# TOP ATTACKS AND BREACHES

- The Ukrainian IT army has disrupted Russia's alcohol distribution by performing DDoS attacks to limit access to a portal called State Automated Alcohol Accounting Information System (EGAIS) used by the Russian government.

- Pro-Ukrainian actors have used compromised Docker Engine honeypots to execute two Docker images downloaded over 150,000 times to launch a denial-of-service (DoS) attack. The attack targets Russian and Belarusian websites included in the Ukraine government-backed Ukraine IT Army target list.

- Researchers have found a Chinese affiliated hacking group linked to China's People's Liberation Army Strategic Support Force (PLA SSF) that has been attacking several Russian governmental organizations and companies in the defense industry.

- A new APT group tracked UNC3524 has breached corporate email accounts to gain financial information through content related to corporate development, mergers and acquisitions, large corporate transactions, and IT security. UNC3524 appears to be a sophisticated threat actor, remaining undetected in victims' environments, likely to perform cyber espionage campaigns.

- Chinese state-sponsored APT actor Winnti (aka APT41, BARIUM, and Blackfly) has operated a campaign of intellectual property asset theft such as patents, copyrights, and trademarks. The group has been performing these cyber-espionage campaigns since 2019.

  *Check Point Threat Emulation provides protection against this threat* *(Backdoor.Win32.Winnti)*

- The National Health System (NHS) in the UK has been a victim of a phishing campaigns targeting email accounts since at least April 2022. More than a thousand phishing messages were sent from two NHS IP addresses, delivered from hijacked email accounts belonging to 139 employees in England and Scotland.

- Chinese APT actor Moshen Dragon has been targeting Central-Asia telecommunication service providers in Central-Asia in a new cyber-espionage campaign. Threat actors abused security products for DLL sideloading of five ShadowPad and PlugX malware variants.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against these threats* *(RAT.Win.PlugX; Trojan.Win32.PlugX; Backdoor.WIN32.Plugx; RAT.Wins.ShadowPad; Backdoor.Win32.Shadowpad)*

# VULNERABILITIES AND PATCHES

- Google has released an Android update to patch an actively exploited Linux kernel vulnerability, CVE-2021-22600, which could lead to memory corruption and eventually DoS attacks or arbitrary code execution.
- F5 has issued an alert concerning a flaw in its BIG-IP networking devices and modules, that may allow unauthenticated attackers with network access to perform remote code execution attacks. Tracked CVE-2022-1388, it could allow undisclosed requests to bypass iControl REST authentication.
- Cisco has patched three security flaws found in the Enterprise NFV Infrastructure Software. Tracked CVE-2022-20777, CVE-2022-20779, and CVE-2022-20780, the vulnerabilities could allow an attacker to send an API call from a VM and have it executed on the NFVIS host with root-level privileges, leading to full compromise of the host.
- An unpatched flaw in the domain name system (DNS) component of a popular C standard library in IoT products has been unveiled. Tracked CVE-2022-30295, it may allow attackers to perform DNS poisoning attacks against the targeted device.

# THREAT INTELLIGENCE REPORTS

- Security researcher has found exploits using vulnerabilities in multiple strains of ransomware such as Conti, REvil and LockBit. These vulnerabilities could be exploited to stop file encryption.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against these threats* *((Ransomware.Win32.Conti); (Ransomware.Win.Revil.ja; Ransomware.Win32.REvil.TC; Trojan.Win32.Sodinokibi); (Ransomware.Win.Lockbit Ransomware.Win32.LockBit. lockbit.TC))*
- The US Department of State offers $15 million reward for information leading to Conti ransomware gang.
- The US Department of Treasury has issued sanctions on a cryptocurrency mixer Blender.io, a service used by North Korean hacking group Lazarus to obfuscate the origin and destination of bitcoin transactions. The Lazarus group was accused of laundering illicit proceeds, stealing hundreds of millions of dollars' worth of cryptocurrency tied to popular online game Axie Infinity.

  *Check Point Threat Emulation and Harmony Endpoint provide protection against this threat* *(APT.Win.Lazarus)*
- The FBI warns of Business Email Compromise (BEC) scams which have surpassed $43 billion globally since 2016.