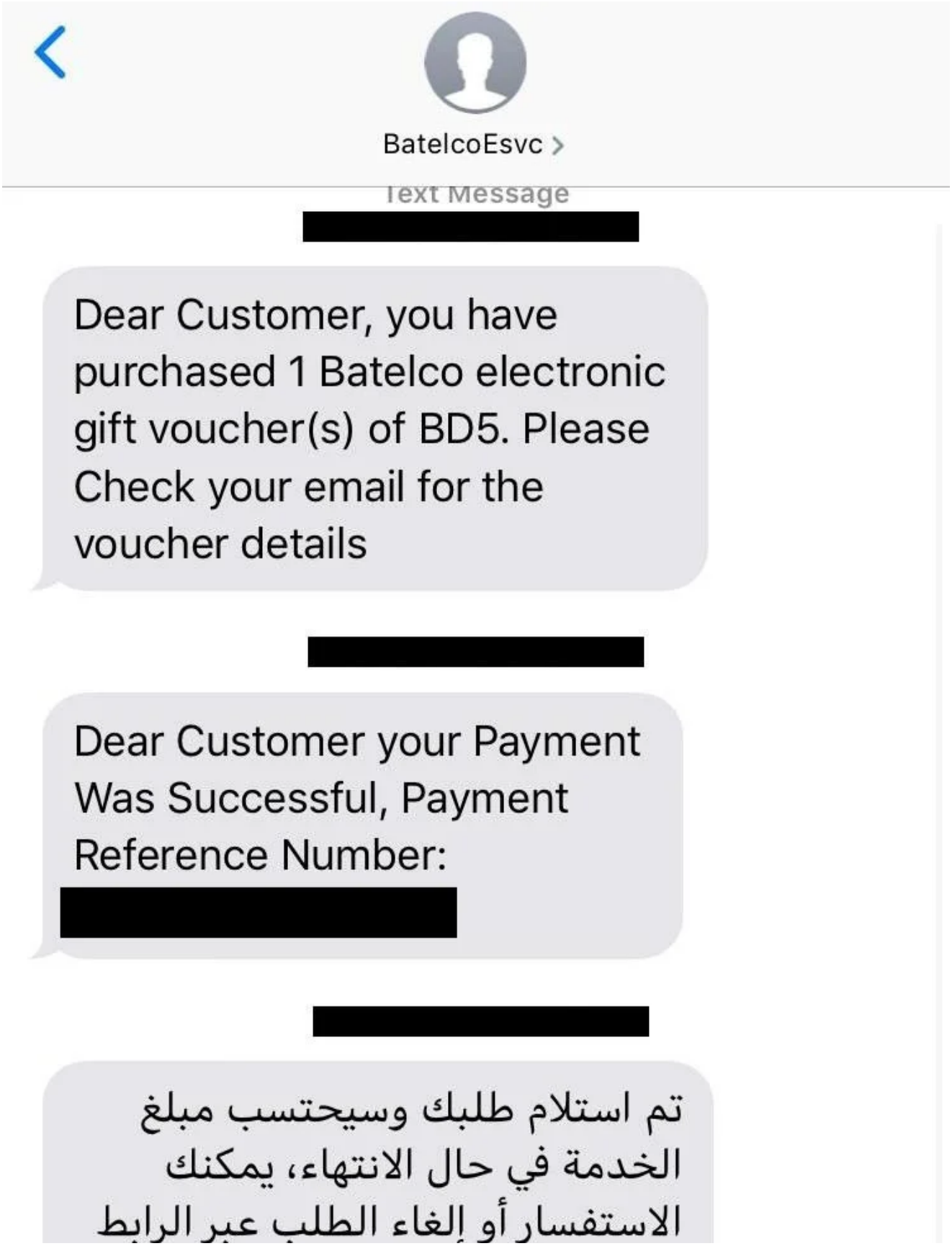
We saw the ***FORCEDENTRY*** exploit successfully deployed against iOS versions 14.4 and 14.6 as a zero-day.

With the consent of targets, we shared these crash logs and some additional phone logs relating to ***KISMET*** and ***FORCEDENTRY*** with Apple, Inc., which confirmed they were investigating.

3. Hacked Again after Going Public

Activist D, a member of the Bahrain Center for Human Rights, was additionally targeted with Pegasus in March 2019 with a Pegasus SMS message from "BatelcoEsvc." **Activist D** discussed the 2019 incident in a 2020 interview in which **Activist D** was interviewed alongside one of the authors of this report. The Bahraini goverment's ***LULU*** operator hacked **Activist D** with Pegasus using the ***KISMET*** zero-click exploit approximately six hours after the interview first aired. This case highlights the risks inherent in going public with instances of hacking.

The 2019 Pegasus SMS appeared in a thread with legitimate messages from **Activist D**'s mobile provider, Batelco. The target was curious about the message, and contacted Batelco, who told them that the message was not of a type sent by Batelco.



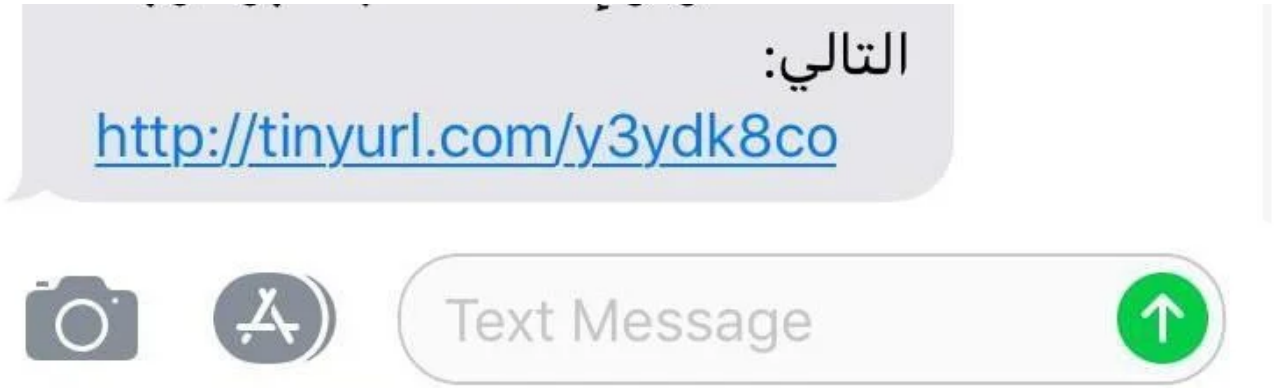


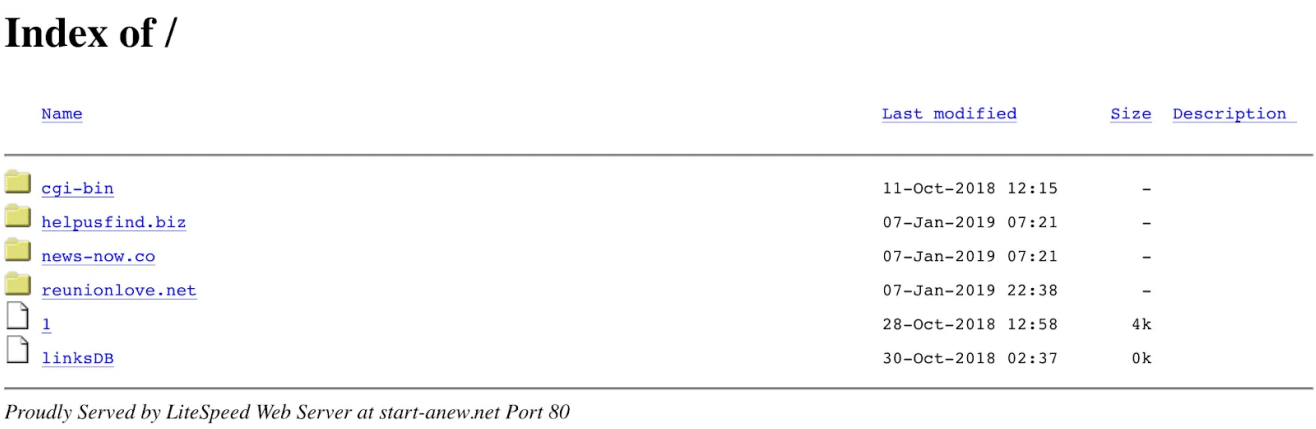
Figure 10: The malicious text (bottom) and legitimate texts from Batelco (above). The text is unusual because it (1) is in Arabic, (2) contains a link, and (3) does not begin with “Dear Customer.”

The link unshortens to a website on info-update[.]org, which redirected to the legitimate Batelco e-services website (https://e.batelco.com/eservices/Login) when submitted to VirusTotal. When we checked it, the link returned a 404.

The info-update[.]org website is connected to the Pegasus spyware, as we show below.

Decoy Page Reveals 2019 Pegasus Sites

NSO Group has occasionally made use of visible *decoy pages*, perhaps in an effort to make their Pegasus infrastructure appear as innocuous servers. We found an interesting server, start-anew[.]net, which displayed an open directory listing that contained a decoy page.



Index of /

Name	Last modified	Size	Description
cgi-bin	11-Oct-2018 12:15	-	
helpusfind.biz	07-Jan-2019 07:21	-	
news-now.co	07-Jan-2019 07:21	-	
reunionlove.net	07-Jan-2019 22:38	-	
1	28-Oct-2018 12:58	4k	
linksDB	30-Oct-2018 02:37	0k	

Proudly Served by LiteSpeed Web Server at start-anew.net Port 80

Figure 11: How start-anew[.]net looked in a web browser.The directory contained a file, *1*, which contained HTML source code for a website maintenance decoy page. The page was entitled *“While maintenance:”* and contained the text *“Working hard to create a new website design. Stay in touch!”*

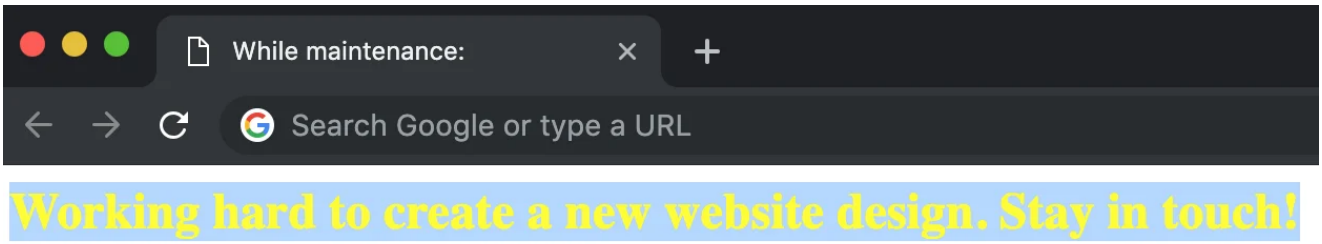


Figure 12: How the decoy page (1) looks in a browser.
The title *"While maintenance:"* and the text *"Working hard to create a new website design. Stay in touch!"* exactly matched pages returned by two Pegasus servers that matched a fingerprint we used in our Hide and Seek report. These two servers were part of a group of Pegasus servers that were spun up in 2018 *after* Amnesty Tech and Citizen Lab published reports about the targeting of an Amnesty International staffer with Pegasus, but *before* Citizen Lab's Hide and Seek report.

IP	Domain	Dates Matching Decoy Page[1]	Dates Matching *Hide and Seek* Fingerprint[2]
209.250.237.55	**youneedjelly[.]net**	**8/28/2018 – 10/14/2018**	**8/31/2018 – 9/6/2018**
92.222.71.144	**visiblereminder[.]net**	**8/28/2018 – 9/11/2018**	**8/31/2018 – 9/6/2018**

From the contents of start-anew[.]net, we surmised that the following websites were part of the new Pegasus infrastructure:

- reunionlove[.]net
- news-now[.]co
- helpusfind[.]biz

Scanning Shared Web Hosters

We noted that these three domains were hosted on *shared web hosting* providers. In other words, the IP addresses that they pointed to had dozens of other innocuous domains also pointing to them. In previous iterations of NSO Group's Pegasus infrastructure, each domain name pointed to a separate IP address.

Scanning websites on shared web hosting required us to adjust our scanning infrastructure to use *domain names* rather than *IP addresses*. The usage of shared hosting providers appears to have begun after we published our Hide and Seek report in September 2018. We disclose our fingerprinting and scanning pipeline below, because it is no longer capable of detecting Pegasus servers.

Step	Description	Approx. # Domains
S1	**Generate a list of interesting domain names to scan using TLS certificates from specific issuers.**	**~ 6 million**
S2	**For all domains above, send a GET request for */robots.txt*, and check whether the response status line is *404 Not Found* with a *Content-Type* header mentioning *text/html*, but with no response body. We also excluded any responses with an *ETag* or a *Set-Cookie* header.**	**~ 500**
S3	**For matching domains above, send a GET request for / and check whether the response is the same as above.**	**175**

We devised these scanning steps based on the configuration of the three domain names found on start-anew[.]net.

A Window into 2019 Pegasus SMS Infection Infrastructure

Our scan results comprise 175 domain names, and included the domain name info-update[.]org from the SMS sent to **Activist D**. Our scan results also include one domain name that appears to be directly related to human rights (human-rights-news[.]com), as well as domain names that indicate potential targeting in the USA (washington-today[.]com, breakingnewyork[.]info), as well as apparent targeting in relation to the Bahraini elections (i-election-online[.]com).

We also found several interesting websites linked to Azerbaijan, including siyasimehbus[.]com (*"political prisoners"*) and mitinq23fevral[.]info, which is a reference to *"Rally 23rd February,"* a protest planned by the opposition Popular Front Party on February 23, 2019. The protest was not authorized by authorities.

4. Historical Context

Bahrain: One Monarchy, Two Constitutions

The Kingdom of Bahrain is an archipelago situated off the east coast of the Kingdom of Saudi Arabia. From the sixteenth century until the nineteenth century, Bahrain was occupied by a succession of ruling powers, until Sheikh Ahmed Bin Mohammed Al Khalifa (known in Bahrain as "Ahmed the Conqueror") seized control of Bahrain in 1783. The rule of the Al Khalifa family has persisted until the present day, despite numerous internal and external challenges to their authority, including during the period from 1820 to 1971 when Bahrain was a British protectorate under the General Maritime Treaty of 1820.

Bahrain declared independence from Britain on August 15, 1971, after the withdrawal of British troops. Six months later, Bahrain's then-Emir, Sheikh Isa bin Salman Al-Khalifa, decreed that a constituent assembly would draft a new constitution. In 1973, the assembly issued their constitution, which provided for an elected unicameral parliament with an advisory, rather than legislative role. However, after Bahrain's first parliament saw a contentious debate on a state security decree, the Emir dissolved the parliament in 1975, and suspended the Constitution.

Between 1975 and 2001, the Bahraini government engaged in numerous forms of repression. Human Rights Watch described abuses in the country during this time as "wide-ranging" and covering a broad spectrum of offences, including arbitrary detention, the psychological abuse of detainees, and the "broad denial of fundamental political and civil liberties."

Figure 13: A billboard along a major highway put up by an advertising company salutes Bahrain's King Hamad as "King of Glory." (Author: Bill Marczak)

Sheikh Isa was succeeded by his son Sheikh Hamad Bin Isa Al Khalifa in 1999. Sheikh Hamad's rule began with reform measures including the release of political prisoners. Sheikh Hamad also appointed a committee to draft a "National Action Charter" to address political

grievances. On February 14, 2001, Bahrainis approved the Charter with 98.4% of the vote. The next year, Sheikh Hamad declared Bahrain a Kingdom and promulgated a new constitution that broke one of the Charter's key vows. While the Charter called for a bicameral parliament with sole legislative power vested in an elected lower house, Bahrain's 2002 constitution allowed the parliament's appointed upper house to exercise a de-facto veto over legislation passed by the lower house. As a result, several political societies in Bahrain boycotted the first elections under the new constitution in 2002.

Additionally, electoral districts for the parliament's lower house were drawn to be of unequal sizes, in order to diminish the opposition's political power. For example, in Bahrain's 2012 parliamentary elections, the voting power of an individual in a pro-government district was roughly 21 times the voting power of an individual in an opposition stronghold.

A Brutal History of Repression

Since 1938, organized political movements have demanded greater popular representation in Bahrain. However, the government has responded with repression and violence that continues to the present day. Bahrain saw a brief period of improvement in human rights following Sheikh Hamad's reforms, though as is often the case in Bahrain, perceived challenges to the monarchy led to the rollback of reforms.

In 2010, prior to the Arab Spring, the Haq Movement, the Islamic Wafa Movement, and the Bahrain Freedom Movement called for a boycott of parliamentary elections that were scheduled to take place on October 23, 2010. In response, immediately before the elections, the government cracked down on opposition activists.

Figure 14: Protesters began to gather at Pearl Roundabout on February 15, 2011. (Author: nbdbahrain2@gmail.com; Licensed under CC-BY-SA 3.0).

As part of the Arab Spring uprising, Bahrainis took to the streets on the tenth anniversary of the National Action Charter's approval (February 14, 2011) demanding democratic political reform, freedom, justice, and equal distribution of wealth and power. The pace of protests increased as security forces targeted and killed protesters.

Figure 15: A montage of two stills from a state television broadcast show Saudi troops cheering and saluting television cameras as a convoy of armored vehicles rolls into Bahrain

to suppress protests.

Drawing inspiration from Egypt's Tahrir Square, Bahraini demonstrators quickly occupied the Pearl Roundabout, a major traffic circle located that contained a towering monument of six sails holding up a giant pearl. The pearl monument quickly became an opposition symbol. On March 18, 2011, Bahraini forces, backed by troops from Saudi Arabia and the United Arab Emirates, forcibly evicted the protesters. Security forces arrested and tortured hundreds of Bahrainis. The government also began a campaign to expunge the Pearl Roundabout and its symbolic monument from Bahrain. The government demolished the monument, paved over the roundabout, and even recalled coinage featuring the monument.

Figure 16: After the demolition of the pearl monument, authorities converted the Pearl Roundabout into a traffic junction. (Author: nbdbahrain2@gmail.com; Licensed under CC-BY-SA 3.0).

Under international pressure following the killings of dozens of protesters and detainees by security forces, Bahrain's king formed the Bahrain Independent Commission of Inquiry to investigate the events of February to March 2011. The Commission's report, issued on November 23, 2011, concluded that the authorities were responsible for "grave violations of human rights, including the arbitrary deprivation of life, torture, and arbitrary detention."

Figure 17: A 2011 political billboard against the Bahraini protests says: “We request of the government.. The ultimate punishment. NO PARDON.. For the leaders of the sedition (fitna) and the deviant group.”

In 2016, the Bahraini authorities expanded their efforts to ban and dismantle opposition movements. The government dissolved Al-Wefaq and jailed its leader Ali Salman for life. The government also stripped the citizenship of Sheikh Isa Qassim, a natural born Bahraini and prominent Shia cleric regarded as the spiritual leader of Al-Wefaq. Bahrain stepped up repression measures in 2017. The government reinstituted the death penalty and authorities continued to employ arbitrary revocation of citizenship as a new means of repression. Hundreds of activists were stripped of their citizenship and remain stateless.

In March 2017, the Bahraini Justice Ministry dissolved and then charged Waad with “advocating violence, supporting terrorism and incitement to encourage crimes and lawlessness” after the political group issued a statement on the anniversary of the 2011 uprising saying that Bahrain was suffering from a “constitutional political crisis.” This event was followed by the permanent suspension of *Al Wasat* newspaper in June 2017. At the time, *Al Wasat* was Bahrain’s only independent newspaper, and had been briefly suspended several times since its inception in 2002.

Figure 18: Al Wasat's sign is removed from its headquarters following the permanent suspension of the newspaper by authorities in 2017.

Recent events suggest that the government of Bahrain will continue its repressive policies. Under the pretext of addressing COVID-19, the Bahraini government has imposed further restrictions on freedom of expression. Further, while Bahrain released a number of prisoners in March 2020 due to COVID-19, authorities excluded political prisoners from that release.

Bahrain's Internet Censorship

Freedom of expression is enshrined in Articles 23, 24, and 26 of the 2002 Bahraini Constitution. Despite this veneer of legal protection, Bahrain ranks 168 out of 180 countries on the 2021 World Press Freedom Index. The Bahraini government maintains tight control over the Internet by requiring all websites hosted in Bahrain to be registered with the Information Affairs Authority (IAA). The government imposes strict filtering policies.

One of the first instances of website censorship in Bahrain was the 2002 blocking of popular online forum BahrainOnline.org. The website, which was hosted outside of Bahrain, was central in facilitating public debate and discussion critical of the Bahraini government, from planning for the February 2011 protests to sharing videos and photos of human rights violations and protests.

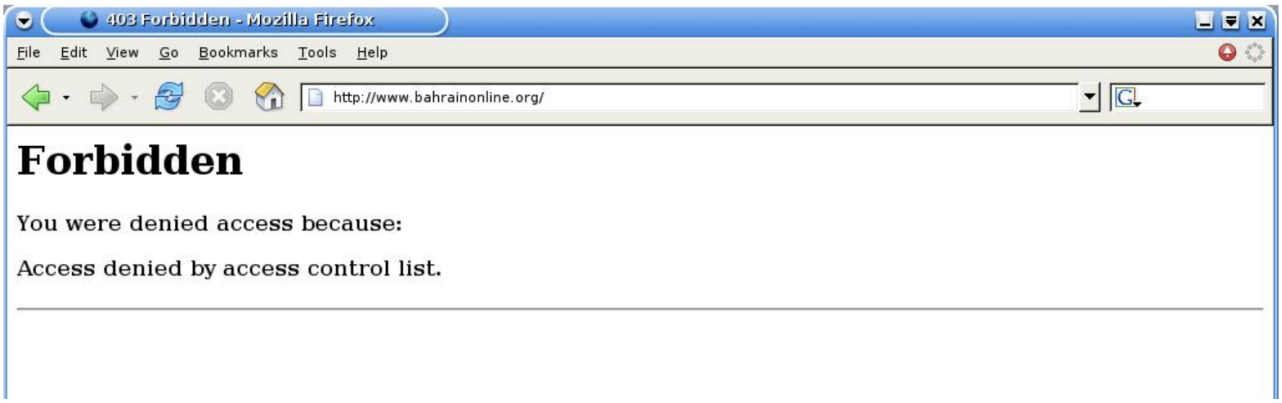


Figure 19: A 2005 screenshot from the OpenNet Initiative demonstrates censorship of BahrainOnline.org.

Bahrain formalized its Internet censorship regulations in 2009, when the Ministry of Culture and Information issued a resolution requiring all ISPs to install website blocking software chosen by the Ministry, and to comply with requests from the Ministry to block specific websites. The websites of political opposition, human rights organizations, and online newspapers were blocked in 2009. The same policies have been applied to social media platforms. In late 2010, the authorities blocked the Facebook page of Abdul Wahab Hussien, a Bahraini opposition leader.

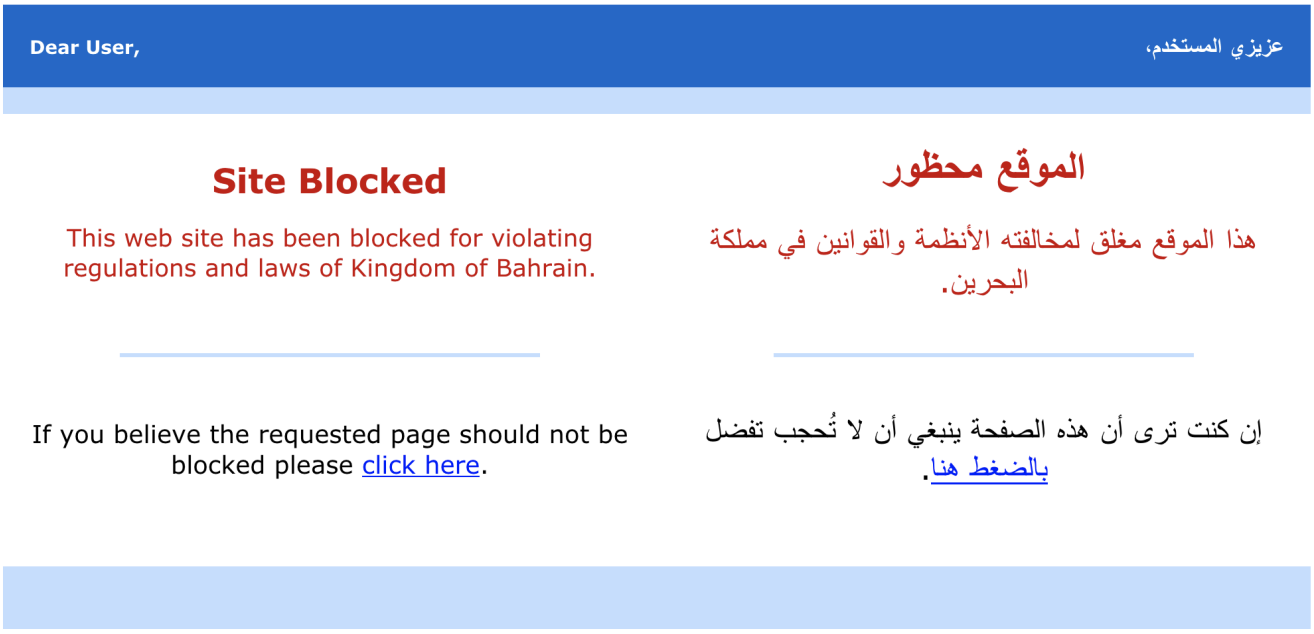


Figure 20: A Bahrain website blockpage from 2018.

After the uprising in 2011, the Bahraini authorities expanded Internet controls in the country by targeting political and religious and human rights content. Websites, live-streaming platforms, and some social media sites were censored.

In 2013, the Citizen Lab documented the presence of censorship and surveillance technology (namely, ProxySG devices and PacketShaper devices) produced by Blue Coat Systems in Bahrain. In 2016, the Citizen Lab reported that Internet-filtering technology produced by Netsweeper, Inc. was present on the networks of nine Bahrain-based ISPs.

Testing on the ISP Batelco showed that at least one of these Netsweeper installations was being used to filter political content, including content related to human rights, opposition political websites, Shiite websites, and local and regional news sources.

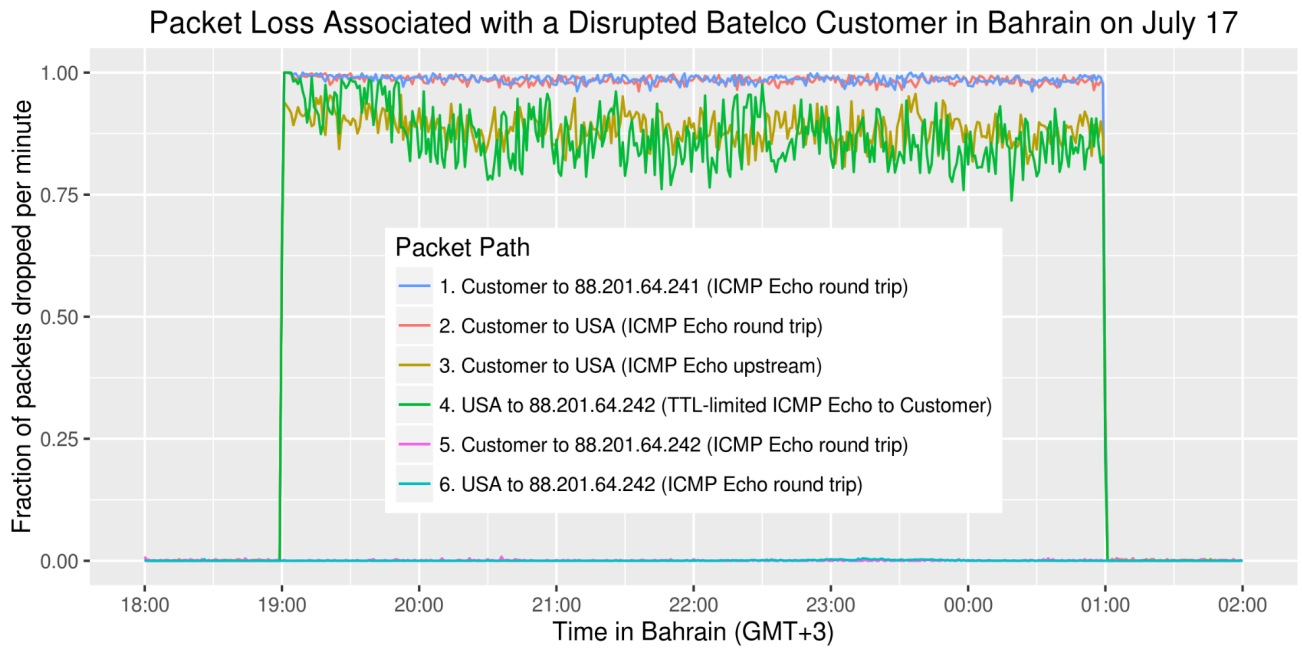


Figure 21: Astronomical latency was introduced into subscribers' Internet traffic by a device located inside Bahrain, between the hours of 7:00PM and 1:00AM every night during a protest in the village of Duraz.

Also in 2016, a nightly Internet disruption was reported in the Bahraini village of Duraz. The disruption coincided with peaceful nightly protests outside the house of Al Wefaq's de-facto spiritual leader, Isa Qassim, that started when the Bahraini government revoked his citizenship. An investigation by Bahrain Watch found that both landline and mobile Internet services were disrupted. Landline connections were disrupted by artificially introducing astronomical latency and packet loss between specific hours (Figure 21) on IP addresses assigned to subscribers in Duraz. During the same hours, all data services on cell towers serving Duraz were disabled. Outside of the disrupted hours, the Internet in Duraz appeared to function normally.

As of 2020, Bahrain continues to be categorized as "Not Free" by Freedom House. In its most recent Freedom on the Net report, Freedom House states "numerous websites continued to be blocked, social media users were continuously interrogated at the security department and were pressured to remove content, and citizens were arrested and jailed for content posted online," among other developments.

Surveillance of Bahraini Dissidents

In addition to the authorities expanding Internet controls in Bahrain, there have been numerous reports regarding Bahrain's use of surveillance technology against human rights activists, dissidents, and members of the political opposition, domestically and

transnationally.

In 2011, Bloomberg reported that Trovicor GmbH (previously related to Nokia Siemens Networks) sold interception equipment to Bahrain, which the authorities then used to spy on dissidents' communications. One such target was Abdul Ghani Al Khanjar, a Bahraini activist, who publicly described how he was confronted with transcripts of his SMS text messages while being detained and tortured by the authorities between August 2010 and February 2011. The transcripts of Al Khanjar's text messages were reportedly obtained from Trovicor's system.

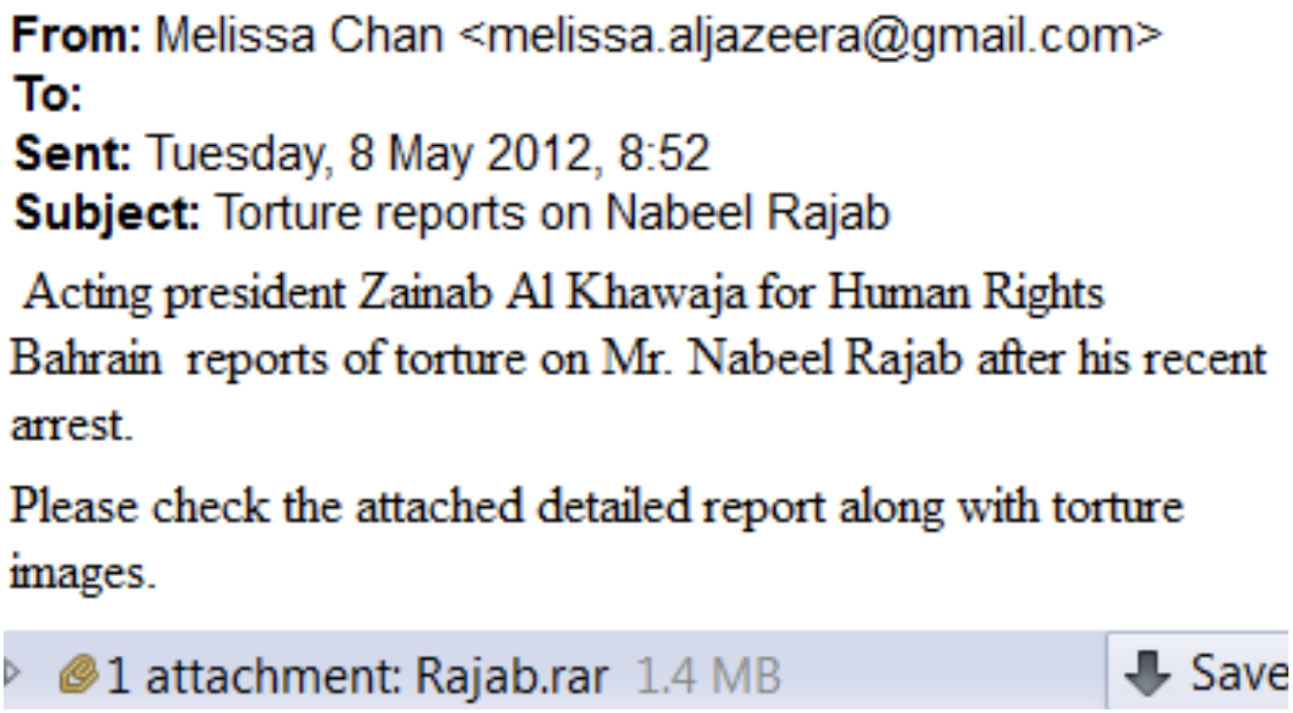


Figure 22: Emails like this one were sent to Bahraini activists. The attachments contained FinFisher spyware that sent information back to the Bahraini government.

In 2012, the Citizen Lab released a report describing the targeting of Bahraini activists and human rights defenders, using surveillance malware from a UK-German company, FinFisher. A subsequent leak of files from FinFisher indicated that the Bahraini government used FinFisher's spyware to spy on large swathes of the opposition at home and abroad. A leaked target list showed that the computer of a prominent Bahraini lawyer was hacked on the same day as a blackmail attempt against him. The lawyer received a CD containing instructions that the lawyer should stop defending activists, otherwise a video included on the CD would be publicized. The lawyer viewed the CD on his computer, and found that it contained a private video of him with his wife, recorded from a hidden camera installed in the ceiling of his house. A copy of the video was ultimately published when the lawyer refused to accede to the blackmail.

A 2013 report by Bahrain Watch documented how the Ministry of Interior's Cyber Crime Unit was deanonymizing pseudonymous Twitter activists by sending them *IP logger* links, and then requesting subscriber data from local ISPs for the IP address that clicked on the link.

Activists who clicked were arrested or fired from their jobs. For example, a high school student allegedly clicked on the IP logger link in the Facebook chat message in **Figure 23** that was sent from the account of an arrested activist. The student was sentenced by a Bahraini court to one year in prison because the account to which the IP logger link was sent had earlier published tweets deemed offensive to Bahrain's king.

Figure 23: IP Logger links included in messages like this one offering translation services were used to identify those who clicked.

Leaked documents and investigations have revealed a number of additional surveillance contracts between Bahrain's government and foreign companies. In 2013, Bahrain's Ministry of Interior acquired Hacking Team's spyware in 2013, though no Bahraini targets of Hacking Team's spyware were ever publicly identified. A 2016 investigation by Bahrain Watch and *The Intercept* that reviewed Bahraini court documents showed that the Bahraini government was using phone forensics technology sold by Cellebrite to extract private data from arrested activists' phones. Finally, a 2018 investigation by *Haaretz* revealed that Verint Systems Inc. provided Bahrain with technology for social media monitoring.

5. Conclusion

Despite a half-decade of being implicated in human rights abuses, NSO Group regularly claims that they are, in fact, committed to protecting human rights. The company has even published a "Human Rights Policy," a "Transparency and Responsibility Report," and claimed to subscribe to the *United Nations Guiding Principles on Business and Human Rights*. However, this purported concern is contradicted by a growing mountain of evidence that its spyware is used by authoritarian regimes against human rights activists, journalists, and other members of civil society.

Most recently, the Pegasus Project, a collaboration between Amnesty International and the Forbidden Stories collective, has revealed that a wide range of countries have leveraged Pegasus spyware to target and infect members of civil society, and their friends and family members, around the globe. In the context of this report, we shared a list of the targeted phone numbers we identified with Forbidden Stories. They confirmed that numbers associated with five of the hacked devices were contained on the Pegasus Project's list of potential targets of NSO Group's customers, data that Forbidden Stories and Amnesty International describe as dating from 2016 up to several years ago.

Bahraini Misuse of NSO Spyware was Tragically Predictable

While NSO Group regularly attempts to discredit reports of abuse, their customer list includes many notorious misusers of surveillance technology. The sale of Pegasus to Bahrain is particularly egregious, considering that there is significant, longstanding, and documented evidence of Bahrain's serial misuse of surveillance products including Trovicor, FinFisher, Cellebrite, and, now, NSO Group.

As highlighted in this report, Bahrain's human rights track record is equally notorious:

- According to Freedom House, Bahrain "has become one of the Middle East's most repressive states," and has "systematically eliminated a broad range of political rights and civil liberties, dismantled the political opposition, and cracked down harshly on persistent dissent in the Shiite population."
- In 2019, Human Rights Watch said that Bahrain's authorities had engaged in "unabated repression," and were "virtually eliminating all opposition."
- In 2017, the UN High Commissioner for Human Rights, Zeid Ra'ad Al Hussein, remarked that "the government of Bahrain has imposed severe restrictions on civil society and political activism through arrests, intimidation, travel bans and closure orders, with increasing reports of torture by the security authorities," adding that "the democratic space in the country has essentially been shut down."
- Bahraini human rights advocates are imprisoned, monitored, and intimidated at home, and those in exile are also subjected to digital and traditional means of repression.

These human rights abuses and prior sales of surveillance technologies are all a matter of public record. These documented abuses should have been obvious "red flags" if NSO Group was genuinely concerned about undertaking proper due diligence of its clients. The fact that Bahrain used NSO Group's spyware to target political opposition and activists, given the country's track record, was predictable. For NSO Group to sell Pegasus to Bahrain in light of this evidence is gross negligence in the name of profit.

Protecting against Zero-Click Attacks involves Tradeoffs

We believe that the specific attacks we mention in this report could have been prevented by disabling iMessage and FaceTime. However, NSO Group has successfully exploited other messaging apps in the past to deliver malware, such as WhatsApp. Thus, disabling iMessage and FaceTime would not offer complete protection from zero-click attacks or spyware. Additionally, disabling iMessage means that messages exchanged via Apple's built-in *Messages* app would be sent unencrypted (i.e., "green messages" instead of "blue messages"), making them trivial for an attacker to intercept.

6. Acknowledgements

Ali Abdulemam’s work on this project was supported by Access Now. Financial support for this research has been provided by the John D. and Catherine T. MacArthur Foundation, the Ford Foundation, Open Societies Foundation, the Oak Foundation, and Sigrid Rausing Trust. Thanks to Miles Kenyon and Mari Zhou for communications, graphics, and editing support, and Adam Senft and Bahr Abdul Razzak for editorial review.

---

1. From Sonar-HTTPS scans.↩
2. From our scans.↩