Issued 6/22/18

This New Windows Malware wants to Add your PC to a Botnet - or Worse

A new malware campaign is roping systems into a botnet and providing the attackers with complete control over infected victims, plus the ability to deliver additional payloads, putting the victims' devices at risk of Trojans, keyloggers, DDoS attacks and other malicious schemes. The malware comes equipped with three different layers of evasion techniques which have been described by the researchers at Deep Instinct who uncovered the malware as complex, rare and "never seen in the wild before". Dubbed Mylobot after a researcher's pet dog, the origins of the malware and its delivery method are currently unknown, but it appears to have a connection to Locky ransomware -- one of the most prolific forms of malware during last year. The sophisticated nature of the botnet suggests that those behind it aren't amateurs, with Mylobot incorporating various techniques to avoid detection. They include anti-sandboxing, anti-debugging, encrypted files and reflective EXE, which is the ability to execute EXE files directly from memory without having them on the disk. The technique is not common and was only uncovered in 2016, and makes the malware ever harder to detect and trace. On top of this, Mylobot incorporates a delaying mechanism which waits for two weeks before making contact with the attacker's command and control servers -- another means of avoiding detection. "The reason to do 14 days of sleep is to avoid any network and malicious activity, thus bypassing cyber security solutions like endpoint detection and response, threat hunting and sandboxing," Tom Nipravsky, Deep Instinct security researcher told ZDNet. Once installed on a system

Mylobot shuts down Windows Defender and Windows Update, while also blocking additional ports on the firewall -- all tactics to ensure that its malicious activity can operate without being impeded. In addition to this, it actively targets and deletes any other instances of malware which have previously been installed on the machine, even specifically aiming for other botnets. Once a computer is part of the botnet, the attacker can take complete control of the system and further payloads and instructions can be delivered from the command and control server. "The botnet is trying to connect to 1,404 different domains -- at the time of writing this research, only one was alive. This is an indication for big resources in order to register all those domains," said Nipravsky.