# WEEKLY THREAT REPORT
# June 2nd 2020

## Welcome to our third edition of the "One Intelligence" Weekly Report. This high-level report is 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.

Several financial technology applications are said to be targeted, as threat actors on both the deep web and dark web express interest in buying and selling accounts for such applications. Some of these apps are dedicated to personal finance activities and often contain highly sensitive data. The data retrieved from these apps is also being used as a method of payment on the deep and dark webs. Although the financial technology apps are apparently not being targeted any more than the traditional financial institutions, these types of applications contain payment details, mortgage details, credit card information etc that can be exploited for fraudulent purposes. Organisations that have had a significant number of fraud-related references across the deep and dark webs include Credit Karma (previously Noddle), Plaid and Square Cash. It is recommended that passwords for all online accounts are updated regularly to prevent access in the event of a password leak. Learn more about Flashpoint's Intelligence Platform.

Another large financial and retail technology company Diebold Nixdorf (a major provider of ATM machines) was hit by a ransomware attack earlier this month. The group behind the attack, ProLock Ransomware, is a relatively new group that uses phishing emails to gain initial entrance (as with most ransomware). It then uses incorrectly configured Remote Desktop services and attempts to steal login credentials for networks using only a single authentication method. Once the attackers gain access, they then identify backups, including Microsoft's built-in shadow copies, and aim to delete or encrypt them, making it more difficult to restore the data. Many ransomware variants are now stealing data before they encrypt it to use against the organisation in an attempt to obtain the ransom amount. It is not yet known how much this has cost Diebold Nixford. Learn more about the last line of defence from BullWall.

A new variant of the information stealing malware family "racoon" has been discovered. These new variants are said to impersonate popular legitimate programs such as Revo Uninstaller. The latest version aims to collect sensitive data, as well as capturing the screen and collecting keystrokes of the users. PowerShell scripts are used to disable Windows Defender and modify various registry key values to remove the admin prompt that would usually be displayed when making changes to the system. These new techniques are forever changing and becoming more complex and the best way to prevent them is to spot the indicators of compromise early with systems such as behavioural analysis defences. Anomali arms security teams with machine learning optimised threat intelligence and identifies hidden threats targeting their environments.

Since last week's report, Adobe has released another set of critical patches for its products, this time including Character Animator, Premier Pro, Audition and Premiere Rush. These patches are said to prevent critical buffer overflow vulnerabilities, which could provide threat actors with the ability to execute remote code onto a target system. With these various critical patches, some vulnerabilities are classified as "out-of-bounds" meaning that disclosing what the patches are fixing could disclose sensitive information for threat actors to further manipulate. Get Complete and Contextual Visibility with Skybox Security.

A new Bluetooth vulnerability has been found that affects all modern devices capable of Bluetooth pairing, including IoT devices, laptops, smartphones, and tablets. The vulnerability (CVE-2020-10135) relates to how devices are pared with Bluetooth using a link key. Threat actors can masquerade as genuine devices and gain access with the link key. Bluetooth chips used by Apple, CSR, Intel, Samsung, and Qualcomm are all vulnerable to these attacks unless patched.

# WEEKLY THREAT REPORT
# June 2nd 2020

A hacker is reportedly selling details of 9 million Zoomcar users for $300 on the dark web. This data includes names, email addresses, passwords, mobile numbers, and IP addresses. The data is said to have been obtained in a 018 data breach. Zoomcar's CEO claims that its data is "absolutely secure" and a breach involving its customers' data is untrue. Learn more about Flashpoint's Intelligence Platform.

Researchers have measured the prevalence of exposed sensitive assets at leading banks, including exposed databases, remote login services and development tools. It is reported that 23% of banks had at least one misconfigured database exposed to the internet, meaning this data could potentially be leaked. 54% of the banks had at least one Remote Desktop Protocol exposed to the internet, 31% had at least one vulnerability to remote code execution and Multiple File Transfer servers with anonymous authentication were discovered. Although banks usually have well established security structures, which are heavily regulated, up to 84% of the exposed assets are likely to fall under IT and security teams' radars and out of the scope of traditional asset management and security tools. It is imperative to understand and have visibility of internet facing assets to manage and mitigate the risks. Get Complete and Contextual Visibility with Skybox Security.

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