

Vrtulník s termokamerou

Termokamera zachytí a zobrazí kde co v řádu až setin stupně, podstatné ale je, jak obraz vyhodnotí lidská obsluha. Při přeletu vrtulníku monitor ukazuje neustále obrovské množství teplotních rozhraní, změn a výkyvů a je jen na obsluze, co konkrétně hledá a jak umí zobrazovanou teplotní mapu přečíst.

Absolutně se to nedá zobecnit. Vyhodnocuje se celková složená informace vyplývající z teploty hledaného objektu, jeho velikosti, případného pohybu, tvaru atd.

Podstatné je také zadání vyhledávání, hledají se jiné markanty pokud se pátrá po živých osobách v zalesněném terénu, jiné to je při pátrání po mrtvole a něco zcela jiného je zase vyhledávání nelegální pěstírny marihuany v městské zástavbě.

To vyhledávání potápěče je značně komplikovaná odpověď. Do hloubky cca 0,5m stojaté vody je lidské tělo vidět na kameře krásně, hlouběji záleží na proudění. Ve stojaté vodě může voda ohřátá od těla potápěče vytvořit místní, víceméně ohraničenou teplotní anomálii na termu dobře viditelnou. Otázkou zase ale je, jak ji vyhodnotí obsluha termokamery. Zda jako člověka, nebo třeba jako tlející pařez atd. Myslím, že cca od dvou metrů hloubky v rychleji proudící vodě, je termokamera bez šance.

Voda je vůbec všeobecně dobrý ochranný materiál. Potápěči v třímetrové hloubce neublíží ani výstřel z Odstřelovačky vz.96 FALCON bezprostředě od hladiny.

Detektor lži

Typický test na detektore lži, polygrafe pozostáva z otázok rozdelených do troch skupín na:

1. Irelevantné otázky, ako napríklad: "Aký dnes máme deň?"

-tie sa dajú odpovedať pravdivo a bez stresu

2. Relevantné otázky, ako napríklad: "Spáchali ste čin z ktorého ste obvinený?"

- odpovedajú vinný i nevinný rovnako NIE

3. Kontrolnej otázky

- sú formulované naproti tomu tak aby na ne obvinený, testovaný nemohol dať zápornú odpoveď, bez pocitu zlého svedomia napríklad:

"Zranili ste niekedy úmyselne niekeho človeka?"

Pri vlastnej skúške, ktorá trvá desať až pätnásť minút vychádzajú vyšetrovatelia z toho, že na testovanom vinníkovi sa prejavujú známky stresu, pokiaľ podľa očakávania odpovedá na Relevantné otázky "NIE".

Zostáva však relatívne kludný keď odpovedá na Kontrolné otázky.

U nevinného by mala byť reakcia presne opačná

klud pri Relevantných otázkach, a ľahký stres pri Kontrolných otázkach.

Rozrušenie testovaného sa zisťuje tromi rôznymi spôsobmi:

1. spôsob - elektródy na rukách merajú elektrickú vodivosť pokožky, ktorá sa mení podľa množstva vylučovaného potu

2. spôsob - manžeta na paže zisťuje krvný tlak a pulz

3. spôsob - dva pásy na hrudníku zaznamenávajú hĺbku dýchania

Pri klamaní dochádza k - zvyšovaniu vodivosti pokožky

- dych je menej hlboký

- stúpa krvný tlak

Tieto veličiny vyhodnotí počítač. O výsledku rozhoduje:

70% vodivost' kože

20% dýchanie

10% krvný tlak

V závislosti od procedúry je metóda omylná do 30%.

CHURÁŇ, Milan a kolektív: Encyklopedie špionáže , Nakladatelství Libri,

Praha 2000 , ISBN 80-7277-020-9

na strane 97 sa zmieňuje o metóde ako oklamať polygraf :

"Jednou z metód, jak toho dosáhnout, byl proslulý "špendlík" (v bote a pod.), který si vyslýchaný při neutrální otázce zabodl, aby nastartoval "prudké" reakce.

"Oblafnutí" detektoru se dělá metodou informačního zahlcení. Je to stejné jako se znehodnocování kriminalistických stop na místě (vašeho) činu.

Pokud někde někoho zabiju a poteče při tom krev, bude velmi pravděpodobné, že se mi nepodaří odstranit všechny stopy krve a i ty nejmenší kapičky vyšetřovatelé najdou...

Pokud si ale sebou vezmu kanystr třeba hovězí krve, místo činu důkladně vyčistím a zbavím všech krevních biologických stop které dokážu sám najít (UV lampa ve výbavě samozřejmostí) a následně po místnosti pečlivě rozčákám deset litrů zvířecí krve (lidská se shání o dost hůř a je to drahé - mít známého v krevní bance...), tak mám pravděpodobnost hraničící s jistotou, že kriminalisté případnou pravou stopu, co jsem eventuelně ještě neodstranil, prostě nenajdou.

Stejně je to s detektorem.. Detektor neodhaluje lež ale určité reakce těla. Tyto reakce nelze potlačit, ale lze je simulovat.

Příklad:

Těžko asi potlačíte výkřik, když vás někdo nečekaně píchne rozžhaveným hřebíkem. To prostě většinou nejde překonat.

Prakticky stejný výkřik ale můžete sami vydat kdykoliv o své vůli, i když vás nikdo ničím nepíchne. Pocit bolesti prostě simulujete.

No a na tom je založeno ne OKLAMÁNÍ ale ZAHLCENÍ detektoru lži. O svoje reakce na ožehavé otázky se VÚBEC NESTARÁTE!!! Klidně ať detektor ukazuje, že v té konkrétní věci nemluvíte pravdu.

Naopak se soustředíte na produkování klamných "lživých reakcí" na běžné otázky.

Potom přístroj ukazuje tělesné reakce obvyklé pro lež nebo rozrušení i při odpovědích na věci, které jsou prokazatelně pravdivé. Celý test na detektoru je potom NEPRÚKAZNÝ a tudíž naprosto nepoužitelný jako důkaz.

Produkování klamných reakcí je jednodušší, než by se mohlo zdát. Stačí si ve svém životě vybavit jednu dvě věci, kdy vám hrozil skutečný průser. Podvedli jste svoji ženu? Osahávali jste nějaké dítě? Okradli jste svého zaměstnavatele?

Tak si prostě představujte, co by se dělo, kdyby se na to přišlo. Pokaždé, když se vám vybaví možné následky, produkuje váš mozek emoční vlny totožné s emočními vlnami jako když nemluvíte pravdu.

A nebo si při testu na detektoru u některých otázek zkuste živě vybavit, jak by to asi vypadalo, kdyby chlap co ho nenávidíte, někam zatáhl a ojel vaši ženu. Představte si to v živých barvách, jak z ní stahuje gatky, ona křičí, on to do ní s hekáním cpe, važe žena začíná potupou brečet, on ji trochu proliská, aby byla povolnější, sprostě jí nadává zatímco ji přirážá.

Pak se do ní s hekáním udělá, vrazí ji facku a utře si penis do jejích roztrhaných šatů. Vaše žena je zraněná, pošpiněná, vyděšená a pravděpodobně i oplodněná...

No? Představujete si? ...a už cítíte ten odpor ve vaší hlavě, ...horké tváře, nastupující vztek? Cítíte to?

No a teď si představte, co takto vyvolané pocity udělají s rafičkama detektoru...

Jinak jako u každého výsledku, tak i u výsledku na detektoru platí zlaté pravidlo:

"Mlčení je nejlepší advokát!"

Policejní sledování světové počítačové sítě

Každý uživatelův krok světem Internetu je zaznamenán na navštívených webových serverech, odkud lze poté zpětně zjistit některé potenciálně citlivé informace. Na vině jsou automaticky předávané HTTP hlavičky, které dokáží prozradit řadu údajů.

Otestovali jsme v praxi možnosti utajení webového surfování a vyhodnotili anonymitu nejen podle logu testovacího webového serveru.

1. [Šifrování](#)

Každý během svého putování Internetem občas touží po takové míře soukromí, aby jeho kroky byly co možná nejméně vystopovatelné. Cest, kterými toho lze dosáhnout, existuje hned několik. Řádky tohoto dvoudílného článku se zaměří na představení a test následujících technik:

- **Specializované aplikace** – povětšinou jednoúčelové programy, které se instalují na klientský počítač a dovolují maskovat surfařovu identitu.
- **Veřejné proxy brány** – volně dostupné servery, jichž lze využít pro surfování Internetem a které pomáhají při utajení.
- **Webové anonymizéry** – takové stránky WWW, které zprostředkovávají anonymní přístup na cílový server.

Úvod do problematiky anonymizérů a soukromí při surfování webem: [Máte co skrývat?](#)

Podíváme-li se na oblast anonymního surfování z pohledu přenášených dat, pak soukromí může být chráněno zejména blokováním některých HTTP hlaviček. Díky nim lze totiž poměrně snadno zjistit některé podstatné informace o vašem prohlížeči, IP adrese, použitém proxy serveru apod. Zde jsou příklady těch hlaviček, které nás budou při dalším zkoumání anonymního surfování obzvláště zajímat:

- REMOTE_ADDR – udává IP adresu počítače, který se připojil. Při běžném surfování tak webový server získá přesnou identifikaci vašeho stroje, anonymní surfování by mělo zajistit změnu originální hodnoty.
- REMOTE_HOST – název připojivšího se počítače. V případě anonymního surfování by se také zde měla objevit jiná hodnota, než která odpovídá vašemu stroji. Jak u REMOTE_ADDR, tak REMOTE_HOST samozřejmě závisí na typu připojení – zda k Internetu přistupujete přímo, nebo prostřednictvím některého poskytovatele (tedy například nemáte vlastní veřejnou adresu).
- REFERER – udává adresu předchozí stránky, z níž uživatel přišel. Typickým příkladem mohou být webové vyhledávače.
- USER_AGENT – dovoluje webovému serveru zjistit, který internetový prohlížeč používáte, navíc připojuje také některé další podrobné informace. Příklad prozrazených informací v případě nepříliš anonymního surfování může vypadat například takto:
Mozilla/5.0 (Windows; U; Windows NT 5.1; cs-CZ; rv:1.7.12) Gecko/20050919 Firefox/1.0.7.

Následující kategorie HTTP hlaviček souvisí zejména s přístupem na web prostřednictvím proxy serveru, v případě skutečně anonymního surfování by neměly být předávány hodnoty:

- HTTP_VIA – poskytuje informace o použité proxy bráně, textový řetězec může obsahovat například název odpovídajícího serveru, IP adresu, na které naslouchá apod. Ukázková hlavička jednoho z transparentních proxy serverů:
1.0 squid.hartcom.net:3128 (squid/2.5.STABLE3).
- X_FORWARDED_FOR – skutečná IP adresa klienta, může obsahovat hodnotu privátní adresy v lokální síti.

Pokud si chcete sami ověřit, co o vás druhá strana ví, můžete využít služeb některého z řady online testů soukromí. Za všechny jmenujme například [PC Privacy Test](#) na serveru 2Privacy.com či [Proxy Judge Test](#) ze stejného umístění. Druhá kontrola poskytuje výstup přímo v podobě jednotlivých, výše představených HTTP hlaviček – podobně tomu je také v případě [testu](#) na Tools.rosinstrument.com. V rámci našeho testování jsme se nejprve zaměřili na skupinu specializovaných aplikací, jmenovitě utility Steganos Internet Anonym 2006, ArchiCrypt Stealth, WinSweep a GhostSurf. Přístup k jednotlivým HTTP hlavičkám jsme získali díky využití logů jednoho ze serverů vydavatelství Internet Info. V případě neanonymního přístupu z neveřejné IP adresy linkou Karnevalu záznam vypadal následovně:

```
proxy1.karneval.cz - - [10/Jan/2006:16:18:40 +0100] "GET /akce.phtml?ukaz=autori HTTP/1.0" 200
11598 "Mozilla/5.0 (Windows; U; Windows NT 5.1; cs-CZ; rv:1.7.12) Gecko/20050919 Firefox/1.0.7"
```

X-Forwarded-for="10.76.131.100" Accept-Language="cs,en-us;q=0.7,en;q=0.3" Remote-Addr=81.27.192.18

Předán tedy byl název počítače proxy1.karneval.cz, detailní informace o použitém prohlížeči, hlavička X_FORWARDED_FOR odhalila privátní IP adresu a ušetřena nebyla ani položka REMOTE_ADDR. Díky názvu počítače s jeho IP adresou je možné snadno zjistit, že uživatel je klientem Karnevalu. To není zase tak špatný výsledek, z pohledu anonymity na tom jsou totiž nejhůře majitelé veřejných IP registrovaných na svou osobu - na každém webovém serveru pak zanechají prakticky svůj podpis. Hlavička obsahující popis použitého prohlížeče a operačního systému sama o sobě přímé riziko nepředstavuje, potenciálně však může dobře posloužit při bližší identifikaci uživatele a stroje, případně cíleném zneužití zranitelnosti v odpovídajícím softwaru. Každé odhalení privátní IP adresy v hlavičce X_FORWARDED_FOR napovídá o struktuře vnitřní sítě a IP je vázáno přímo na konkrétního uživatele (jako v tomto případě fyzického zákazníka Karnevalu).

Steganos Internet Anonym 2006

Homepage: Steganos.com

Screenshots:



Tato zajímavá a snadno použitelná utilita od renomované společnosti Steganos využívá sítě anonymních proxy serverů, které dovoluje střídat dokonce po jedné vteřině. Ve výpisu webového logu se pak objeví pouze název použitého proxy serveru spolu s odpovídající IP adresou.

Steganos Internet Anonym dále nedává příliš šancí ani informacím hlavičky REFERER, zamezit lze také předávání informací USER_AGENT – kamufláž referuje pouze řetězec Anonymized by Steganos Internet Anonym 2006. Kompletní struktura logovaných údajů na našem serveru vypadala následovně:

```
ce7305-or-mde.orbitel.net.co - - [11/Jan/2006:09:49:50 +0100] "GET / HTTP/1.0" 302 0 "-"  
"Anonymized by Steganos Internet Anonym 2006" X-Forwarded-for="-" Accept-Language="cs"  
Remote-Addr=200.30.79.126
```

Bližším zkoumáním lze zkritizovat i vložení řetězce Anonymized by Steganos Internet Anonym 2006 - nikdo přece nemusí být explicitně upozorňován na to, že se skrýváme... Naopak z uvedené IP adresy cizího serveru štouhal o naší osobě příliš nezjistí. O něco horší je to v případě neodstraněné hlavičky ACCEPT_LANGUAGE, kde alespoň přibližnou lokaci napovídá označení "cs". Rychlost surfování dosahovala i při jednovteřinové rotaci proxy serverů slušných výsledků. Steganos Internet Anonym 2006 podporuje funkci optimalizace použití proxy serverů, kdy v předem stanovených časových intervalech kontroluje jejich rychlost.

ArchiCrypt Stealth

Homepage: Archicrypt-shop.com

Screenshoty:



Anonymizér ArchiCrypt Stealth zpočátku potěší především snadností obsluhy, posléze také schopnostmi skrýt uživatelskou identitu. Pro korektní funkčnost je zapotřebí změnit nastavení webového prohlížeče na surfování skrze proxy na localhostu (127.0.0.1) a implicitním portu 8080 (lze změnit). ArchiCrypt pak již sám přeměruje komunikace trasou přes vhodný anonymní proxy server.

Příjemná je možnost úmyslné modifikace některých hlaviček, viz například ukázka z testovacího logu:

```
210.91.119.199 - - [10/Jan/2006:16:52:28 +0100] "GET /style.css HTTP/1.1" 200 1021  
"http://www.woko.cz/akce.phtml?ukaz=autori" "prohlizec" X-Forwarded-for="yahoo.com,  
microsoft.com, netscape.com, aol.com" Accept-Language="ak" Remote-Addr=210.91.119.199
```

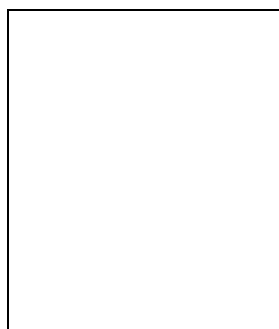
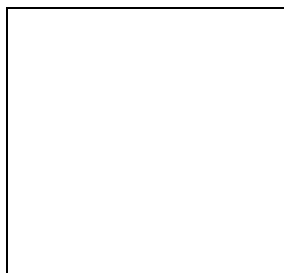
Název i IP adresa počítače jsou opět pozměněny ku prospěchu anonymity surfaře, úspěšně dopadlo také podvržení hlaviček USER_AGENT (prohlizec), X_FORWARDED_FOR či ACCEPT_LANGUAGE. Díky možnosti změny těchto údajů dokáže být surfování nejen anonymní, ale také méně nápadné na první pohled - například v kontrastu s výše uvedeným upozorňováním Anonymized by Steganos Internet Anonym 2006.

Surfování bohužel nebylo natolik svižné jako v případě Steganos Internet Anonym 2006 (alespoň s automaticky použitým proxy serverem během testu).

WinSweep

Homepage: Winsweep.net

Screenshoty:



Aplikace WinSweep slouží pro komplexnější úklid počítače a blokování reklam, mezi jeho funkcemi však nechybí ani možnost anonymního surfování skrze automaticky použité proxy servery. Pro nastavení webových prohlížečů si vytvoří skript automatické konfigurace a námi získané hlavičky vypadaly následovně:

```
83.175.203.222 - - [10/Jan/2006:17:23:10 +0100] "GET /akce.phtml?ukaz=autori HTTP/1.0" 200
11598 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; cs-CZ; rv:1.7.12) Gecko/20050919
Firefox/1.0.7" X-Forwarded-for="-" Accept-Language="cs,en-us;q=0.7,en;q=0.3" Remote-
Addr=83.175.203.222
```

S odstraněním hlavičky o použitém prohlížeči si WinSweep problémy nedělá, přímo z programu přitom uživatelé nečekají prakticky žádné možnosti nastavení anonymního surfování a výjimkou nejsou ani problémy s funkcími používaných proxy serverů.

WinSweep tedy naplňuje označení multifunkčního programu, kdy si širší nabídka možností vybrala svou daň právě na síle utajení - ze záznamu lze bohužel vyčíst použitý operační systém, odtušit přibližnou lokaci uživatele a získat přesné označení použitého prohlížeče...

GhostSurf 2005 Standard

Homepage: Tenebril.com

Screenshoty:



Tato utilita začínající uživatele dostatečně ochrání s pomocí implicitní konfigurace anonymního surfování, záznam našeho testovací web logu neodhalil prakticky žádné informace:

```
ev1s-66-98-226-42.ev1servers.net - - [10/Jan/2006:17:11:16 +0100] "GET /akce.phtml?ukaz=autori HTTP/1.0" 200 11598 "-" "-" X-Forwarded-for="-" Accept-Language="-" Remote-Addr=66.98.226.42
```

Jediné, co lze ze záznamu vyčíst, jsou název a IP adresa použitého serveru, zbytek hlaviček byl úspěšně odstraněn. Pokročilí uživatelé mohou přímo specifikovat libovolné hlavičky, které chtějí blokovat. GhostSurf se jeví jako univerzální řešení pro anonymní surfování, jelikož jak ve svém standardním nastavení, tak zejména s pokročilým blokováním libovolných hlaviček neprozradí o uživateli zhora nic.

Všechny testované aplikace si ohledně anonymizace uživatele vedly relativně dobře, do určité míry pokulhával pouze program WinSweep. Snadností použití se vylíhl Steganos Internet Anonym 2006, dvojice GhostSurf 2005 Standard a ArchiCrypt Stealth zase potěší možností ruční modifikace či blokování jednotlivých HTTP hlaviček. Příští díl se zaměří na možnosti anonymizace připojení bez nutnosti instalace specializovaných aplikací a zároveň shrne získané výsledky v podobě žebříčku.

Řádky tohoto pokračování navazují na [první díl](#), kde se můžete dočíst o základních technikách anonymního surfování, souvisejících HTTP hlavičkách a výsledcích testu specializovaných aplikací. Posledně zmiňovaná skupina programů vyžaduje instalaci na klientský počítač, což je ne vždy možné, existují proto další řešení, jak putovat světem Internetu anonymně – řeč bude o anonymních proxy bránách a webových anonymizérech.

Na Internetu existuje nepřehledné množství více či méně aktuálních seznamů anonymních proxy serverů, jejichž služeb může využít každý uživatel. Stačí k tomu mít oprávnění pro změnu konfigurace webového prohlížeče a nastavit odpovídající IP adresu, samozřejmě doplněnou o číslo portu. Abychom stále nechodili kolem horké kaše, ukázkové a pravidelně aktualizované seznamy si prolistujte například na

Publicproxyservers.com či Samair.ru. Posledně jmenovaný seznam rozlišuje jednotlivé proxy servery na "anonymous" a "elite", které se liší v míře utajení:

- anonymous blokuje pouze hlavičku HTTP_X_FORWARDED_FOR, takže nebude možné zjistit vaši skutečnou IP adresu,
- elite odstraňuje trojici hlaviček HTTP_X_FORWARDED_FOR, HTTP_VIA a HTTP_PROXY_CONNECTION, podle záznamu tedy vzdálená strana nebude schopna ani zjistit použití proxy serveru.

Ačkoliv jsou seznamy anonymních proxy zpravidla velice obsáhlé a přehledně strukturované, nalezení funkčního a pro příjemné surfování dostatečně rychlého serveru bohužel může zabrat hodnou chvíli. Srovnáme-li míru utajení se specializovanými aplikacemi představenými v minulém dílu, veřejné proxy servery sice nevyžadují instalaci žádného programu, nicméně jejich schopnosti odstranění hlaviček jsou zpravidla na mnohem nižší úrovni.

Specializované aplikace testované v prvním dílu vyžadovaly instalaci na klientský počítač, výše zmíněné anonymní proxy servery zase změnu konfigurace webového prohlížeče. Oběma mezikrokům se lze vyhnout použitím online anonymizérů, tedy internetových stránek provádějící utajení "ad hoc". Opět jsme vyzkoušeli přístup na náš testovací server Woko.cz, a sice s použitím anonymizérů, které jsou zdarma (byť třeba s omezenou funkcí) a ani nevyžadují žádnou registraci.

Anonymouse.org

Prvně testovanou se stala stránka Anonymouse.org, která nenabízí žádné volitelné možnosti nastavení utajení, a automaticky tak zpracuje zadané URL. V našem logu jsme pak našli následující hlavičky, které toho skutečně mnoho nevyzrazují:

```
85.195.119.22 - - [10/Jan/2006:16:21:01 +0100] "GET /akce.phtml?ukaz=autori HTTP/1.0" 200 11598  
"- "http://Anonymouse.org/ (Unix)" X-Forwarded-for="unknown" Accept-Language="-" Remote-  
Addr=85.195.119.22
```

[Proxy Judge Test](#) odhalí v hlavičce HTTP_VIA i použití odpovídajícího proxy serveru, [Privacy Test](#) příliš podrobností nevystopuje. Drobnou výtku bychom mohli mít proti explicitnímu uvedení použitého anonymizéru mezi hlavičkami. Anonymouse.org při anonymním přístupu na stránku zobrazí uprostřed okna reklamu, která se však dá jediným kliknutím zavřít.

[Proxify.com](http://proxify.com)

Server Proxify.com automaticky kamufluje informace hlavičky USER_AGENT, tedy údaje o použitém webovém prohlížeči, svou přítomnost pak dává najevo zobrazením banneru v horní části navštívené stránky. Disponuje funkcí kódování URL, takže například přístup na www.seznam.cz je proveditelný skrze odkaz

<http://proxify.com/p/011110A1000110/687474703a2f2f777772e73657a6e616d2e637a2f>

Výhoda kódování URL spočívá zejména v tom, že například váš ISP podle záznamu okamžitě nezjistí, na kterou stránku jste přistupovali. Zdarma dostupná verze bohužel nedovoluje přistoupit na žádný ze serverů, které testují funkce anonymních proxy serverů.

[Pureprivacy.com](http://pureprivacy.com)

Test tohoto anonymizéru [odhalil](#) informace o klientském operačním systému i detailní údaje týkající se použitého webového prohlížeče. To není nejlepší výsledek, protože například podle použitého jazyka by bylo možné odhadnout přibližnou lokaci uživatele. Naproti tomu skutečná IP adresa i hlavička REFERER byly odstraněny beze stop, PurePrivacy automaticky odstraňuje veškeré obrázky z cílové stránky. Svou rychlostí spadá do kategorie pomalých.

Na Internetu je zdarma k dispozici velké množství serverů, které zprostředkovávají anonymní přístup na zadané stránky, můžete vyzkoušet rychlost, spolehlivost a bezpečnost například následujících zástupců:

[Guardster.com](http://guardster.com) - skrývání HTTP hlaviček REFERER a USER_AGENTM, možnost blokování skriptů, obrázků, cookies, kóduje cílovou adresu a zobrazuje reklamní banner v horní části obrazovky. Výsledky [Proxy Judge Test](#) a [Privacy Test](#) ukazují, že nedošlo k úplnému odstranění hlavičky USER_AGENT, nicméně plné detaily nevyzrazuje. Naopak zjistit lze verzi použitého operačního systému.

[Anonymizer.com](http://anonymizer.com) - spolehlivý anonymizér, který neprozradí prakticky žádné hlavičky – viz výsledky testů [Stealthtests.lockdowncorp.com](http://stealthtests.lockdowncorp.com), [Proxy Judge](#) a [Privacy Test](#). Ze získaných informací není možné vyčíst informace o použitém prohlížeči, operačním systému ani detailní údaje týkající se použití proxy serveru.

Pokud chcete vyzkoušet některé další anonymizéry, relativně obsáhlý seznam naleznete například na Kryptonian-x.blogspot.com. Na základě námi získaných výsledků jsme všechny testované aplikace i online anonymizéry ohodnotili v několika kategoriích a vytvořili následující finální žebříček:

Žebříček anonymizérů

Příčka	Anonymizér	GUI	Anonymita	Rychlost	Typ	Licence
1.	GhostSurf 2005	1	1	2	Aplikace	Shareware
2.	Steganos Internet Anonym 2006	1	2	1	Aplikace	Shareware
3.	ArchiCrypt Stealth	1	1	3	Aplikace	Shareware
4.	Anonymizer.com	2	1	2	WWW	Omezeně zdarma
5.	Proxify.com	3	1	1	WWW	Omezeně zdarma
6.	Anonymouse.org	2	2	2	WWW	Omezeně zdarma
7.	WinSweep	2	3	3	Aplikace	Shareware
8.	Guardster.com	3	2	3	WWW	Omezeně zdarma
9.	Pureprivacy.com	3	3	4	WWW	Omezeně zdarma

Poznámka: Hodnocení probíhalo jako ve škole (1-výborně, 5-nedostatečně), u online anonymizérů jsme ve sloupci GUI zohledňovali objem automaticky zobrazené reklamy.

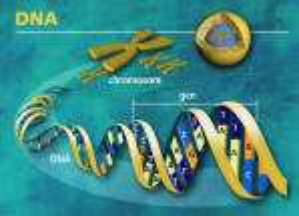
Míra ztráty soukromí působí údiv

Kam dnešní ztráta soukromí došla svými technologiemi i rozsahem, to by již nevymyslel žádný scénárista. Realita překonává veškerá očekávání a nejdivočejší sny.



Když jsem zkoumal podklady pro tento text, napadlo mě jediné - "jsme totálně ztraceni", výstižně řečeno. Zapomeň na soukromí, zapomeň na svobodu a pozorně poslouchej, v jak podivném a profízlovaném světě žiješ. Kecy o demokracii a svobodě platily možná počátkem 90. let, ale dnes je situace naprosto jiná. Každým rokem je to horší a závažnější, ten kdo je bit, je občan. Zase, odpusť si řeči o tom, že nic neděláš a proto je ti to jedno.

Měl bys vědět, že jsou o tobě permanentně sbírány stohy informací a bude-li třeba, budou fest použity proti tobě, že se ti protočí panenky. O to jde. Nelze si krátkozrace



říkat, že se tě problém netýká, smést ho ze stolu a vesele si žít ve svých snech o svobodě. Pak jednou uděláš sebemenší chybičku a okamžitě máš klepeta, jako nikdo druhý. Ber to tak, že pomalu, ale jistě míříme v těch příslovečných čipům v hlavách, co budou skenovat tvoje myšlení - ostatně, proč by sis ho do té hlavy nedal, když jsi nevinnej a tudíž ti jeho existence může být lhostejná? Pořád ti nedocvakává, oč tu jde? Kontrola, tichý sběr informací o tobě ze všech možných hledisek, který způsobí, že tvoje chování, činy i vlastnosti bude někdo zcela přesně znát a pak mi již neříkej nic o svobodě. Pojďme si povědět více o tom, jaké strašlivé možnosti dnes Velký bratr má a samozřejmě je s chutí používá.

Začnu tím nejzásadnějším hard-core, proti kterému naprosto není obrany a jeho důsledky jsou natolik závažné, až se člověku zamotá hlava. Je to **DNA**, resp. možnosti, které poskytuje dnešní věda ohledně její analýzy. Více jsem se o tomto fenoménu zmiňoval v článku **DNA jako ultimátní nástroj identifikace**, ale bohužel pro tebe je identifikace podle DNA jen vrcholek ledovce. Mnohem závažnější je, že kdosi je zcela bezpečně schopen poznat tvou povahu, vlastnosti, slabiny, sklon k nemocím a problémům, genetické zatížení, prostě má tě přečteného, jako kdyby ti pitval mozek. Ach, zapomeň na nějaké rodokmeny a podobné směšné věci! Zapomeň na psychologické zkoumání tvou mysl! Zde jsi naprosto nepotřebný. Tyto výsledky nezfixluješ, nemůžeš je ovlivnit a ví se o tobě obrovské kvantum věcí, které nevíš ani ty sám!

Ostatně, přečti si uvedený článek a sám si udělej obrázek. Problém je ještě aktuálnější, protože právě ve dnech psaní tohoto článku se jako duch zjevila jakási soukromá (!) společnost, která se jmenuje "**Forezní DNA servis**" a hrdě nabízí různé zajímavé (sic!) služby, které jsou podmíněny maličkostí, odevzdáním tvého vzorku DNA. FDS se nijak netají databázovým zpracováním vzorků a dokonce deklaruje vznik jakési "genetické mapy národa", do které můžeš přispět. Naprosto irelevantní je její chabá obrana o tom, že osobní údaje o lidech jsou odděleny od DNA dat. Asi cítíš, jaké masivní možnosti se tu nabízejí a pozor, již zde nemluvíme o nějaké veřejnoprávní "zločinecké" databázi DNA, ale o aktivitách čistě soukromého subjektu, který nějakým zázrakem vesele prošel pod ostřížím zrakem úřadu na ochranu osobních údajů. Si vezmi, ty se tu dnes bráníš publikaci svého rodného čísla, přitom nějakým podnikatelům stačí mikrokapka tvé sliny na špejli, aby věděli i to, co sám nevíš. Tak co, půjdeš tam a dáš jim ten vzorek? Ihned se vynořují otázky, zda se ty údaje nedají zneužít např. na obchod s lidskými orgány, naprosto nechápu, jak mohl stát dovolit podnikání soukromému subjektu v tak choulostivé a zásadní činnosti. Rozhodně bude třeba činnost společnosti Forezní DNA servis pozorně sledovat a snad i nějací osvícení občané začnou proti jejím aktivitám legálně bojovat. Protože toto je skutečný boj o svobodu. Nikdo neví, zda se skutečně do databáze dostanou jen "dobrovolné" vzorky, protože jak píšou ve výše uvedeném článku, pro získání DNA stačí doslova mikroskopická část či sekret tvého těla a jak doba bude pokračovat, bude potřeba část ještě menší a menší. Nakonec se posadíš na židli či vezmeš za kliku a mají tě. Natož se napít ze sklenice či podepsat nějaký papír. Kdo ví? Třeba časem vzniknou regulérní bezdrátové scannery, které budou vzorky sbírat BEZ jakéhokoliv kontaktu osoby?

DNA je zkrátka velký průser dnešní doby a dávej si na něj pozor. Podcenění bude znamenat přímé i nepřímé důsledky. Proti údajům DNA bude klasická policejní práce čajíčkem pro batolata, protože objem takových informací nikdy nebude tak extenzivní, hluboký a precizní - omyl je zcela vyloučen. Jednou se jistě psychologické profily lidí nebudou dělat pomocí psychologického vyšetření, ale jen podle DNA. U soudu pak budeš jistě zírat, co se o sobě dozvíš. A zmást nějak ten soud, aby jsi získal výhodu na svou stranu? Zapomeň.



Druhá věc jsou rozhodně **kamerové systémy**. Stejně jako DNA se jim totiž nemůžeš bránit (protože po ulici chodit musíš), zatímco čipy a počítače užívat nemusíš, o nich bude řeč dále. O tom, že nás sleduje čím dál více kamer, se ví. Mnohé lidi by ale

překvapil předně skutečný rozsah tohoto sledování a zejména, schopnosti těchto zařízení. Vezmi si, že běžný automatický úsekový radar, jako je třeba v Praze na Jižní spojce, naprosto bez problému automaticky vyhodnotí SPZ i typ vozidla. Tyto OCR systémy (systémy optického rozpoznávání) udělaly za poslední roky výrazný skok kupředu a nejhorší je, že jejich současné možnosti nikdo nezná. Co když jsou s to identifikovat i lidi? Představ si kvalitní kameru s dobrým OCR softem, který v sobě má uloženy údaje z tvé DNA. Pak se projdeš pod kamerou a systém okamžitě ví, kdo jsi a že jsi to právě ty, aniž by viděl občanku či kameru sledoval živý operátor! Může dát neprodlenou hlášku švestkám, i tiše dál sbírat údaje. Kam půjdeš dál? Co tam budeš dělat? S kým se setkáš? Třeba kamery u vstupů do nákupních center jsou jen počátkem a uvnitř jsi skutečně jak v reality show Velký bratr, protože nákupní centra jsou jak očividnými, tak skrytými kamerami prošpikována. Ostatně, jeden obrázek je více, než tisíc slov.



Co si myslíš, že to je? Lampička? Kdepak, kamaráde. Kvalitní panoramatická kamera s vysokým rozlišením a možností značného optického přiblížení, je-li to třeba. Snímá tedy prostor celých 360 stupňů. Takové kamery visí nad vchody do nákupních center, ale kdepak těsně nad nimi, aby viděli jen ty, kdo vcházejí. Zabírají totiž široké okolí, což je již samozřejmě ilegální. Ostatně, podívej se na následující obrázek a posuď sám, zda ještě tyto kamery sledují jen vchod.



Tesco, Praha, Národní třída. Kdo to místo zná, při pohledu na umístění kamer jasně chápe, jaký dosah a možnosti tyto kamery mají. Jednoznačně kontrolují celou tuto pražskou tepnu. Čí jsou? Státní, městská policie? Soukromá firma? Nevíš. Jdi se zeptat na ouřad, čí jsou. Co myslíš, že ti bude odpovězeno? Foto: Big Brother Awards



Nezapomínej ovšem ani na nejnovější "srandu", kterou jsme si zaplatili z daní - ano, jedná se o nechvalně známý **systém elektronického mýtného**, který kromě nevzhledných kovových konstrukcí na silnicích a dálnicích přinesl i novou kvalitu ohledně sledování všech projíždějících vozidel. Ostatně jak si myslíš, že mýtná brána pozná osobák od nákladáku a jeho SPZ? Opět jsme u sofistikovaných OCR systémů. Nejsou-li mýtné brány využívány ke šmírování veškerého provozu nyní, budou brzy. Začne to sledováním rychlosti všech aut a skončí to důkladným analyzováním pohybu vozidel. O celé záležitosti je více psáno v článku **Možnosti mýtných bran - nezapomínej na ně**, kde se dozvíš další rozměry této akce.



Dalším hitem dneška je pochopitelně používání rozličných elektronických zařízení, jako jsou **počítače, mobilní telefony a GPS systémy**. Jasně, teoreticky bys je používat nemusel, ale kdo to udělá? Jisté je, že mobilní telefon je absolutně dokonalá nejen štěnice, ale i precizní možnost zaměření osoby, sranda je, že si ho do té kapsy strčíš zcela dobrovolně a systémy tiše a vytrvale sbírají údaje o tvém pohybu a činnosti. Vše, kam se pohneš či s telefonem uděláš, se archivuje a vyhodnocuje.

Spolupráce operátorů s bezpečnostními složkami se ani nedá nazvat úzkou, to je pokrevní propojení. Nějaká soudní povolení? Ach, kde žiješ. Vše se dá navléct na "bezodkladnost" a stejně se v tom nikdo rýpat nebude. Občas sice nějaký opoziční poslanec rozkalí vodu, kolik že je u nás odposlechů, ale velmi záhy to zase zapadne a jede se vesele ve starých kolejích.

Jenom ti připomínám, že kromě perfektní možnosti tvé lokalizace pomocí SIM-karty (*IMSI - International Mobile Subscriber Identity*) jsi identifikován taktéž podle čísla *IMEI* telefonu a je otázka, podle čeho všeho dalšího, protože zkušený hacker si *IMEI* dokáže změnit. To znamená, že zahodit SIM opravdu nestačí a nebudeš první, kdo na to dojel - vzpomeň si na tu švestku, co prodávala fotky mrtvého Svobody, od něj bych čekal více přehledu, ale holt to byl jen obyčejný pochůzkář odněkud z Kostelce.

Mobilní telefon je tedy, ač jinak obrovsky pohodlná a praktická věc, také bezpečnostním rizikem prvního řádu, které jeho používáním podstupuješ zcela dobrovolně dnes a denně. Rapidní vývoj mobilní komunikace našemu Velkému bráchovi velmi příjemně nahrává.



O počítačích a jejich identifikaci toho již bylo napsáno hodně a v Šedé Zóně jsem této problematice široce věnoval, např. v článkách "**Potkal jsem ho na nádraží - Wi-Fi chrání občana**" či starším seriálu "Virtuální špióni a záškodníci" zde v sekci **Bezpečnost**. Zopakuji tedy ještě jednou - každý počítač na Internetu je identifikován nejen podle IP adresy (kterou má "v rukou" poskytovatel připojení neboli *ISP*), ale taktéž dle *MAC* adresy síťové karty, která slouží k připojení k Internetu. Každá

tato síťová součást, ať již *WLAN* či *LAN* karta nebo router, má tuto adresu jedinečnou, neměnnou a tedy dokonale identifikovatelnou (pochopitelně jsou možnosti změny, ale je otázka, jak tato bude účinná a celkově je to věc složitější). Různé *proxy* tedy nejsou žádnou zárukou anonymity. Jediná možnost, jak zmařit identifikaci, je popsána ve výše uvedeném "nádražním" článku - anebo Internet nepoužívat. Protože jisté je, že cokoli na Internetu děláš, je ti čteno přes rameno. Možnosti v této oblasti jsou již dlouhá desetiletí mimo tvoje chápání, mimo jiné možnost čtení údajů přímo z monitoru počítače **NA DÁLKU** bez přímé viditelnosti. K čemu jsou ti pak složitá hesla, když si někdo snadno vše potřebné přečte přímo z monitoru? Nemáš šanci.



Další věci v hitparádě jsou **čipové záležitosti, primárně platební karty**. Zamyslel ses někdy nad tím, že všechny transakce, co kartou uděláš, jsou nejen zaznamenávány, ale je i bance předán jejich obsah? Vědí tedy, co přesně a kdy kupuješ a kde, mohou tak precizně plánovat reklamní kampaně a znát "svého" klienta, nabídnout ten správný produkt. Opět, sbírají o

tebě zevrubné informace, protože podle nákupů člověka fest poznáš. Máš rád sladké? Pivo? Kouříš? Jaké čteš noviny? Jakou značku oblečení preferuješ? To vše poznají, protože jim to vesele odejde s každou transakcí do centrály a ruku na srdce, kdo by se dnes tahal s hotovostí, když máš přece kouzelnou a pohodlnou platební kartu? Je to stejné, jako u mobilů. Zdánlivě ti to ulehčuje život, ale rozhodně ne zadarmo. Platíš ztrátou soukromí a předáváním údajů do neznáma. Banka je ještě zlatá. Ale co ty další subjekty, firmy, co snímají tvůj obličej, soukromá databáze DNA apod.? Neprůhledné, zcela neprůhledné. Nicméně, platební kartu nemusíš používat, ačkoliv takových lidí mnoho nebude, zejména mladých. Rozhodně se bez ní však žít dá. Mimochodem, o tom, že všechny transakce z tvého účtu jsou perfektně zaznamenávány a zejména analyzovány, o tom se snad nemá cenu ani zmiňovat...



Jako poslední věc zmíním **doklady s biometrickými údaji**, které jsou sice zdánlivě věcí budoucnosti, ale nemyl se - bůhví,

jaká je situace dnes. Ostatně, prohlédni si svou občanku dobře. Vidíš dlouhý, zcela nesrozumitelný pás čísel na ní? Kdo ví, co to je za kód? Zlé jazyky tvrdily, že se má jednat o jakýsi popis "tváře" či vzhledu v číselném kódu, ale skutečnost bude pravděpodobně ještě zásadnější. Co když si pak jednou do plastové fólie zavaříš i svůj vzorek DNA, aby ho scannery pro dokonalou identifikaci mohly snadno číst? Technicky jistě nepůjde o nic těžkého a při pokroku dnešní vědy... to bude perfektní! Žádné směšné otisky, nyní už identifikaci nikdo neunikne. A kruh se uzavírá.

Vážně není zapotřebí lidi plašit tím, jak jsou sledováni. Není to třeba, stačí pouze popsat realitu. A to pouze tu známou část současnosti. Pravdu nikdo nezjistí. Jisté však je, že každým dnem bude situace zásadnější, jak se technické možnosti budou zlepšovat a budou přicházet nové vynálezy, mající za cíl jediné - kontrolovat, analyzovat, shromažďovat data.

Rizika domácí Wi-Fi sítě

*Podívejme, takže sis domů přinesl kvalitní, odzkoušený **router**, odpojil ty hloupý zastaralý LAN kabely, chodíš si s laptopem po bytě včetně hazjlíku, užíváš si svobody a připadáš si jako dráty-jíž-nespoutanej-král... nikdo na Tebe nemůže, páč sis to přece zabezpečil krutým, neprolomitelným WPA2... přibrzdí s tím nadšením na chvíli.*



Nainstalovat si doma Wi-Fi router je jako chodit s holkama bez ochrany - je to příjemné, ale sakra rizikové. A zatímco styk neprovádíš tak často, router neúprosně vysílá 24 hodin denně do okolí signál, který si leckterý hacker vykládá jasně: "Vezmi si mě! Znásilni mě! Pronikni do mě!"

OK, omlouvám se za ten úvod maličko v tónu patosu, ale výše popsané jsou přirozené lidské pocity poté, co přejdeš z tábora "drátových" do tábora "bezdrátových". A jedno je jisté - již nebude nic stejné. Jak v tom smyslu, že nyní si můžeš surfovat v posteli, kuchyni, předsíni... tak v tom smyslu, že zatímco původně tvoje data šly relativně (sic!) bezpečným LAN kabelem, tak nyní je pěkně otevřeně, demokraticky posíláš do celého širého okolí - kdo na to má, ten si je prostě může rozlousknout.

Jasně, pokud "nezasockuješ" a nenecháš AP bez zabezpečení či nezvolíš nějaké směšné zabezpečení jako WEP, můžeš mít při WPA2 dobrý pocit z toho, že jsi pro bezpečí svých dat i identity udělal maximum. Ale je to asi tak stejný pocit, že na dýze "sbalíš" *důru*, uděláš jí to naostro (páč kdo by se páral s nějakými šprckami, no né, dodává **známý životní praktik Jouda**) a pak si říkáš, že to "ASI" bude OK, protože v celém tom našem Banánistánu budou max. stovky HIV pozitivních, takže vyfasování "peška" je nepravděpodobné.

Takže si pojďme opět jednou rozlít čisté víno a povídat si o tom, jaké dveře jakého světa jsi dneškem pootevřel. Proč tomu tak je? Rozum ti napoví, že dokud si Internet vedl domů po kabelu, možnost "napojení" byla velmi nízká a většina útočníků k ní nemá prostředky, ani potřebu. Ale Wi-Fi síť, kterou Tvůj router vyzařuje až stovky metrů daleko? To je jiná káva. Jen si to představ. 24 hodin denně Tvůj router hlásí okolí "tady jsem" a to je setsakramentské lákadlo pro spoustu závadových, leč bohužel pro Tebe zároveň i technicky až příliš zdatných lidí... mají čas, mají klid na práci, mohou ihned zmizet, nepotřebují přímý přístup k Tvému HW, zkrátka pro útočníka ideální stav.

V zásadě ti hrozí následující rizika, která pro Tebe mohou znamenat vážné důsledky včetně, ale nekonče, trestněprávních:

- 1) **krádež identity**
- 2) **krádež internetového připojení**
- 3) **krádež dat**

Krádež identity je bezesporu tím nejvíce nebezpečným, s čím si zahráváš. Asi si sám představíš, o co půjde - někdo napíše do internetové diskuze příspěvek, porušující zákony. Někdo pošle z Tvojí IP výhrůžku, opět s trestněprávními důsledky. Někdo se za Tebe zkrátka vydává, a zatímco on zmizí anonymně v dáli, Tobě začnou chodit pozvánky k výsledkům...

Krádež internetového připojení - nemávej nad ní rukou. Nejen, že někdo zneužije Tvou linku, ale vzhledem k tomu, že vše půjde přes Tvůj router, tento čin úzce souvisí s výše uvedenou krádeží identity. Co když někdo např. nauploaduje do Internetu přes Tvou linku nějaký "horký" obsah? Pro koho si pak přijdou?

Krádež dat - jak cenný jsou data, co máš v domácím PC, resp. všech strojích, co přistupují k netu přes router? Posud' sám. A co by se stalo, kdyby se k těm datům dostal někdo cizí, kdo snadno sklouzne k vydírání, pokud "objeví" nějaký evidentní zlatý důl? Jsi na to připravený? Co že jsi říkal o internetovém bankovníctví a 1M na účtě... kde že bydlíš? ;-)



Rozhodně zbystrí, pokud v okolí zaparkuje takové nápadné a podivnou anténou opatřené vozidlo. Pamatuj - že jsi paranoidní neznamená, že po tobě nejdou.

Wi-Fi, milé děti, dospělí i kmeti, není žádná legrace. Ano, obecná teorie říká, že "**co je za routerem, nemusí být ve vlastníkově vůli**". Obrana před orgány v tom smyslu, že se někdo "napojil" a spáchal dotyčné skutky, může být účinná. Otázka je, jak příjemné to vyšetřování bude a jak hluboko zasáhne do Tvého života. Nic moc... ale o tom již v článku na odkazu výše.

A jak se tedy bránit potenciálním problémům? Základní tipy jsem uvedl v textu o routeru **Linksys WRT54GC**, včetně příslušných nastavení. To nejzákladnější tedy je: skrytí SSID, omezení DHCP serveru, omezení na MAC adresy. Je vhodné také průběžně kontrolovat logy routeru i objem "protečených" dat, které jasně ukazují, jakému zařízení DHCP server přidělil adresu. Správně by v seznamu měly být jen ta zařízení, která máš doma. Pokud by se vyskytlo nějaké cizí, potom pozor - uvažoval bych dokonce o dočasném vypnutí Wi-Fi a zcela samozřejmě změně konfigurace včetně hesel. Stejně tak bude jistě vhodné, vypínat bezdrátovou část sítě, pokud ji nevyužíváš. Čím méně Wi-Fi pro svět existuje, tím lépe pro Tebe.