NASK

CERT POLSKA

Raport

Analiza domen rejestrowanych za pośrednictwem Domain Silver, Inc.

31 lipca 2013

Spis treści

1 Wprowadzenie **2**

2 Rejestr, operator rejestru oraz rejestrator **3**
2.1 Rogue registrar 3
2.2 Domain Silver 4

3 Rozkład domen **4**

4 Botnety **5**
4.1 Citadel 5
4.2 Dorkbot (NgrBot) 6
4.3 Zeus Ice IX 6
4.4 Andromeda (Gamarue) 6
4.5 RunForestRun 7
4.6 Ransomware 7

5 Infrastruktura proxy do C&C **8**

6 Co dalej z domenami? **9**

Skracanie linków za pomocą bit.ly

Niektóre z linków umieszczonych w tym raporcie zostały skrócone za pomocą serwisu `bit.ly` w celu poprawienia czytelności. Aby zobaczyć pełen adres wystarczy na ich końcu dodać znak plusa (+). Strona znajdująca się pod takim adresem zawiera informacje o skróconym linku.

1 Wprowadzenie

Niniejszy dokument zawiera opis domen rejestrowanych za pośrednictwem firmy Domain Silver, Inc. rejestratora działającego w domenie `.pl`. Rejestrator ten, którego siedziba znajduje się na Seszelach, rozpoczął swoje działanie w maju 2012 roku. Od tego czasu zespół CERT Polska zaczął obserwować duży wzrost liczby rejestrowanych złośliwych domen (w tym do rozpowszechniania i zarządzania złośliwym oprogramowaniem) oraz otrzymywać wiele skarg z zewnątrz na domeny rejestrowane za pośrednictwem Domain Silver. W maju 2013 doszło do przejęcia i sinkhole'owania kilkudziesięciu złośliwych domen przez CERT Polska. Większość domen `.pl` zawierających złośliwą treść byłą rejestrowana właśnie przez Domain Silver. Po dalszych bezskutecznych próbach naprawienia tej sytuacji, NASK podjął decyzję o wypowiedzeniu umowy z partnerem. W kolejnych rozdziałach tego dokumentu omawiamy do czego wykorzystywane były zarejestrowane za pośrednictwem Domain Silver domeny (status na 9 lipca 2013), jakie rozpowszechniano złośliwe oprogramowanie i dlaczego stanowiło to zagrożenie dla Internautów.

Najważniejsze ustalenia:

- Ze wszystkich domen zarejestrowanych – 641 domen (stan na 9 lipca 2013 plus domeny wcześniej sinkhole'owane) - tylko jedna aktywna była nieszkodliwa (`domainsilver.pl`)
- 404 domeny były jednoznacznie szkodliwe, z czego 179 służyło jako serwery C&C.
- Domeny były wykorzystywane do zarządzania i rozpowszechniania botnetów takich jak Citadel, Dorkbot, ZeuS Ice IX, Andromeda, RunForestRun a także ransomware'u.
- Zidentyfikowaliśmy co najmniej 16 instancji wyżej wymienionych botnetów.
- 179 domen było używanych jako strony reklamujące farmaceutyki lub rekrutujące muły. Adresy URL tych stron były rozpowszechniane za pomocą kampanii spamowych.

Wszelkie zmiany danych domen zarejstrowanych przez Domain Silver są obecnie zablokowane, a partner nie ma już dostępu do rejestru domen. Domeny te mają jako rejestratora wpisaną nazwę `vinask`. Domeny te będą systematycznie przenoszone na serwery sinkhole'a CERT Polska.

2 Rejestr, operator rejestru oraz rejestrator

Ze względu na podobieństwo angielskich nazw, następujące trzy pojęcia bywają często ze sobą mylone: rejestr nazw domenowych (ang. *registry*), rejestrator nazw domenowych (ang. *registrar*) oraz abonent nazwy domenowej (ang. *registrant*). Zakładając, że rola abonenta wydaje się oczywista, poniżej tłumaczymy role rejestru oraz rejestratora nazw domenowych oraz różnice między tymi pojęciami.

Rejestr nazw domenowych (ang. *domain name registry*) to baza danych zawierająca wszystkie nazwy zarejestrowane w jednej domenie internetowej (np. `.pl`), kojarząca nazwy domenowe z danymi ich abonentów oraz z nazwami serwerów na które są delegowane. Rejestry nazw domenowych mogą być tworzone na różnych poziomach hierarchii systemu DNS. I tak, operatorem rejestru najwyższego poziomu (ang. *root-level*) jest IANA (czyli *Internet Assigned Numbers Authority*), która z kolei deleguje zarządzanie rejestrami kolejnych poziomów (ang. *top-level*) innym organizacjom. Rolą operatora rejestru nazw domenowych, zwanego także NIC (czyli *Network Information Centre*), jest utrzymywanie infrastruktury technicznej rejestru, tworzenie polityk rejestracji domen, a przede wszystkim aktualizacja rejestru i baz danych serwerów DNS. Naukowa i Akademicka Sieć Komputerowa jest operatorem rejestru nazw domenowych dla domeny krajowej `.pl`.

Zarządzanie czynnością rejestracji nazwy domenowej jest rolą podmiotu zwanego rejestratorem nazw domenowych (ang. *domain name registrar*). Jest to organizacja bądź firma komercyjna, współpracująca z operatorami rejestrów i posiadająca bezpośredni dostęp do wprowadzania i modyfikacji danych przechowywanych w rejestrze. Rejestrator dysponuje odpowiednim poziomem uprawnień, pozwalającym mu na dokonywanie zapytań do rejestru i zarządzanie pulą nazw domenowych należących do jego klientów. Operator rejestru może, lecz nie musi sam pełnić rolę rejestratora. W wielu przypadkach powierza ją firmom zewnętrznym, które zobowiązują się do stosowania polityk danego rejestru. W Polsce, NASK ma podpisane umowy z ponad 190 partnerami pełniącymi role rejestratorów nazw domenowych. Wśród nich wiele jest firm zagranicznych. Abonent może samodzielnie wybierać rejestratora, z usług którego będzie korzystał przy rejestracji nazwy domenowej, a także dokonywać przenoszenia nazwy pomiędzy rejestratorami.

2.1 Rogue registrar

Uprzywilejowana pozycja rejestratora, umożliwiająca mu dokonywanie rejestracji nowych nazw domenowych, delegowanie ich na serwery nazw, a także kontrolę nad danymi abonenta, może być niestety nadużywana. Z pozycji rejestratora łatwo można bowiem wprowadzać do rejestru serie nowych nazw domenowych, wykorzystywanych następnie do phishingu, spamu czy zarządzania złośliwym oprogramowaniem, jako dane abonentów podając informacje niezweryfikowane lub, w skrajnym przypadku, samodzielnie wygenerowane. W przypadku wykrycia nadużycia, prośby o reakcję trafiają zazwyczaj w pierwszej kolejności do rejestratora. Pozwala mu to na ignorowanie ich przez pewien czas, lub podejmowanie działań w taki sposób, aby nie zagrażały całości infrastruktury – na przykład usuwanie problematycznych nazw dopiero po stworzeniu nowych i odpowiedniej aktualizacji złośliwego oprogramowania.

To, co z zewnątrz wygląda na rażącą nieskuteczność w zwalczaniu problemu, w połączeniu z posiadanym przez rejestratora portfelem domen, w którym zdecydowaną większość stanowią nazwy wykorzystywane do nadużyć różnego rodzaju, pozwala domniemywać, że działania i zaniedbania takiego rejestratora są w pełni świadome. Mówimy wtedy o tak zwanym *rogue registrar*, którym w skrajnym przypadku może być firma założona wyłącznie w celu ułatwienia przestępcom dostępu do rejestru domen.

2.2 Domain Silver

Domain Silver jest jednym z rejestratorów, który swoją działalność rozpoczął w maju 2012 roku. Firma jest zarejestrowana pod następującym adresem:

```
Domain Silver Inc.
1st Floor, Sham-Peng-Tong
Plaza Building, Victoria, Mahe
Seychelles
e-mail: support@domainsilver.pl
tel.: +1.3236524343
```

Pierwsze skargi na działalność tego rejestratora CERT Polska otrzymał w drugiej połowie 2012 roku. Skargi te dotyczyły obecności serwerów C&C oraz stron, do których prowadziły linki z kampanii spamowych pod domenami zarejestrowanymi przez Domain Silver. Do 29 lipca 2013 za pomocą Domain Silver było zarejestrowanych 2926 domen.

3 Rozkład domen

Poniższa tabela prezentuje statystyki dotyczące szkodliwych domen, których registrarem był Domain Silver i które miały status zarejestrowanych 9 lipca 2013 roku, wliczając w to domeny, które były już wcześniej przez nas sinkholowane. Wszystkich domen `.pl`, które miały status zarejestrowanych w Domain Silver 9 lipca 2013 roku było 641.

Rodzaj zawartości	Liczba	Udział procentowy
Serwery C&C[1]	179	27.9%
Produkty farmakologiczne, rekrutacja mułów lub spam[2]	179	27.9%
Złośliwe oprogramowanie[3]	20	3.1%
Domeny umieszczone na blacklistach[4]	17	2.7%
Erotyka dziecięcia	5	0.8%

Tabela 1: Rozkład szkodliwych domen

[1]W tym serwery nazw, na których znajdowały się rekordy DNS serwerów C&C.
[2]W tym serwery nazw, na których znajdowały się rekordy DNS tych stron.
[3]W tym serwery nazw, na których znajdowały się rekordy DNS tych stron.
[4]Wyłączając domeny zaklasyfikowane do innych kategorii.

Spośród wszystkich domen 63% (404 domeny) stanowiły domeny zdecydowanie szkodliwe dla użytkowników. Z pozostałych domen tylko jedna (`domainsilver.pl`) zawierała, nieszkodliwą, treść, a reszta nie zawierała żadnej treści. 150 domen z pozostałej grupy zostało zarejestrowanych tego samego dnia – 18 marca 2013, w ciągu 15 minut.

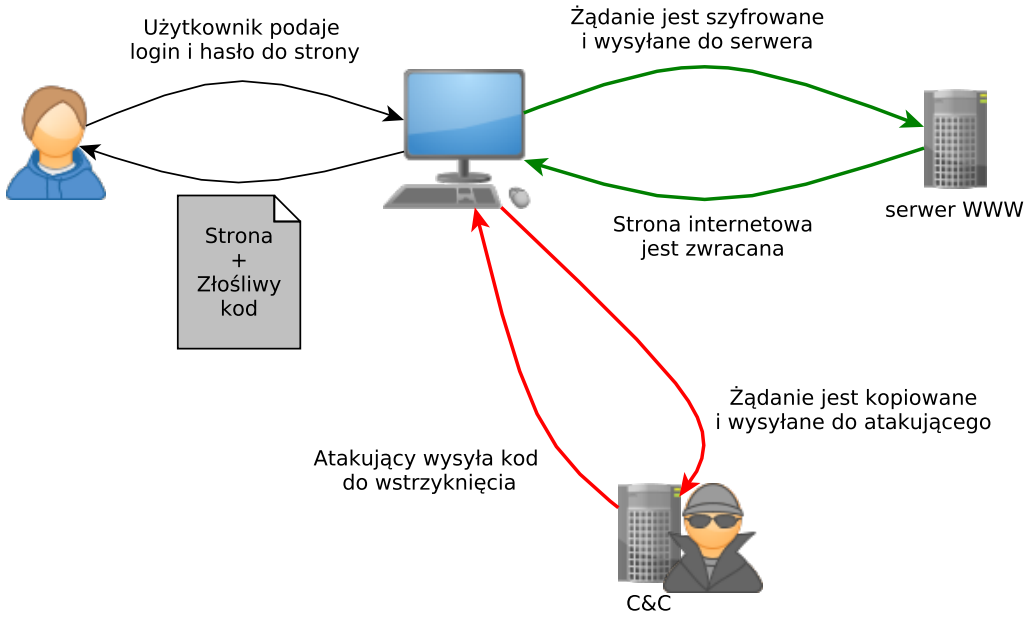
Oprócz tego, wśród domen zarejestrowanych wcześniej, byliśmy w stanie zidentyfikować 35 domen używanych przez serwery C&C oraz 12 wykorzystywanych w kampanii spamowej produktów farmakologicznych. Pomiędzy 6 a 10 lipca 2013 roku, w ramach *Domain Name Tasting*, czyli możliwości czternastodniowego testowania nazwy domeny, zarejestrowano w Domain Silver 597 nazw domenowych, które służyły do promocji pigułek pomagających schudnąć i były wykorzystywane w kampaniach spamowych używających botnetów.

4 Botnety

Poniżej przedstawiamy krótkie opisy rodzajów botnetów, które znajdowały się na wspomnianych wyżej domenach. Domeny zarejestrowane w Domain Silver były wykorzystywane w co najmniej 16 różnych, zidentyfikowanych przez nas, instancjach botnetów.

4.1 Citadel

Citadel jest złośliwym oprogramowaniem, które jest dystrybuowane jako *crimeware kit* – zestaw aplikacji pozwalających na stworzenie własnej instancji botnetu. Rozwinął się on z kodu innego bota – Zeusa, który to kod wyciekł w 2011 roku.



Rysunek 1: Schemat ataku *man in the browser*

Citadel wykorzystywany był najczęściej do wykradania danych logowania do instytucji finansowych oraz ataków z wykorzystaniem inżynierii społecznej. Używał w tym celu ataków typu *man in the browser*. Na rysunku 1 zaprezentowany jest schemat takiego typu ataku.

Więcej informacji na temat botnetu Citadel można znaleźć w naszym raporcie na temat przejęcia instancji `plitfi`: `http://www.cert.pl/news/6900`. Jest to jedna z instancji znajdujących się na domenach zarejestrowanych w Domain Silver.

4.2 Dorkbot (NgrBot)

Dorkbot jest złośliwym oprogramowaniem posiadającym dużą funkcjonalność. Jedną z bardziej zaawansowanych jest instalacja rootkita w trybie użytkownika, dzięki czemu może on ukrywać swoją obecność w systemie – zarówno obecność samego pliku ze złośliwym oprogramowaniem, jak i jego aktywność na liście procesów. Pozostałe możliwości oprogramowania to między innymi:

- infekowanie dysków USB,
- pobieranie i uruchamianie dodatkowego oprogramowania,
- wykradanie haseł z serwisów społecznościowych, hostingowych i innych,
- rozprzestrzenianie się przez Skype, MSN, Facebook czy inne serwisy społecznościowe,
- przeprowadzanie ataków typu *flood* czy *slowloris*.

Więcej informacji na temat Dorkbota oraz jego instancji, które wykorzystywały domeny w Domain Silver można znaleźć w jednym z wpisów na naszym blogu pod adresem: `http://www.cert.pl/news/6434`.

4.3 Zeus Ice IX

Kolejną po Citadelu gałęzią złośliwego oprogramowania, powstałego na podstawie ujawnionego kodu Zeusa, jest Ice IX. Posiada on te same możliwości co Zeus, czyli potrafi zarówno przechwytywać hasła użytkowników zainfekowanych systemów jak i przeprowadzać ataki *man-in-the-middle* takie jak ten przedstawiony powyżej.

Więcej na temat tej odmiany Zeusa można znaleźć na blogu RSA pod adresem `http://bit.ly/11WI8u7`.

4.4 Andromeda (Gamarue)

Andromeda jest modularnym botem stworzonym w taki sposób, by umożliwić łatwe dodawanie do niego nowych funkcji. System sprzedaży tego botnetu opiera się na udostępnianiu kolejnych pluginów za dodatkową opłatą. Pluginy te umożliwiają między innymi następujące operacje:

- pobranie i uruchomienie dodatkowego oprogramowania,

- wykradanie danych logowania z różnych serwisów,
- tworzenie z komputera ofiary serwera pośredniczącego (proxy).

Bot ten zawiera również dużą liczbę technik chroniących go zarówno przed analizą dynamiczną z wykorzystaniem oprogramowania VirtualBox czy VMWare, jak i przed debugowaniem. Sposobem rozprzestrzeniania się botnetu były wiadomości e-mail sugerujące, iż załączony do niej plik to bilet elektroniczny na podróż samolotem. Drugim sposobem było użycie popularnego *exploit kita*, czyli zbioru aplikacji wykorzystujących luki we wtyczkach przeglądarki internetowej lub w samej przeglądarce.

Więcej informacji na temat tego złośliwego oprogramowania i kampanii związanej z Domain Silver można znaleźć na blogu firmy Trend Micro: `http://bit.ly/SW2dr3`.

4.5 RunForestRun

RunForestRun jest złośliwym oprogramowaniem wycelowanym w serwery WWW. Do każdego pliku HTML na serwerze dodawany był złośliwy JavaScript tworzący ramkę (*iframe*) w obecnej stronie. Ramka ta kierowała użytkownika na adres zawierający szkodliwy kod (exploit kit lub reklamy). RunForestRun ma zaimplementowany algorytm generowania nazw domenowych (z ang. *Domain Generation Algorithm*, w skrócie DGA). Rozwiązanie to jest rzadko spotykane wśród złośliwego oprogramowania przeznaczonego na serwery WWW. W przypadku jednej z wersji RunForestRun, oprogramowanie nawet kilkukrotnie w ciągu dnia generowało nową nazwę domenową z końcówką `.waw.pl` powodując, iż blokowanie domen z którymi oprogramowanie się łączyło nie rozwiązywało problemu. Zablokowanie domeny wykorzystywanej danego dnia nie spowoduje odcięcia komunikacji z serwerem C&C, gdyż dnia kolejnego wykorzystywana jest inna domena.

Więcej informacji na temat tego złośliwego oprogramowania i DGA tworzącego domeny w `.waw.pl`, które następnie były rejestrowane poprzez Domain Silver można przeczytać na blogu Unmask Parasites: `http://bit.ly/OLynll`.

4.6 Ransomware

Na 16 domenach założonych po 9 lipca 2013 znajdował się serwer C&C oprogramowania typu *ransomware*. Jest to rodzaj złośliwego oprogramowania blokujący komputer użytkownika aż do otrzymania okupu. Oprogramowanie to, po zainfekowaniu komputera, łączyło się z domeną zarejestrowaną poprzez Domain Silver i pobierało z niej plik DLL, w którym znajdowała się miedzy innymi strona, która była wyświetlana. Znajdująca się na niej treść sugerowała, że komputer został zablokowany ze względu na złamanie przepisów i użytkownik musi zapłacić grzywnę w wysokości 500 złotych. Strona była dostosowywana do ustawień językowych użytkownika, tak, aby wzbudzić jego większe zaufanie. Na rysunku 2 znajduje się zrzut ekranu z zablokowanego komputera.

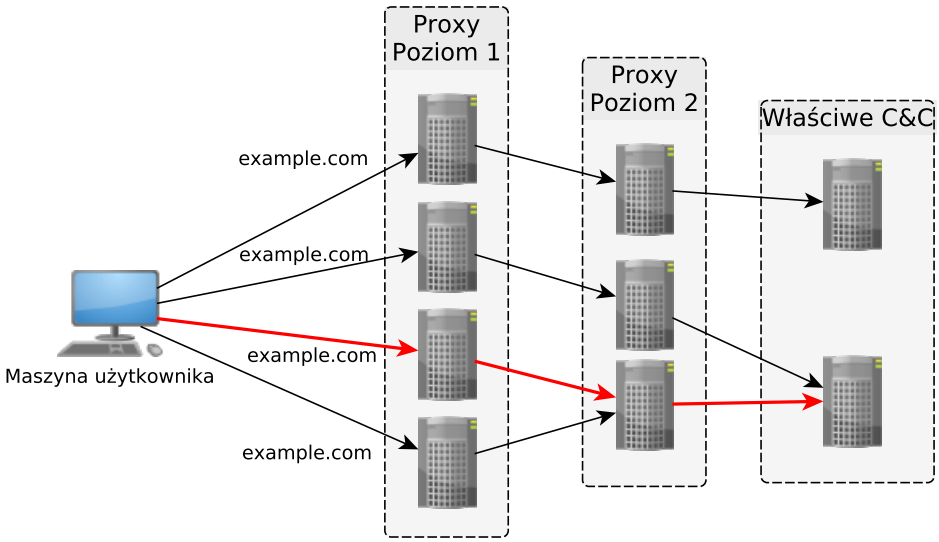
Rysunek 2: Polska wersja strony informującej o blokadzie komputera

Więcej informacji na temat tego typu oprogramowania można znaleźć na naszym blogu: `http://www.cert.pl/news/5483`.

5 Infrastruktura proxy do C&C

Niektóre z wyżej wymienionych botnetów, w celu lepszej ochrony adresu prawdziwego serwera C&C, wykorzystywały serwery proxy. Serwery używane w tym celu zostały najprawdopodobniej przejęte w wyniku włamania.

Za każdym razem gdy zainfekowana maszyna próbuje połączyć się z wpisaną w jej konfiguracji domeną (np. `example.com`) musi wybrać jeden z adresów IP z nią związanych. Najczęściej jest to pierwszy adres IP na liście odpowiedzi serwera DNS. Następnie przesyła pod ten adres IP zgromadzone dane oraz pobiera od niego instrukcje. Ten adres odpowiada jednemu z serwerów oznaczonych na rysunku 3 jako *Proxy Poziom 1*. Jest to maszyna, z którą bezpośrednio komunikuje się komputer ofiary.



Rysunek 3: Architektura proxy do C&C

Na każdym z serwerów poziomu 1 znajduje się oprogramowanie, które przekierowuje wszystkie żądania HTTP do jednego z serwerów oznaczonych jako *Proxy Poziom 2*. Analogicznie, każda z tych maszyn przekierowuje żądania do właściwego serwera C&C, który je przetwarza i tą samą drogą przesyła odpowiedź.

6 Co dalej z domenami?

NASK 30 lipca 2013 roku wypowiedział umowę z partnerem Domain Silver, Inc. Wszystkie domeny, które zostały zarejestrowane przez Domain Silver, Inc. znajdują się obecnie w stanie de facto zamrożenia. Oznacza to, że wszelkie zmiany w Rejestrze dotyczące tych domen są niedozwolone. Domeny mają wpisanego, jako registrara, nazwę `vinask`. Domeny te będą systematycznie przenoszone na serwery sinkhole'a CERT Polska.