Check Point SOFTWARE TECHNOLOGIES LTD.

May 31 – June 06, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has identified a new cyber espionage weapon called SharpPanda being used by a Chinese threat group, in an ongoing surveillance operation targeting a Southeast Asian government. The attack starts with spear phishing emails leveraging old Microsoft vulnerabilities.

  Check Point Threat Emulation provides protection against this threat

- JBS, the United States-based meat processing giant, has been hit by a ransomware attack affecting its North American and Australian operations. The FBI has attributed the attack to the REvil ransomware.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win32.Revil)

- University of Florida Health has suffered a ransomware attack forcing two hospitals to operate by pen and paper after shutting down a portion of their IT network.

  Check Point Harmony Endpoint provides protection against this threat

- Japanese multinational conglomerate Fujifilm has been hit by a ransomware attack forcing the company to take down portions of its network worldwide. According to some reports, Fujifilm had been infected with Qbot Trojan, which might have pulled the ransomware payload.

  Check Point Harmony Endpoint, Threat Emulation and Anti-Bot provide protection against this threat (Trojan-Downloader.WIN32.Qbot)

- Nucleus Software, an Indian company providing financial software to banks and retail stores, has been hit by new ransomware named "BlackCocaine". The attack crippled some of the company's internal network and encrypted sensitive business information.

  Check Point Harmony Endpoint provides protection against this threat

- Mobile County in Alabama, US, and Comune di Porto Sant'Elpidio, Italy, are the latest victims of the Grief ransomware group. The attack on Mobile County servers exposed nearly 7GB of government documents.

  Check Point Harmony Endpoint provides protection against this threat

- AMT Games mobile game Battle for the Galaxy has suffered a data leak affecting 6 million users. Researchers found over 1 terabyte of unencrypted user data including emails and purchase information on an unprotected server.
- The Tokyo Olympics organizing committee has suffered a data breach leaking the personal information of 170 people from 90 organizations involved in hosting the Olympics. The breach was sourced to a cyber-attack against a Japanese government contractor's data-sharing tool.

VULNERABILITIES AND PATCHES

- Researchers have disclosed ten critical vulnerabilities impacting CODESYS automation software that could be exploited for remote code execution on programmable logic industrial controllers and in denial of service attacks (CVE-2021-30186 – CVE-2021-30195).
- Apple has released a software update for AirTags following concerns that they could be used to monitor users' real-time location.
- Cisco has fixed multiple vulnerabilities including high-severity flaws in Webex player, SD-WAN software, and ASR 5000 series software.
- A cross-site-scripting (XSS) vulnerability has been found in a popular HTML editor used by over 30,000 websites. The security flaw (CVE-2021-28114) is found in the way HTML sanitizing is performed.
- Researchers have found multiple flaws in the Realtek RTL8170C Wi-Fi module that could be exploited to elevate privileges and hijack wireless communications.

THREAT INTELLIGENCE REPORTS

- Threat actors are actively scanning for internet-exposed VMware vCenter servers vulnerable to the recently-patched critical remote code execution vulnerability impacting all vCenter deployments (CVE-2021-21985).
- A critical zero-day vulnerability (CVE-2021-24370) in Fancy Product Designer, a WordPress plugin installed on over 17,000 sites, has been actively exploited to upload malware onto vulnerable sites.
- Researchers have discovered new features in the Necro Python-based bot, targeting Linux and Windows machines. Necro, first revealed by Check Point Research in a campaign dubbed "FreakOut", added exploits for vulnerabilities in SMB protocol and in VMware vSphere, SCO OpenServer, and the Vesta Control Panel.

  Check Point IPS and Anti-Bot provide protection against this threat
- New Phishing campaign is abusing the recent ransomware attack on the colonial pipeline with well-crafted emails tailored as an urgent notification from their helpdesk to download and install a fake system update that would defend against the latest ransomware strain. The payload is in fact Cobalt Strike.