May 3-9, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Ransomware attack has shut down the routine operations of Colonial Pipeline, which carries 45% of the fuel consumed in the US East Coast, including diesel, petrol and jet fuel. The alleged Russian DarkSide ransomware criminal group, which operates in an as-a-service model, is speculated to be behind this attack.
- Belnet, a prominent ISP in Belgium providing internet services for much of the country's public sector, has suffered a massive DDoS attack that deprived 200 government, public and education entities from internet access, among them the parliament.
- Ryuk ransomware has been deployed in an attack against a biomolecular institute in Europe involved in COVID-19 research. The incident has led to a week's data loss. The attack was made possible by a student who downloaded an unlicensed software.

  Check Point Check Point SandBlast and SandBlast Agent provide protection against this threat (Ransomware.Win32.Ryuk)
- US Intelligence officials have reported that Chinese state-sponsored threat actors have leveraged an exploit dubbed 'Chaos' for iPhone devices in an espionage campaign that targets the Uyghur minority in China. The exploit has been developed by a researcher from Qihoo 360 in 2018 as part of a Chinese hackathon.
- Cyber criminals accessed the identifying information of about 10,000 people through the email accounts of 12 Brevard County School Board employees. Email accounts contained information from students and adults, including some social security numbers.
- Scripps Health, a healthcare provider operating 5 hospitals in San Diego and several clinics, has suffered a ransomware attack that caused disruption to their IT environment. Staff and patients could not access records and emails for almost a week.

VULNERABILITIES AND PATCHES

- Check Point Research found a security vulnerability in Qualcomm's mobile station modem (MSM), the chip responsible for cellular communication in nearly 40% of the world's phones. If exploited, the vulnerability would have allowed an attacker to use Android OS itself as an entry point to inject malicious and invisible code into phones, granting them access to SMS messages and audio of phone conversations.
- Pulse Secure has released a security update addressing a critical flaw affecting the Pulse Connect Secure appliance. The vulnerability, assigned CVE-2021-22893, allows a remote unauthenticated attacker to execute arbitrary code.
- Researchers have uncovered a vulnerability in a DNS resolver software that can be leveraged to launch DDoS attacks against authoritative DNS servers. The issue, dubbed 'TsuNAME', has been patched by Google and Cisco for their DNS servers.

THREAT INTELLIGENCE REPORTS

- Researchers have exposed documents belonging to a strategic unit in China's People's Liberation Army (PLA), indicating that the unit has attempted to purchase English-language Antivirus software from major security providers in the US, Europe and Russia, possibly for vulnerability and exploit research.
- CISA has issued a report reviewing the recent FiveHands ransomware campaign, that leveraged a zero-day vulnerability in a VPN product and a custom RAT called 'SombRAT', used to download and execute further payloads.

  Check Point Anti-Virus and Anti-Bot provide protection against these threats *(Ransomware.Win32.Fivehands; SombRAT)*
- Three new malware families have been deployed as part of a spear-phishing campaign executed by the financially motivated cybercrime group referred to as 'UNC2529'. Among them is a backdoor dubbed 'DoubleBack', which doesn't rely on hardcoded functionalities and is thus configured per target.
- The Cyber Threat Alliance (CTA) has released an up-to-date security assessment of the cyber threats to the upcoming Tokyo Olympics. Researchers believe that related entities and vendors will be heavily targeted by ransomware, and that supply-chain attacks similar to the SolarWinds incident might be observed.
- Researchers have reviewed the current threat landscape of attacks bypassing Multi-Factor Authentication (MFA), including a recent zero-day vulnerability in Pulse Secure VPN, Microsoft Exchange 'ProxyLogon' flaws and the SolarWinds supply-chain attack.
- Evil Corp, a Russian cybercrime group known for the distribution of the Dridex banker and Locky ransomware, is now suspected to be operating on behalf of a Russian intelligence agency, collecting sensitive information requested by government entities and disguising its agenda with ransomware.