# Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units

crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Adam Meyers

12/21/2016


**Update** – As of March 2017, the estimated losses of D-30 howitzer platform have been amended. According to an update provided by the International Institute for Strategic Studies (IISS) Research Associate for Defence and Military Analysis, Henry Boyd, their current assessment is as follows: “excluding the Naval Infantry battalion in the Crimea which was effectively captured wholesale, the Ukrainian Armed Forces lost between 15% and 20% of their pre-war D–30 inventory in combat operations.”

---

In June CrowdStrike identified and attributed a series of targeted intrusions at the Democratic National Committee (DNC), and other political organizations that utilized a well known implant commonly called X-Agent. X-Agent is a cross platform remote access toolkit, variants have been identified for various Windows operating systems, Apple’s iOS, and likely the MacOS. Also known as Sofacy, X-Agent has been tracked by the security community for almost a decade, CrowdStrike associates the use of X-Agent with an actor we call FANCY BEAR. This actor to date is the exclusive operator of the malware, and has continuously developed the platform for ongoing operations which CrowdStrike assesses is likely tied to Russian Military Intelligence (GRU). The source code to this malware has not been observed in the public domain and appears to have been developed uniquely by FANCY BEAR.

Late in the summer of 2016, CrowdStrike Intelligence analysts began investigating a curious Android Package

(APK) named ‘Попр-Д30.apk’ (MD5: 6f7523d3019fa190499f327211e01fcb) which contained a number of Russian language artifacts that were military in nature. Initial research identified that the filename suggested a relationship to the D-30 122mm towed howitzer, an artillery weapon first manufactured in the Soviet Union in the 1960s but still in use today. In-depth reverse engineering revealed the APK contained an Android variant of X-Agent, the command and control protocol was closely linked to observed Windows variants of X-Agent, and utilized a cryptographic algorithm called RC4 with a very similar 50 byte base key.


The filename ‘Попр-Д30.apk’ was linked to a legitimate application which was initially developed domestically within Ukraine by an officer of the 55th Artillery Brigade named Yaroslav Sherstuk. In media interviews Mr. Sherstuk claims that the application, which had some 9000 users, reduced the time to fire the D-30 from minutes to seconds. No evidence of the application has been observed on the Android app store, making it unlikely that the app was distributed via that platform.

*D-30 Howitzer in service with Ukrainian military* personnel

Today CrowdStrike is releasing publicly an intelligence report which was circulated to CrowdStrike Falcon Intelligence customers detailing the use of the trojanized 'Топр-Д30.apk' application by the Ukrainian military and the deadly repercussions inflicted on that platform by Russian forces. The key points of this report are:

- From late 2014 and through 2016, FANCY BEAR X-Agent implant was covertly distributed on Ukrainian military forums within a legitimate Android application developed by Ukrainian artillery officer Yaroslav Sherstuk.
- The original application enabled artillery forces to more rapidly process targeting data for the Soviet-era D-30 Howitzer employed by Ukrainian artillery forces reducing targeting time from minutes to under 15 seconds. According to Sherstuk's interviews with the press, over 9000 artillery personnel have been using the application in Ukrainian military.
- Successful deployment of the FANCY BEAR malware within this application may have facilitated reconnaissance against Ukrainian troops. The ability of this malware to retrieve communications and gross locational data from an infected device makes it an attractive way to identify the general location of Ukrainian artillery forces and engage them.
- Open source reporting indicates that Ukrainian artillery forces have lost over 50% of their weapons in the 2 years of conflict and over 80% of D-30 howitzers, the highest percentage of loss of any other artillery pieces in Ukraine's arsenal.
- This previously unseen variant of X-Agent represents FANCY BEAR's expansion in mobile malware development from iOS-capable implants to Android devices, and reveals one more component of the broad spectrum approach to cyber operations taken by Russia-based actors in the war in Ukraine.
- 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), and works closely with Russian military forces operating in Eastern Ukraine and its border regions in Russia.

The following Snort rule matches on the X-Agent-Android C2 beacon request:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (\
msg: “CrowdStrike FANCY BEAR X-Agent Android C2 Request”; \
flow: established,to_server; \
content: “lm=”; http_uri; \
pcre: “/^\/(watch|search|find|results|open|close)\/\?/U”; \
pcre: “/[\?\&](text|from|ags|oe|aq|btnG|oprnd)=/U”; \
classtype: trojan-activity; metadata: service http; \
sid: XXXX; rev: 20160815;)
```

Join Dmitri Alperovitch and me live on January 4, 2017 at 2pm EST for Bear Hunting: History and Attribution of Russian Intelligence Operations to learn more about FANCY BEAR and linkages to the GRU. Register now.

For continuous access to the industry-leading intelligence that powers CrowdStrike Falcon — *to include strategic, operational, and technical reporting as well as indicator feeds and APIs of more than 80+ Targeted Intrusion, Hacktivist, and eCrime adversary groups, their TTPs, and associated campaigns* — request info.

*As Vice President of Intelligence, Adam Meyers oversees all intelligence gathering and cyber adversary monitoring for CrowdStrike, the leader in cloud-delivered endpoint protection, threat intelligence and response services. Falcon Intelligence is part of the CrowdStrike Falcon Platform, which helps organizations stop cyber breaches. At CrowdStrike, the value of threat intelligence lies in its ability to proactively protect your environment from attacks, through a deep understanding of the adversary and what it takes to stop them.*