GRU'S ALICE DONOVAN PERSONA WARNED OF A WANNACRY-LIKE EVENT A YEAR BEFORE IT HAPPENED

As I disclosed last month, I provided information to the FBI on issues related to the Mueller investigation, so I'm going to include disclosure statements on Mueller investigation posts from here on out. I will include the disclosure whether or not the stuff I shared with the FBI pertains to the subject of the post.

In this post, I suggested that The Shadow Brokers persona served as a stick to the carrots Vladimir Putin dangled in front of Donald Trump. When Donald Trump took an action — bombing Syria to punish Bashar al-Assad — that violated what I believe to be one of the key payoffs in the election quid pro quo, Shadow Brokers first bitched mightily, then released a bunch of powerful NSA tools that would soon lead to the WannaCry global malware attack.

It turns out GRU warned of that kind of attack a year before it happened.

One of the tidbits dropped into a very tidbit-filled GRU indictment is that GRU ran the Alice Donovan propaganda persona.

> On or about June 8, 2016, and at approximately the same time that the dcleaks.com website was launched, the Conspirators created a DCLeaks Facebook page using a preexisting social media account under the fictitious name "Alice Donovan."

That tidbit has led to some follow-up on the Donovan figure, including this typically great

DFRLab piece arguing that Russia had two parallel streams of troll campaigns, the Internet Research Agency one focused on the election, and the GRU one focused on foreign policy.

Donovan was first exposed in December of last year after WaPo reported on and CounterPunch did a review of "her" work after then WaPo reporter Adam Entous contacted CP after learning the FBI believed "she" had some tie to Russia.

> We received a call on Thursday morning, November 30, from Adam Entous, a national security reporter at the *Washington Post*. Entous said that he had a weird question to ask about one of our contributors. What did we know about Alice Donovan? It was indeed an odd question. The name was only faintly familiar. Entous said that he was asking because he'd been leaked an FBI document alleging that "Alice Donovan" was a fictitious identity with some relationship to Russia. He described the FBI document as stating that "Donovan" began pitching stories to websites in early 2016. The document cites an article titled "Cyberwarfare: Challenge of Tomorrow."

As both pieces emphasize, the first article that Donovan pitched — and "she" pitched it to multiple outlets — pertained to cyberattacks, specifically to ransomware attacks on hospitals.

The article was first published in Veterans Today on April 26, 2016. That's the same day that Joseph Mifsud first told George Papadopoulos Russia had emails — emails hacked by Donovan's operators — they planned to leak to help defeat Hillary Clinton.

CounterPunch published the cybersecurity article on April 29. That's the day the DNC first figured out that GRU (and FSB's APT 29) had hacked them.

Those dates may well be coincidences (though they make it clear the Donovan persona paralleled the hack-and-leak campaign). I'm less sure about the third publication of the article, in Mint Press, on August 17, 2016, just four days after Shadow Brokers went live. So just days after Shadow Brokers had called out, "!!! Attention government sponsors of cyber warfare and those who profit from it !!!" an article was republished with the penultimate paragraph accusing the US of planning to shut down Iran's power grid.

> Moreover, the U.S. has been designing crippling cyber attack plans targeting the civilian sector. In case its nuclear negotiations with Iran failed, the U.S. was prepared to shut down the country's power grid and communications networks.

The basis for that accusation was actually this article, but "Donovan" took out the reference (bolded below) to GRU's attack on Ukraine's power grid in the original.

> Today such ransomware attacks are largely the work of criminal actors looking for a quick payoff, but the underlying techniques are already part of military planning for state-sponsored cyberwarfare. Russia showcased the civilian targeting of modern hybrid operations in its attack on Ukraine's power grid, which included software designed to physically destroy computer equipment. Even the US has been designing crippling cyberattack plans targeting the civilian sector. In case its nuclear negotiations with Iran failed, the US was prepared to shut down the country's power grid and communications networks.
>
> Imagine a future "first strike" cyberattack in which a nation burrowed its way deeply into the industrial and commercial networks of another state and

> deployed ransomware across its entire private sector, flipping a single switch to hold the entire country for ransom. Such a nightmare scenario is unfortunately far closer than anyone might think. [my emphasis]

And “Donovan” adds in this sentence (from elsewhere in the Forbes article).

> Government itself, including its most senior intelligence and national security officials are no better off when a single phishing email can redirect their home phone service and personal email accounts.

When this article was first published, the memory was still fresh of the Crackas with Attitude hack, where self-described teenagers managed to hack John Brennan and James Clapper and forward the latter’s communications (among the men serving prison sentences for this attack are two adult Americans, Andrew Otto Boggs and Justin Liverman).

Most of the rest of the article uses the threat of malware attacks on hospitals to illustrate the vulnerability of civilian infrastructure to cyberattack. It cites a Kaspersky proof of concept (recall that Shadow Brokers included a long play with Kaspersky). It cites an FBI agent attributing much of this hacking to Eastern Europe.

> Stangl said the hackers, most of them from Eastern Europe, have increasingly targeted businesses, which are often able to pay more than individuals to unlock data. The hackers “scan the Internet for companies that post their contact information,” then send them email phishing attacks. Unsuspecting employees, Stangl said, are asked to click on what seem to be innocuous links or attachments — perhaps something as

> simple as a .PDF purporting to be a customer complaint — and before they know it, their computers are infected.

And the "Donovan" article explains at length — stealing from this article — why hospitals are especially vulnerable to malware attacks.

> Such attacks may all sound like nightmare scenarios, but the experts say they're becoming almost routine. And hospitals have not made cybersecurity a priority in their budgets. On average hospitals spent about 2 percent on IT, and security might be 10 percent of that. Compare that percentage to the security spending by financial institutions: for example, Fidelity spends 35 percent of its budget on IT.
>
> Moreover, medical facilities are vulnerable to these attacks in part because they don't properly train their employees on how to avoid being hacked, according to Sinan Eren, who has worked in cybersecurity for government and health-care organizations for two decades.
>
> "It's not like the financial-services industry, where they train employees how to spot suspicious emails," said Eren, general manager at Avast Mobile Enterprise. Also, many hospital computer systems are outdated, bulky and in dire need of upgrades or newer software, he said. But such institutions often don't have — or don't want to spend — the money to make sweeping changes.

While it's still unclear which computer WannaCry first infected in May 2017, Britain's National Health Service was easily the most famous victim, with about a third of the system being shut down. Not long after WannaCry, NotPetya similarly spanned the globe in wiperware

designed to appear as ransomware (though the latter's use of NSA tools was mostly just show). While the US and UK have publicly attributed WannaCry to North Korea (I'm not convinced), NotPetya was pretty clearly done by entities close to GRU.

And a year before those global pseudo-ransomware worms were launched, repeated just days after Shadow Brokers started releasing NSA's own tools, GRU stole language to warn of "a nation burrow[ing] its way deeply into the industrial and commercial networks of another state and deploy[ing] ransomware across its entire private sector, flipping a single switch to hold the entire country for ransom. Such a nightmare scenario is unfortunately far closer than anyone might think."

(h/t TC for the heads up on this file and a number of the insights in this piece)

Update: MB noted that the "added" sentence actually also comes from the original Forbes article (it links to an earlier column that notes the Crackas tie explicitly).