Eliminace škodlivých či podvržených domén, sociálních účtů, obchodních značek, aplikací a dalších formou služby Take-Down.

Shrnutí:

Tento dokument je určen k pokrytí typů incidentů a technických prostředků aktérů hrozeb, které může systém CYFIRMA detekovat a zlikvidovat.
Služby Take-Down, čili eliminace škodlivých nebo podvržených domén lze od CYFIRMA vyžádat za následujících podmínek:

- XX žádostí za měsíc.
- Žádost bude potvrzena do 1 pracovního dne. Doba dodání bude dohodnuta na žádosti vzhledem k různé povaze jednotlivých žádostí.
- Není stanovena žádné pevné SLA vzhledem k různé povaze/jurisdikci/zákonům, které se mohou vztahovat na každý požadavek.
- Tato služba nezahrnuje:
  - Soudní spory v cizích zemích.
  - Místní vymáhání.
  - Přítomnost v místních jurisdikcích.
  - Vyřazení z uzavřených komunit/temných webových fór.

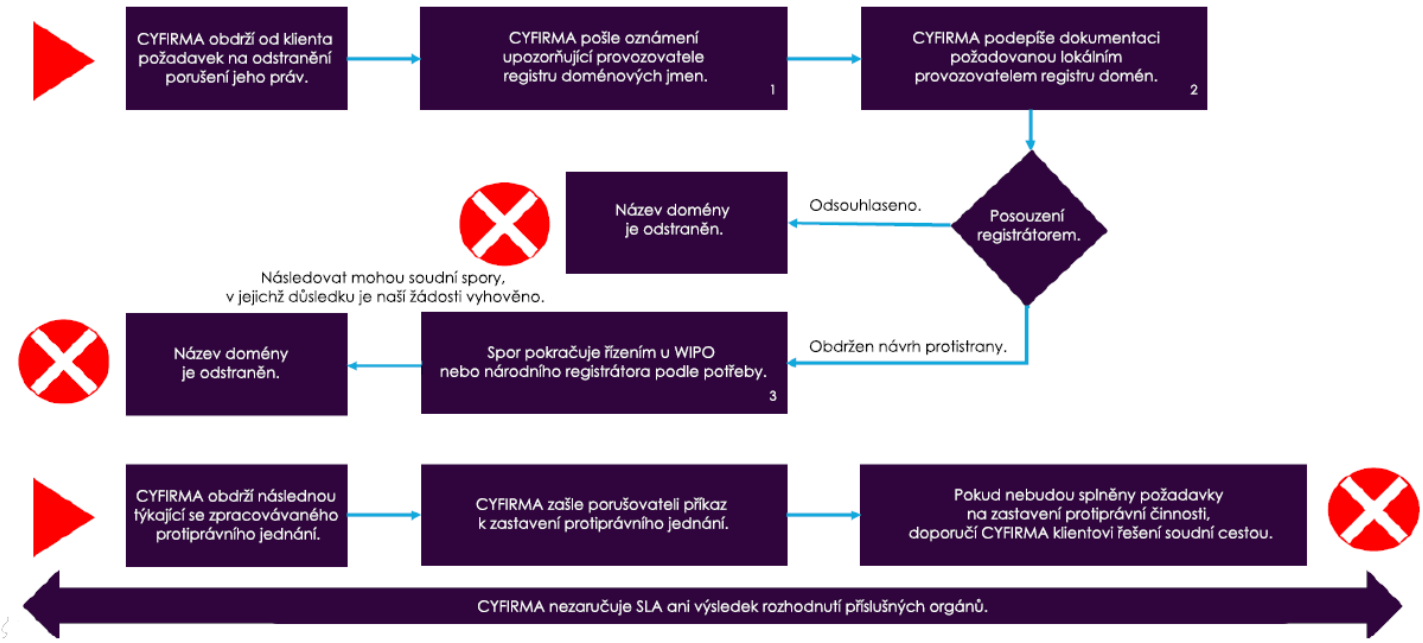
Kategorie hrozeb, na něž mohou být aplikovány služby Take-Down jsou definovány následujícím způsobem:

Ukázka ilustrace procesu

Společnost CYFIRMA může v rámci svých služeb Take-Down poskytnout následující řešení.

Řídíme celý proces od začátku až do konce. Týká se to jak přípravy právních dokumentů, e-mailů a dalších dokumentů, přípravy telefonické korespondence, tak i zařazení na černou listinu.

Následující obrázek ilustruje příklad vyřazení squatované domény:



[1] Bude vyžadováno, aby klient předložil informace o autorských právech a vlastnictví.
[2] Časové lhůty budou odpovídat platným postupům příslušných zemí.
[3] Případné další soudní spory budou mimo oblast působnosti společnosti CYFIRMA.

Kategorie hrozeb a jejich popis

Phishing

Hacknuté webové stránky

Definice: Hacknutá webová stránka slouží často jako phishingová webová stránka, která je zaměřena na značku a je umístěna na webu, který byl napaden.
Zločinci se nabourávají do nezabezpečených domén a používají je jako základnu pro své phishingové útoky, což jim šetří čas, protože nemusí vytvářet nové domény, a také ztěžuje jejich odhalení. Nelze totiž snadno vysledovat zdroj phishingových útoků.

Škodlivé domény

Definice: Doména, která byla zaregistrována speciálně za účelem napadení značky klienta. Na příklad pokud ABC Bank byla chráněnou značkou a vlastnila doménu abcbank.com, mohl by si zločinec zaregistrovat podobnou doménu abcbank.net a umístit na tuto doménu phishingové stránky.

Vezměte prosím na vědomí, že pouhý fakt, že doména má podezřelý název, bohužel není důkazem k tomu, abyste přistoupili k odebrání domény, pokud je v současné době neaktivní nebo je doména zaparkovaná.

Přesměrování

Definice: Adresa URL, která přesměrovává na podvodné webové stránky jakéhokoli druhu.

Subdoména

Definice: Phishingová adresa URL, která je hostována na subdoméně. Může se jednat buď o subdoménu vytvořenou zločincem na kompromitovaném webu nebo na webu, který si zaregistroval.

POSTování na URL třetí strany

Definice: Některé phishingové webové stránky "POSTují" ukradené přihlašovací údaje na URL adresu třetí strany, která je umístěna na jiné doméně než phishingová webová stránka.
Phishingové přílohy HTML nebo formuláře mohou být také rozesílány e-mailem a ty musí "POSTovat" ukradené údaje na adresu URL někde na internetu, aby fungovaly.

Zkracovač adres URL

Definice: Zkracovače URL adres jsou služby určené k poskytování kratších odkazů/přesměrování namísto dlouhých URL. Běžné platformy zahrnují bit.ly, x.co a tinyurl.

Hosting zdarma

Definice: Phishingové webové stránky hostované u poskytovatele bezplatného hostingu. Zpravidla si zločinci zaregistrují nové účty u poskytovatelů hostingu a spustí na nich phishingové kampaně.

Pharming IP

Definice: Pharming IP je škodlivá IP adresa/server, který byl nakonfigurován tak, aby odpovídal vždy tím, že zobrazí phishingové stránky. Když je navštívíte z kompromitovaného počítače nebo zařízení, uživatelé si myslí, že navštěvují legitimní adresy URL, ale přitom kompromitované zařízení odesílá již provoz na škodlivou IP, kterou ovládá zločinec. Obvykle se používají ve spojení se škodlivými pharmingovými DNS servery nebo malwarem naprogramovaným tak, aby uměl měnit hostitelské soubory.

Vishing (Voice phishing)

Vishing (neověřený)

Definice: Neověřené Vishingové číslo je číslo, které bylo nahlášeno do systému CYFIRMA, ale náš SOC tým zatím nepotvrdil škodlivou aktivitu na tomto čísle. Obvykle se jedná o podvržené telefonní hovory přicházející z online služeb nebo systémů VoIP.

Vishing (ověřený)

Definice: Ověřené Vishingové číslo je číslo, které náš tým úspěšně prověřil a zároveň na tomto čísle potvrdil škodlivou činnost nebo podvodné vydávání se za chráněnou značku.

Messaging - zasílání zpráv

E-mail (škodlivý)

Definice: E-mail, který se buď vydává za značku klienta, nebo za osobu, která pracuje v organizaci klienta. Může se jednat buď o podvržení domény klienta, nebo o registraci domény třetí strany, která má podobnou povahu jako doména klienta, nebo o registraci z bezplatného e-mailového účtu.

Jednotná komunikace – Unified Communications

Definice: Účet v komunikační síti, který se vydává za značku klienta, a to buď prostřednictvím škodlivých zpráv nebo vydáváním se za jméno/zobrazený obrázek. (Skype, WeChat atd.)

SMiShing

Definice: Škodlivá SMS zpráva, která je zasílána spotřebitelům a obvykle je směřuje na phishingové stránky nebo na stránky s malwarem.

Zneužití značky

Falešný průzkum

Definice: Falešný průzkum, který je šířen s použitím informací nebo obsahu chráněné značky bez oprávnění. Tyto průzkumy často nabízejí na konci falešné ceny, například dárkovou kartu za vyplnění a slouží ke shromažďování údajů uživatelů, které jsou pak prodávány nebo rozdávány.

Hazardní stránky

Definice: Falešné stránky s hazardními hrami jsou na internetu velmi rozšířené a většinou se vydávají za různá kasina z celého světa. Často také uvádějí, že přijímají platby od různých bankovních institucí. Většinou se jedná o banky ze stejných zemí, jako je dané kasino, za které se zrovna v danou chvíli vydávají.

Falešné zprávy

Definice: Falešné zprávy se mohou skládat z falešných článků, které hovoří o firmě nebo jednotlivci z firmy, kterou CYFIRMA chrání. Tyto typy článků se často šíří v naději, že lidé uvěří, že článek je pravdivý, protože za ním stojí společnost, kterou spotřebitel zná a které důvěřuje. CYFIRMA se s těmito typy článků často setkává. Takové články jsou sdíleny v sociálních médiích, kde velmi rychle získají velkou popularitu.
Vezměte prosím na vědomí, že svoboda projevu a cítění je velmi reálná a velká hodnota, která platí napříč internetem a že tudíž negativní názory nebo nepravdivé recenze o organizaci nemohou být jen tak odstraněny.

Únik dat

Definice: Pokud dojde k úniku důvěrných informací online, ať už ze strany pachatelů trestné činnosti nebo někoho zevnitř organizace, je to klasifikováno jako únik dat a CYFIRMA se může pokusit o jejich převedení do offline režimu.

Pornografie

Definice: V některých extrémních případech může dojít k tomu, že jsou značky klientů umístěny na webových stránkách obsahujících také pornografii, což může mít vážné důsledky pro pověst značky a organizace.

Inzeráty s nabídkou práce

Definice: Falešné pracovní inzeráty jsou velmi časté. Často se setkáváme s umístěním značky klienta na různých falešných pracovních nabídkách, které jsou zveřejňovány nebo inzerovány pod značkou (značkami) jejich organizací bez oprávnění klienta.

Marketplace - tržiště

Definice: Tržiště lze definovat jako falešné tržiště, které buď používá značky klienta na produktech bez jeho souhlasu nebo používá duševní vlastnictví klienta za účelem peněžního zisku opět bez jeho souhlasu.

Placené vyhledávání

Definice: Zločinci mohou propagovat škodlivé odkazy ve vyhledávačích tím, že zaplatí za určitá klíčová slova, aby se zobrazovala při vyhledávání například v Bingu nebo Googlu. Jedná se o způsob, jakým mohou zločinci nasměrovat uživatele na podvodné webové stránky, když se uživatelé snaží vyhledat legitimní značku.

Všeobecná ochranná známka

Definice: Často se setkáváme s tím, že se ochranné známky na internetu nepoužívají v souladu s pravidly jejich používání. Dochází k porušování ochranných známek klientů nebo jejich zveřejňování na webových stránkách bez souhlasu a v mnoha z těchto případů jsou v důsledku toho poškozeny značky nebo pověst našich klientů.

Adresáře

Definice: Adresář s kontaktními informacemi na společnost nebo jednotlivce. Může se jednat o telefonní číslo, e-mailovou adresu nebo klasickou adresa sídla a pobočky.

Zaparkovaná doména

Definice: Doména, která je zaregistrována a má podobnou povahu jako legitimní doména, na příklad abc-bank.com a abc1bank.com, ale buď na ní není žádný obsah, nebo je aktivně zaparkovaná.

Zneužití značky na sociálních sítích

Profil

Definice: Profil na sociální síti, který se zaměřuje na značku klienta a využívá jeho značky a neoprávněně používá její obsah. Tyto značky mohou tvořit značky vlastněné firmami nebo jednotlivci, kteří pro organizaci pracují. [4]

Důkazy: Důkazy o tom, že se jedná o profil, který je v rozporu se zákonem o ochraně osobních údajů mohou být následujícího charakteru.

- Kopie aktuálních informací o ochranné známce, která je porušována na profilu nebo kopie průkazu totožnosti vydaného vládou, která prokáže, že náš tým je oprávněn jednat jejich jménem.
- Autorizační dopis, který uvádí, že společnost CYFIRMA je oprávněna jednat jménem dotyčné osoby/značky koncového klienta.

Stránka

Definice: Zneužívající stránka na sociální síti, která používá chráněné značky bez oprávnění dané ochranné známky nebo se vydává za jednotlivce bez jeho souhlasu. [5]

Důkazy: Důkazy o tom, že se jedná o stránku na sociální síti, která je v rozporu se zákonem o sociálních sítích mohou být následujícího charakteru.

- Kopie aktuálních informací o ochranné známce, která je porušována na profilu nebo kopie průkazu totožnosti vydaného vládou, která prokáže, že náš tým je oprávněn jednat jejich jménem.
- Autorizační dopis, který uvádí, že společnost CYFIRMA je oprávněna jednat jménem dotyčné osoby/značky koncového klienta.

Skupina

Definice: Skupina na sociálních sítích, která se vydává za značku klienta, nebo za jednotlivce bez oprávnění. [6]

Důkazy: Důkazy o tom, že se jedná o skupinu na sociální síti, která se chová v rozporu se zákonem o sociálních sítích mohou být následujícího charakteru.

- Kopie aktuálních informací o ochranné známce, která je porušována na profilu nebo kopie průkazu totožnosti vydaného vládou, která prokáže, že náš tým je oprávněn jednat jejich jménem.
- Autorizační dopis, který uvádí, že společnost CYFIRMA je oprávněna jednat jménem dotyčné osoby/značky koncového klienta.

[4] Vezměte prosím na vědomí, že toto nezahrnuje negativní názory nebo nálady.

[5] Vezměte prosím na vědomí, že toto nezahrnuje negativní názory nebo nálady.

[6] Vezměte prosím na vědomí, že toto nezahrnuje negativní názory nebo nálady.

Příspěvek (post)

Definice: Zlomyslný příspěvek na síti sociálních médií, který buď šíří nepravdivé informace o značce nebo je zaměřený na značku klienta s úmyslem ji znevěrohodnit nebo poškodit. [7]

Důkazy: Důkazy o tom, že se jedná o post, který je v rozporu se zákonem o ochraně osobních údajůmohou být následujícího chrakteru.

- Odkaz na příspěvek.
- Pokud jsou porušovány nějaké ochranné známky, budou vyžadovány aktualizováné informace o ochranných známkách.

Autorizační dopis, který uvádí, že společnost CYFIRMA je oprávněna jednat jménem značky klienta.

Událost

Definice: Škodlivá událost na síti sociálních médií, jejíž umístění je nastaveno na klientovu adresu nebo událost zveřejněná jménem klienta bez jeho souhlasu.

Důkazy: Důkazy o tom, že se jedná o škodlivou událost nebo, že autor události není v kontaktu s klientem mohou být následujícho charakteru.

- Odkaz na událost.
- Pokud dochází k porušování ochranných známek, budou vyžadovány aktualizováné informace o ochranných známkách.
- Pověřovací dopis, který uvádí, že společnost CYFIRMA je oprávněna jednat jménem společnosti klienta.
- Potvrzení, že příspěvek je 100% neautorizovaný.

[7] Vezměte prosím na vědomí, že toto nezahrnuje něčí negativní zkušenost nebo názor proti značce.

Mobilní aplikace (neautorizovaná)

Kopie legální aplikace

Definice: Adresa URL v obchodě třetí strany, která inzeruje nezávislé stažení souboru APK, který je přímým klonem klientské aplikace.[8]

Důkazy: Důkazy o tom, že se jedná o aplikaci, která je v rozporu se zákonem mohou být následujícího charakteru.

- Odkaz na původní obsah, který je porušován (Google Play / iTunes store).
- Autorizační dopis, který uvádí, že společnost CYFIRMA je oprávněna jednat jménem značky klienta.

Adware

Definice: Soubor APK/IPA, který používá značku klienta, ale instaluje do mobilního zařízení adware. Často se jedná o aplikace klienta, které jsou oficiálně inzerovány, ale jejich kód byl pozměněn bez oprávnění. To způsobuje negativní zážitek, který si uživatelé spojují se značkou klienta.

Důkazy: Důkazy o tom, že se jedná o reklamní kampaň, která je v rozporu se zákonem mohou být následujícího charakteru.

- Autorizační dopis, který uvádí, že společnost CYFIRMA je oprávněna jednat jménem značky klienta.
- Informace o ochranné známce jsou v těchto případech velmi přínosné, ale nejsou ze své podstaty vyžadovány.

Malware v mobilních zařízeních

Definice: Škodlivá mobilní aplikace, která využívá značku klienta k infikování zařízení. Lze ji také definovat jako aplikaci, která zákeřně krade přihlašovací údaje, když se uživatel pokouší přihlásit k účtu legitimní aplikace klienta na svém infikovaném zařízení.

Důkazy: Důkazy o tom, že se jedná o škodlivou aplikaci, která používá v prostředí značku klienta mohou být následujícího chrakteru.

- Autorizační dopis, který uvádí, že společnost CYFIRMA je oprávněna jednat jménem značky klienta.
- Informace o ochranné známce jsou v těchto případech velmi přínosné, ale nejsou bezpodmínečně nutné.

Přesměrování

Definice: Přesměrování, které uživatele přesměruje na jiný podtyp mobilní aplikace, který CYFIRMA pokrývá.

Důkaz: Důkazy o tom, že se jedná o škodlivé přesměrování na jiný podtyp mobilní aplikace, která využívá značku klienta mohou být následujícího chrakteru.

- Odkaz na škodlivé přesměrování, aby jej analytici CYFIRMA mohli prošetřit a přijmout opatření.

Zneužití značky mobilní aplikace

Definice: Seznam mobilních aplikací třetích stran, který není škodlivý ani neinzeruje přímé stažení, ale vydělává na seznamu legitimních aplikací našeho klienta, jelikož peníze se obvykle vydělávají prostřednictvím generování příjmů z reklamy.

Důkazy: Důkazy o tom, že se jedná o reklamu na mobilní aplikace, která je v rozporu se zákonem mohou být následujícího charakteru.

- Odkaz na seznam.
- Aktualizované informace o ochranné známce.
- Odkaz na původní seznam v legitimním obchodě (Google Play / iTunes).

[8] Všimněte si, že odkaz ke stažení musí být umístěn na místě třetí strany a musí odkazovat na oficiální obchod.

O PLATFORMĚ CYFIRMA

CYFIRMA je externí platforma pro správu externích hrozeb. Propojujeme informace o kybernetickém zabezpečení s odhalováním útočných ploch a ochranou před digitálními riziky, abychom poskytli prediktivní, personalizované, kontextové, outside-in a vícevrstvé poznatky. Využíváme naši cloudovou analytickou platformu založenou na AI a ML, abychom společnostem pomohli proaktivně identifikovat potenciální hrozby ve fázi plánování kybernetických útoků. Náš jedinečný přístup, který spočívá v poskytování pohledu hackera a hlubokého přehledu o vnějším kybernetickém prostředí, pomohl klientům připravit se na budoucí útoky.

CYFIRMA spolupracuje s mnoha společnostmi ze seznamu Fortune 500.
Společnost má pobočky v zemích APAC, USA a EU.

www.freedivision.com | +420 220 972 426