GRU ADOPTED THE IDENTITY OF TWO UK JOURNALISTS TO PHISH THE OPCW

Yesterday, the government rolled out another indictment against GRU. DOJ earlier indicted those involved in the 2016 election operation and those behind the WADA hack; one person, Antoliy Kovalev, was named in both yesterday's indictment and the election one, and a second unit of the GRU was named in the earlier indictments along with Unit 74455, on which this focuses.

Down the road I'll circle back to some of the similarities and differences between these three indictments (I compared the earlier two here). For now, I want to look at how the hackers targeted for spearphishing people at the Organisation for the Prohibition of Chemical Weapons (OPCW) and Defence Science and Technology Laboratory, which runs Porton Downs, after the two organizations attributed the Sergey Skripal attack on GRU.

The spoofed actual journalists:

> 66. On or about April 5, 2018, KOVALEV created an email account with a username that mimicked the name of a German national weekly newspaper. Shortly after creating the account, KOVALEV sent spearphishing emails regarding the "Incident in Salisbury," purporting to be from a German journalist, to approximately 60 official DSTL email addresses. The next day, KOVALEV used the above-described Email Service to send emails, with malware attached, that appeared to be from a legitimate DSTL email address.
>
> 67. Also on or about April 6, 2018, the Conspirators conducted three related

> spearphishing campaigns that targeted the OPCW and U.K. agencies involved in the investigation of the poisoning.
>
> a. On or about April 6, 2018, the Conspirators used an operational account which was created on or about April 5, 2018, and had a username mimicking the name of a U.K. journalist working for a U.K. media entity-to send approximately 20 spearphishing emails with the email subject line "Salisbury Spy Poisoning Investigation" to official OPCW email addresses. In the emails, the Conspirators purported to have information to share regarding the poisoning.
>
> b. After the Conspirators received an email from OPCW directing them to instead share their information with certain U.K. authorities at three particular email addresses, the Conspirators used the same operational account to send spearphishing emails to those three email addresses.
>
> c. Also on or about April 6, 2018, the Conspirators created another operational account, with a username mimicking the name of another U.K. journalist at the same U.K. media entity, and shortly thereafter sent approximately 19 spearphishing emails with the subject line "Salisbury Spy Poisoning Investigation" to official OPCW email addresses. In the emails, the Conspirators again purported to have information to share regarding the poisoning.

They provide no hints about who the journalists were (though I have some guesses), but obviously they would have pretended to be people with close ties and significant trust in the national security community. Effectively, then, they were banking on the trust NatSec officials would have

in familiar journalists.

The tactic is particularly interesting given the way GRU has targeted journalists in phishing attempts in recent years, preferring the kind of NatSec friendly ones that might be useful for such a phish.

The indictment provides no other information about whether the GRU succeeded in this hack, and if so, what they did with it, leaving out any details obtained when the Netherlands caught the field hackers in the act later that year.

It’s as if this passage in the indictment exists solely to make public this tactic and signal that Kovalev (the one person also involved in the 2016 operation) was part of it.