Hacking (Back) and Influence Operations

By x0rz

Published: 2019-04-19 · Archived: 2026-04-05 16:47:42 UTC

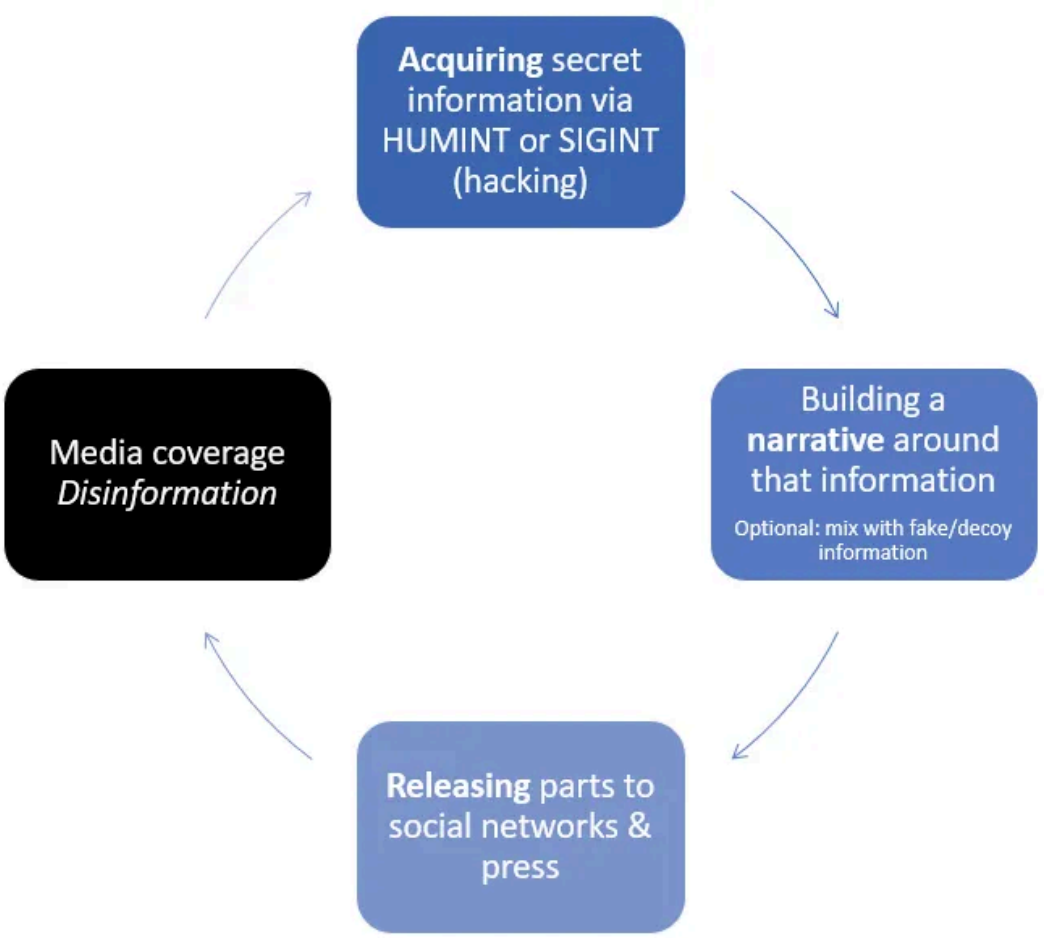
The new convergence of disinformation tactics and CNE in the Middle East

We all are collateral victims of very famous information operations, also known as influence operations. In the cyber realm they take full power: stealing information (via hacking or other means) is already a full time job, and disseminating that information through the press or social networks to fit a narrative is generally the easy part.

For example the Shadow Brokers leaks could be categorized as an IO (Information Operation), disrupting the NSA and the US intelligence agencies while making them appear weak and evil-minded (see the WannaCry aftermath and how the NSA has been held accountable for it). And it's not the first time leaking is related to hacking: Guccifer 2.0 was an IO as well, now widely acknowledged to be part of a Russian Intelligence disinformation campaign.

There are plenty other examples of these "*hack & publish*" operations, such as the Macron Leaks, this time released through Wikileaks. It was later suspected that Russia was involved.

> Hacking, bots, media amplification, disinformation: the new convergence of disinformation tactics and CNE



Steps to a “hack & *publish*” information operation

According to the US doctrine:

> The Secretary of Defense characterizes IO (Information Operations) as the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to **influence**, **disrupt**, **corrupt**, or **usurp** the decision making of adversaries and potential adversaries while protecting our own.

Source: Joint Publication 3–13

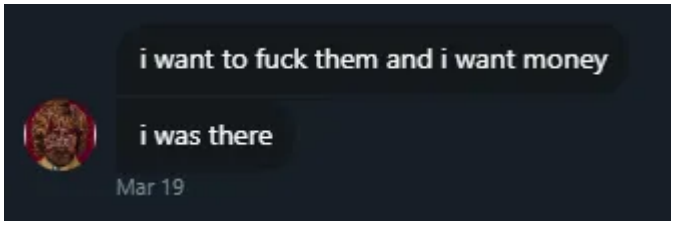
But would you believe other countries are doing the exact same thing?

Operation Lannister

On March 18th 2019 I was contacted by a mysterious *Mr_L4nnist3r*, brand new Twitter account, that explicitly wanted to leak information regarding APT34, a hacking group believed to be originating from the MOIS, the **Ministry of Intelligence of Iran** also known as VAJA (وزارتِ اطّلاعات جُمهوریِ اِسلامیِ ایران *Vezarat-e Ettela’at Jomhuri-ye Eslami-ye Iran*). This *Mr_L4nnist3r* said he was a former developer for APT34, he wanted money but most of all **he seemingly wanted to leak the data**, even for free. Odd, but why not?

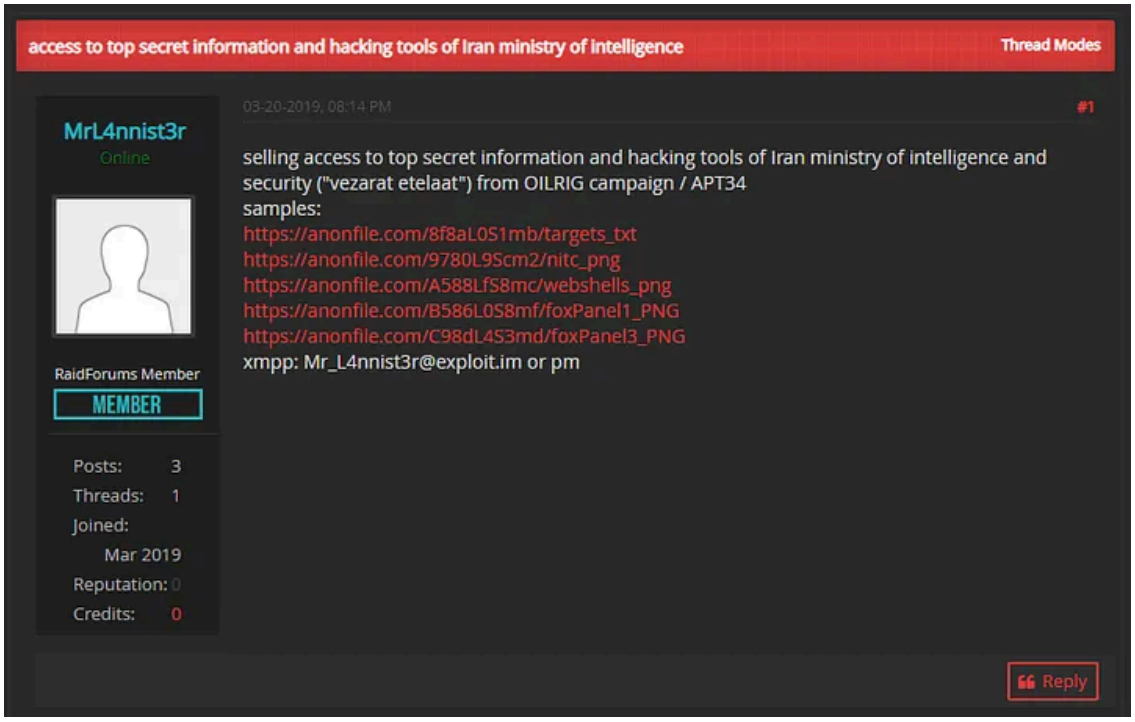
Mr_L4nnist3r contacting me

The files contain screenshots of the tools used, a target list and an archive with the BONDUPDATER malware source code (a Node.JS server acting as the C2 and the Powershell payload). At this point it is clear that the files are genuine, coming from the APT34 hacking team, and most likely from operators or at least some sort of internal infrastructure (similar to what the Shadow Brokers published). More technical details can be found on Misterch0c's blog.



Now why would a former developer working for the Iranian government would want to publish such documents? He was apparently selling the data a few days later on some hacking forum, but somehow **never mentioned a price to me, even if he said he wanted money**. Intriguing. Also *Mr_L4nnist3r* claimed to be responsible for DNSpionage, a cyberattack campaign attributed to Iran.

Press enter or click to view image in full size



MrL4nnist3r forum post trying to sell its documents

The files are clearly related to hacking activities, mentioning internal servers of targets, webshell URLs and such. Only what a threat actor could harvest. Which means that either *Mr_L4nnist3r* is a former operator from APT34, or that APT34 (the MOIS) **has been breached by a third party**. This is also known as **fourth-party collection (**see this [whitepaper by Juan Andres Guerrero-Saade & Costin Raiu](#)**):**

> Fourth-party collection involves interception of a foreign intelligence service's 'computer network exploitation' (CNE) activity in a variety of possible configurations. Given the nature of Agency-A as a cyber-capable SIGINT entity, two modes of fourth-party collection are available to it: passive and active. […]

Why Mr Lannister probably isn't from APT34

I personally believe this leak is being orchestrated by an outside party. He claimed to have been employed because of his “cyber knowledge”, but wasn’t aware of the *Shadow Brokers* when I mentioned it, which is really odd for someone apparently doing the same thing.

Get x0rz’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

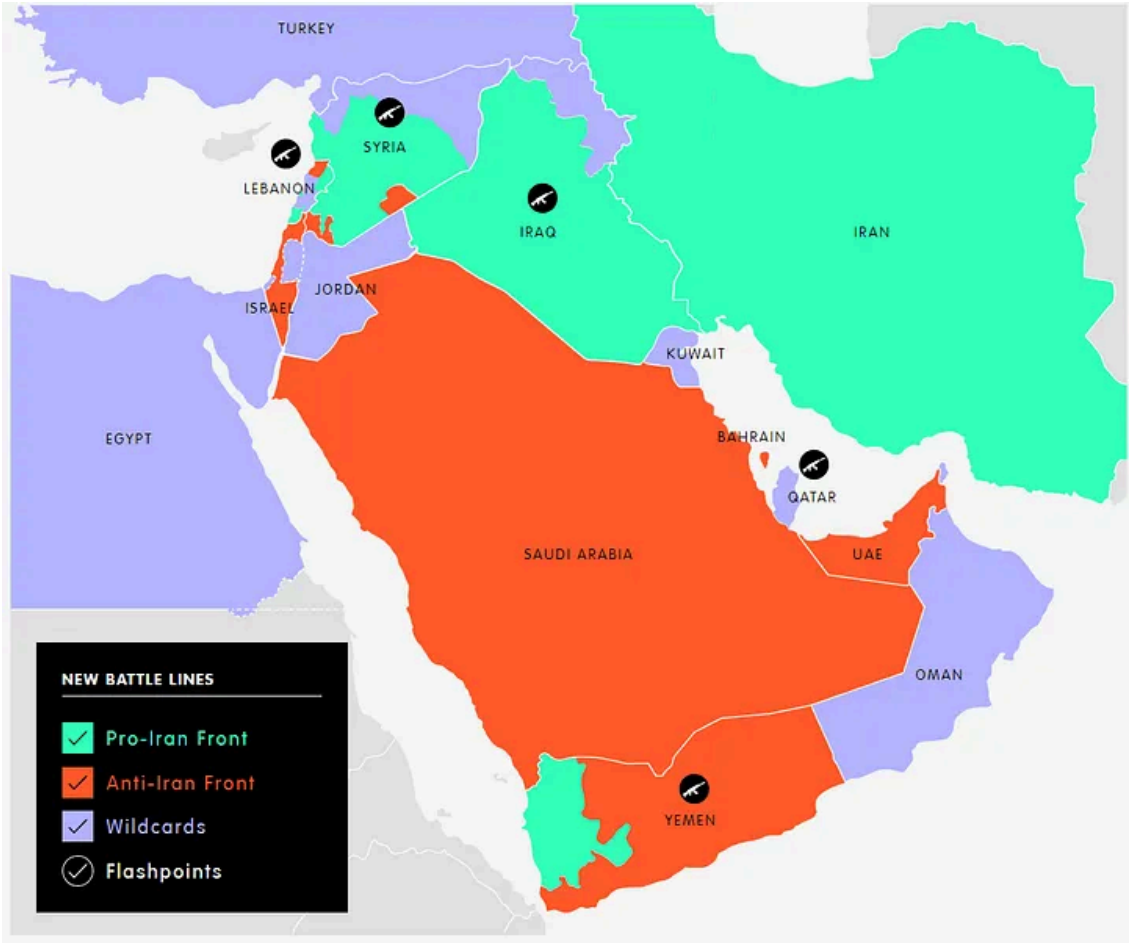
When confronted about his motivations, he was pretty vague and only wished to publish in order to “fuck the MOIS”. Well, that’s not really a strong stance for someone allegedly risking its life in Iran, you would at least be a little more passionate about your goal here. If you’re ready to die or get thrown into jail for a cause, you would at least write a manifesto or be a little bit more convincing than “fuck the government”. If he was a former APT34 member, the MOIS would know his name and they have the capability to execute people outside their territory, he

wouldn't be safe anywhere. Yet, *Mr_L4nnist3r* is available for a chat on Twitter and Jabber like nothing could happen to him. This story is just implausible.

Whistleblower ≠ third-party leaker

Also, the documents leaked are relatively scarce (meticulously selected?), I believe a developer or operator from APT34 would have accessed much more valuable information. Why not leaking the whole infrastructure? Why dropping documents without any context to it? Where are all the fun details? We've seen the Project Raven investigation uncovering the hacking efforts of UAE and what a former operator/analyst could describe. From the process of targeting people and how an operation is carried away down to the physical description of the offices. This is what is missing here to make it an authentic "internal" whistleblower. And why I don't believe this story — as it is being fed to the media.

Press enter or click to view image in full size



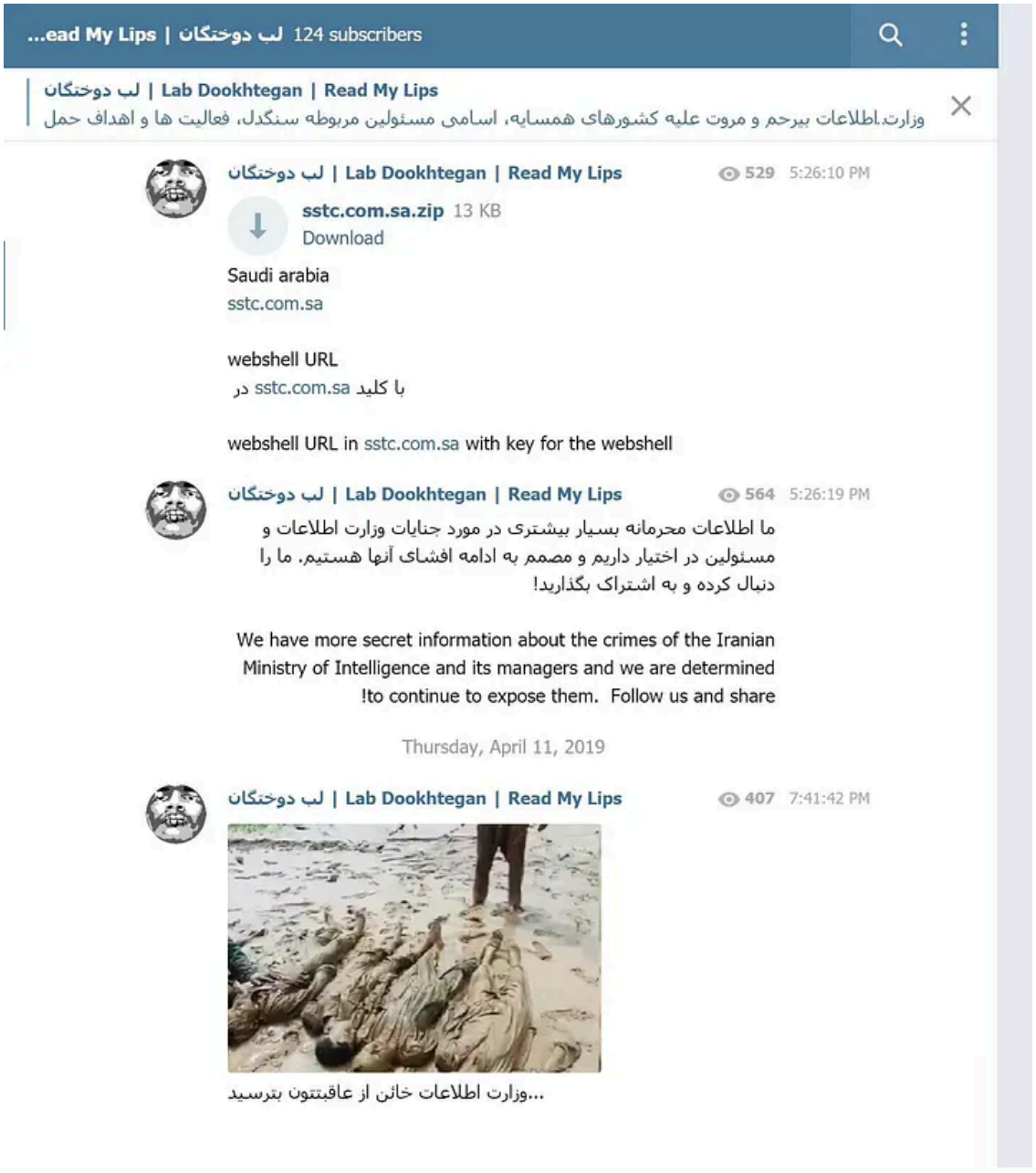
Middle East Battle Lines (source: European Council on Foreign Relations)

Attribution

Well, who would want to hurt Iranian offensive capabilities the most? Probably a lot of countries, Israel and the US at the top. Given the regional landscape and the current state of affairs, its neighboring countries are also good candidates. APT34 being particularly active in the Middle East, where it is reported to be targeting Middle Eastern

governmental agencies. This could very well be a counter-operation to the Iranian CNE efforts from one of its retaliating victims. Is this when Hack Back meets Information Warfare?

Press enter or click to view image in full size



Telegram group “Lab Dookhtegan” (origin of the leak) with political content against the Iranian Ministry of Intelligence

Considering the current media attention towards Saudi Arabia (notably the use of NSO hacking products in the Khashoggi case), it would make sense to think they could have done something to 1) shift media coverage against Iranian hacking activities and 2) disrupt current APT34 operations known to target Saudi Arabia and its regional allies. ***But then again, who knows?***

Operation assessment

So far, this doesn't appear to be as damaging to what the Shadow Brokers has done but all things considered I'm pretty sure it succeeded in disrupting the CNE efforts of the Iranian intelligence services. Shifting the media attention to Iran? Not there yet, very few documents in the dataset, and journalistically not that interesting to cover. Although ZDnet and others covered the leak :

But Catalin Cimpanu correctly warns the reader :

> In our Twitter conversation, the leaker claimed to have worked on the group's DNSpionage campaign, but this should be taken with a grain of salt, as the leaker could very well be a member of a foreign intelligence agency trying to hide their real identity while giving more credence to the authenticity of Iran's hacking tools and operations.

Interestingly, our gut feelings tell us there's something fishy going on with the leaker, something simply doesn't add up.

I think there's something missing for that leak to be originating from Iran, especially if the motive is political. Of course all of this is still a mystery and will probably stay that way. This is why these information operations are damn effective and generally hard to formally trace : plausible deniability and the lack of available information to debunk a story.

Disinformation

This may seem a bit counterintuitive but this is **disinformation**, even if the documents are **genuine**. I couldn't phrase it more accurately than the grugq :

We are only being served one side of the story, which happen to benefit one side only.
