Gothic Panda possibly used DoublePulsar a year before the Shadow Brokers leak

Reference: Memo [190517-1] Date: 17/05/2019 - Version: 1.0
Keywords: APT, DoublePulsar, China, US, Equation Group
Sources: Publicly available sources

Key Points

- Gothic Panda may have used an Equation Group tool at least one year before the Shadow Brokers leak.
- It is unknown how the threat group obtained the tool.
- This is a good example of a threat actor re-using cyber weapons that were originally fielded by another group.

Summary

According research conducted by Symantec, the Chinese threat actor known as Gothic Panda (APT3, UPS, SSL Beast, Clandestine Fox, Pirpi, TG-0110, Buckeye, G0022, APT3) had access to at least one NSA-associated Equation Group tool a year before they were leaked by the Shadow Brokers threat actor.

On April 14, 2017, a threat actor called the Shadow Brokers released a bundle of cyber-attack tools purportedly coming from the US NSA, also referred to as the Equation Group. Among the released material there was the DoublePulsar backdoor implant tool, which was used alongside EternalBlue in the May 2017 destructive WannaCry attack.

DoublePulsar is a memory-based kernel malware that allows perpetrators to run arbitrary shellcode payloads on the target system. It does not write anything on the hard drive and will thus disappear once the victim machine is rebooted. Its only purpose is to enable dropping other malware or executables in the system.

According to Symantec, Gothic Panda used the DoublePulsar exploit as early as in 2016, a full year before the Shadow Brokers release. It was delivered by Bemstour, a tool that was specially designed for this purpose. Bemstour exploited several Windows vulnerabilities, two of them were zero-days at that time. The version of DoublePulsar that Gothic Panda used is different from the on leaked by the Shadow Brokers. This, and the fact the Gothic Panda used it before it had been leaked to the public, gives reason to believe that they had obtained it separately.

According to open sources, Gothic Panda is likely a contractor of the Chinese Ministry of Security Services. It has been active since at least 2014 and targets telecommunications companies as well as research and educational organisations in Hong Kong, the Philippines, Vietnam, Belgium, and Luxembourg. Gothic Panda seems to have stopped operating in mid-2017. In November 2017, three alleged members of the group were indicted in the US. However, this did not end the use of the Gothic Panda toolkit. According to Symantec, the most recently observed sample of Bemstour was compiled in March 2019. It is unknown if the current user of the tool is a new incarnation of Gothic Panda or some other threat actor the tool kit may have been shared with.

Comments

Symantec's report has not been backed up by other sources. Also, it is not clear how Gothic Panda may have obtained the NSA hacking tools. It is plausible that they may have found it on their victims' systems who may have also been targeted by the Equation Group. It is unlikely that they found the tool on a compromised Equation Group computer because, according to sources, they did not seem to have had access to the malware binaries and had thus re-developed the tool themselves. Additionally, Gothic Panda only seems to have used the DoublePulsar exploit from among the treasure-trove of other exploits and tools that the Shadow Brokers leak exposed. Accordingly, if Symantec's report is true, Gothic Panda is likely to have observed DoublePulsar in the wild and taken it from an infected machine or extracted it from network traffic it has had access to.

CERT-EU wrote about the Equation Group's attack tools and their proliferation in CITAR-Flash-2017-009 and TLR2017Q2.