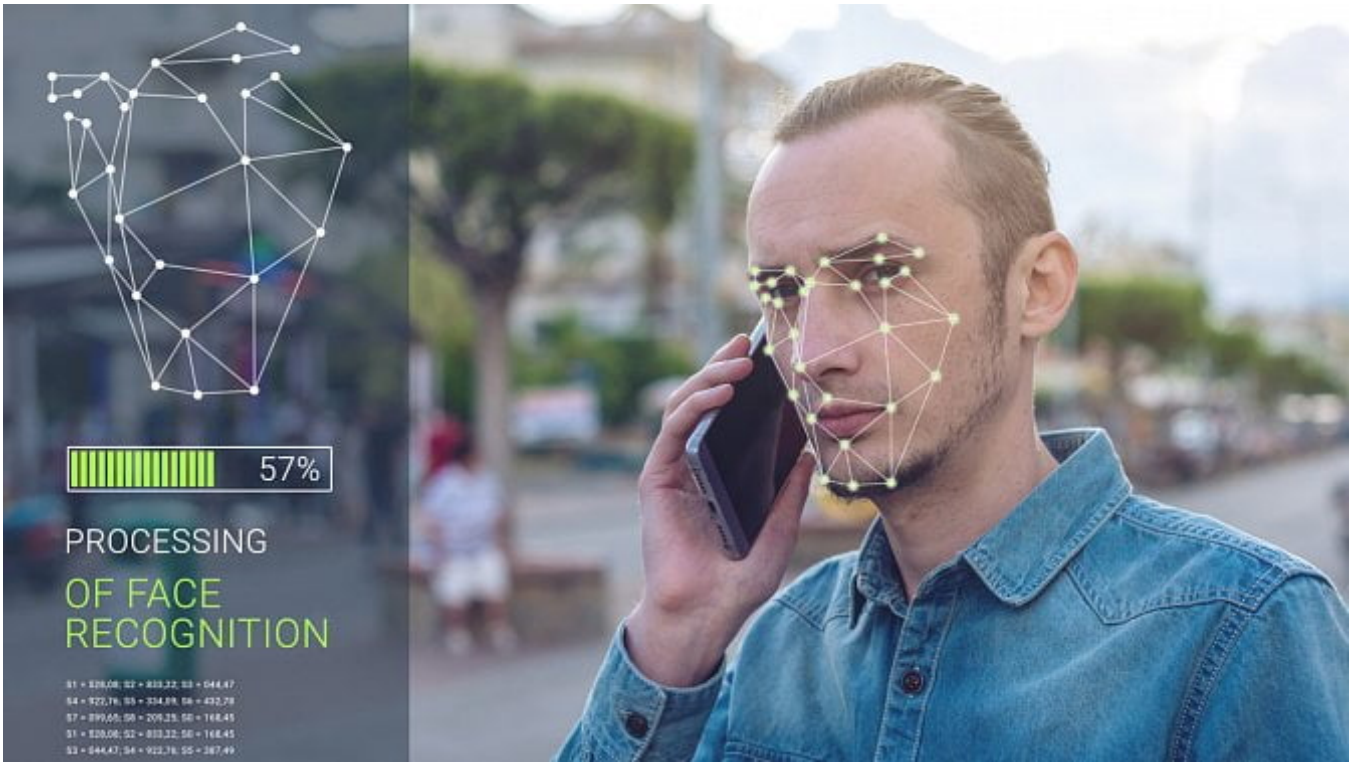
Postřehy z bezpečnosti: přesměrujte svůj deepfake



Autor: Depositphotos
Seznámíme vás s asijským gangem, který přesměruje přes telefon oběti falešný videozáznam jejího obličeje. Dále vás nalákáme třeba na čtení o digitálním bezpečí dětí nebo evropské kyberbezpečnostní certifikaci.

Deepfakes pro obcházení ověřování obličeje

Ani tento týden se nám deepfake nevyhne. Skupina hackerů známá pod jménem GoldFactory vyvinula malware GoldPickaxe, který dokáže zaměnit obličej oběti za obličej útočníka, což je poté využito pro ověření identity v mobilním bankovnictví. Jako obyčejně začínají tyto útoky sociálním inženýrstvím, kdy po navázání kontaktu útočník svou oběť přiměje k instalaci malwaru do telefonu.

Útočníci se vydávají za bankovní a vládní úředníky. Součástí instalace je pro účely ověření totožnosti a zabezpečení pořízení videa obličeje, které později slouží jako data pro tvorbu deepfake videa. Malware GoldPickaxe funguje jako proxy server a během přihlašování do internetového bankovnictví je veškerá datová komunikace směrována přes IP adresu oběti, což ještě více znesnadňuje odhalení útoku.

GoldFactory má na svědomí i podobný malware, nazvaný GoldDigger, a GoldPickaxe je jeho přímý nástupce. Jeho vylepšení se skrývá právě ve využití tvorby falešného videa pro ověření identity.

Poprvé se GoldDigger objevil v červnu 2023 a stále je v oběhu, a to hlavně mezi občany v oblasti Thajska a Vietnamu. Následně se začala objevovat i jeho vylepšení s názvem GoldDiggerPlus (září 2023) a GoldKefu, sloužící jako klon populárních chatovacích aplikací pro komunikaci s falešnými bankovními úředníky.

GoldFactory je všestranná, dobře organizovaná skupina využívající nejrůznější techniky sociálního inženýrství a zároveň disponující vlastním vývojovým týmem pro tvorbu aplikací, jako je GoldDigger a GoldPickaxe. Gang působí v Asii, nicméně podobné případy se mohou objevit i v jiných částech světa.

Na co by si měli dát rodiče pozor v roce 2024?

V této době moderních technologií je věk, ve kterém se děti seznamují s digitálním světem a technologiemi, stále nižší. Tento digitální zážitek však může být poškozen potenciálními riziky číhajícími online. Jak technologie postupují, vyvíjejí se také nové taktiky a strategie používané kyberzločinci k zacílené na mladé uživatele internetu a jejich zneužívání.

Proto je klíčové, aby rodiče zůstali informováni o nejnovějších kybernetických hrozbách zaměřených na děti, aby je mohli lépe chránit před potenciálním poškozením. V tomto příspěvku zkoumáme některé z klíčových trendů kybernetické bezpečnosti, kterých by si rodiče měli být vědomi, a poskytujeme tipy, jak zabezpečit online aktivity svých dětí.

Evropské certifikace ICT produktů

Evropská komise udělala v oblasti kybernetické bezpečnosti významný krok vpřed, když 31. ledna 2024 přijala prováděcí nařízení k prvnímu dobrovolnému certifikačnímu schématu založenému na Common kritériích (dále jen „EUCC“). Toto schéma, které bylo přijato na základě legislativního rámce stanoveného aktem o kybernetické bezpečnosti, představuje zásadní průlom v zabezpečení produktů informačních a komunikačních technologií (ICT produktů) v rámci Evropské unie.

Prováděcí nařízení pak bylo dne 7. února 2024 zveřejněno v Úředním věstníku Evropské unie a vstoupí v platnost dvacátým dnem po tomto vyhlášení, tedy 27. února 2024. Samotné certifikace mohou být udělovány o rok později, tedy od 27. února 2025. V tomto období mají subjekty posuzující shodu prostor pro získání akreditace (popř. autorizace) a výrobci mají prostor k přípravě výrobků tak, aby splnily podmínky pro certifikaci.

Automatizace útoků na VMware ESXi

RansomHouse je RaaS působící škodu převážně v USA a západní Evropě. Podle zprávy společnosti Trellix se jedná o skupinu s vyspělými TTP využívající např. CDN pro exfiltraci dat nebo Tor pro komunikaci s napadenými oběťmi. Používá vlastní ransomware zvaný Mario ESXi založený na uniklém kódu Babuk. Vydělává pomocí dvojitého vydírání a část získaných prostředků se zřejmě rozhodla reinvestovat do nástroje přezdívaného MrAgent. Ten je určen pro běh na hypervizorech VMware ESXi (a Windows) a jeho hlavním účelem je automatizovat nákazu ransomwarem a sledovat ji.

Ve zkratce se dá činnost tohoto nástroje popsat takto: po spuštění sestaví jednoznačné ID oběti ve tvaru hostname-MAC, získá lokální IP adresu napadeného stroje a vypne mu firewall. Pak začne „volat domů“ na své řídicí servery, od kterých dostává další pokyny. Výměnu zpráv a udržování konfigurace a aktuálního stavu formátuje pomocí JSON. Jakmile dostane pokyn „Exec“, začne se šifrováním. Předtím ještě volitelně změní heslo roota a vypne vzdálenou správu vCenter.

Jde o znepokojující zprávu, zvláště ve světle ukončení bezplatné verze ESXi, která se leckde používá v produkčním prostředí a která pravděpodobně na některých z těch míst i zastará (pokud se tak už nestalo).

ESET eskalace privilegií

ESET opravil chybu umožňující eskalaci privilegií. Podle analýzy může uživatel s běžnými přístupovými právy mazat soubory se systémovými oprávněními. Chyba se týká antiviru a systémů zabezpečujících koncové stanice, servery Windows a Azure. Záplaty byly vydány pro produkty NOD32 Antivirus, Internet Security, Smart Security Premium, Security Ultimate, Endpoint Antivirus and Endpoint Security for Windows, Server Security for Windows Server, Mail Security for Exchange Server and IBM Domino a ESET Security for SharePoint Server. Chybě bylo přiřazeno označení CVE-2024–0353 a ESET doporučuje okamžitou aktualizaci.

Starý Linux a nové bezpečnostní riziko u Ivanti Pulse Secure

Reverse engineering firmwaru běžícího na zařízeních Ivanti Pulse Secure odhalil řadu zranitelností. Bylo zjištěno, že Pulse Secure běží na 11 let staré verzi Linuxu, která není podporována od listopadu 2020. Útočníci kvůli tomu můžou zneužívat řady bezpečnostních chyb objevených v branách Ivanti Connect Secure, Policy Secure a ZTA k doručení široké škály malwaru, a to včetně webových shellů či různých backdoorů.

Mezi nedávné aktivně zneužívané zranitelnosti patří například CVE-2023–46805, CVE-2024–21887 a CVE-2024–21893. Minulý týden Ivanti také zveřejnil další chybu ve softwaru (CVE-2024–22024), která by mohla umožnit útočníkům přístup k jinak omezeným prostředkům bez jakéhokoli ověření. Bezpečnostní pracovníci také upozorňují, že od 9. února 2024 po zveřejnění proof-of-concept (PoC) společností watchTowe se zvýšila skenovací aktivita zaměřená na CVE-2024–22024.

Ve zkratce

- NÚKIB nechce mít v mistrovství hokej
- Hrozba aktivních účtů bývalých zaměstnanců
- QBot skrytý pod falešným instalátorem Adobe
- Randomware Rhysida rozšifrován
- Pozor na command-not-found v Ubuntu

Pro pobavení

Autor: Programming Humour

O seriálu

Tento seriál vychází střídavě za pomoci pracovníků Národního bezpečnostního týmu CSIRT.CZ provozovaného sdružením CZ.NIC a bezpečnostního týmu CESNET-CERTS sdružení CESNET, bezpečnostního týmu CDT-CERT provozovaného společností ČD Telematika a bezpečnostních specialistů Jana Kopřivy ze společnosti Nettles Consulting a Moniky Kutějové ze sdružení TheCyberValkyries. Více o seriálu…

Vstoupit do diskuse (1 názor)

Autor článku

CSIRT.CZ

Národní bezpečnostní tým CSIRT.CZ je provozován sdružením CZ.NIC. Podílí se především na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice.

Vsichni pisou jak zabezpecit to ci ono aby dite neprislo k uhone. Me by zajimalo, jak nechat deti se kontrolovane spalit. Stejne jako deti ucim, ze trouba je horka, tim ze jim ruku kontrolovane priblizim k troube, tak bych to chtel udelat s mobily/internetem/pocitaci. Synove dostali mobil. Bezhlave tam Instaluji jednu hru za druhou. Porad doufam, ze si do mobilu natahnou nejaky malware a budou jim, cojavim, skakat reklamy pres celou obrazovku, cokoliv. Ale ono furt nic. Ted je to jeste dobre,…

K>