October 7-13, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Hackers have breached Volusion, provider of cloud hosted online stores, and used it to delivers malicious JavaScript code and steal payment card details entered by end customers. Volusion has more than 20,000 customers and at least 6,500 of have been actively exploited in this attack. The attack has been attributed to Magecart group 6, previously identified as FIN6 threat actor.
- Data of 8.7 million customers of the Russian internet service provider Beeline, compromised in a 2017 breach, has recently been shared online. The data includes names, addresses, mobile and home phone numbers of Russian residents.
- Personal medical data of about one million people in New Zealand has been exposed in an intrusion to the systems of Tū Ora Compass Health organization. A hacker under the name of Vanda The God has offered to sell the information. Investigations revealed the systems were hacked on four different occasions.
- Attor, a sophisticated cyberespionage platform targeting Russian speaking diplomats and government personas, has been uncovered. Existence of certain modules of Attor suggest it was specifically designed to target custom GSM platforms, often used in diplomatic or intelligence operations.
- A victim of the Muhstik ransomware has hacked the hacker's server and released decryption keys for all Muhstik victims, in addition to a decryption tool. He got his revenge after having payed the ransom, which gave him some insight into the attack infrastructure.
- Three Alabama DCH hospitals which had been hit by a Ryuk ransomware attack early last week have paid the attackers in order to receive decryption keys. DCH announced that encryption process is progressing and expected to gradually allow hospitals to return to normal operations.

  Check Point SandBlast provides protection against this threat

VULNERABILITIES AND PATCHES

- A zero day vulnerability in the Bonjour component of iTunes and iCloud for windows has been exploited to infect Windows computers with ransomware. Apple released a patch to protect from this vulnerability but users who previously used and uninstalled iTunes or iCloud must verify that the Bonjour component, which is not automatically removed, is deleted from their systems.

- In its October Patch Tuesday, Microsoft has released a total of 59 patches of which nine were identified as critical and the rest labeled as important or moderate. None of these vulnerabilities is known to have been actively exploited.

  Check Point IPS blade provides protection against these threats (Microsoft VBScript Remote Code Execution (CVE-2019-1238); Microsoft VBScript Remote Code Execution (CVE-2019-1239); Microsoft Edge Chakra Scripting Engine Memory Corruption (CVE-2019-1366; etc))

- Critical RCE (Remote Code Execution) vulnerability has been detected in four D-Link router models (DIR-655, DIR-866L, DIR-652, and DHP-1565), tracked as CVE-2019-16920. Although two of the models have only been discontinued in 2018 and some are still sold by third party sellers, D-Link announced it shall not issue patches since the products have entered End of Life support.

- Critical shell injection vulnerability in Sophos Cyberoam firewalls (CVE-2019-17059) could allow remote attackers to gain access to targets' internal network without authentication. With more than 96,000 internet facing Cyberoam devices worldwide, Sophos has released a patch but mentioned that not all devices have yet been updated.

THREAT INTELLIGENCE REPORTS

- Report links Magecart Group 4, responsible for attacks on British Airways, Ticketmaster, MyPillow and more, to the Cobalt cybercrime Gang. The Cobalt gang is a Russian group which has been active since 2016 and focused especially on financial institutions and banks, and the report points at the similarity of email name conventions in their activities. Similar to FIN6 Magecart activity (Group 6), this might be part of a trend for financially motivated threat actors to diversify their activity.

- Details regarding Simjacker have been released, including a list of countries in which mobile operators still offer misconfigured SIM cards vulnerable to this attack. The vulnerability allows attackers to track location, send SMS messages and more on targeted mobile devices using specially formatted binary SMS messages. Active exploitations of the vulnerability have been detected in Mexico, Colombia and Peru.