V SOUVISLOSTI SE SVĚTOVOU VÝSTAVOU EXPO 2025 V JAPONSKÉ ÓSACE LZE OČEKÁVAT ZVÝŠENÝ ZÁJEM AKTÉRŮ KYBERNETICKÝCH HROZEB. PŘÍKLADEM JE PHISHINGOVÁ KAMPAŇ ZNEUŽÍVAJÍCÍ TEMATIKU EXPO 2025. NÚKIB DOPORUČUJE ZVÝŠENOU OBEZŘETNOST

SHRNUTÍ

- **Japonské město Ósaka letos od 13. dubna do 13. října hostí Expo 2025. Vzhledem k mezinárodnímu charakteru a vysoké exponovanosti akce lze očekávat zvýšený zájem řady kybernetických aktérů. Hrozby mohou cílit na pozvané účastníky, návštěvníky, zájmové osoby či organizace.**
- **Významné akce obecně bývají často cílem celé řady zejména státem sponzorovaných aktérů, orientovaných zejména na kybernetickou špionáž. V souvislosti s Expo 2025 již byly zaznamenány případy útoků aktéra spojovaného s Čínskou lidovou republikou. Jedním z cílů byla diplomatická organizace ve střední Evropě.**
- **NÚKIB doporučuje v souvislosti s výstavou Expo 2025 zachovávat zvýšenou obezřetnost. Při e-mailové komunikaci je vhodné důkladně ověřovat e-mailovou adresu odesílatele a neotevírat podezřelé odkazy či soubory. V případě jakéhokoli podezření neváhejte kontaktovat bezpečnostní tým vaší instituce, případně můžete škodlivé či podezřelé e-maily související s Expo 2025 hlásit přímo NÚKIB na adrese cert.incident@nukib.gov.cz.**
- **Součástí tohoto přehledu je také sada obecných kyberbezpečnostních doporučení pro účastníky Expo 2025, jejichž cílem je omezit potenciální kybernetická rizika spojená s návštěvou této akce.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací, které jsou veřejně dostupné, byly získány v rámci činnosti NÚKIB či pocházejí od partnerů.

Od 13. dubna do 13. října 2025 probíhá v japonské Ósace světová výstava Expo 2025. **S ohledem na význam akce, potenciální účastníky i atraktivní témata zahrnující využití inovativních technologií lze očekávat zvýšený zájem řady kybernetických aktérů. Hrozby mohou cílit jak na pozvané účastníky, potenciální návštěvníky, tak na jiné zájmové osoby či organizace.**

V průběhu konání Expo 2025 lze očekávat vyšší aktivitu útočníků, a proto je důležitá zvýšená obezřetnost v případě veškeré komunikace spojené s touto výstavou.

Významné akce obecně bývají často cílem celé řady zejména státem sponzorovaných aktérů, obvykle orientovaných na kybernetickou špionáž. **V souvislosti s Expo 2025 byly zaznamenány případy útoků aktéra spojovaného s Čínskou lidovou republikou. Podle společnosti ESET skupina MirrorFace cílila již v srpnu 2024, tedy téměř tři čtvrtě roku před začátkem výstavy, na nejmenovanou středoevropskou diplomatickou organizaci.** Jednalo se o spear-phishing zneužívající právě tematiku světové výstavy (více ke kampani viz Příloha 1). Dle společnosti ESET šlo o první případ, kdy daný aktér mířil na evropský subjekt. [1] **Tato skutečnost ukazuje, že letošní světová výstava může vyvolat zájem i těch aktérů, kteří se doposud soustředili na jiné cíle.** Pozornost útočníků mohou přitáhnout zejména technologická témata a organizace působící v sektorech s nimi spojených.

Nejedná se navíc o zcela ojedinělý případ, kdy aktéři kybernetických hrozeb využívali významné akce za účelem provádění phishingových kampaní. Z poslední doby lze zmínit například mezinárodní bezpečnostní konferenci IISS Prague Defence Summit probíhající loni v září. Útočníci v rámci kampaně zaměřené na účastníky konference využívali mimo jiné reálných pozvánek ke zvýšení důvěryhodnosti svých phishingových e-mailů.[2]

Na nynější světovou výstavu může být navázána také řada podvodné či jiné kyberkriminální činnosti. Samotní organizátoři varovali před falešnými účty na sociální síti X, které se vydávají za oficiální účet Expo 2025 a lákají uživatele na různé benefity. V následné komunikaci mohou útočníci oběť navést na škodlivé stránky, kde mohou usilovat o získání citlivých informací či o stažení škodlivých souborů do zařízení oběti.[3] **Společnost Trend Micro pak v březnu 2025 potvrdila existenci falešných webových stránek imitujících oficiální web světové výstavy v Ósace.** Falešné stránky měly pravděpodobně sloužit ke krádeži osobních údajů uživatelů. Podle společnosti také došlo k několika pokusům o získání doménových jmen, která jsou podobná těm, jež používá oficiální stránka výstavy Expo (https://www.expo2025.or.jp/). **Trend Micro také upozorňuje, že v blízké budoucnosti se mohou objevit další falešné stránky.**[4] **NÚKIB proto doporučuje pečlivě kontrolovat a ověřovat správnost a legitimitu oficiálních účtů a webových stránek před jakoukoli interakcí.**

Potenciální rizika mohou být spojená také se samotnou návštěvou, resp. účastí na dané akci. Výstavy Expo 2025 se bude účastnit celá řada českých i zahraničních entit s unikátním know-how. Útočníci mohou cílit na zařízení účastníků za účelem okamžité exfiltrace citlivých informací nebo za účelem využití zařízení jako vstupního bodu pro následnou kompromitaci organizace, v jejímž rámci daná osoba působí. **Z tohoto důvodu NÚKIB sdílí obecná doporučení s cílem omezit potenciální kybernetická rizika, která mohou být spojena s návštěvou světové výstavy Expo 2025 (viz Příloha 1).**

Příloha 1: Základní kyberbezpečnostní doporučení v souvislosti s EXPO 2025

Dbejte zvýšené pozornosti před phishingem

Vzhledem k povaze a významnosti akce lze předpokládat škodlivé aktivity v kyberprostoru, jež mohou směřovat mimo jiné vůči účastníkům akce. V minulosti byly obdobné události zneužívány k zasílání phishingových zpráv s cílem získat citlivé informace. **Před akcí i v jejím průběhu je proto třeba dbát zvýšené opatrnosti při stahování dokumentů či otevírání příloh v rámci internetové komunikace. Zejména je důležité dbát obezřetnosti při otevírání příloh či odkazů od cizích odesílatelů.** Typicky tyto útoky využívají legitimně vypadající oficiální dokumenty, jako jsou pozvánky na recepce, programy jednání či naopak zápisy a jiné výstupy podobných akcí. Dále je vhodné vždy zkontrolovat správnost e-mailové adresy odesílatele. V některých případech mohou útočníci zneužívat tzv. typo squatting, tj. obtížně rozeznatelné překlepy v e-mailové či webové adrese ke zneužití identity např. kolegy, nadřízeného nebo legitimního webu.

Minimalizujte využívání veřejných Wi-Fi sítí

Veřejné sítě na letištích, v hotelech či různých restauracích a na dalších veřejných místech velmi často nedisponují dostatečným zabezpečením. Útočníkům tím poskytují potenciální příležitost sledovat vaši komunikaci a zachytávat tak kromě potenciálně citlivých informací například také přihlašovací údaje a hesla. **Je tudíž doporučeno, pokud možno tyto sítě využívat pouze okrajově, případně se skrze ně alespoň nepřihlašovat například do internetového bankovnictví nebo dalších obdobných služeb a nesdělovat skrze ně citlivé informace.**

Pokud přece jen potřebujete připojení skrze takovou Wi-Fi, využívejte VPN služby. Ty zajišťují šifrování provozu a vytváří „bezpečnější tunel" pro vaše internetové aktivity.

Pokud chcete maximalizovat své zabezpečení, preferujte datový roaming spolu s VPN a end-to-end šifrováním

Naopak nejbezpečnější variantou je využití datového roamingu. Dodatečně lze využít také některou z VPN služeb a komunikovat skrze aplikace s end-to-end šifrováním. V takovém případě se riziko narušení důvěrnosti vaší komunikace výrazně minimalizuje.

Nenechávejte svá zařízení bez dozoru a nezamčená

Dále je doporučeno za žádných okolností nenechávat svá elektronická zařízení bez dozoru, a to primárně s ohledem na možnost dalších typů kompromitace ze strany útočníka. Pokud je to však potřeba, je vždy vysoce žádoucí dané zařízení uzamknout. V tomto případě se možnosti útočníka kompromitovat zařízení snižují.

Zabezpečte svoje služby dvoufázovým ověřením

Pokud přesto ke kompromitaci nebo záchytu vaší komunikace útočníky dojde, je vhodné mít dodatečnou úroveň ochrany vámi používaných služeb ve formě dvoufázové autentizace (2FA). Tu podporuje většina služeb jako jsou e-mailové aplikace, účty na sociálních sítích či internetové bankovnictví. Použití 2FA významně minimalizuje škody, jež může útočník napáchat i v případě, že dojde ke krádeži vašich přihlašovacích údajů.

Dávejte si pozor na využívání neznámých USB disků

V rámci veřejných akcí i mimo ně je důležité být obezřetný při manipulaci s USB disky, které nepocházejí z důvěryhodného zdroje. Útočníci často využívají taktiku, kdy pohozením nebo nabídnutím neznámého USB disku obětem zavedou malware do jejich zařízení. **Doporučujeme, abyste se vyhýbali připojování USB disků, které jste našli nebo vám byly nabídnuty cizími osobami, a vždy pečlivě prověřili jakékoli externí zařízení před jeho připojením k vašemu zařízení.**

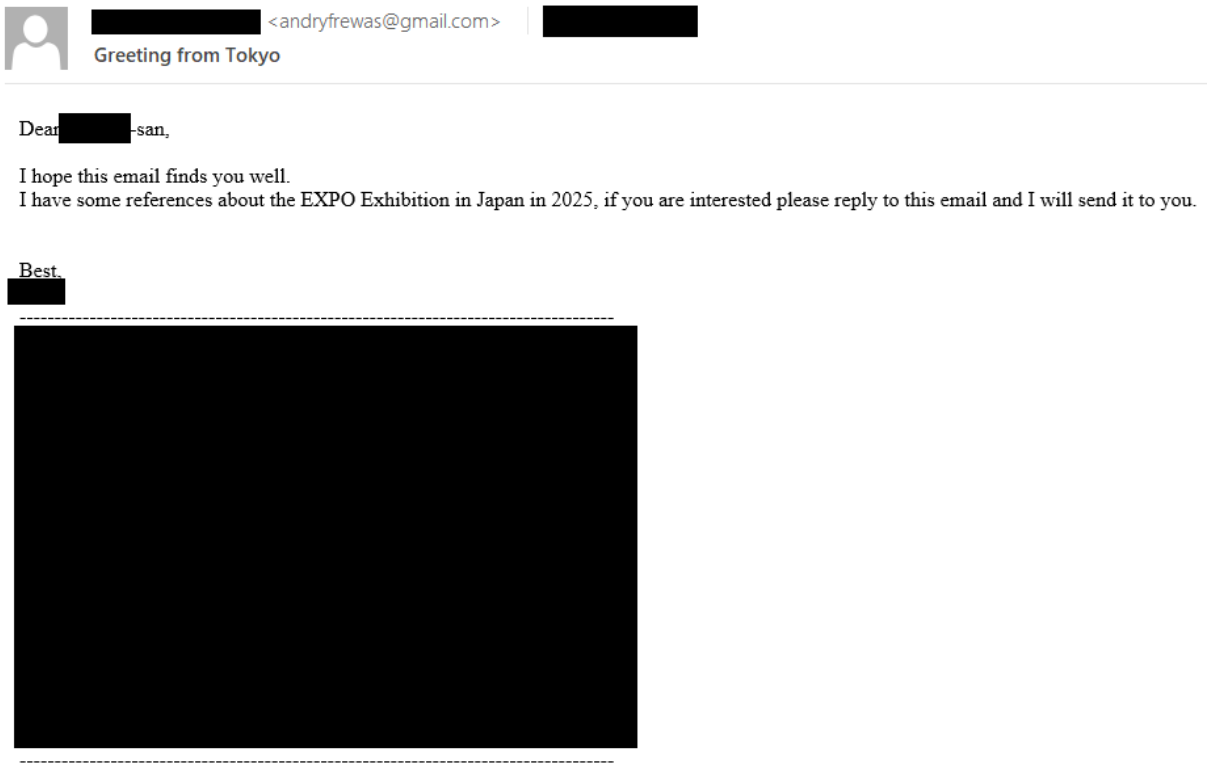
Příloha 2: Kampaň aktéra MirrorFace zneužívající téma EXPO 2025

V srpnu 2024 výzkumníci společnosti ESET detekovali kyberšpionážní kampaň, za kterou má stát skupina MirrorFace. Kampaň této skupiny, firmou ESET spojované s Čínskou lidovou republikou, cílila mimo jiné proti středoevropskému diplomatickému institutu a v rámci spear-phishingového útoku zneužila téma výstavy Expo 2025. Analýza společnosti ESET popisuje dva případy zahrnující oběť v Japonsku a výše zmíněný cíl ze střední Evropy. Tento text se bude věnovat popisu útoku na druhou zmíněnou oběť.

Skupina MirrorFace v rámci daného útoku poslala e-mailovou zprávu (Obr. 1), která odkazuje na předchozí legitimní interakci mezi institutem a japonskou nevládní organizací, jež byla pravděpodobně získána z některé dřívější kampaně skupiny. **Tato spear-phishingová zpráva odkazuje na nadcházející výstavu Expo 2025 a neobsahuje žádný škodlivý obsah.**

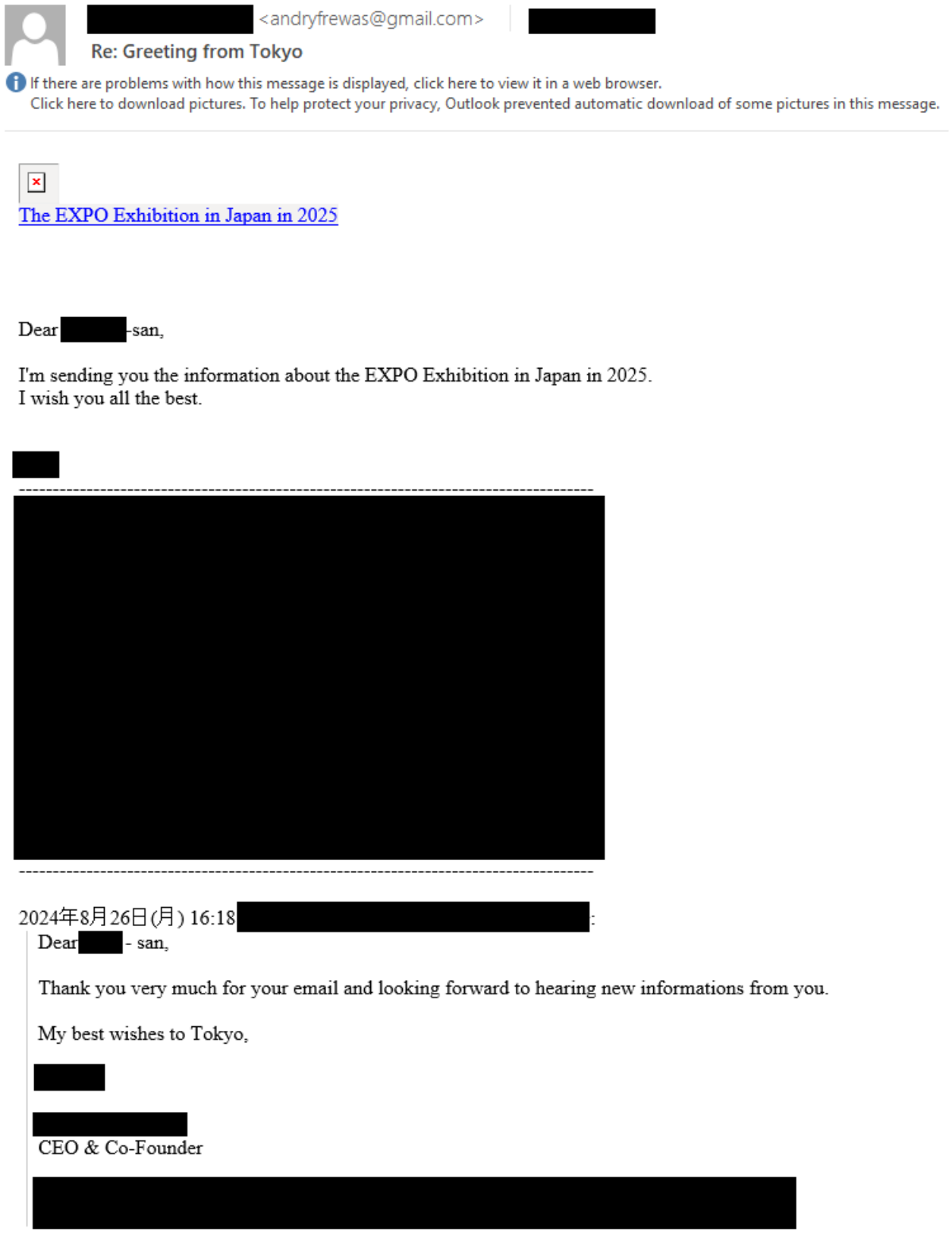
Jakmile však oběť na zprávu zareagovala, útočníci odeslali další e-mailovou zprávu se škodlivým odkazem na OneDrive vedoucím k archivu ZIP se souborem LNK (viz Obr. 2). Tento LNK soubor je maskován jako dokument aplikace Word s názvem The EXPO Exhibition in Japan in 2025.docx.lnk („Výstava EXPO v Japonsku v roce 2025.docx.lnk“). **Po otevření LNK souboru dojde ke spuštění škodlivých souborů a zároveň k otevření samotného dokumentu týkajícího se Expo 2025.**

Obr. 1: První e-mail zaslaný oběti



Zdroj: welivesecurity.com

Obr. 2: Druhý zaslaný e-mail obsahující odkaz na škodlivý archiv ZIP umístěný na OneDrive



Zdroj: welivesecurity.com

Zdroje

[1] ESET. 2025. Operation AkaiRyū: MirrorFace invites Europe to Expo 2025 and revives ANEL backdoor https://www.welivesecurity.com/en/eset -research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/
[2] Hunt.io. 2024. ToneShell Backdoor Used to Target Attendees of the IISS Defence Summit https://hunt.io/blog/toneshell-backdoor-used-to-target-attendees-of-the-iiss-defence-summit
[3] Japan Association for the 2025 World Exposition. 2024. Be Careful of Fake Accounts. https://www.expo2025.or.jp/en/news/news-20240724-03/
[4] NHK. 2025 Cybersecurity firm warns fake website is posing as official Expo ticket site. https://www3.nhk.or.jp/nhkworld/en/news/20250328_08/

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Zelená TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.