

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **26** ze dne **19.1.2023**

Rok 2022 z pohledu kybernetických hrozeb

Vývoj kybernetických hrozeb v roce 2022 značně ovlivnila válka na Ukrajině – vrátil se nechvalně známý malware Industroyer, který cílil na velkou část ukrajinské vysokonapěťové elektrické sítě, nebo se objevily scammy zneužívající solidarity lidí s Ukrajinou. Nejčastějším cílem ransomwarových útoků se naopak stalo Rusko. V Česku narůstala oblast běžného malwaru, šíření dezinformací, scammy a phishingové kampaně, které jsou rizikem nejen pro jednotlivce, ale stále více také pro firmy. Velkým tématem letošního léta se staly phishingové podvody na internetových bazarech, které opět nabraly na intenzitě před koncem roku. Během celého roku narůstaly v Česku také detekce škodlivého kódu, a to zejména spywaru. Shrnutí vychází z pravidelných bezpečnostních statistik společnosti ESET.

V době, kdy byla zahájena invaze na Ukrajinu, objevili analytici ze společnosti ESET dvě nové rodiny malwaru typu wiper (HermeticWiper a IsaacWiper), které cílily na ukrajinské organizace a měly za cíl mazat data v zařízeních. V dubnu poté ESET odhalil útok škodlivým kódem Industroyer2, jehož autorem byla ruskojazyčná útočná skupina Sandworm. Útok byl zaměřen na rozvodnou síť distribuující elektřinu na území Ukrajiny.

S válečným konfliktem na Ukrajině se také odstartovala vlna podvodných humanitárních sbírek, tedy scamů, které se šířily jak e-mailem, tak prostřednictvím sociálních sítí. Aktuálně jsou phishingové útoky, které se vyznačují manipulativní komunikací a cílí na uživatele všech operačních systémů a platforem, jednou z nejrychleji rostoucích oblastí hrozeb, a to i v Česku.

Rapidně vzrostl počet podvodů na internetu

Scammy na internetu se ale netýkaly jen podvodných sbírek. Letos v létě se staly rizikem pro uživatele podvody na internetových bazarech, při nichž útočníci zneužívali jména přepravních společností. V Česku se jednalo zejména o tuzemské přepravní společnosti – Českou poštu a Zásilkovnu.

Útoky jsou čím dál sofistikovanější a útočníci letos zneužívali k útokům i legitimní nástroje jako Google AdSense nebo WordPress. Prostřednictvím online reklamy mimo jiné lákali na investiční nabídky nebo nákup potravinových doplňků. Případně oběti přihlašovali k prémiovým mobilním službám. Podvodný obsah se objevoval v několika jazykových mutacích, včetně češtiny a útočníci jeho prostřednictvím zneužívali jména celebrit nebo známých společností, například skupiny Agrofert nebo ČEZ.

Celkově počet detekovaných případů phishingu podle bezpečnostních expertů letos narostl o stovky procent oproti roku předchozímu. *"Z dat, která máme k dispozici, můžeme skutečně vyčíst narůstající trend phishingových kampaní. Jde o metodu, kdy se útočník vydává za důvěryhodnou autoritu s cílem získat citlivá data oběti. Takový způsob útoku označujeme jako sociální inženýrství a vedle útoků prostřednictvím malwaru, jako jsou infostealery nebo ransomware, se již dnes jedná o jednu z nejčastějších strategií, jak zaútočit na citlivá data domácích i firemních uživatelů,"* popisuje Martin Jirkal, vedoucí analytického týmu společnosti ESET.

Hlavním rizikem zůstává také spyware

Spyware po celý rok v Česku útočil především přes nebezpečné e-mailové přílohy a hlavním cílem útoků zůstávají uživatelská hesla, především ta, která si uživatelé ukládají do internetových prohlížečů. Ty totiž nejsou

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **26** ze dne **19.1.2023**

před těmito útoky dostatečně zabezpečené.

Mezi hrozbami pro operační systém Windows v roce 2022 dominovaly spywary Agent Tesla (21,45 % případů), Formbook (12,96 %) a password stealer Fareit (9,72 %). Za nimi (3,38 %) ještě následuje SPY Agent AES, dříve přiřazovaný ke spywaru Agent Tesla. Téměř všechny nejčastěji detekované hrozby jsou nějakým způsobem zadní vrátka do systému (backdoory), které mohou nainstalovat do zařízení další malware, jako ransomware, poté co odcizí ze systému hesla, nebo jiné osobní údaje.

"V Česku se pravidelně objevují české překlady celosvětových útočných kampaní, což svědčí o tom, že je Česká republika na seznamu cílových zemí. Nebezpečné přílohy mají svými názvy uživatele přesvědčit, že se jedná o reálnou fakturu, účtenku, nebo doklad k objednávce a přimět je tak k otevření souborů, čímž umožní spywaru infikovat jejich zařízení," říká Jirkal.

Stalkerware a bankovní malware ustupují škodlivé reklamě

V případě zařízení s operačním systémem Android se ukazuje, že nejvíce detekovanou moderní hrozbou se stává nevyžádaná reklama s různými stupni míry invaze do systému.

"Nejběžnějším škodlivým kódem byl letos v Česku Andreed (30,78 % případů), který je nejméně invazivní, což může být důvodem jeho největšího přetrvávání. Ustupuje stalkerware, který dominoval minulý rok a také malware Cerberus, který byl v ČR začátkem roku 2022 velice aktivní. Uživatelé by ale neměli propadat falešnému pocitu bezpečí - například malware Triada, který se v menších či větších číslech v ČR pohybuje celoročně, dokáže v systému napáchat uživateli již nemalé škody," dodává Martin Jirkal.

Hrozby pro firmy

Ransomware je v současnosti jednou z největších hrozeb pro firmy a jeho výskyt ještě zhoršil trend hybridní práce. Malé a střední podniky se stávají stále atraktivnějším cílem útoků, a to proto, že ačkoli uchovávají spoustu cenných zákaznických a finančních dat, často jim chybí komplexní bezpečnostní opatření, která používají velké korporace.

"Ransomware se může do sítě společnosti dostat přes služby vzdálené správy nebo právě pomocí phishingových kampaní. Útoky jsou čím dál sofistikovanější a útočníci využívají i nově objevených zranitelností systémů, případně provádějí útoky na dodavatelský řetězec, kdy infikují nebo manipulují se softwarovým produktem dodavatele," říká Robert Šuman, vedoucí pražské virové laboratoře společnosti ESET.

Jak vyplynulo ze zprávy SMB Digital Security Sentiment Report 2022 ransomware je jednou z nejobávanějších hrozeb pro malé a střední podniky, v ČR se ho obává 65 % z těchto firem. Více se čeští respondenti obávají pouze virů a malwaru (75 %). Za zmínku stojí i vysoké procent českých firem (62 %), které se obávají Business E-mail Compromise (BEC), při kterých dochází ke zneužití identity zaměstnance, kterou útočník odcizí nejčastěji pomocí technik sociálního inženýrství, včetně phishingu.

Kryptoměny je výhodnější krást

V letošním roce přetrvával trend miningu kryptoměn v prohlížečích a cryptostealers útoky. Hrozby v oblasti kryptoměn obvykle korelují s jejich směnnými kurzy. Směnné kurzy kryptoměn a ochotu obchodovat nebo je těžit ale negativně ovlivnily rostoucí ceny energií. Stále výhodnější je tedy kryptoměny spíše odcizit jejich držitelům.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **26** ze dne **19.1.2023**

Masivně narostly i pokusy o podvodné vylákání kryptoměn na diskuzních platformách typu Discord nebo Telegram, kde se útočníci vydávali za správce témat, oficiální zástupce kryptoburz nebo support tým. Phishingové útoky se také skrývaly za tváře známých osobností např. Elona Muska, kdy se jednalo o falešné rozdávání dárků a bonusů (tzv. giveaways), jejichž cílem bylo z oběti vylákat menší množství kryptoměny s vidinou získání násobného počtu dané kryptoměny.

"Kryptoměny budou nadále jednou z hlavních oblastí, přes kterou mohou útočníci monetizovat, budou využívány pro různé podvody jako je phishing, vishing atd. Pravděpodobně budeme často vídat pokusy ukrást přístupy k peněženkám nebo k účtům na burzách a podvodné investice do kryptoměn," říká Šuman.

"Celkově se příští rok budeme setkávat se stálými hrozbami, neočekáváme výrazné změny trendu. Nadále porostou phishingové útoky, jako byly letos například podvody na online bazarech, a poroste tak potřeba, aby byl i běžný uživatel internetu stále informovanější a opatrnější. Dominovat budou nadále infostealery jako jsou spywary nebo password stealery a můžeme počítat i se sofistikovanými útoky na firmy prostřednictvím ransomwaru. Rizikem zůstávají také útoky typu dodavatelský řetězec nebo penetrační průniky přes zranitelnosti s komplexním vytěžením informací, strojového času apod. v infikované společnosti," shrnuje Šuman z ESETu.

Zdroj: ESET