FINFISHER™

EXCELLENCE IN
CYBER INVESTIGATION

Keith Bagley
Jodi Delgado
Tyler Sizemore
Steven Martinez
Alison Graham
William Lan

What is or was the exploit, vulnerability or threat actor?

The Threat Actor is believed to be BlackOasis, part of Gamma Group.
An attacker can jailbreak the phone, if they have physical access to it.
It takes over your device by using Adobe Flash Zero-day to remotely deliver the latest version.
Sending Phishing emails and malicious Microsoft Word documents. Zero-days can be highly disruptive and take over quickly. The attacks can all happen at the same time and in the same region. Showing interest in important figures in the United Nations.

What exactly is Finfisher?

- Cyber solution protecting against organized crime
- Partners exclusively with Law Enforcement and Intelligence Agencies
- Priorities include:
  - Develop leading technology
  - Assistance and support
  - Improvements of customers' skill set
  - Enables customers to set up and run successful cyber operations

What Damage has it caused?

Most of the damage by Finfisher was done by governments to people or activists that were trying to oppose them.

They were in question to have broken the law by exporting powerful spying software without a permit by German officials.

Recently in July of 2019, there were findings of this spyware on mobile phones in Myanmar.

One day in 2011, Moosa opened the Facebook Messenger app on his iPhone. What he saw was chilling: someone else typing under his name to an activist friend of his in Bahrain. Whoever it was kept posing personal questions prodding for information, and Moosa watched unfold right before eyes. He panicked.

"It was like, ‘What’s going on? What’s happening?’" he recalls. He changed his password, alerted his friend, and stopped using Facebook Messenger — but the intrusions kept coming.

In another instance, Moosa noticed that someone posing as him solicited his female Facebook friends for sex — part of an effort, it seemed, to blackmail or perhaps defame him in Bahrain’s conservative media. Facebook was only the beginning. Unbeknownst to him, Moosa’s phone and computer had been infected with a highly sophisticated piece of spyware, built and sold in secret. The implant effectively commandeered his digital existence, collecting everything he did or said online.

https://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist

As recent as July 2019 they have found upgraded versions of FinFisher which can now obtain large amounts of information from phones, giving access to contacts, texts, emails, schedules, locations, photos, and saved information such as passwords. The damage that it can continue to cause with that information is endless and can range anywhere from a few minor purchases to complete identity theft.

Kaspersky says they have identified infected phones across 20 different countries, targeting both iOS and Android, with the majority of infected devices being Android.

Due to a recent IOs update, it appears that based on clues in the implant code that appears to only work if the device has been jailbroken thus requiring physical access to an Apple device

How to Mitigate

- Installing Anti-virus software on your device as a preventative measure.
- If you suspect your device has already been affected by this malware, you can scan for a Finfisher and take the necessary steps to remove it.
- Being that Finfisher is a type of Trojan-Horse malware, a step to prevent the malware from infecting your device would be to scan new software you download.
    - A Trojan-Horse is malware that is embedded into legitimate software and once a user downloads said software, the malware also is imported into your device.
    - ESET's Internet Security company provides an online scanner that identifies potential malware within download links, this too can be very beneficial prior to using download links for potential infected software.
- This specific Trojan-Horse malware takes place when one clicks on a download link their Internet Service Provider, reroutes the user to the infected link rather than the original software link.
    - This type of attack is known as a man-in-the-middle (MitM) attack
    - A potential safeguard may also be to download the link while using a VPN, to prevent a user's ISP from rerouting them to the malicious link.