Check Point
SOFTWARE TECHNOLOGIES LTD.

Mar 1-7, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- SITA, a communications and IT vendor for 90 percent of the world's airlines, has been breached in a massive supply-chain attack, compromising frequent-flyer data across many carriers such as United, Singapore Airlines, Lufthansa, and more.
- Spirit Airlines has suffered a data breach by "Nefilim" ransomware. A first batch of customer data has been released on the dark web, exposing over 40GB of data including credit card numbers and personal information.

  Check Point SandBlast Agent provides protection against this threat
- Maza, an elite Russian forum where reputable cybercriminals can connect to collaborate in malicious operations, has been under attack, leaving members worried that their identities would be revealed.
- JFC International, a major wholesaler and distributor of Asian food products in the US, has been hit by a ransomware attack disrupting its IT systems.

  Check Point SandBlast Agent provides protection against this threat
- CompuCom, US managed service provider, has been hit by malware, potentially DarkSide ransomware. The attack led to service outages and to customers disconnecting from the MSP's network to prevent the spread of malware.

  Check Point SandBlast Agent provides protection against this threat
- Williams Formula One team has suffered a breach to their augmented reality mobile app, meant to be used in to launch their new car model, forcing them to remove it from Google Play and Apple App Store.
- Qualys, a Cybersecurity firm, was the latest victim to have suffered a data breach published by Clop ransomware gang after a zero-day vulnerability in Accellion FTA server was exploited to steal hosted files.

VULNERABILITIES AND PATCHES

- Microsoft has released an emergency patch for Exchange email server vulnerabilities recently exploited in the wild by Hafnium, a Chinese state-sponsored hacking group. The group has reportedly hacked over 30,000 organizations, trying to steal their corporate emails.

  Check Point IPS and SandBlast Agent provide protection against this threat (relevant protections)

- Cisco has warned about a vulnerability (CVE-2021-1285) in its Snort detection engine, which exposes several of its products to denial-of-service (DoS) attacks.
- Samsung has released a security update addressing 37 vulnerabilities, including a patch for a critical flaw in the system component tracked as CVE-2021-0397.
- Researchers have found two flaws in Apple's Find My feature. The flaws in the crowdsourced Bluetooth location tracking system can lead to a location correlation attack and unauthorized access to the location history of the past seven days.

THREAT INTELLIGENCE REPORTS

- New malware families used in the SolarWinds attack, suspected to be affiliated with a Russian APT group, have been revealed. "GoldMax", "Sibot" and "GoldFinder" are executed in late stages of the attack, after lateral movement from the SolarWinds server, and use reputable domains for their C2 communication.

  Check Point Anti-Bot provides protection against this threat (Backdoor.WIN32.SUNSHUTTLE)

- Researchers have spotted a new ransomware called "Hog". The ransomware encrypts users' devices and only decrypts them if they join the developers' Discord server.

  Check Point SandBlast Agent provides protection against this threat

- Researches have reported a campaign by Ursnif banking Trojan, targeting at least 100 banks in Italy. The operators behind the attack have successfully stolen financial data and credentials.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan.WIN32.Ursnif.)*

- The US Financial Industry Regulatory Authority (FINRA) has issued a regulatory notice warning US brokerage firms and brokers of an ongoing phishing campaign using fake compliance audit alerts to harvest information.