Jak całkowicie usunąć dziecięcą pornografię z Internetu.

1. Zgłaszać odkrytą w Internecie pornografię z dziećmi.

W każdej przeglądarce oprócz przycisku czy menu **Dodaj Zakładkę** powinien być przycisk **Zgłoś CP**. Jego naciśnięcie wywoła okienko w którym będziemy można dodać słowny opis tego, co wzbudza nasze podejrzenie i potwierdzić, że w naszym odczuciu są to strony (albo filmy czy czaty) oferujące pornografię z udziałem nieletnich lub propagujące pedofilię. Po potwierdzeniu, przeglądarka przez bezpieczny serwer pośrednika prześle zaszyfrowany komunikat do oficerów łącznikowych Policji w każdym kraju, w którym działa dostawca internetu w którego sieci znajduje się wykryta pornografia z dziećmi.

Proste, szybkie, anonimowe: jedno naciśnięcie **Zgłoś CP**, potem naciśnięcie **OK**. W tym momencie ruszy procedura: żądanie usunięcia treści (z serwera hostingu, z komputera w kawiarence) dotrze od Policji do osób zarządzających siecią w której ta treść się znajduje. Jeśli nie zareagują, do ich nad-dostawcy internetu trafi żądanie odcięcia od internetu „za niereagowanie". [Opis „Jak działa internet i jak można odcinać": na drugiej stronie].

UWAGA! W Polsce wciąż obowiązuje „zakaz" zgłaszania. (Nb ciekawe, jaką „orientację" ma autor tej IO...)
„Zgodnie z procedurą" zgłaszającemu na Policję fakt natknięcia się na dziecięcą pornografię zabiera się komputer, płyty i inne nośniki „w celu sprawdzenia czy to nie pedofil" albo tylko „zabezpieczenia dowodów".

2. Usuwać zło tam, gdzie ono się znajduje. 3. Odcinać tych, co usunąć zła nie chcą.

To da się usuwać coś z Internetu? Da się! Od dawna i bez żadnych nowych nakładów.

Produkcja i dystrybucja dziecięcej pornografii są przestępstwami we wszystkich krajach świata. Świadome przyzwolenie na dystrybucję dziecięcej pornografii (i kilka innych działań „przeciwko sieci") w kontraktach hurtowych i szkieletowych operatorów jest wyszczególnione jako możliwy powód zaprzestania świadczenia transmisji danych bez odszkodowania. Czyli po prostu odcięcia klienta, z jego winy, od węzłów i Internetu.

Detaliczni dostawcy internetu i firmy hostingowe **są odcinani od globalnej sieci** za brak reakcji na uciążliwości powodowane przez ich klientów takie jak: *udostępnianie stron* phishingowych, *operowanie botnetami* czy *masowy spam*. Czas by były odcinane za brak reakcji na udostępnianie dziecięcej pornografii.

Operacja odcięcia polega na fizycznym wyjęciu wtyczek w węzłach (najprostsze) lub usunięciu wpisów z numerami sieci klienta z ruterów. Technicznie możliwe jest też całkowite odcięcie obcego dostawcy od Europy. Gdziekolwiek by ten dostawca nie działał. Skutkiem będzie jego bankructwo.

Komisja Europejska i Parlament Europejski, zamiast nawoływać do stworzenia mechanizmów cenzury prewencyjnej i masowej kontroli własnych obywateli, powinny w Dyrektywie [...] wezwać kraje członkowskie do tego by uniezależnić usuwanie źródeł dziecięcej pornografii od kontraktów między firmami. Czyli:

1. uznać za samodzielne przestępstwo pomocnictwa zaniechanie działań zmierzających do usunięcia bezpośredniego[1] dostępu[3] do miejsca rozpowszechniania pornografii z udziałem dzieci[4], jeśli osoba lub podmiot zarządzające węzłem, siecią lub fragmentem sieci uzyskają od policji[5] lub też od wskazanej agencji rządowej[5] informację o tym, że w będącym pod ich nadzorem węźle, sieci lub fragmencie sieci znajduje się zidentyfikowane miejsce udostępniające pornografię z udziałem dzieci[4].

2. wyłączyć odpowiedzialność cywilną i umowną za zaprzestanie transmisji danych w przypadku, gdy zaprzestanie takie nastąpiło w celu usunięcia pośredniego[2] lub bezpośredniego dostępu do miejsca rozpowszechniania pornografii z udziałem dzieci[3]. [To umożliwi odcinanie od Europy dostawców poza naszą jurysdykcją].

[1] – dostęp jest bezpośredni, jeśli całość transmisji danych od ich źródła do rutera brzegowego lub węzła jest pod kontrolą osoby lub podmiotu zarządzającego węzłem, siecią lub jej wydzielonym fragmentem. Albo gdy dane znajdują się w sprzęcie kontrolowanym przez wspomniane osobę lub podmiot. To dotyczy każdej sieci: w każdej występuj ten ostatni bezpośredni odcinek, który ma swojego administratora lub właściciela. [2] – dostęp jest pośredni we wszystkich innych przypadkach.
[3] – zablokować dostęp, czyli zablokować możliwość pozyskania danych. Można np. zablokować dostęp do treści przez usunięcie serwerowi uprawnień do odczytu katalogu w której ta treść się znajduje. Można zablokować zamówienia na dane kierowane do wspólnego dla wielu klientów serwera przez usunięcie konfiguracji dla konkretnego miejsca (domeny).
[4] – Wspólna definicja będzie trudna do wynegocjowania. Ale jesteśmy jedną Unią i potrafimy to zrobić.
[5] – Tylko Policja lub odpowiednia agencja mogą mieć bezpośrednią kontrolę nad usuwaniem pedofilskich treści, także w przypadku, gdy decyzję podejmował będzie niezawisły sąd. Pozostawienie dostępu do treści umożliwi prowadzenie legalnych prowokacji. Policja też powinna dostać uprawnienia do selektywnego pozostawienia dostępu do treści mających ulec usunięciu. Np przez pozostawienie dostępu ze znanych jej wcześniej adresów ściganych pedofili.

Jak to wszystko działa?

[Uwaga! Dużo techniki. Poniżej jest też wersja dla osób bardzo nietechnicznych.]

Podstawową zasadą i siłą Internetu jest to, że dowolny komputer może przesłać dane do dowolnego innego komputera. Dlatego globalna sieć często jest przedstawiana jako „chmura". Z punktu widzenia użytkownika końcowego, Internet jest bowiem taką chmurą w którą z jednej strony pakiety z danymi wpadają a potem „automagicznie" wypadają z niej we właściwym miejscu. Żeby jednak ta „chmura" działała, wszyscy jej użytkownicy – oraz ukryci wewnątrz „chmury" uczestnicy – muszą być fizycznie połączeni. Czy będzie to przewód miedziany, czy łącze radiowe czy też światłowód, zawsze będzie to połączenie fizyczne.

Co jest wewnątrz „chmury"? Z punktu widzenia pakietu do przesłania składają się na tę „chmurę" cztery rodzaje uczestników: detaliczni dostawcy internetu (ISP), hurtowi dostawcy internetu (t-ISP), operatorzy sieci szkieletowej (BB) oraz operatorzy węzłów wymiany, zwanych węzłami IX. Przy czym operator szkieletowy może prowadzić wiele swoich węzłów i uczestniczyć w węzłach prowadzonych przez inne firmy, operator hurtowy może też mieć swoich klientów detalicznych itd. Do węzłów, poza uczestnikami „chmury", są podłączeni też dostawcy usług hostingowych i wielcy dostawcy treści, choć nie są oni uczestnikami „chmury". Pakiet zawsze „wchodzi w chmurę" przez węzeł najbliższy nadawcy i „wychodzi" z niej w węźle najbliższym odbiorcy. Wewnątrz „chmury" jego droga może być różna.

Najkrótsza droga przykładowego pakietu – paczki z zamówieniem danych – może sprowadzać się do jego przesłania tylko przez jeden węzeł do którego są podpięci zarówno ISP jak i dostawca usług hostingowych. Najdłuższa może wieść przez wiele węzłów różnych firm i wiele segmentów sieci szkieletowej.

Żaden dostawca internetu, żadna firma hostingowa czy nawet większy portal nie mogą istnieć w internecie bez podłączenia przez choćby jeden węzeł. Ale też żaden mały dostawca internetu, ani nawet żaden większy dostawca usług hostingowych nie jest podłączony do więcej niż kilku węzłów, ponieważ do węzła musi być podłączony fizycznie światłowodem, co sporo kosztuje. Kosztuje też ruch wychodzący poza węzeł.

> Dla przykładu: zgodnie z podanymi na stronie firmowej danymi, największy z polskich dostawców usług hostingowych uczestniczy w trzech węzłach wymiany krajowej, a ruch z zagranicą wymienia w jednym węźle operatora szkieletowego. Aby tego dostawcę hostingu całkiem odciąć od internetu, nakaz takiego odcięcia musiałby trafić do dokładnie pięciu firm „wyżej".

Ta struktura powtarza się na całym świecie. Obecny Internet to:

Globalna sieć szkieletowa, która jest własnością trzydziestu trzech ponadnarodowych firm:

> (360networks AboveNet AT&T Btnaccess Bell Canada Cogent Electric Lightwave Fiber Network Solutions Global Crossing GlobalNAPs Globix Hurricane Electric IDT Corporation Level3 McLeodUSA MegaPath Multacom Mzima Oxford Networks PPL Telcom Quest (Asia) Qwest Comm. Sago Networks SAVVIS Sonic.net Sprint Wholesale Teleglobe (VSNL) TeliaSonera Telstra Inc. (Asia, USA) Time Warner Telecom Verio (NTT) Verizon Business XO Comm. Xspedius)

Poniżej jest kilka tysięcy firm zwanych operatorami krajowych sieci szkieletowych, dostawcami hurtowymi lub dostawcami tranzytowymi. Firmy te posiadają fizyczną sieć na terenie kraju lub kilku sąsiadujących krajów.

> W Polsce są to np firmy: Exatel GTS Energis NASK Netia TP S.A Tel-Energo TK Telkom

Na samym dole znajdują się średni i mali detaliczni dostawcy internetu. Na całym świecie to około dwudziestu tysięcy firm.

Samych węzłów IX jest kilkaset, z czego 127 jest w Europie.

!!! Wszystkie te węzły, wszyscy operatorzy sieci szkieletowej i hurtowi dostawcy internetu są przyłączeni do osobnej bezpiecznej sieci łączności głosowej INOC-DBA. Na klawiaturze „telefonu" wystarczy wybrać numer sieci z której przychodzi atak (spam malware itp) a system automatycznie połączy nas z osobą odpowiedzialną za tą sieć. Pod tymi „telefonami" zawsze dyżurują ludzie. 24 godziny na dobę, 365 dni w roku. Oni odpowiadają za zarządzanie sieciami. Bardzo nie lubią pedofili. Mogą ich wyłączyć w minutę, jeśli tylko będą mogli to zrobić legalnie. Potrzebujemy prawa, które będzie usuwać zło u źródła.

Podsumowanie „techniki":
Dużo łatwiej jest pedofilskie treści całkiem z internetu usuwać niż blokować. Od co najmniej dziesięciu lat wszystkie potrzebne do tego mechanizmy „szybkiego reagowania" są i działają. Ludzie Internetu, ci administratorzy sami często walczą z pornografami, ale politycy domagają się wdrożenia drogiej, zawodnej i zagrażającej naszej przyszłości kontroli. Sami dystrybutorzy pornografii będą się z blokowania cieszyć: dostaną i mechanizm ostrzegania przed wpadką, i nikt już nie będzie ich zgłaszał.

O działaniu internetu, blokowaniu treści i odcinaniu pedofili dla „poetów i symfoników”.

Podstawowe pojęcia. Jak działa internet**.**

Domena internetowa. Drogowskaz do miejsca w internecie. Np. „**blogi.site*.com***” można wyobrazić sobie jako wskazówkę: „w wirtualnym mieście **com** przy ulicy **site** będzie magazyn stron firmy **blogi**”.

Adres numeryczny IP. Adres zrozumiały dla komputera zapisywany samymi cyframi np. „***1.2.3.4***”.
Działa jak kod pocztowy. Ten sam kod mogą mieć magazyny **blogi.site.com**, **male.slonie.pl**, **www.moto.cc** i inne w tym samym miejscu. Naszemu komputerowi indywidualny adres IP (kod) nadaje dostawca internetu.

Pakiet. Paczka, w której są dane do przesłania w sieci. Na każdej paczce umieszczone są kody nadawcy i odbiorcy. Kod odbiorcy umieszczony jest po to, by adresat wiedział, gdzie zwrotnie odesłać zamówione dane. Nasz komputer domowy taką paczkę z danymi przekazuje przez łącze do **Dostawcy Internetu (ISP)**.

Węzeł. To jest punkt w którym przekazywane są paczki z danymi. W każdym węźle spotykają się światłowody i przewody od wielu różnych firm – dostawców internetu lub dostawców treści.
Każda z firm ma w węźle swoje gniazdo do którego wpięta jest wtyczka łącza od **rutera**. (Zobacz węzeł PLIX).

Ruter. To sortownia paczek. Każdy ruter ma przynajmniej dwa łącza, a każde z nich prowadzi do innego węzła. W jednym węźle ruter paczkę odbiera, w drugim podaje ją dalej. Paczka podawana jest zawsze do tego rutera, który jest bliżej odbiorcy. Pierwszy w łańcuszku jest ruter u ISP do którego przyłączony jest nadawca, ostatni to ruter u ISP do którego bezpośrednio przyłączony jest odbiorca. Do ustalania który ruter i w którym węźle jest bliżej odbiorcy, rutery używają listy, na której podane są: kod sieci odbiorcy i trasa.

Protokół internetowy. Mówi o tym, kto (jaki program) po stronie odbiorcy powinien odebrać paczkę z przesyłką. Np. przesyłka protokołem jako „**http://**” będzie dostarczona w komputerze odbiorcy do „*Pana Serwera WWW*” a protokołem „**ftp://**” - będzie dostarczona do „*Pana Serwera Plików*”.

Adres URL. To dokładne określenie położenia informacji. Np. ”**http://*blogi.site.com/docs/strona.html***„ oznacza że „*w magazynie* **blogi** *położonym przy ulicy* **site** w wirtualnym mieście **com** *w szafie* **/docs/** *znajduje się* **strona.html**. *Zamówienia na tę stronę obsługuje protokołem* **http://** *Pan Serwer WWW*”.

JAK UZYSKUJEMY DOSTĘP DO USŁUGI LUB STRONY W INTERNECIE?

Gdy klikamy na link ”**http://*blogi.site.com/docs/strona.html***„, nasz komputer tworzy zamówienie na stronę, które wygląda tak: „**`GET /docs/strona.html host: blogi.site.com`**”.

Następnie nasz komputer pyta bazę nazw i kodów (czyli *DNS*): „Jaki jest kod dla miejsca „***blogi.site.com***”.
Baza nazw i kodów odpowiada: „***blogi.site.com*** ma kod ***1.2.3.4***”.

Nasz komputer wkłada przygotowane zamówienie do nowej paczki opisanej kodem adresata „*1.2.3.4*”. i przekazuje ją przez łącze (przewodowe lub radiowe) do *rutera* naszego dostawcy internetu. *Ruter* dostawcy przekazuje paczkę w odpowiednim *węźle* ruterowi, który jest najbliżej docelowego miejsca „*1.2.3.4*”. W ten sposób paczka z naszym zamówieniem wędruje przez kolejne rutery i *węzły* aż w końcu trafia do rutera, który bezpośrednio obsługujące miejsce o kodzie „*1.2.3.4*”. To *ruter* końcowy., Ten – znów przez łącze – dostarcza nasze zamówienie do adresata, czyli pana *Serwera WWW* działającego pod IP **1.2.3.4**.

Serwer WWW sprawdza, dla którego z magazynu jest zamówienie (**`host: blogi.site.com`**).
Jeśli magazyn się zgadza, to z szafy **/docs/** w magazynie **/blogi-site-com/** pobierany jest plik **strona.html**.
Kopia pliku zostaje zapakowana do zaadresowanej zwrotnie paczki z odpowiedzią. Zamówiona przesyłka wędruje teraz z powrotem przez *węzły* i *rutery* aż w końcu trafia do przeglądarki, która ją nam wyświetli.

JAK MA DZIAŁAĆ BLOKOWANIE?

Blokowanie wymaga narzucenia wszystkim dostawcom internetu obowiązku dokładnego kontrolowania tego co przesyłają ich klienci. Kontrola ta wymaga zaglądania do wszystkich wysyłanych paczek, i odczytania zawartych w nich treści. Tylko tak można sprawdzić, po jakie informacje (strony czy usługi) chce sięgnąć użytkownik, oraz czy informacje te nie zostały przez rząd zakazane.

W tym celu Dostawca musi odczytać każdy pakiet wysłany przez użytkownika i sprawdzić, czy nie występuje w tym pakiecie żądanie strony czy usługi: (np. żądanie http „**`GET /docs/strona.html host: blogi.site.com`**”).

Jeśli w pakiecie występuje takie żądanie, to Dostawca musi sprawdzić, czy domena lub URL nie zostały przez rząd zakazane. Jeśli żądanie danych nie występuje – pakiet przekazywany jest dalej.

Jeśli domena lub URL występują na liście stron i usług niedozwolonych, to użytkownik będzie przekierowany do innego serwera, który użytkownika poinformuje, że strony lub usługi, do których użytkownik chciał uzyskać dostęp, zostały przez rząd zakazane. Serwer ten może być prowadzony np przez policję lub CBA.

ZAGROŻENIA ZWIĄZANE Z BLOKOWANIEM.

Nawet jeśli serwer taki (np 6.6.6.6) nie byłby prowadzony bezpośrednio przez agencję rządową, to zgodnie z prawem o retencji danych, operatorzy będą musieli przechowywać i udostępniać na życzenie policji informacje o użytkownikach, którzy łączyli się do serwera **6.6.6.6**. „Przy okazji" filtrowania uzyskujemy więc gotową listę osób, które w ostatnich dwóch latach były zainteresowane zakazanymi przez rząd informacjami lub usługami.

Raz wprowadzony mechanizm zaglądania do treści wędrujących w paczkach może być w przyszłości użyty także do wyszukiwania jakichkolwiek innych wyrazów lub zdań. Można będzie – już bez blokowania – rejestrować kto i do jakich treści uzyskuje dostęp.

Teraz Policja i służby mają dostęp tylko do danych o adresach numerycznych, nie zaś do samej treści zamówienia na dane. Mechanizm blokowania może więc umożliwić retencję także danych o dostępie do określonych treści lub nawet rejestrowanie tego, czy w korespondencji używamy określonych słów.

==========

Marzec 2011

Wojciech S. Czarnecki.
[mail: ohir at fairbe.org]