Postřehy z bezpečnosti: Američané zakazují sdílení dat s některými zeměmi

Autor: Depositphotos.com, podle licence: Rights Managed
Tentokrát si můžeme přečíst o zemích přidaných na Bidenův blacklist, znovuzrození LockBitu, zneužívání respektovaných domén, ale i nových zbraních skupiny Lazarus či pádu největšího německého trhu s ilegálním zbožím a službami.

Bidenův blacklist

Prezident USA Joe Biden podepsal minulou středu výkonné nařízení, týkající se nakládání s osobními údaji občanů USA. Dané nařízení zakazuje hromadný prodej a přenos zmíněných dat do konkrétních zemí, mezi něž patří ČLR, Rusko, Írán, Severní Korea, Kuba a Venezuela.

Přístup k osobním údajům amerických občanů ze strany škodlivých aktérů z daných zemí je vnímán prezidentem USA jako ohrožení národní bezpečnosti. Aktéři z daných zemí totiž údajně zneužívají soukromé údaje ke sledování a vydírání vytipovaných lidí, kteří jsou předmětnými státy vnímáni jako disidenti. Kromě toho se USA touto reakcí snaží chránit osobnosti v akademické sféře, politiky, novináře, či aktivisty z neziskových organizací, kteří se nějakým způsobem vůči daným státům vymezují.

Tento krok má vést k posílení ochrany osobních údajů, a dává pravomoc Ministerstvu spravedlnosti USA zabránit státům představujícím hrozbu v získání nejcitlivějších údajů Američanů. Mezi tato data patří biometrické, zdravotní, geolokační, finanční a genetické údaje všech občanů USA.

Operace Cronos: konec LockBitu… nebo ne?

Před nedávnem proběhla bezpečnostní komunitou zpráva, že díky společnému mezinárodnímu úsilí se v rámci operace Cronos podařilo přerušit funkčnost infrastruktury jednoho z komerčně velmi úspěšných vyděračských programů (ransomware) – LockBit 3.

Netrvalo ale dlouho a bezpečnostní firma TrendMicro uveřejnila informaci o tom, že zachytila novou verzi nazvanou operativně „LockBit-NG-Dev“, která využívá nové a neotřelé techniky, což bohužel signalizuje celému světu, že výše zmíněné vítězství pravděpodobně není trvalé.

Tomu nasvědčuje i skutečnost, že nedlouho po „pádu LockBit 3“ se na darknetu vynořila nová stránka propagující služby LockBit, a také internetová identita vystupující pod přezdívkou LockbitSupp, která o sobě veřejně prohlašuje, že je jedním z administrátorů a že na obnovení funkcionality celého ekosystému se intenzivně pracuje, navzdory všem zatčením a zabaveným účtům (kterých bylo údajně přes 14 000).

Domény zvučných jmen zneužívány k rozesílání spamu

Více než 8 tisíc legitimních domén, patřících často známým a respektovaným organizacím a firmám, bylo zneužito k phishingové kampani nezvyklých rozměrů, při níž bylo denně rozesíláno kolem 5 milionů e-mailů. Mezi postižené patří taková jména, jako jsou VMware, Marvel, McAfee Symantec, Java.net, MSN, ale také NYC.gov, The Economist, Cornell University, nebo třeba UNICEF.

Kampaň je nazvaná SubdoMailing, a využívá celou paletu technik, jak obejít mechanismy bránící rozesílání nevyžádaných zpráv. Mezi ně patří zejména tzv. únos CNAME, kdy útočník cíleně vyhledává subdomény důvěryhodných značek a názvů, které jsou pomocí CNAME směrovány na jiná, aktuálně již neregistrovaná doménová jména. Tyto si pak útočník zaregistruje, a využije faktu, že subdoména často dědí SPF politiku a další nastavení „nadřazené“ domény, která propůjčují emailům z ní odeslaným svoji legitimitu a pomáhají obcházet antispamové ochrany.

Využívá se také špatně nakonfigurovaných SPF záznamů. Jeden z nich v důsledku rekurzivního odkazování například obsahoval přes 17 tisíc IP adres, kterým umožňoval odesílat zprávy tak, jako by pocházely z autorizovaných zdrojů v msn.com. Často jsou také využívány legitimní DKIM a DMARC záznamy.

Podle výzkumníků z izraelské společnosti Guardio Labs, kteří problematiku detailně rozebírají zde, je cílem celého komplexního systému manipulace s DNS záznamy tisíců domén to, aby bylo možné doručit obrovské objemy nevyžádaných zpráv koncovým uživatelům. Následně ale také zprostředkovat sérii přesměrování a odkazů, na které mohou uživatelé kliknout jako na tlačítka v obdržených zprávách, tvářících se „klasicky“ např. jako oznámení o vypršení předplatného streamovací služby, varování před zcizením údajů k účtu sociální sítě, a tak podobně.

Kampaň je připisována skupině „ResurrecAds“, která dlouhodobě shromažďuje tzv. mrtvé domény, tedy takové, které byly např. v minulosti použity pro jednorázovou reklamní akci, ale dále ponechány bez správy. Po vypršeni jejich registrace původním subjektem je skupina, např. přes službu Namecheap, zaregistruje pro sebe. Tato kampaň dobře demonstruje, že i důmyslné způsoby ochrany, původně zamýšlené k potlačení phishingu a spamu, mohou být obcházeny či dokonce využívány technologicky pokročilejšími „hráči“ na tomto poli. Dokud zkrátka na SPAM ve své poštovní schránce klikne dostatek uživatelů, najde se odpovídající počet těch, kteří se o doručení takového SPAMu postarají.

Společnost Guardio Labs vytvořila webový nástroj, SubdoMailing Checker, pomocí kterého je možné zkontrolovat, zda byla určitá doména v této kampani zneužita. Stránka je denně aktualizována a doplňována o nově nalezené zneužívané CNAME a SPF záznamy.

Lazarus vytahuje stále nové zbraně

Bezpečností tým dodavatele antivirových řešení AVAST oznámil, že severokorejská skupina, známá jako Lazarus Group, nalezla konkrétní cestu ke zneužití již dříve známé zranitelnosti CVE-2024–21338. AVASTem vyvinutý proof-of-concept byl Microsoftu zaslán v srpnu 2023, oprava pak byla vydána letos v únoru. Dosud však nebyl znám případ úspěšného zneužití zranitelnosti škodlivými aktéry.

AVAST dále upřesňuje, že útočník je schopen na kompromitovaném systému zvýšit svá oprávnění, a získat přímý přístup k objektům jádra. Toho pak využívá nová varianta jeho rootkitu FudModule. Ten je známý již od roku 2022, kdy jej poprvé mj. reportoval ESET.

Jak uvádí výzkumník AVASTu Jan Vojtěšek, FudModule patří mezi nejpokročilejší nástroje v arzenálu Lazarus Group, dlouholetého, a bohužel velmi plodného zástupce této scény.

Největší německý trh s kyberkriminalitou má utrum

Němečtí vyšetřovatelé ve spolupráci s partnery ze zahraničí již dlouhodobě sledovali platformu Crimemarket. Ta se prezentovala jako největší online trh s nelegálními službami a zbožím v Německu. Platforma byla označována jako tzv. hub pro obchod s drogami, narkotiky, službami v oblasti kyberzločinu, mezi než patřily i návody na páchání trestné činnosti různého druhu.

Během večera 29. února tohoto roku vyrazila policie do akce a provedla 102 domovních prohlídek na celém území Německa. Hlavní důraz byl kladen na oblast Severního Porýní-Vestfálska, kde byli zatčeni tři lidé, včetně 23letého muže, jenž je hlavním podezřelým. Celkem bylo zatčeno šest lidí.

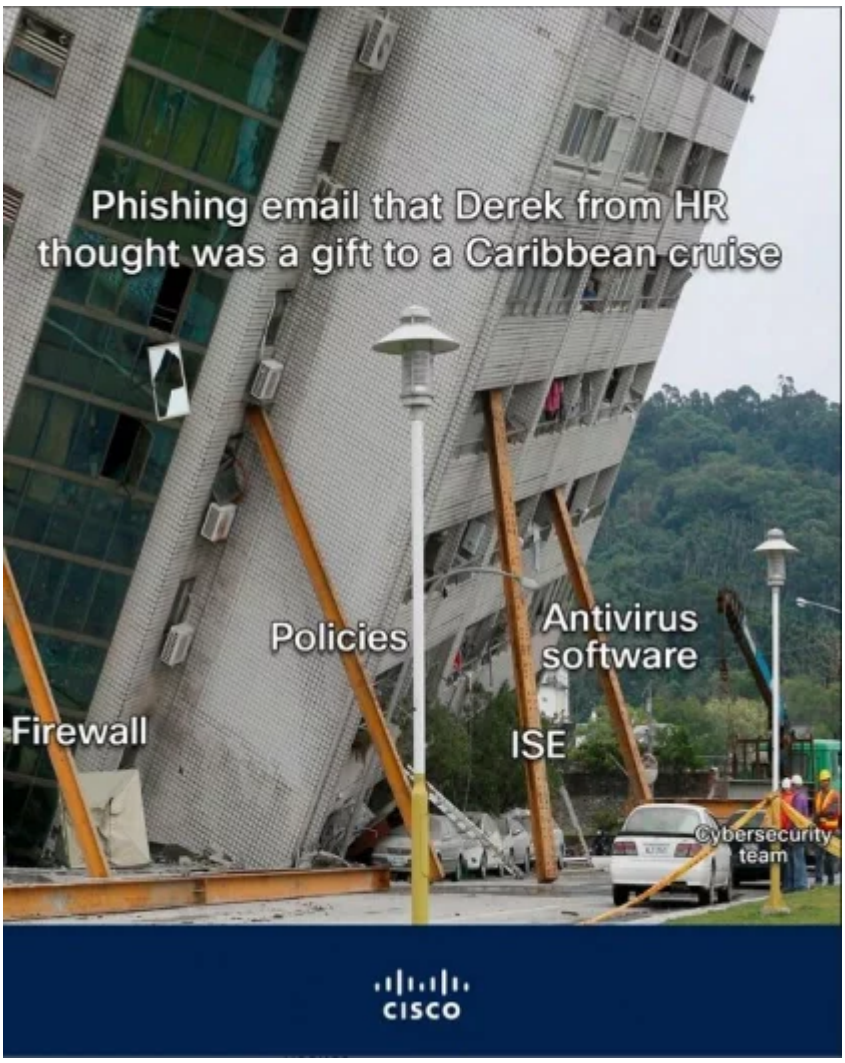
V rámci domovních prohlídek bylo zabaveno mnoho důkazů, zahrnujících mobilní telefony, IT zařízení, a datové nosiče. Ve 21 případech došlo k zabavení narkotik, včetně 1 kilogramu marihuany a různých druhů tablet extáze. Dále pak přibližně 600 000 euro v hotovosti, a další movité věci.

Samotná operace nebyla mířena pouze proti provozovatelům dané platformy, ale i vůči jejím uživatelům, jichž bylo kolem 180 000. Ti si již delší dobu stěžovali na výpadky přihlašování na webové stránky Crimemarketu. Nyní se ukázalo, že tyto potíže nebyly způsobeny technickými problémy, nýbrž souvisely právě s policejní aktivitou. I po zabavení dané platformy policií ji vyšetřovatelé ponechali z části aktivní z důvodu získávání identifikačních, přihlašovacích a dalších údajů uživatelů. V době psaní tohoto článku je aktivní pouze domovská stránka, zatímco veškeré další stránky vázané na danou doménu zobrazí oznámení o zabavení platformy.

Ve zkratce

- 10 věcí, které nepsat na sociální sítě – a proč
- Hacknutá Ivanti VPN je zranitelná i po factory resetu
- Nový malware Bifrost pro Linux napodobuje doménu VMware
- Seznamte se s „Leo“ – novou AI prohlížeče Brave

Pro pobavení



Chudák Derek opět nic nevyhrál

Autor: Cisco

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