Check Point Research
# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The FBI announced operation 'Duck Hunt' dismantling the Qakbot (Qbot) malware operation that is active since at least 2008. Qakbot has been known to infect victims via spam emails with malicious attachments and links, while also serving as a platform for ransomware operators. It has impacted over 700,000 computers worldwide including financial institutions, government contractors and medical device manufacturers.
  Check Point Research is sharing its analysis of the Qakbot malware and its operations over the years.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat* *(Trojan.Wins.Qbot; Trojan.Win.Qbot; Trojan.Downloader.Win.Qbot; Trojan-PSW.Win32.Qakbot; Trojan.WIN32.Qakbot)*

- Major clothing brand Forever 21 has disclosed a data breach that affected almost 540K current and former employees. The leaked data consists of personal information such as names, dates of birth, Social Security numbers, bank account numbers and employees' health plans information.

- American golf gear company Callaway has suffered a data breach that affected the personal information of over 1M of its clients. The exposed information includes account passwords and answers to security questions, as well as names, addresses, emails, phone numbers and order histories. According to the company, no payment card numbers or Social Security numbers were leaked.

- American entertainment giant Paramount Global has confirmed a data breach that potentially resulted in the exposure of clients' and employees' personal information. The leaked data includes names, dates of birth, Social Security numbers, driver's license numbers and passport numbers.

- The University of Michigan has experienced a cyber-attack resulting in the loss of internet access and other business functions across the university. As a precaution, the school took all of its services offline.

- AI-powered coding platform Sourcegraph has revealed a data breach potentially affecting clients' information such as license keys, names and email addresses. Sourcegraph claim that the access gained by the threat actors didn't lead to a modification or copying of private data or code.

- BlackCat (AlphV) ransomware group has taken responsibility for the attack on Forsyth County, Georgia, which happened in last June. The attack resulted in the encryption of over 350GB of data.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat*
  *(Ransomware.Win.BlackCat, Ransomware_Linux_BlackCat)*

# VULNERABILITIES AND PATCHES

- Threat actors are actively exploiting critical RCE vulnerabilities (CVE-2023-36844 to CVE-2023-36847) in Juniper EX switches and SRX firewalls, after a proof-of-concept exploit was released. Successful exploitation will allow unauthenticated attackers to remotely execute code on unpatched devices. Juniper has also warned of a denial-of-service bug (CVE-2023-4481) in Junos OS and Junos OS Evolved.
- A proof-of-concept exploit code has been shared for a critical SSH authentication bypass vulnerability (CVE-2023-34039) in VMware's Aria Operations for Networks analysis tool (patched with the release of version 6.11). Successful exploitation could allow remote attackers to bypass SSH authentication on unpatched appliances and access the tool's command line.
- Netgear has released patches for two high-severity vulnerabilities (CVE-2023-41182 and CVE-2023-41183) affecting one of its router models and its network management software.
- Researchers have identified a critical severity vulnerability (CVE-2023-40004) in All-in-One WP Migration Extensions, a popular WordPress plugin used for website migrations. Successful exploitation could result in an unauthenticated access token manipulation.

# THREAT INTELLIGENCE REPORTS

- Check Point Research has published a technical analysis highlighting the similarities between the Rhadamanthys info stealer and the Hidden Bee coin miner. The similarities include their overall analogous design, implementation, and other custom executable formats.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat* *(InfoStealer.Wins.Rhadamanthys.C/D)*

- Researchers have observed a new campaign suspected as related to FIN8 hacking group, now targeting Citrix NetScaler ADC and Gateway servers while exploiting the critical-severity RCE vulnerability CVE-2023-3519 which had been patched last July.

  *Check Point IPS provides protection against this threat* *(Citrix NetScaler Remote Code Execution (CVE-2023-3519))*

- Researchers detail post remediation efforts by UNC4841, a threat actor suspected as a Chinese hacker group, which targeted US government email servers using a zero-day vulnerability in Barracuda Email Security Gateway (ESG) appliances. The attacks resulted in the compromise of email accounts and the theft of sensitive data.

  *Check Point IPS and Threat Emulation provide protection against this threat* *(Barracuda Email Security Gateway Command Injection (CVE-2023-2868); Trojan.Wins.Saltwater; Exploit.Wins.CVE_2023_2868)*