MoonBounce:

The Dark Side of UEFI Firmware

MoonBounce is a firmware rootkit that was discovered at the end 2021, the rootkit has been detected by Kaspersky's Firmware Scanner. The attacks seem to be associated with APT41, a threat actor that has been widely reported to be Chinese. The targets seem to be focused mostly on companies and organizations that deal with advanced technology transportation. The MoonBounce firmware is a tampered version of a UEFI firmware made to embed a malicious code. The reason it took so long to discover this is due to the fact that the code itself lives in the SPI flash, which is located on the motherboard instead of the hard disk, this makes it harder to detect and allows it to affect the system even if the operating system is reinstalled. MoonBounce is able to install and deploy user-mode malware which can download malicious payloads from the internet, in doing so it does not leave traces on the hard drive, facilitating a fileless attack with a small footprint. Although firmware rootkits are not new, older rootkits generally are more easily detectable, this points to an evolution in both firmware rootkit complexity and a highly funded attacker. Kaspersky managed to track down the user logs of the attackers after they had gained a foothold on the network. It appears the attackers are trying to earn a permanent foothold on the network, by modifying the Active Directory domain and creating a permanent and invisible remote command connection. Although MoonBounce is not inherently malicious, the attackers are able to carry out attacks unseen due to the camouflage provided by the MoonBounce firmware.

MoonBounce is a threat to primarily system integrity and authenticity. MoonBounce does not directly affect confidentiality, the goal of MoonBounce is to have a backdoor into a system that allows for the discrete download of malicious software, that software is then used to compromise confidentiality. In addition, the goal of MoonBounce is not to break the system beyond use like in a denial of service attack, instead it is meant to be an invisible agent that lies within the system even after re-installing the operating system. MoonBounce is a threat to integrity because the system data can be altered or new data can be added without the consent of the user and it can be done in a way in which the user would never know the attack is occurring. In addition MoonBounce is able to authenticate malicious software and allow the software to be installed on the system remotely without leaving logs in the hard disk memory. Because MoonBounce can circumnavigate the users inputs and actively hide modifications made to the system, it is a major threat to the integrity of not only the active system but also any network the system is connected to.

Source:

https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/