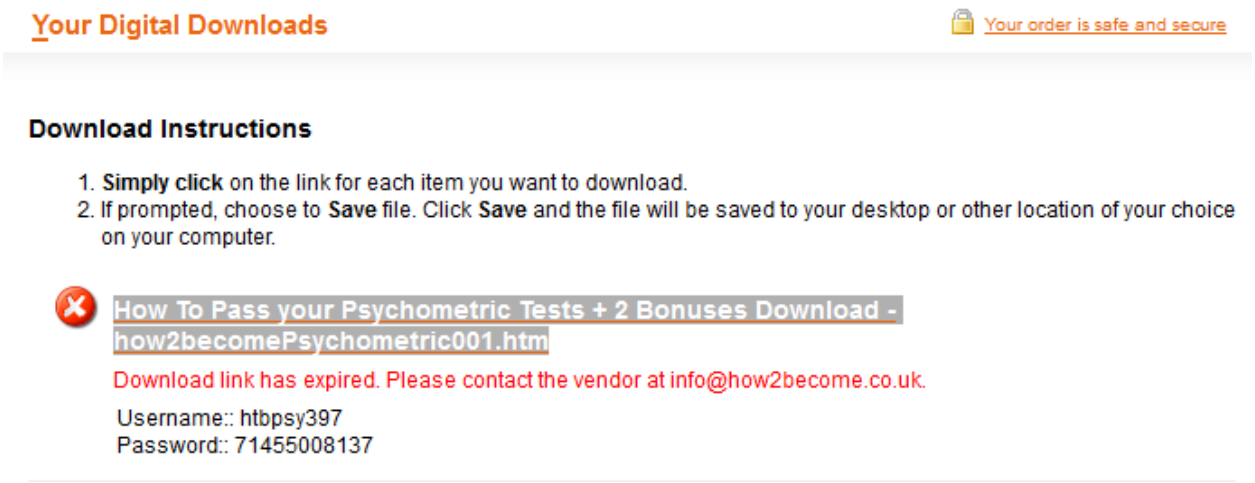
Necurs – analiza malware (1)

W trakcie analizy powłamaniowej w systemie jednego z klientów Orange Polska uzyskano nową próbkę złośliwego oprogramowania. Do jednego z elementów architektury tego zagrożenia w trakcie analizy kodu przyporządkowana została sygnatura złośliwego oprogramowania Necurs. Raport ten opisuje szczegółowo analizę modułu PE32 o następujących skrótach kryptograficznych:

Md5	`12eaeeaec7dae81c6d9bfead301b7c2a`
Sha256	`869ddc6e34f4f555e1d20c86cd0a630c3936818fbabb4b04c2cc8e90e6b7fa7b`
Sha512	`80f41c07d6477011a3362b5b00fe3198320c673aca35fa6e0e7c7088bed24657df2a148d3ae05e2698843ea8286b019464f8bd18235caa499af85a9283a2343f`

Próbka trafiła do CERT Orange Polska w listopadzie 2017 roku jako element maila z ofertą darmowych ebooków. W wiadomości znalazły się linki do ebooka oraz programu przedstawionego jako czytnik ebooków, który w istocie okazał się być dropperem opisywanego malware Necurs.



Rysunek 1: Zaproszenie ofiary do pobrania ebooka

Organizacja próbki

Kod analizowanej próbki w kontekście jego funkcji można podzielić na dwie części organizacyjne – protektor i dropper. Rolą protektora jest zapobieżenie zaklasyfikowania próbki przez zainstalowane w systemie oprogramowanie defensywne jako złośliwego oprogramowania. Protektory utrudniają też dokładną analizę funkcjonalności oprogramowania również na etapie drobiazgowej analizy próbek już zaklasyfikowanych jako złośliwe.

Protektor

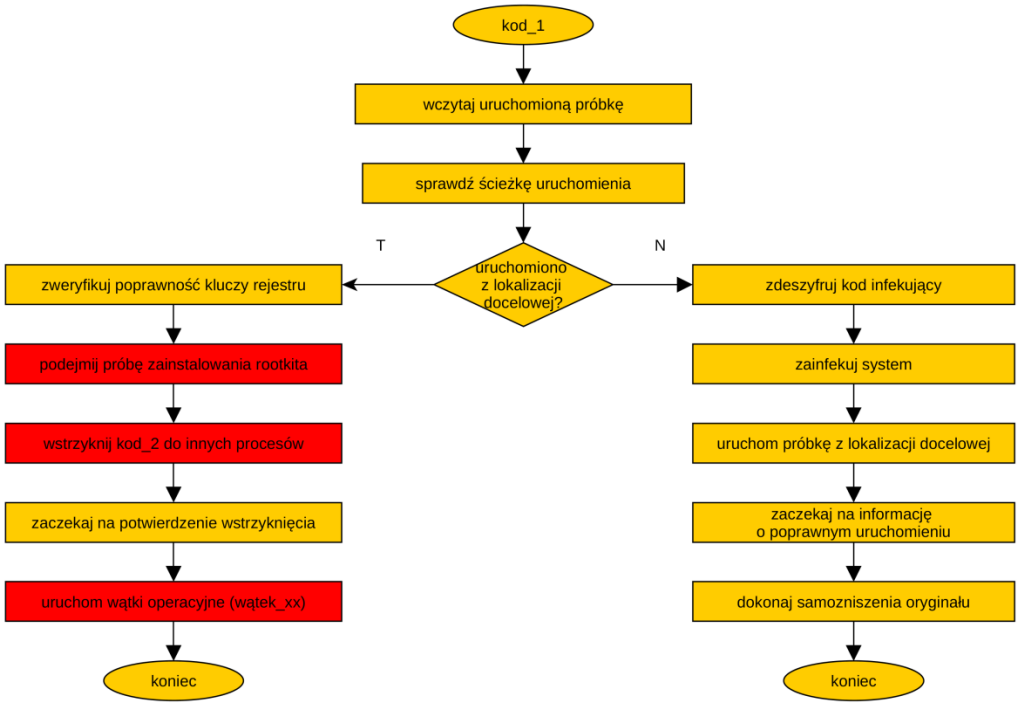
Protektor Necurs jest relatywnie prosty. Po zastosowaniu serii wywołań systemowych, ukrywających faktyczną rolę programu i kamuflujących go jako uprawnioną część oprogramowania, program przystępuje do zaalokowania pamięci na kod deszyfrujący, wypakowanie kodu ze swoich zasobów i przekazanie sterowania. Zdeszyfrowany kod deszyfruje następnie fragmenty pamięci programu odpowiedzialne za podstawowe funkcje operacyjne i infekujące, w kolejnym kroku przekazując do nich sterowanie.

Dropper

Podstawowym zadaniem droppera po pierwszym uruchomieniu programu jest rozmieszczenie komponentów złośliwej aplikacji w systemie ofiary (de facto „zainstalowanie" jej) i zapewnienie, by były one uruchamiane przy każdym starcie systemu. Ogólny schemat działania droppera w próbce Necurs przedstawiony został na poniższym diagramie. Ciekawą cechą tego gatunku jest fakt, że potrzebne fragmenty kodu jedynie w razie potrzeby są deszyfrowane i następnie wykonywane.

```
.text:00455C34 mov     eax, dwSize
.text:00455C39 push    eax
.text:00455C3A push    0
.text:00455C3C push    0FFFFFFFFh
.text:00455C3E call    ds:VirtualAllocEx
.text:00455C44 mov     [ebp+var_6C], eax
.text:00455C47 mov     [ebp+var_3C], 6B16h
.text:00455C4E mov     [ebp+var_68], 19h
.text:00455C55 mov     [ebp+var_34], 7C69h
```

Rysunek 2: Alokacja kodu na potrzeby rozpakowywanych fragmentów

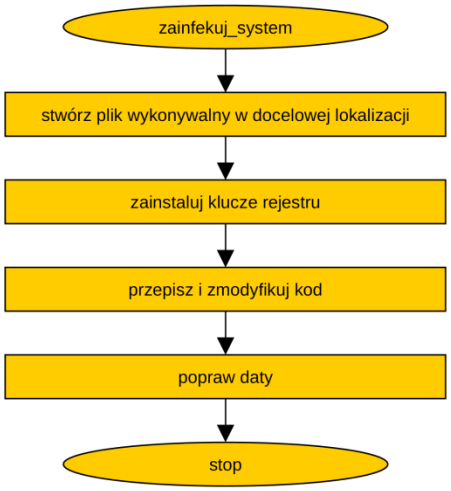


Rysunek 3: Ogólny schemat działania droppera Necurs

Przy pierwszym uruchomieniu (tj. nie z lokalizacji docelowej próbki) Necurs wykonuje procedurę instalacji. Polega ona na stworzeniu podkatalogów w katalogu domowym użytkownika

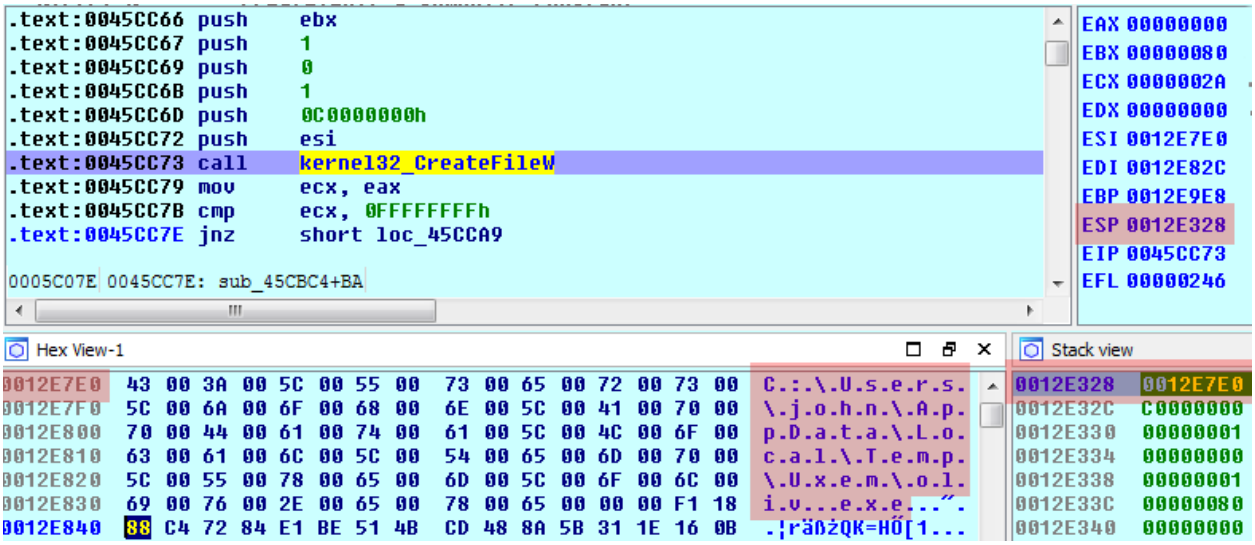
(C:\Users\<User>\AppData\Local\<pseudorandom_1>\<pseudorandom_2>.exe)

i stworzeniu w nim nowego pliku próbki.



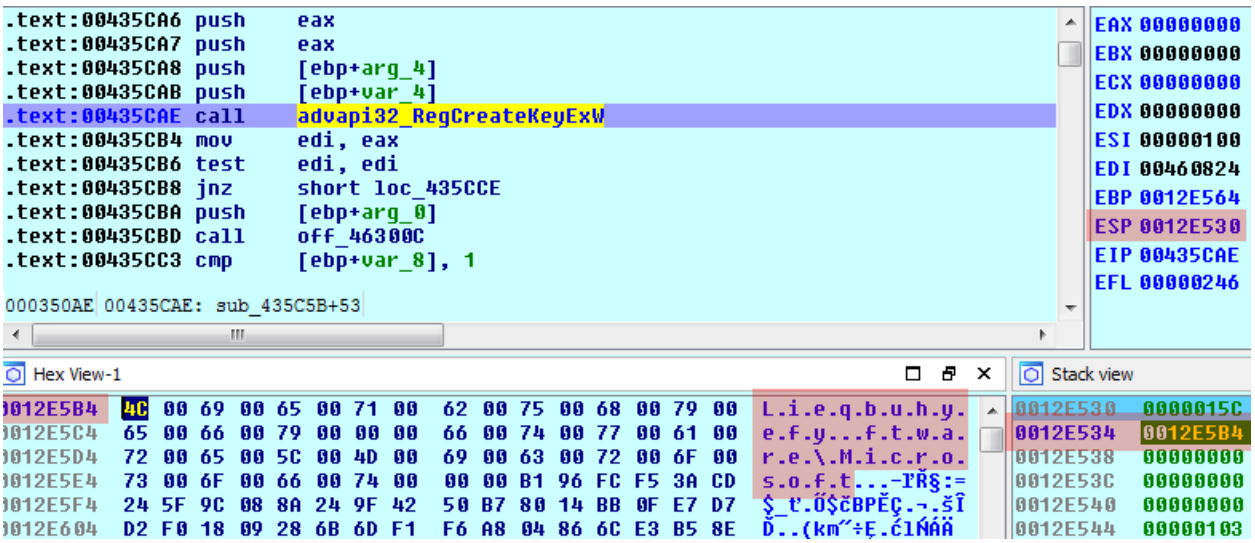
Rysunek 4: Schemat procedury infekcji Necurs

Dropper wczytuje oryginalną próbkę, jednak przed zapisaniem kodu do lokalizacji docelowej wprowadza do niej modyfikacje, dlatego dla dokładnej analizy zachowania próbki po infekcji, nie wystarczy jedynie zasymulować uruchomienia z docelowej lokalizacji. Proces infekcji musi zostać wcześniej przeprowadzony do końca.



Rysunek 5: Stworzenie nowego pliku wykonywalnego w docelowej lokalizacji

Necurs w trakcie instalacji tworzy również potrzebne klucze rejestru, którymi będzie się posługiwał w kolejnych etapach działania.



Rysunek 6: Tworzenie kluczy rejestru w trakcie infekcji

Jednym z działań, mających na celu ukrycie zainstalowanych plików, jest modyfikacja szczegółowych danych docelowej próbki na datę katalogu domowego użytkownika.

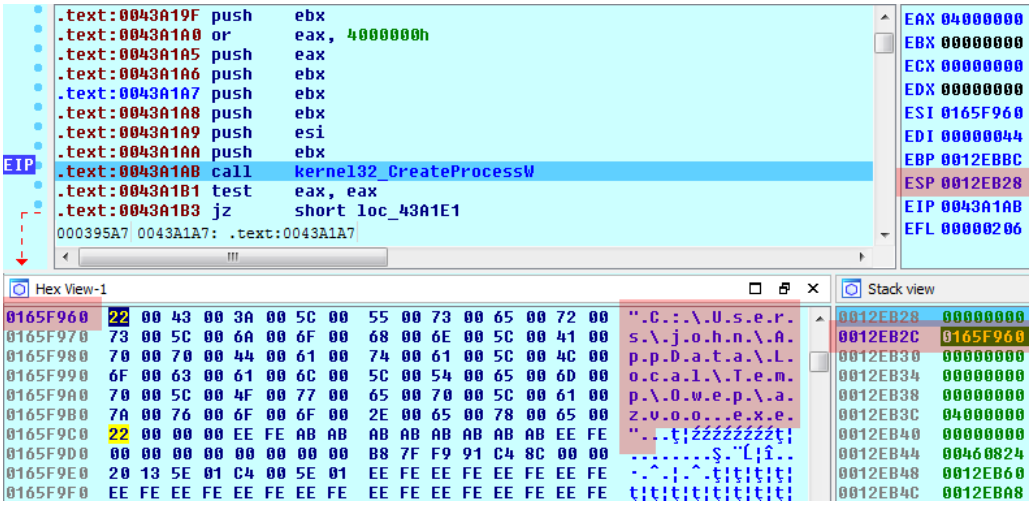
```
.text:0045EE8E push    eax
.text:0045EE8F push    [ebp+arg_4]
.text:0045EE92 push    [ebp+arg_0]
.text:0045EE95 push    dword ptr [ebx]
.text:0045EE97 call    kernel32_GetFileTime
.text:0045EE9D test    eax, eax
.text:0045EE9F jz      short loc_45EE80
.text:0045EEA1 test    esi, esi
.text:0045EEA3 jz      short loc_45EEB6
.text:0045EEA5 test    edi, edi
```

Rysunek 7: Pobranie daty modyfikacji katalogu domowego ofiary

```
.text:0045EDEC push    0
.text:0045EDEE push    dword ptr [edi]
.text:0045EDF0 call    ds:kernel32_SetFileInformationByHandle
.text:0045EDF6 neg     eax
.text:0045EDF8 sbb     eax, eax
.text:0045EDFA neg     eax
```

Rysunek 8: Przypisanie daty modyfikacji do nowo utworzonych składników złosliwej aplikacji

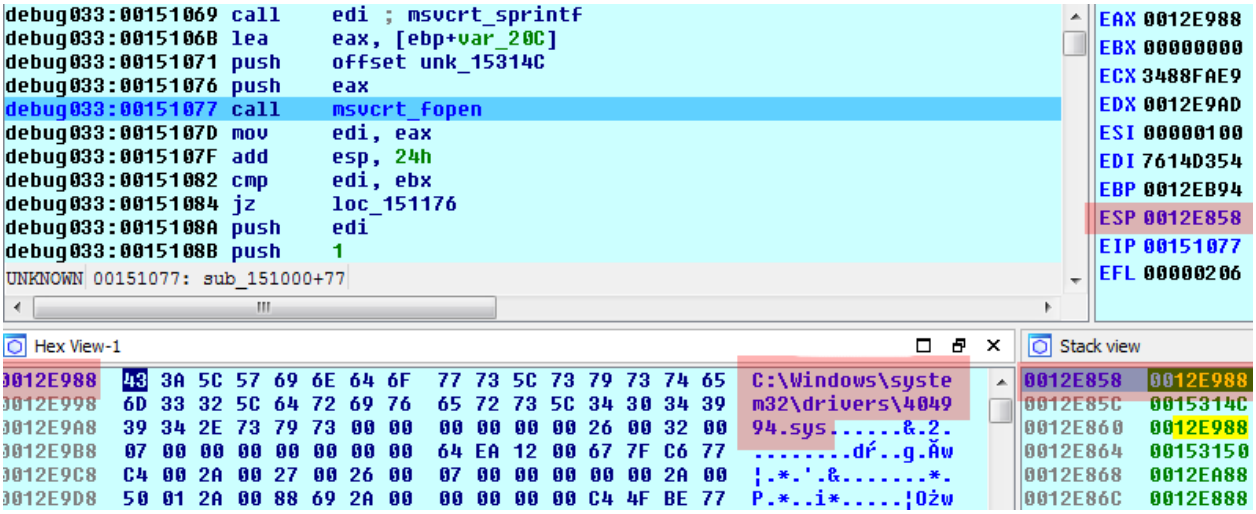
Zakończenie procedury infekowania stanowi uruchomienie zmodyfikowanej próbki z lokalizacji docelowej.



Rysunek 9: Uruchomienie próbki z lokalizacji docelowej

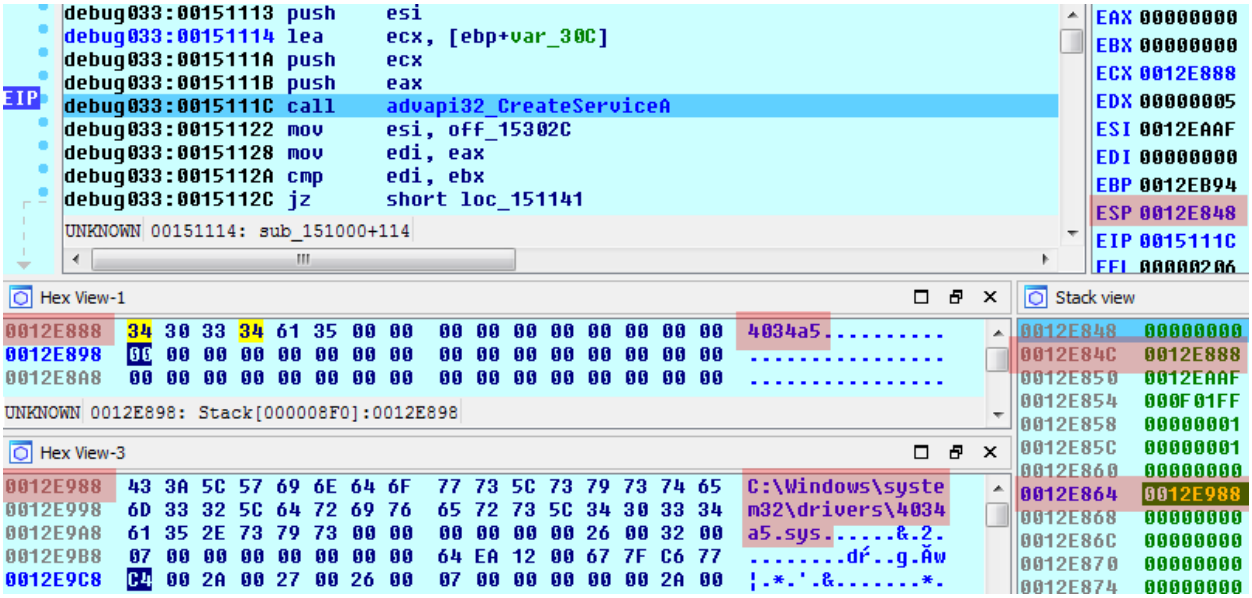
Uruchomienie z lokalizacji docelowej

Po uruchomieniu z lokalizacji docelowej Necurs podejmuje próbę zainstalowania rootkita. Jest nim sterownik, który w sytuacji, gdy konto ofiary posiada uprawnienia administracyjne, jest wypakowywany i zapisywany w lokalizacji C:\Windows\system32\drivers.



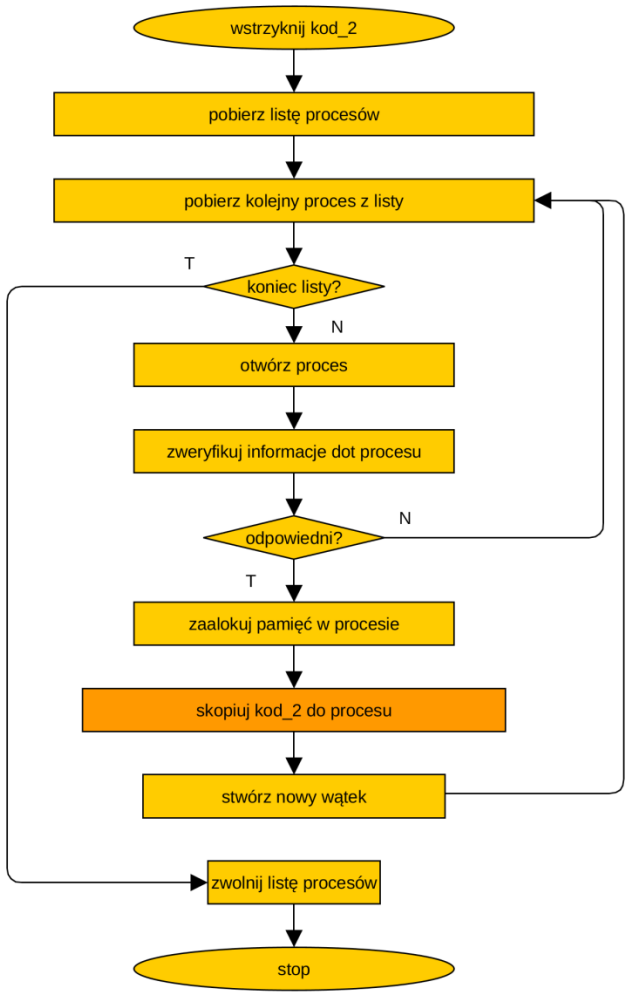
Rysunek 10: Wypakowywanie sterownika

W przypadku sukcesu w poprzednim kroku, dropper posługuje się wywołaniami Nadzorcy usług, by zarejestrować i uruchomić nową usługę. W efekcie doprowadza to do załadowania rootkita do jądra systemu ofiary. **Działanie rootkita Necurs zostanie opisane w kolejnych częściach raportu.**



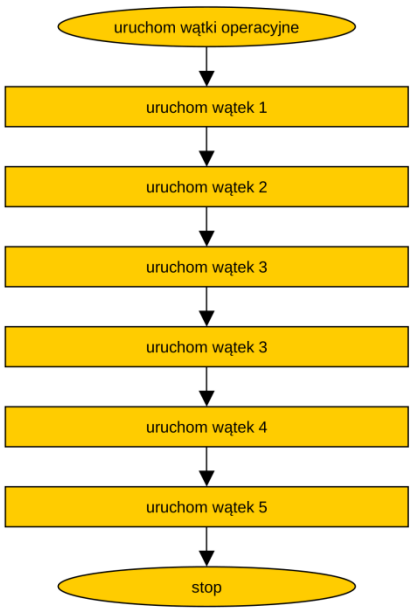
Rysunek 11: Załadowanie rootkita do jądra systemu ofiary

Kolejny krok po próbie załadowania rootkita stanowi wstrzyknięcie operacyjnego kodu do innych procesów działających w systemie. Dropper tworzy listę uruchomionych procesów i przegląda ją w poszukiwaniu kandydatów do wstrzyknięcia kodu. Dla każdego procesu działającego w systemie program weryfikuje, czy użytkownik ma prawo pisać do pamięci tego procesu oraz utworzyć w nim nowy wątek. W przypadku pozytywnej weryfikacji następuje wstrzyknięcie.



Rysunek 12: Schemat przeglądania procesów w poszukiwaniu kandydata do wstrzyknięcia kodu

Finalnym i najważniejszym etapem działania zainstalowanej próbki jest rozpoczęcie docelowych złośliwych operacji. Oprócz wstrzykniętych wątków sama próbka też rozpakowuje fragmenty kodu operacyjnego oraz uruchamia wykonujące go wątki, odpowiedzialne m.in. za monitorowanie i utrzymanie infekcji oraz komunikację do serwera Command&Control i wykonywanie otrzymanych tą drogą rozkazów oraz próbek. **Działanie tych wątków zostanie dokładniej przedstawione w kolejnych częściach raportu.**



Rysunek 13: Uruchamianie wątków operacyjnych Necurs w ramach zainstalowanej próbki

Podjęte działania

W ramach obsługi incydentu zgłoszonego przez klienta CERT Orange Polska aktywnie ograniczył zasięg zagrożenia. Po dalszej analizie zidentyfikowanych próbek, rozpoznane adresy IP i domeny scentralizowanej części kanału C&C zostały zablokowane, podobnie jak ruch do stron zawierających dropper Necurs.

W ramach niniejszej publikacji przedstawiliśmy architekturę infekcji w systemie zaatakowanego użytkownika. W kolejnych odcinkach raportu przedstawimy dokładną analizę wątków operacyjnych, komunikacji za pośrednictwem składników kanału C&C oraz podsumowanie telemetrycznych obserwacji z naszych sieci.

CERT Orange Polska radzi:

Pamiętaj, że Twój system jest atrakcyjnym celem dla cyberprzestępców. Dbaj o jego bezpieczeństwo. Jeśli nie posiadasz oprogramowania antywirusowego – zainstaluj je, a jeśli masz zainstalowane – aktualizuj regularnie bazę informacji o zagrożeniach. Nie uruchamiaj programów, które nie pochodzą ze zweryfikowanych źródeł, nie otwieraj załączników z wiadomości e-mail jeśli nie masz absolutnej pewności co do ich nadawcy.