US, UK, and Canada's COVID-19 research targeted by APT29

blog.f-secure.com/covid-19-vaccines/

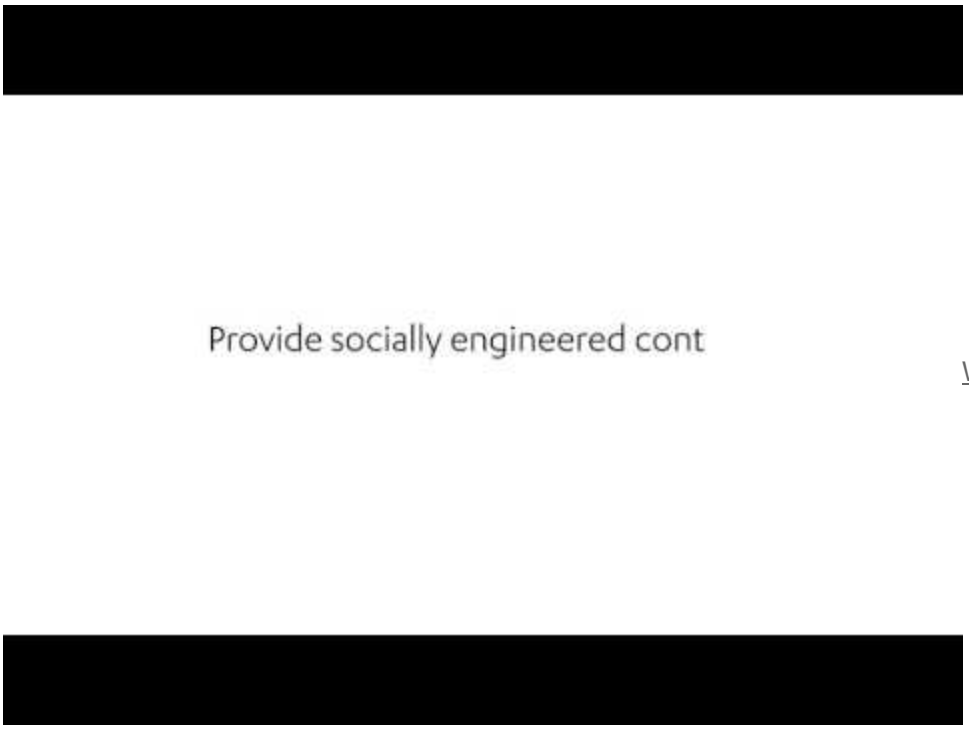
July 16, 2020

Earlier today, government agencies in the US, UK, and Canada warned that APT29, or The Dukes as they're known in some circles, has been targeting organizations' working on COVID-19 vaccines.

Speaking with reporters earlier today, F-Secure Director of Strategy and Corporate Development Artturi Lehtiö, who was the lead researcher in a 2015 analysis of the group's activities, said these kinds of organizations are not traditional targets for The Dukes. However, he also highlights that the attacks are consistent with The Dukes' alignment with national security interests – of which the coronavirus pandemic certainly qualifies.

> Not the traditional kind of target organization for APT29 aka Dukes. But COVID-19 is obviously a national security priority and those most definitely are the traditional remit of APT29. https://t.co/D3Zvl7whZS
>
> — Artturi Lehtiö (@lehtior2) July 16, 2020

According to a report published by the UK's NCSC, The Dukes are using public exploits against unpatched software to gain footholds in systems with the intent to steal information related to COVID-19 vaccines. After this initial access, they use malware to steal information. The report says The Dukes are also using spear phishing attacks – similar to the one in the video below – to manipulate users into disclosing login credentials.



https://youtu.be/9BnzwQRpq8o

Artturi points out that while The Dukes have compromised research organizations, such as universities, in the past, they've done so primarily to leverage that access in attacks against organizations more directly related to governments. In this case, Artturi thinks that The Dukes' sudden interest in stealing intellectual property could signal a shift in their priorities due to the severity of the pandemic in Russia.

"APT29 has traditionally focused on intelligence to inform national and security policy, rather than the theft of intellectual property. However, COVID-19 could be such a major national security priority for Russia that they need all hands-on deck. For what it's worth, APT29's history of targeting universities has been, to the best of our knowledge, a stepping stone to targeting think tanks and eventually governmental targets. But, since they've traditionally had access to these other networks, perhaps that's also now being utilized for this new priority."

You can follow Artturi on Twitter if you want to hear more on his thoughts about The Dukes, or you can listen to this episode of F-Secure's Cyber Security Sauna podcast to hear his reflections on The Dukes.

Categories

Threats & Research