The PLA and the 8:00am-5:00pm Work Day: FireEye Confirms DOJ's Findings on APT1 Intrusion Activity

By by Fireeye Labs

Published: 2014-05-20 · Archived: 2026-04-05 22:27:27 UTC

Yesterday, the U.S. Department of Justice (DOJ) announced the indictment of five members of the Second Bureau of the People's Liberation Army (PLA) General Staff Department's Third Department, also known as PLA Unit 61398. This is the same unit that Mandiant publicly unmasked last year in the APT1 report. At the time it was originally released, China denounced the report, saying that it lacked sufficient evidence. Following the DOJ's indictment, however, China's usual response changed from "you lack sufficient evidence" to "you have fabricated the evidence", calling on the U.S. to "correct the error immediately." This is a significant evolution in China's messaging; if the evidence is real, it overwhelmingly demonstrates China's unilateral attempts to leapfrog years of industrial development -- by using cyber intrusions to access and steal intellectual property.

The evidence provided in the indictment includes Exhibit F (pages 54-56), which shows three charts based on Dynamic DNS data. These charts indicate that the named defendants (Unit 61398 members) were re-pointing their domain names at a Dynamic DNS provider during Chinese business hours from 2008 to 2013. The China work day, particularly for government offices, is very predictable, as noted on this travel site:

"Government offices, institutions and schools begin at 8:00 or 8:30, and end at 17:00 or 17:30 with two-hour noon break, from Monday to Friday. They usually close on Saturday, Sunday and public holidays."

What Exhibit F shows is a spike of activity on Monday through Friday around 8am in Shanghai (China Standard Time), a roughly 2-hour lull at lunchtime, and then another spike of activity from about 2pm to 6pm. The charts also show that there were very few changes in Dynamic DNS resolution on weekends.

At Mandiant (now a FireEye company), we can corroborate the DOJ's data by releasing additional evidence that we did not include in the APT1 report. In the APT1 report, we specified the following:

- Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their hop infrastructure from 832 different IP addresses with Remote Desktop.
- Of the 832 IP addresses, 817 (98.2%) were Chinese and belong predominantly to four large net blocks in Shanghai which we will refer to as APT1's home networks.
- In order to make a user's experience as seamless as possible, the Remote Desktop protocol requires client applications to forward several important details to the server, including their client hostname and the client keyboard layout. **In 1,849 of the 1,905 (97%) APT1 Remote Desktop sessions we observed in the past two years**, the keyboard layout setting was "Chinese (Simplified) — US Keyboard."

One thing we did not originally provide was an analysis of the time of day and day of week that these 1,905 Remote Desktop (RDP) connections occurred. However, when we look at these connections in bar chart format,

obvious patterns appear:

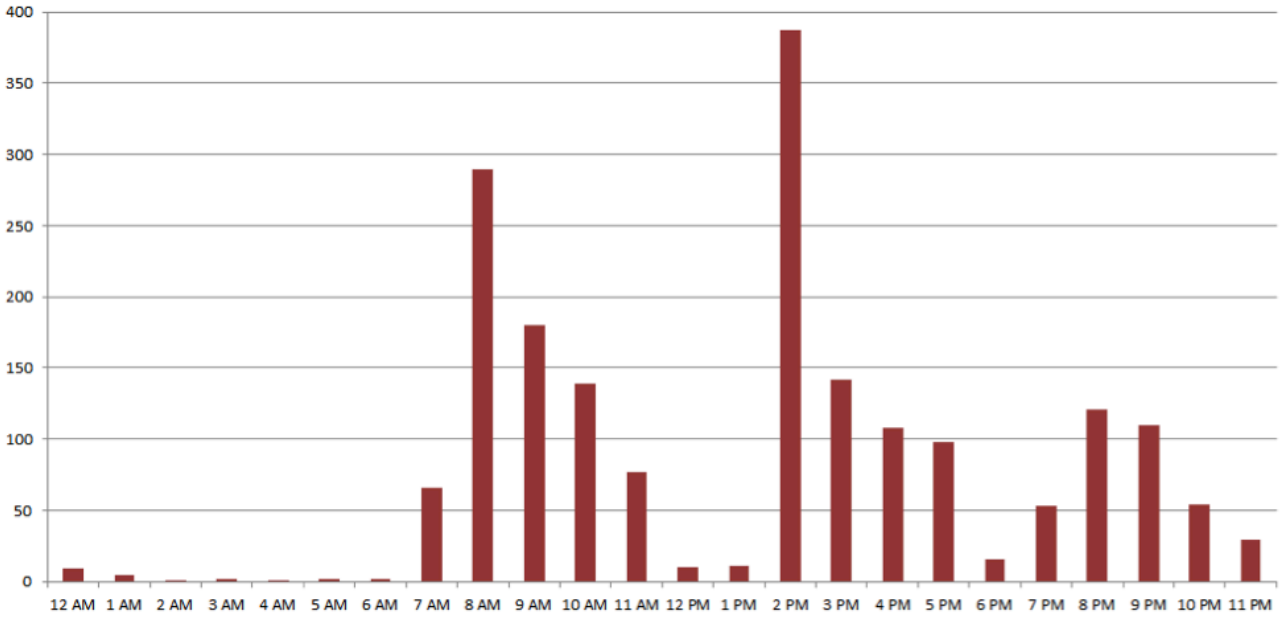

Figure 1: APT1 Remote Desktop login times distributed by hour of day (China Standard Time)

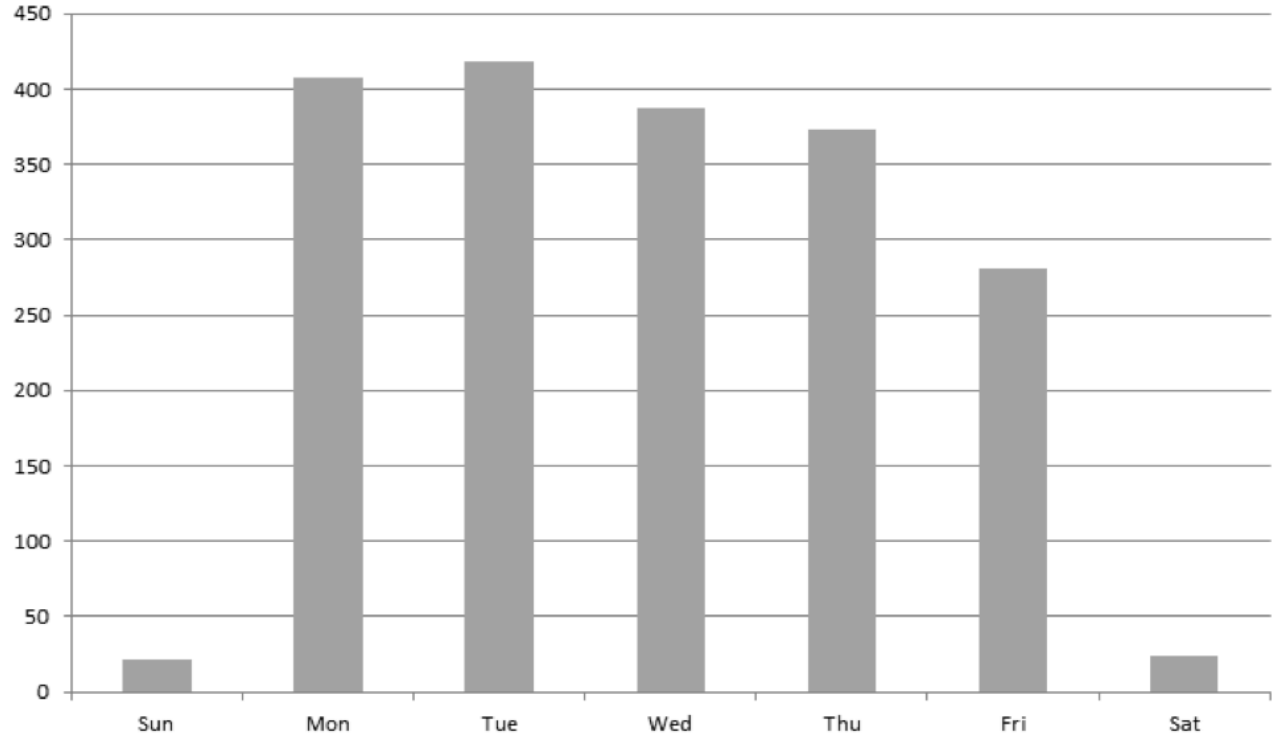

Figure 2: APT1 Remote Desktop login times distributed by day of week (China Standard Time)

Essentially, APT1 conducted almost all of the 1,905 RDP connections from 2011 to 2013:

- (1) On week days (Monday through Friday),
- (2) between 8am and noon, 2pm and 6pm, and 7pm and 10pm CST.

On some occasions, APT1 personnel appear to have worked on weekends, but these are minor exceptions to the norm. Consider the following evidence together for the 1,905 RDP connections:

- 98.2% of IP addresses used to log in to hop points (which help mask the real point of origin to victim organizations) were from Shanghai networks
- 97% of the connections were from computers using the Simplified Chinese language setting
- 97.5% of the connections occurred on weekdays, China Standard Time
- 98.8% of the connections occurred between 7am and midnight China Standard Time
    - 75% occurred between 8am to noon or between 2pm to 6pm
    - 15% occurred between 7pm and 10pm

The simplest conclusion based on these facts is that APT1 is operating in China, and most likely in Shanghai. Although one could attempt to explain every piece of evidence away, at some point the evidence starts to become overwhelming when it is all pointing in one direction. Our timestamp data, derived from active RDP logins over a two year period, matches the DOJ's timestamp data, derived from a different source -- active Dynamic DNS re-pointing over a five year period. **These data sets show that APT1 is either operating in China during normal Chinese business hours or that APT1 is intentionally going to painstaking lengths to look like they are.**

The data used to produce the charts above are archived in raw format and we are confident that any computer networking expert would certify them as genuine and non-fabricated in a court of law. But, that isn't really the issue. The real issue is: will this activity continue and for how long? Regardless, FireEye remains focused on how these threats evolve over time, in order to reduce the time from "detect" to "fix", as these and other actors continue targeting potential victims.
