WEEKLY THREAT REPORT
June 8th 2020

Our fourth weekly edition of the "One Intelligence" report is a high-level report designed to share intelligence about the most notable attacks, breaches and malware that experts from Anomali, Flashpoint and Silobreaker, who have analysed and highlighted new techniques used by attackers over the last week.

With healthcare-related organisations now in the spotlight across the world, there is a large market for stolen data on both the deep and dark web. These data sets include data from health insurance organisations. Generally, the data obtained from breaches, compromised remote desktop protocols and ransomware. The healthcare industry is notorious for being behind with security, patching, hardware etc and therefore, is easily targeted. Due to the nature of healthcare organisations, significant volumes of PII data on patients is retained, in addition to financial records when healthcare insurance is concerned. This data is an attractive and easy target for threat actors who have been selling the exfiltrated data on the deep and dark web for approximately $0.50 to $1.00 per medical record; however, some posts in early 2020 advertised the medical data for around $2.00 per record. With healthcare organisations being pushed both physically and financially during the first half of this year, they are prime targets for cyber-attacks.

A US-based marketplace for independent artists has disclosed a data breach after a hacker sold a database containing 5 million user records on a dark web marketplace. Exposed data includes names, email addresses, hashed and salted passwords, billing addresses, and more. There is a constant stream of data breaches that are disclosed publicly, all this information can be seen using tools such as Silobreaker.

There has been an alert about malware found in Java projects that can run on Linux, MacOS and Windows operating systems. Vulnerability is in an IDE named NetBeans. Once the user downloads a repository, the malware infects the local machine and spreads into other Java projects, the next step of the malware is to download a Remote Access Trojan, which sniffs for confidential information, including source code, which if exfiltrated could be a huge issue for software development organisations. There are a few things to help in spotting attacks like these. Anomoli can spot the indictors of a compromise early on and if the attack gets to data exfiltration stage, CyGlass is able to alert and stop these kinds of attacks.

Microsoft's IIS servers have been exploited due to a critical vulnerability allowing threats actors to host a cryptominer on the server. The vulnerability allows attackers to gain backdoor and shell access in just two steps. With such a simple attack, it is imperative to ensure a patching schedule is in place and adhered to.

WordPress is yet again being targeted with over 130 million attacks hitting 1.3 million WordPress sites. These attacks attempted to download a file critical to the WordPress installations, which contains backend database credentials, connection information, unique keys, and salts. WordPress has come forward and stated that the attacks are linked to an attacker who previously launched a similar scale attack targeting cross-site scripting flaw. WordPress is quite often left unpatched, meaning that a huge number of websites and backend data are exposed. Several discussions on this matter have been seen on the internet. These attacks can be seen using tools such as Silobreaker.

There has been a critical update released for iOS and iPadOS devices, related to two vulnerabilities in the default email application. These vulnerabilities allow threat actors to corrupt and modify memory or terminate applications. All devices running iOS versions 3.1.3 up to 13.4.1 are vulnerable. Apple has patched these upon the release of 13.5. Forbes reported on these vulnerabilities which were initially discovered by ZecOps and reported to Apple directly.

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