NSA'S SPYING ON LE PEN IS PROBABLY WORKING BETTER THAN GRU'S SPYING ON MACRON

In advance of this report on APT 28 (the hacking group presumed to be tied to Russia's military intelligence, GRU, blamed for the DNC hack-and-leak), Trend Micro got a lot of publicity for its report that APT 28 had targeted Emmanuel Macron, who just won the most votes in France's presidential election and will face a run-off against Marine Le Pen in a few weeks.

At least according to Macron's campaign, the attempts to phish his campaign were unsuccessful.

> Mounir Mahjoubi, digital director of Mr. Macron's campaign, confirmed the attempted hacking, saying that several staffers had received emails leading to the fake websites. The phishing emails were quickly identified and blocked, and it was unlikely others went undetected, Mr. Mahjoubi said.
>
> "We can't be 100% sure," he said, "but as soon as we saw the intrusion attempts, we took measures to block access."

The timing of all this is all rather interesting. Back in early February, France's Le Canard Enchaîné exclusively reported that France's security officials worried that Macron would be hacked, a vague report that was picked up really broadly without confirmation. Shortly thereafter, Macron claimed that his campaign had been the target of thousands of attacks from entities within Russia's border, including a DDOS attack that took down his website for

nine minutes. According to the sole mention of Macron in the Trend Micro report, the OneDrive-based phish targeting Macron took place a month later, on March 15.

These hacking attempts accompanied a great deal of fake news (and leaked gossip) targeting Macron. But at least if Macron's own campaign is to believed, *APT 28 never succeeded* in its attempt to hack the favorite to be France's next president, and so presumably has not yet succeeded in stealing emails that Russia might use to attack Macron during the run-off.

Which gives the hype about APT 28's attempted hack a really curious character. It is treated as if Russia is the only state actor that might be spying on French presidential candidates.

Does anyone honestly believe that the United States is not spying on Le Pen, for example, given that the CIA and NSA have a history of spying on candidates with whom the US is even friendlier than Le Pen? Indeed, earlier this year, WikiLeaks published a tasking order for CIA to collect HUMINT and open source intelligence on all the parties in the 2012 French election, though without any cyber element specified. In 2010, the incumbent Pakistan People's Party was included in NSA's foreign government Section 702 certificate by name. And in 2012, CIA and NSA partnered to target Enrique Peña Nieto and nine of his closest associates in the weeks leading up to his victory. With both the PPP and EPN, these were nominally political parties friendly to US interests.

By comparison, it would seem that targeting Le Pen, at a time when the intelligence community has a very public concern about collusion between Russia and populist parties in Europe to destabilize Europe, would be a no-brainer.

And here's what else gets left out of the coverage of GRU's attempts to spy on Macron: how much easier a job the NSA might have than GRU, even ignoring NSA's greater capabilities.

Many (though not all) of the phishing attempts detailed in the Trend Micro report pretend to be the email log-ins for US-based email providers: with virtually all the most detailed attention on Yahoo, Gmail, and Microsoft. The attempted Macron targeting exploited his campaign's use of OneDrive. That means all the entities GRU targeted with phishes pretending to be US providers are available to NSA via Section 702, or PRISM.

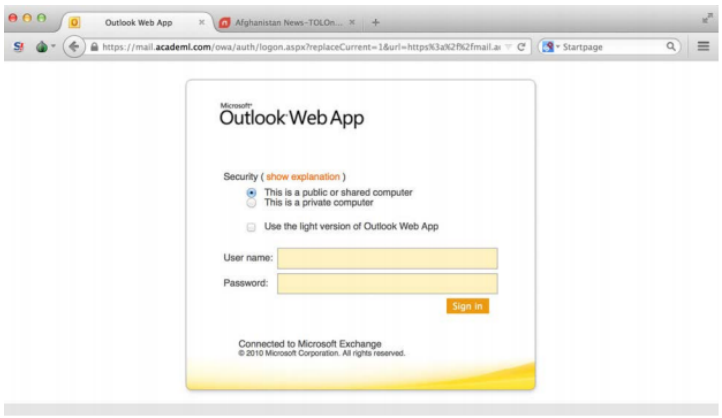

Figure 3. The credential phishing site that was opened in the browser by the tabnabbing trick

In other words, to collect on the very same targets that GRU is targeting via phishing attacks that users continue to be better informed about (and that Macron claims to have withstood entirely), the NSA could just add LePen's email address to the list over 93,000 targets being targeted under Section 702 (as they presumably did with PPP in 2010). And unlike a phishing campaign, which can be made more difficult with the use of two factor authentication, Le Pen would have no defense against collection targeting her or her campaign's PRISM provider accounts, beyond encrypting everything that resided in an American-owned cloud (and even there, there would be a great deal of interesting metadata available). If she or key aides uses any of the major American tech providers, stealing their emails would be as easy as providing a foreign intelligence justification (one that would be bolstered by her close ties with Russia) and tracking to make sure her accounts are detasked when she comes to the US to visit Trump Tower.

All that's on top of any more sophisticated targeting of Le Pen akin to what CIA and NSA did against EPN.

And therein lies the rub, the reason you shouldn't be saying, "So what? We *should* spy on that fascist Le Pen, she's a menace to civilization" (though I agree she is).

The NSA's spying on Marine Le Pen is likely having more success than GRU's spying on Emmanuel Macron. But is there any reason to believe — particularly given CIA's targeting of all French parties in 2012 and given Trump's stated preference for Le Pen — to think that NSA is not also targeting Macron, targeting his OneDrive in a way that would be immune from whatever defenses he is using against phishing attacks?

Here's where folks will say, "but we don't leak stolen communications," in spite of some evidence that we have in the past, albeit perhaps not in a democratic election. (On that note, this Politico story exposing Mike Flynn's ties, via his Turkish lobbying client, to Russia, relies on a WikiLeaks-released email, which is a notable instance where evidence made available by WikiLeaks may help those investigating Russia's influence on the Trump administration.). Of course, GRU can only leak what it can steal, and Macron believes that GRU hasn't succeeded in stealing anything.

Furthermore, *we have no visibility* what US policymakers in the past have done with intelligence collected on political parties. We certainly have no current limits on what Trump can do with it, aside from limits on the dissemination of that actual raw emails. We've always given the President great discretion on such issues, in the name of ensuring a unified foreign policy. And there are plenty of ways Trump's administration could intervene to help Le Pen beyond just leaking any derogatory information on Macron.

All this is not to say that GRU's reported

continued attempts to hack democratic targets is not a concern (indeed, I'm at least as worried that FSB is conducting similar intelligence collection without the same easily identifiable tracks).

But it is to say that, particularly in the era where Donald Trump sets this country's foreign policy, we need to be a lot more mindful of NSA's own far more considerable ability to steal information on democratic candidates.