October 2 - 8, 2023

Check Point Research

# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The American Rock County Public Health Department, which serves more than 160K people across Wisconsin area, has been a victim of a ransomware attack that forced officials to take some systems offline. Cuba ransomware gang has claimed responsibility for the attack, claiming to have stolen financial documents, tax information and more.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat*
  *(Ransomware.Win.Cuba, Ransomware.Wins.Cuba.ta.*)*

- The American genetic testing company 23andMe has disclosed an attack that exposed more than 1.3M clients' records on dark web. The leaked data includes personal information belongs to users of Chinese and Ashkenazi heritage, consists of full names, profile and account ID numbers, profile photos, gender, date of birth, genetic ancestry results, and geographical location.

- The British mobile virtual network operator (MVNO) company Lyca Mobile has been a victim of a cyber-attack that resulted in a widespread disruption of millions of its customers. The threat actors have possibly compromised some of the clients' passwords, and the company has shut down the compromised systems as a precaution.

- The District of Columbia Board of Elections (DCBOE) has experienced a cyber-attack that occurred as a result of a breach into the web server of DataNet, the hosting provider of Washington D.C.'s election authority. The RansomedVC ransomware gang has claimed responsibility for the attack, claiming to have stolen more than 600K records database which consists of US voters' sensitive information. The leaked data allegedly includes names, emails, phone numbers, registration IDs, voter IDs, Social Security numbers, drivers' license numbers, and more.

- The American medical center Mt. Graham Regional Medical Center (MGRMC) has confirmed a cyber-attack that affected its communication and information systems. According to officials, the attack has had limited impact on an unconfirmed amount of patients' personal data.

- Florida's First Judicial Circuit has disclosed a cyber-attack that affected court operations across the Circuit, impacting courts in Escambia, Okaloosa, Santa Rosa, and Walton counties. Officials did not respond to requests for comment about whether it was a ransomware attack and no group has yet claimed responsibility for the attack.

## VULNERABILITIES AND PATCHES

- GPU manufacturers Arm and Qualcomm have published security advisories addressing several critical vulnerabilities affected their GPU products. The vulnerabilities were reported to the companies by Google, who has detected their exploitation in the wild by commercial spyware companies.
- Microsoft has shared an advisory addressing the media library heap buffer overflow vulnerabilities (CVE-2023-4863 and CVE-2023-5217) that were being actively exploited in the wild. The advisory refers to Microsoft Edge, Teams, and Skype.
- Atlassian has released a security advisory addressing a critical remote privilege escalation vulnerability (CVE-2023-22515) in Confluence Data Center and Server. The vulnerability is actively being exploited in the wild.

## THREAT INTELLIGENCE REPORTS

- Check Point Research has published its monthly malware report for September 2023, marking a new stealth large-scale phishing campaign, designed to discreetly deliver the Remcos RAT, targeting over 40 organizations in Colombia. In parallel, Formbook took first place as the most prevalent malware following the collapse of Qbot, and Education remains the most targeted industry.
- Researchers are sharing their analysis of LostTrust - a new multi-extortion ransomware family that shares traits with the SFile and Mindware ransomware families. These similarities include the use of a specific encryption algorithm, the use of similar ransom notes and of similar command-and-control infrastructure.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat* *(Ransomware.Win.Rank; Ransomware.Win.RMShadowCopy.A, Ransomware.Win.FilesMovedOrOverwrites.A)*
- Researchers report on a suspected Chinese-speaking APT group that targeted South American country Guyana's government entities during February 2023, as part of a campaign dubbed “Operation Jacana”. The attack used spear-phishing techniques to eventually deliver DinodasRAT and Korplug malware.

  *Check Point Threat Emulation provides protection against this threat* *(Trojan.Wins.Korplug.ta, Trojan.Wins.Korplug.A)*
- Researchers released a report on the Qbot threat group which now delivers Knight Ransomware and the Remcos RAT, despite the group's supposed takedown. The research suggest the group’s C2 infrastructure was the only part taken down in the operation, while its distribution network was not impacted.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat* *(Ransomware.Wins.Knight.A, RAT.Win.Remcos)*