

ON CROWDSTRIKE'S CURIOUSLY TIMED REPORT CLAIMING NEWFOUND "HIGH" CONFIDENCE IN ITS GRU ATTRIBUTION

Back on December 22, the security firm CrowdStrike released a report claiming that a tool used in the DNC hack had also been used – rewritten for Android – in malware that appeared in an application used by Ukrainian artillery units. The report itself purported to show that a hacking tool used in the DNC hack had also been used to kill Ukrainians fighting Russian separatists.

This implant represents further advancements in FANCY BEAR's development of mobile malware for targeted intrusions and extends Russian cyber capabilities to the front lines of the battlefield.

But the release of the report – released just a few weeks after President Obama called for a review of the intelligence relating to the DNC hack – was pitched to the press as the piece of evidence that CrowdStrike's confidence that Russia's GRU had hacked the DNC was now solid.

While CrowdStrike, which was hired by the DNC to investigate the intrusions and whose findings are described in a new report, had always suspected that one of the two hacker groups that struck the DNC was the GRU, Russia's military intelligence agency, it had only medium confidence.

Now, said CrowdStrike co-founder Dmitri Alperovitch, "we have high confidence"

it was a unit of the GRU. CrowdStrike had dubbed that unit "Fancy Bear."

The logic for that claim went this way:

- Two entities hacked the DNC, the first using tools associated with APT 29 (which CrowdStrike believes is FSB), the second using one tool (X-Agent) associated with APT 28 (which CrowdStrike believes is GRU). As I've explained, only the GRU attribution matters, because they're the ones associated with leaking the DNC documents to Wikileaks.
- CrowdStrike found X-Agent, rewritten for the Android platform, infecting an application used by the Ukrainian military, which is an obvious application for Russia's military intelligence GRU unit.
- Since X-Agent was found being used in an operation with obvious Russian military application, which therefore must be GRU, then GRU must be the entity that also hacked the DNC, because it used a common tool.

CrowdStrike's founder, Dmitri Alperovitch, told PBS that this amounted to DNA tying Russia to both the DNC hack and the Ukrainian artillery

app.

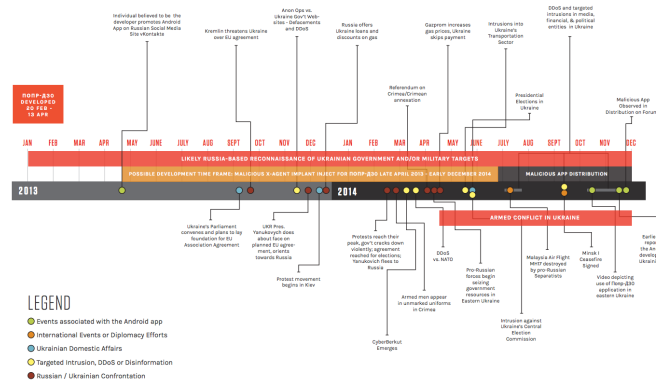
Essentially the DNA of this malicious code that matches to the DNA that we saw at the DNC.

Yesterday, the chief infosec skeptic of the claims that Russian hacked the DNC, Jeffrey Carr, did a post criticizing the CrowdStrike report. He makes several points:

- Two other entities (including an anti-Russian Ukrainian hacker) have gotten access to X-Agent – the tool in question – meaning that any use of it by GRU in one application cannot be said to be proof its use in another application means it was GRU.
- The hacking of the artillery app probably couldn't have had the complete functionality or the effect (devastating Ukrainian artillery units) CrowdStrike says it had.

The second point is interesting. I'd add that the timeline CrowdStrike develops to explain how Russian malware would end up in a Ukrainian artillery app by December 2014, in time to play a part in devastating losses, has some problems, notably that it assumes GRU was developing a tailored app to target Ukrainian soldiers more than six months before Viktor Yanukovich's ouster, at a time when a Russian-Ukrainian war was unforeseen. Why would Russia start developing an app to kill Ukrainian soldiers at a time when they were

still led by someone who was a Russian client? That development timetable appears to be dictated by the necessity of arguing that huge artillery losses that took place in July and August 2014 were due in part to this malware.



None of that is fatal to CrowdStrike’s argument that the malware infecting the Ukrainian artillery app was put there by Russia. I actually think that quite likely, though think CrowdStrike’s various explanations for it are unpersuasive.

But it does highlight how speculative the December 22 report was, creating explanations that *had* to be true because the conclusion – that the same malware used against the DNC had been used to kill Ukrainian soldiers – was presumed. Frankly, the report doesn’t hide that. Here’s just some of the uncertain language it uses:

Successful deployment of the FANCY BEAR malware within this application **may have** facilitated reconnaissance

The collection of such tactical artillery force positioning intelligence by FANCY BEAR further supports CrowdStrike’s previous assessments that FANCY BEAR is **likely** affiliated with the Russian military intelligence (GRU)

Therefore, the implant **likely** targeted military artillery units operating against pro-Russian separatists in Eastern Ukraine.

The promotion of the program was **likely** limited to social media,

At the time of this writing, **it is unclear** to what degree and for how long this specific application was utilized by the entirety of the Ukrainian Artillery Forces.

CrowdStrike Intelligence assesses that the application **likely** came to the attention of Russia-based adversaries around this time frame as a result of ongoing Russian reconnaissance

Because the Android malware could facilitate gross position information, its successful deployment **could have** facilitated anticipatory awareness of Ukrainian artillery force troop movement,

Although traditional overhead intelligence surveillance and reconnaissance (ISR) assets were likely still needed to finalize tactical movements, the ability of this application to retrieve communications and gross locational data from infected devices, **could** provide insight for further planning, coordination, and tasking of ISR, artillery assets, and fighting forces. [my emphasis]

While Carr's piece is *not* fatal to the argument that the X-Agent in the Ukrainian artillery app came from GRU, it does highlight how one person, in less than two weeks, could have found answers to some of things that CrowdStrike still hadn't even tried to answer (say, by interviewing the application developer) at least six months after they started looking into this malware.

More importantly, the first point Carr makes – that others have access to X-Agent – is very important. He notes that the anti-Russian hacker Sean Townsend not only knows that it could be used by others, but that it has been.

In fact, Sean Townsend believes that the Russian security services DO use it but he also knows that they aren't the only ones.

That doesn't mean that GRU wasn't the entity using X-Agent in the DNC server last year. It just means it is not, as CrowdStrike has always claimed, definitive proof that it had to be. If multiple people have access to X-Agent, the Ukrainian app, with its clear Russian military function, may be Russia while the DNC hack may be someone else.

I'll come back to that point later, but for the moment I want to look at how CrowdStrike came to release a speculative report tying the malware in the DNC servers to dead Ukrainians on December 22, less than two weeks after Obama called for a review of the intelligence on the hack.

I asked Alperovitch some questions about the genesis of the report on Twitter.



emptywheel
@emptywheel

.@DAIperovitch Can you disclose who paid CrowdStrike for the research that went into this report?
crowdstrike.com/blog/danger-cl...

10:21am · 3 Jan 2017 · TweetDeck

VIEW TWEET ACTIVITY

REPLY 1 RETWEETS 4 LIKES 8




Reply to @emptywheel @DAIperovitch


 **Dmitri Alperovitch** @DAIperovitch 1d
@emptywheel Yes. No one

 **emptywheel** @emptywheel 1d
@DAIperovitch Thanks for responding. So how did it come to your attention?

 **Dmitri Alperovitch** @DAIperovitch 23h
@emptywheel We uncovered it while hunting for X-Agent implants

 **emptywheel** @emptywheel 23h
@DAIperovitch After June some time?

 **Dmitri Alperovitch** @DAIperovitch 23h
@emptywheel This summer

 **emptywheel** @emptywheel 23h
@DAIperovitch Did you first find it in the RU-language military forum?

Alperovitch revealed that no one had paid for this report: CrowdStrike was apparently doing this work for free (!!). They found the X-Agent malware in the artillery app because they had set out to look for X-Agent implants. But when I asked about timing and/or where they found it, he got less responsive. Indeed, the timing of these discoveries is something the report itself is sort of funny about.

In late June and August 2016, CrowdStrike Intelligence provided initial reporting and technical analysis of a variant of the FANCY BEAR implant X-Agent that targeted the Android mobile platform².

²-For more information, contact CrowdStrike

Barring more clarification on whether they started looking for X-Agents before or after they very publicly accused GRU of hacking the DNC in June, what appears to have happened is this: CrowdStrike found the X-Agent in the DNC servers, accused GRU of doing the hack, and then set out – on their own dime – to find more instances of X-Agent deployment. They did not, however, do basic research (like calling the developer of the Android app, Jaroslav Sherstuk) to confirm their speculative conclusions about it, not over six months time.

Having not done that research, however, they released a report claiming they now had high confidence in their earlier attribution at precisely the time when it would affect the debate about whether GRU really did this hack or not.

Again, none of this means CrowdStrike was wrong about GRU hacking the DNC last spring. Just that this report – the timing of which is as interesting as the speculative claims – should not be regarded as providing the high confidence it claims.