Перспективи інформаційної безпеки та кібер безпеки в Україні

Євген Докукін aka MustLive
http://websecurity.com.ua

Виміри війни Росії проти України.

З початку 2014 року триває російська агресія. Також відбувається економічна, інформаційна та кібер війни.

Росія веде інформаційну війну проти нас на теренах України і на заході, як частину гібридної війни. Яку вона почала задовго до військової агресії проти України.

Росія проводить проти України інформаційну війну. Якщо в 2014 році кібервійна знаходитилася на початковому рівні, то з грудня 2015 року, після атаки на енергосистему України, вона перейшла на новий рівень. В 2016 - друга атака на енергосистему, в 2017 - атака на фінансову систему України.

Це можна побачити по хакерським і DDoS атакам на українські сайти.

Доказом цього є атаки на державні сайти (взломи і DDoS атаки).

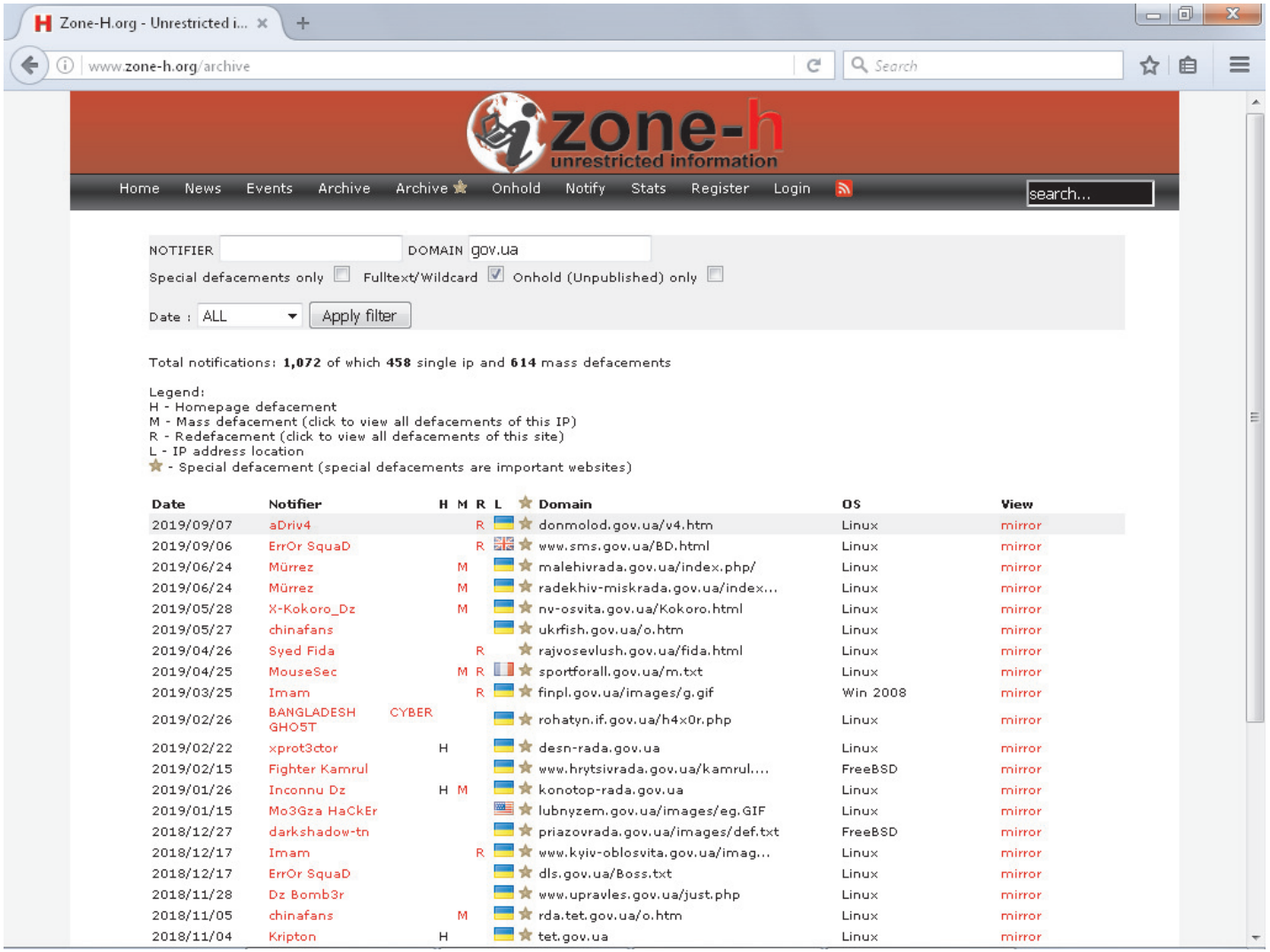
Статистика за 2004-2018 роки:

Статистика за останні три роки:

В 2016 році атаковано 137 державних сайтів, в 2017 році атаковано 109 державних сайтів, в 2018 році атаковано 54 державних сайтів.

Всього за 2001 - 2018 роки було атаковано 1119 державних сайтів (включаючи взломи та DDoS атаки).

Останні хакнуті державні сайти:

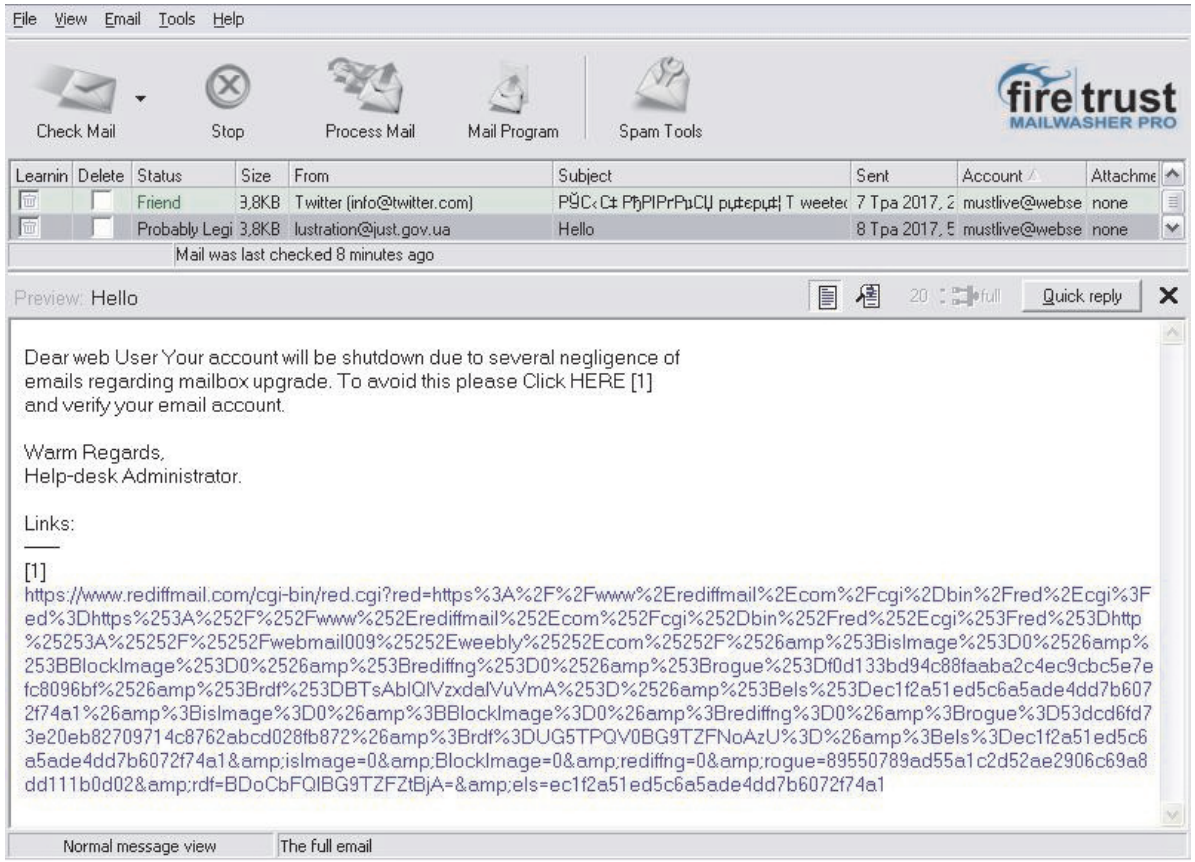


Date	Notifier	H	M	R	L	Domain	OS	View
2019/09/07	aDriv4			R		donmolod.gov.ua/v4.htm	Linux	mirror
2019/09/06	ErrOr SquaD			R		www.sms.gov.ua/BD.html	Linux	mirror
2019/06/24	Mürrez		M			malehivrada.gov.ua/index.php/	Linux	mirror
2019/06/24	Mürrez		M			radekhiv-miskrada.gov.ua/index...	Linux	mirror
2019/05/28	X-Kokoro_Dz		M			nv-osvita.gov.ua/Kokoro.html	Linux	mirror
2019/05/27	chinafans					ukrfish.gov.ua/o.htm	Linux	mirror
2019/04/26	Syed Fida			R		rajvosevlush.gov.ua/fida.html	Linux	mirror
2019/04/25	MouseSec		M	R		sportforall.gov.ua/m.txt	Linux	mirror
2019/03/25	Imam			R		finpl.gov.ua/images/g.gif	Win 2008	mirror
2019/02/26	BANGLADESH CYBER GHO5T					rohatyn.if.gov.ua/h4x0r.php	Linux	mirror
2019/02/22	xprot3ctor	H				desn-rada.gov.ua	Linux	mirror
2019/02/15	Fighter Kamrul					www.hrytsivrada.gov.ua/kamrul....	FreeBSD	mirror
2019/01/26	Inconnu Dz	H	M			konotop-rada.gov.ua	Linux	mirror
2019/01/15	Mo3Gza HaCkEr					lubnyzem.gov.ua/images/eg.GIF	Linux	mirror
2018/12/27	darkshadow-tn					priazovrada.gov.ua/images/def.txt	FreeBSD	mirror
2018/12/17	Imam			R		www.kyiv-oblosvita.gov.ua/imag...	Linux	mirror
2018/12/17	ErrOr SquaD					dls.gov.ua/Boss.txt	Linux	mirror
2018/11/28	Dz Bomb3r					www.upravles.gov.ua/just.php	Linux	mirror
2018/11/05	chinafans		M			rda.tet.gov.ua/o.htm	Linux	mirror
2018/11/04	Kripton	H				tet.gov.ua	Linux	mirror

Тисячі державних сайтів були хакнуті чи інфіковані за 19 років. Але жоден випадок досі не розслідували і жодного чиновника не притягнули до відповідальності.

Правоохоронні органи не розслідували жодного взлому державних сайтів, що згадані в моїй статистиці.

ФСБ Росії захопила пошту Мінюсту 08.05.2017 (веб пошта на just.gov.ua) та надіслала мені фішинг лист.



СБУ і Кіберполіція досі не розслідували жодного взлому державних сайтів. У тому числі з травня 2017 року, коли через хакнуту веб пошту Мінюсту мені розсилали фішинг листи, про що одразу повідомив Міністерство юстиції, СБУ і КП. Восени 2018 року я вияснив, що КП взагалі закрили моє звернення, що ще тоді зареєстрували і сповістили, та взагалі не розслідували його.

Прикладом інформаційної війни Росії проти України є посольства фейкової ДНР (терористичної організації) в країнах ЄС.

1. Посольство ДНР у Франції в Марселі - сайт donetsk-france.org.
2. Представницький центр ДНР у Фінляндії в Хельсінки.
3. В кінці 2016 року в Турині відкрилося перше представництво ДНР на території Італії. В лютому 2019 року у Вероні в Італії відкрилося нове представництво ДНР.

Захист від гібридних загроз.

Враховуючи інформаційну та кібер війну Росії проти України: взломи, інфікування та DDoS атаки на державні сайти та інші мережеві ресурси, а також дві успішні атаки на енергосистему України (в 2015 і 2016) та фінансову систему (в 2017). То потрібні дієві заходи для захисту від інформаційної та кібер війни і від гібридних загроз.

Співпраця з НАТО та ЄС.

Для захисту як України, так і країн НАТО та ЄС від гібридних загроз, зокрема зі сторони Росії, потрібно звернути увагу на наступне:

1. Домени і хостинги в ЄС, США та інших країнах.
2. Рахунки в електронних платіжних системах.
3. Інші мережеві ресурси та сервіси.

Всі ці ресурси використовуються для кібератак та пропаганди Росії.

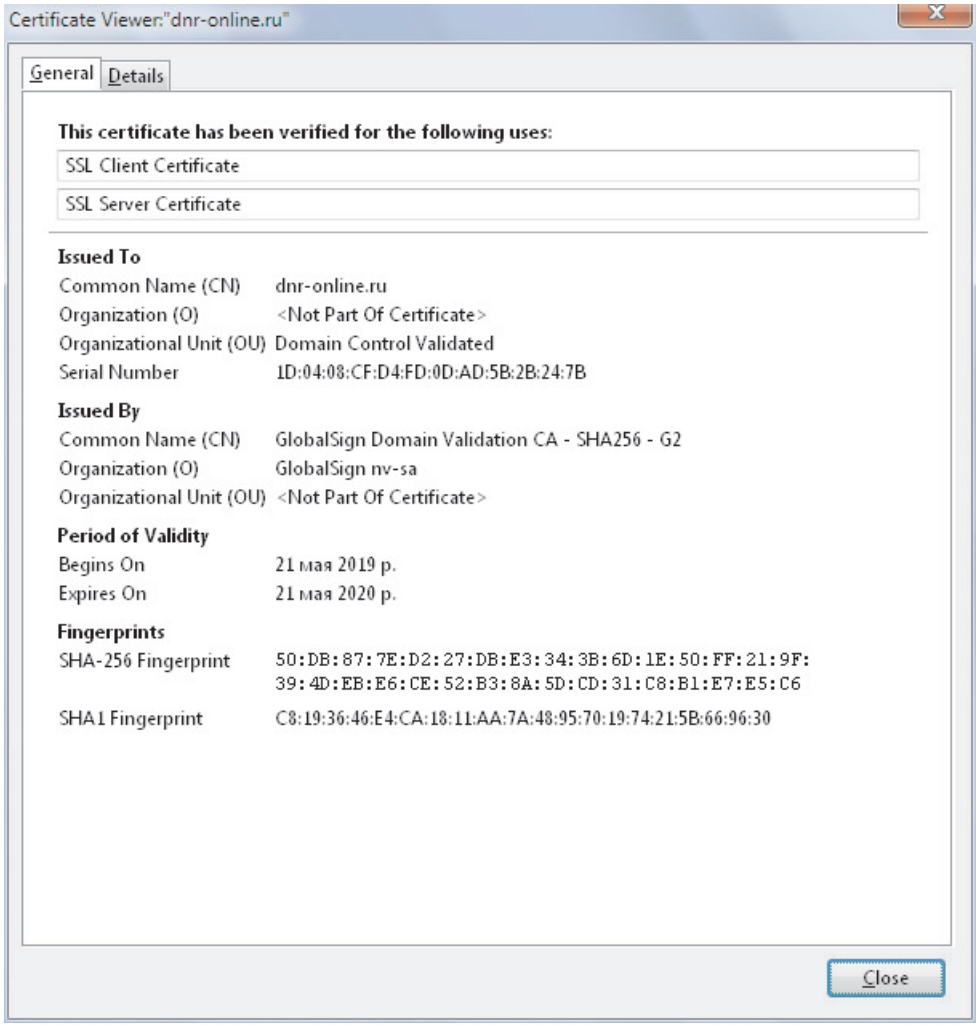
За п'ять років Українські Кібер Війська всього заблокували 537 рахунків терористів.

В 2014 році Українські Кібер Війська отримали дані транзакцій по рахунку терориста в PayPal.

З цих даних ми виявнили суми коштів та країни походження фінансування тероризму.

Громадяни наступних країн фінансували російських терористів в Україні: Росія, США, Канада, Нова Зеландія, Австралія, Німеччина, Нідерланди та інші країни ЄС (надсилали Євро).

Окрім продажу доменів і хостингів для сайтів терористів, також компанії, зокрема з США та Бельгії, п'ять років надають їм SSL сертифікати.



Найбільше компаній в США, що підтримують тероризм і російську агресію проти України. Це Facebook, Twitter, Google, PayPal, CloudFlare та інші компанії.

Фінансування терористів і хакерів, продаж доменів і хостингів, надання SSL сертифікатів, надання акаунтів у соцмережах, захист сайтів. При цьому вони відмовляються блокувати, в т.ч. терористів, які знаходяться під санкціями з 2014 року.

Потрібно юридичними методами змусити ці компанії припинити надавати терористам і хакерам фінансову та технічну підтримку.

Лише спільними зусиллями Україна, НАТО та ЄС зможуть покращити стан власної інформаційної безпеки і кібер безпеки. А також подолати сучасні виклики та всі гібридні загрози!