WEEKLY THREAT REPORT
June 15th 2020

The fifth edition of the "One Intelligence" weekly report is a high-level report designed to share intelligence about the most notable attacks, breaches and malware. Experts from Anomali, Flashpoint and Silobreaker, analyse and highlight new techniques used by attackers over the last week.

Financial data shows a 50% growth in the use of mobile banking since the start of 2020 and we are expecting to see a corresponding increase in number of threat actors targeting these platforms. The FBI has warned that they expect attacks to utilise app-based banking trojans and fake banking apps to target customers. The security of mobile devices has been questioned for a while now, with a huge amount of sensitive data being used and stored on them. A security platform such as ZecOps will look at the underlying system logs of the device and can indicate whether the device has been compromised or not, something no other security organisation is doing.

Conduent, a large US-based business process services company has been hit by Maze, a strain of ransomware that is already well known across the world. The operators of this attack leaked 1GB of data from Conduent's network on the website, stating that they had stolen sensitive data and had encrypted devices. It is thought that they leveraged a vulnerability in a Citrix server that allowed for remote code execution, followed by lateral movement to collect data, and encrypt drives. Several security systems could have prevented the spread of this attack, such as ransomware detection (Bullwall) to stop file encryption and to alert on an attack and a proper patching schedule and configuration management system, such as Skybox.

The death of US citizen George Floyd has sparked global uproar and wherever there is a big worldwide news story, there are opportunities for threat actors to take advantage of the situation. The George Floyd case is no different and far-right extremists across the world have begun to discuss this on both the open web, and deep and dark web. There is the potential for the acceleration of violence via various online communities that are using acronyms such as "ACAB" (All Cops are Bastards), which is causing an increase of violence against law enforcement. It is important for public-facing organisations to understand how the discussion of violence and extremist communications could affect them, and with the use of Silobreaker (for open web discussions) and FlashPoint (for deep and dark web discussions) business decisions can be made around this topic.

One of NASA's IT contractors (Digital Management Inc.) is said to have been breached, when the network was compromised by the operators of the DopplePaymer ransomware. The group leaked 20 files onto its dark web portal to prove legitimacy of the compromise. The data leaked included HR details, project plans and employee records. The breach not only hit NASA, as a total of 2,500 servers and workstations within the Digital Management Inc. internal network had been encrypted and held at ransom. The attack is likely to have entered the network through a phishing attack and side stepped through the network to get to the sensitive systems. Early detection of such attacks would have given Digital Management Inc. the information to stop the attack before too much damage was done. A system such as Anomoli would look for early indicators of a compromise and alert where necessary. Anti-virus and endpoint protection software could be used but cannot guarantee prevention of ransomware, as new strains of ransomware can sometimes take weeks to be patched. A last line of defence system, such as Bullwall, would provide a more reliable prevention technique as it looks at the file headers, extensions, and patterns despite the strain of ransomware, so can stop new strains from day one.

A data breach linked to the Spanish language e-learning platform 8Belts, has exposed PII data of its customers. The breach was a result of misconfigured AWS systems, and affected many hundreds of thousands of users around the world. It is critical to ensure you regularly review the configuration of all hosted systems. A defence-in-depth approach is the best way to defend against advanced attacks, which means having layered security infrastructure to protect against each phase of an attack.

If you would like to learn more about One Intelligence technologies, please get in touch with one of the team via info@onedistribution.co.uk