October 12-18, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Researchers and telecom companies have partnered to execute a coordinated attack aimed at disrupting the infamous Trickbot botnet and Malware-as-a-Service. A Court order granted the researchers control over the botnet's infrastructure. However, the botnet was not fully disabled.

- Dickey's Barbeque Restaurant, an American chain with over 400 locations, has suffered a major data breach. More then three million credit card records, collected from over 100 locations, were stolen and offered for sale on an underground forum.

- MuddyWater, a government-linked Iranian APT, has launched a campaign targeting Israeli organizations using a loader dubbed 'PowGoop', impersonating a Google Update DLL. The loader delivers Thanos, a ransomware with wiper capabilities.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Thanos)*

- The Iranian hacking group 'Silent Librarian APT' has been targeting universities worldwide via spear phishing campaigns, in proximity to the start of the new academic year.

- The American bookseller giant Barnes & Noble has issued a warning to its customers, stating that its network was hacked and customer information may have been stolen. Potentially breached data includes transaction data and purchase history, that might be leveraged by attackers for tailored phishing attacks.

- The operators of the Ryuk ransomware have launched a new spear phishing attack wave after a long silent period earlier this year. The attackers used open source tools to compromise admin accounts to gain access to over 90 systems within the network.

  Check Point SandBlast provides protection against this threat

- Hackers have published private home camera footage from victims in Singapore, Thailand, South Korea, and Canada. The hackers claim they have breached over 50,000 home cameras . The videos, ranging in length, were uploaded to adult websites.

VULNERABILITIES AND PATCHES

- Microsoft has released patches for 87 security vulnerabilities in October, 11 of them critical. Among these is the flaw assigned CVE-2020-16898, a potentially wormable remote code execution flaw for Windows 10 and Window Server 2019.

  Check Point IPS provides protection against this threat (Microsoft Windows TCP/IP Remote Code Execution (CVE-2020-16898))

- The UK National Cyber Security Centre urges organizations to patch a recent Microsoft SharePoint flaw assigned CVE-2020-16952. The warning was published due to the large number of exploitations of SharePoint vulnerabilities observed in attacks against UK organizations.

- Adobe has patched a critical flaw assigned CVE-2020-9746 in Flash Player for Windows, Linux, macOS and Chrome OS. The vulnerability could cause an exploitable crash, resulting in remote code execution.

- Juniper Networks has addressed some 40 vulnerabilities, some of them critical, in the Junos OS, the operating system that runs on Juniper's firewalls, and in the Juniper Networks Mist Cloud UI. Some of these flaws could be exploited to allow a remote attacker to bypass authentication security controls.

- SonicWall, a former Dell subsidiary offering content control and security appliances, has issued a patch for a critical vulnerability in its designated operating system, affecting 800,000 appliances. An unskilled attacker can leverage this bug to execute a persistent denial of service attack.

THREAT INTELLIGENCE REPORTS

- Check Point Research has warned against a surge of attacks leveraging the 2020 US presidential elections. 16% of all election-related domains created in September were malicious, and among new domains, those related to the election are 56% more likely to be malicious.

- Researchers have discovered a set of Bluetooth vulnerabilities in the Linux Kernel dubbed 'BleedingTooth', which can be exploited to gain access to sensitive information or execute arbitrary code, when the attacker is within the Bluetooth range.

- Researchers have investigated APT31, a Chinese threat group that has been targeting personal email accounts of staffers on the Biden and Trump presidential campaigns. Recently, the group has been leveraging GitHub and Dropbox for malware hosting and C&C communications.

- The Europol has published its annual strategic threat report, based on its investigations during the past year. The report highlights the challenges privacy enhancements to cryptocurrency transactions and exchanges pose to the security community when it comes to threat actor detection.