



Necurs – analiza malware (1)



W trakcie analizy powłamaniovej 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	12eaeaaec7dae81c6d9bfead301b7c2a
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.

Your Digital Downloads

Your order is safe and secure

Download Instructions

1. Simply click on the link for each item you want to download.
2. If prompted, choose to **Save file**. Click **Save** and the file will be saved to your desktop or other location of your choice on your computer.



**How To Pass your Psychometric Tests + 2 Bonuses Download -
how2becomePsychometric001.htm**

Download link has expired. Please contact the vendor at info@how2become.co.uk.

Username:: htbpsy397

Password:: 71455008137

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

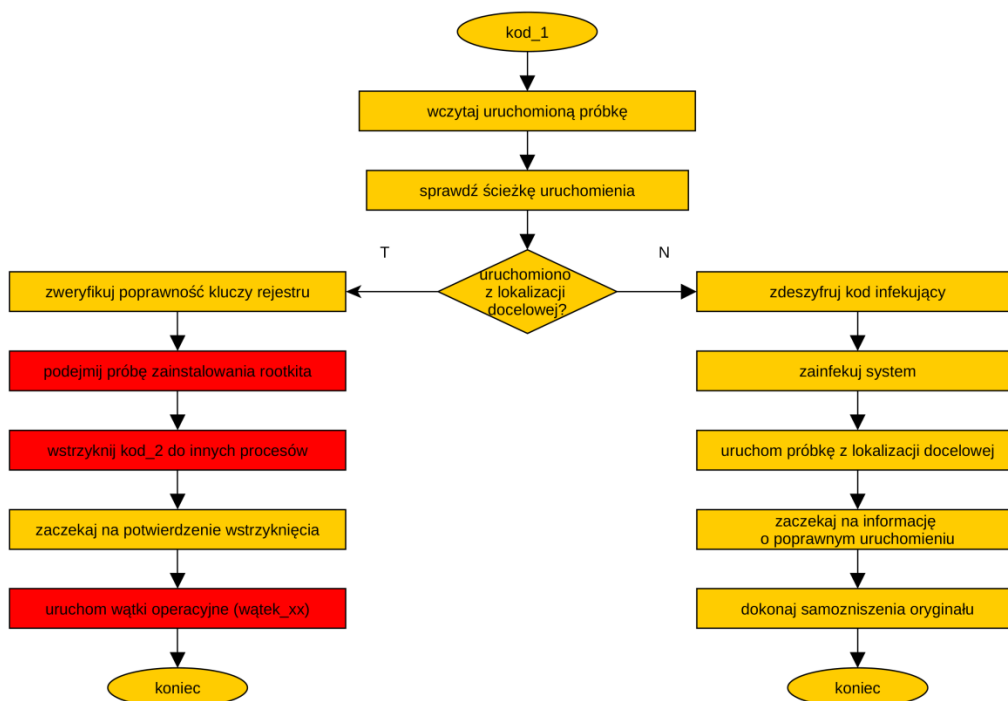
Protektor Necurs jest relatywnie prosty. Po zastosowaniu serii wywołań systemowych, ukrywających faktyczną rolę programu i kamuflujących go jako uprawnioną część oprogramowania, program przystępuje do zaalokowania pamięci na kod deszyfrujący, wypakowanie kodu ze swoich zasobów i przekazanie sterowania. 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 próbkę 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    0FFFFFFFh
.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

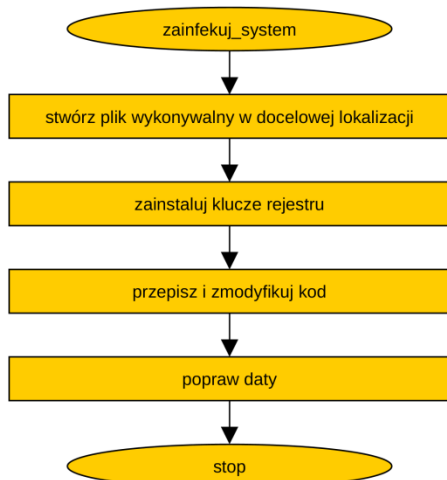


Rysunek 3: Ogólny schemat działania dropera Necurs

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

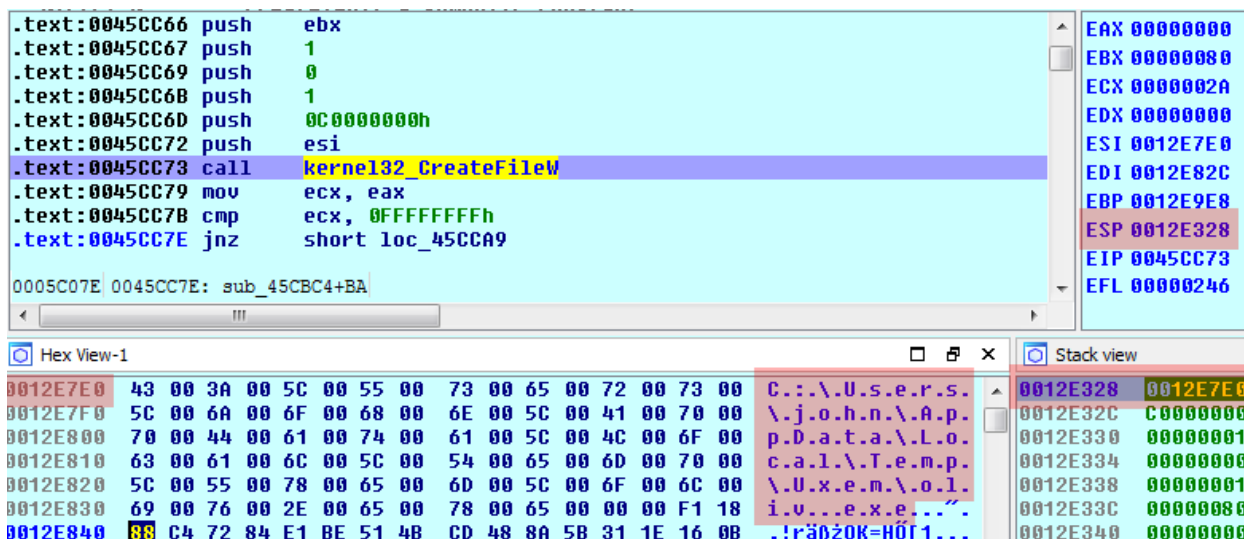
(C:\Users\<User>\AppData\Local\<pseudorandom_1>\<pseudorandom_2>.exe)

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.



```

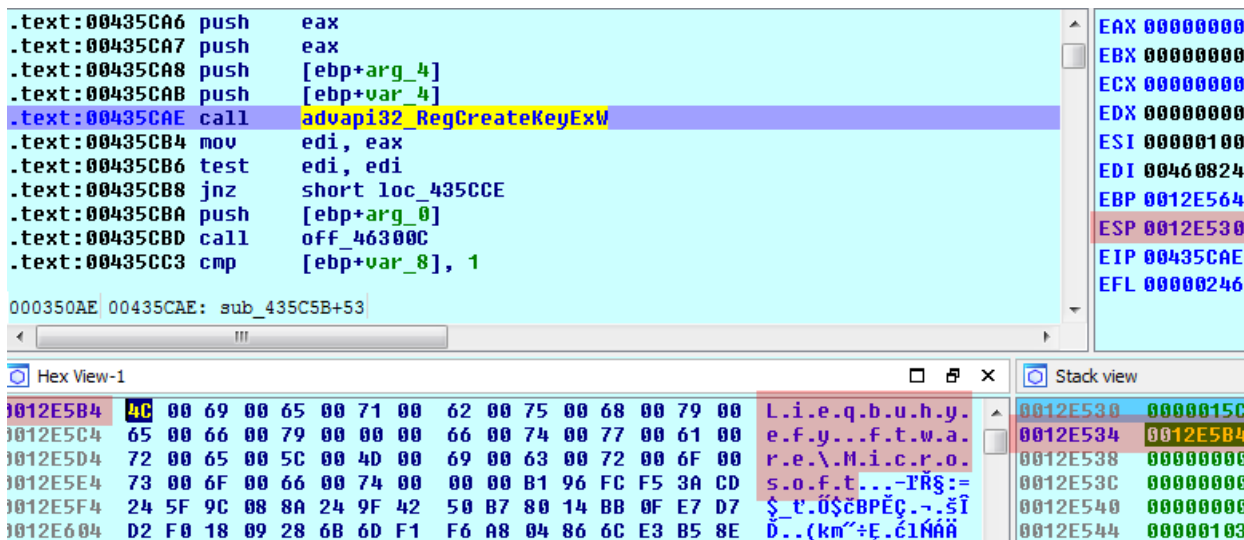
.text:0045CC66 push    ebx
.text:0045CC67 push    1
.text:0045CC69 push    0
.text:0045CC6B push    1
.text:0045CC6D push    0C000000h
.text:0045CC72 push    esi
.text:0045CC73 call    kernel32.CreateFileW
.text:0045CC79 mov     ecx, eax
.text:0045CC7B cmp     ecx, 0FFFFFFFh
.text:0045CC7E jnz     short loc_45CCA9

0005C07E 0045CC7E: sub_45CBC4+BA
  
```

Address	Value
0012E7E0	43 00 3A 00 5C 00 55 00
0012E7F0	5C 00 6A 00 6F 00 68 00
0012E800	70 00 44 00 61 00 74 00
0012E810	63 00 61 00 6C 00 5C 00
0012E820	5C 00 55 00 78 00 65 00
0012E830	69 00 76 00 2E 00 65 00
0012E840	88 C4 72 84 E1 BE 51 4B

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.



```

.text:00435CA6 push    eax
.text:00435CA7 push    eax
.text:00435CA8 push    [ebp+arg_4]
.text:00435CAB push    [ebp+var_4]
.text:00435CAE call    advapi32.RegCreateKeyExW
.text:00435CB4 mov     edi, eax
.text:00435CB6 test    edi, edi
.text:00435CB8 jnz     short loc_435CCE
.text:00435CBA push    [ebp+arg_0]
.text:00435CBD call    off_46300C
.text:00435CC3 cmp     [ebp+var_8], 1

000350AE 00435CAE: sub_435C5B+53
  
```

Address	Value
0012E5B4	4C 00 69 00 65 00 71 00
0012E5C4	65 00 66 00 79 00 00 00
0012E5D4	72 00 65 00 5C 00 4D 00
0012E5E4	73 00 6F 00 66 00 74 00
0012E5F4	24 5F 9C 08 8A 24 9F 42
0012E604	D2 F0 18 09 28 6B 6D F1

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.

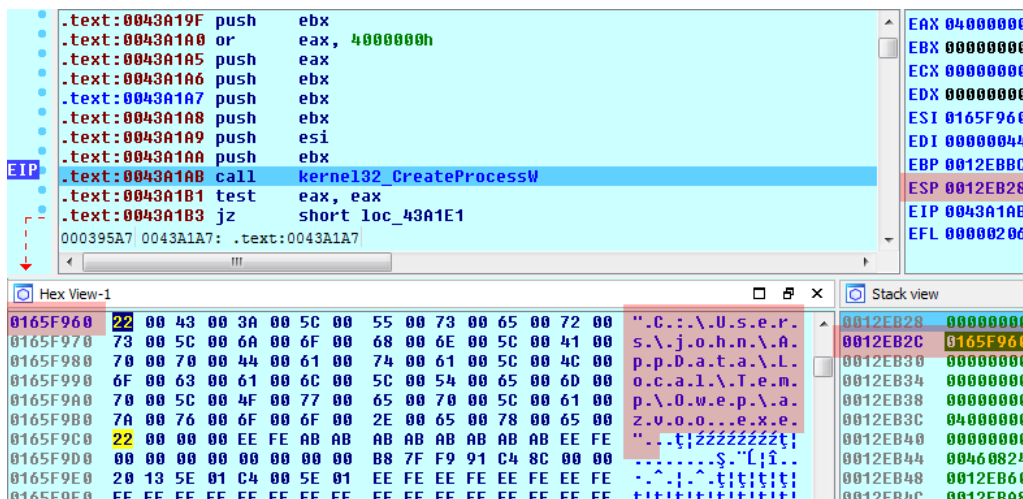
```
.text:0045EE8E push    eax
.text:0045EE8F push    [ebp+arg_4]
.text:0045EE92 push    [ebp+arg_0]
.text:0045EE95 push    dword ptr [ebx]
.text:0045EE97 call    kernel32_GetFileTime
.text:0045EE9D test     eax, eax
.text:0045EE9F jz      short loc_45EE80
.text:0045EEA1 test     esi, esi
.text:0045EEA3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

Rysunek 7: Pobranie daty modyfikacji katalogu domowego ofiary

```
.text:0045EDEC push    0
.text:0045EDEC 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 złośliwej 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.

```

debug033:00151069 call edi ; msvcrt_sprintf
debug033:0015106B lea eax, [ebp+var_20C]
debug033:00151071 push offset unk_15314C
debug033:00151076 push eax
debug033:00151077 call msvcrt_fopen
debug033:0015107D mov edi, eax
debug033:0015107F add esp, 24h
debug033:00151082 cmp edi, ebx
debug033:00151084 jz loc_151176
debug033:0015108A push edi
debug033:0015108B push 1
UNKNOWN 00151077: sub_151000+77
  
```

EAX	0012E988
EBX	00000000
ECX	3488FAE9
EDX	0012E9AD
ESI	00000100
EDI	7614D354
EBP	0012EB94
ESP	0012E858
EIP	00151077
EFL	00000206

0012E988	43 3A 5C 57 69 6E 64 6F 77 73 5C 73 79 73 74 65	C:\Windows\sys	0012E858	0012E988
0012E988	6D 33 32 5C 64 72 69 76 65 72 73 5C 34 30 34 39	m32\drivers\4049	0012E85C	0015314C
0012E988	39 34 2E 73 79 73 00 00 00 00 00 00 26 00 32 00	94.sys.....&.2.	0012E860	0012E988
0012E988	07 00 00 00 00 00 00 00 64 EA 12 00 67 7F C6 77	dř..g.Åw	0012E864	00153150
0012E9C8	C4 00 2A 00 27 00 26 00 07 00 00 00 00 00 2A 00	!.*.'.&.....*	0012E868	0012E888
0012E9D8	50 01 2A 00 88 69 2A 00 00 00 00 00 C4 4F BE 77	P.*..i*.....!0żw	0012E86C	0012E888

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.**

```

debug033:00151113 push esi
debug033:00151114 lea ecx, [ebp+var_30C]
debug033:0015111A push ecx
debug033:0015111B push eax
debug033:0015111C call advapi32_CreateServiceA
debug033:00151122 mov esi, off_15302C
debug033:00151128 mov edi, eax
debug033:0015112A cmp edi, ebx
debug033:0015112C jz short loc_151141
UNKNOWN 00151114: sub_151000+114
  
```

EAX	00000000
EBX	00000000
ECX	0012E888
EDX	00000005
ESI	0012EAAF
EDI	00000000
EBP	0012EB94
ESP	0012E848
EIP	0015111C
EFL	00000206

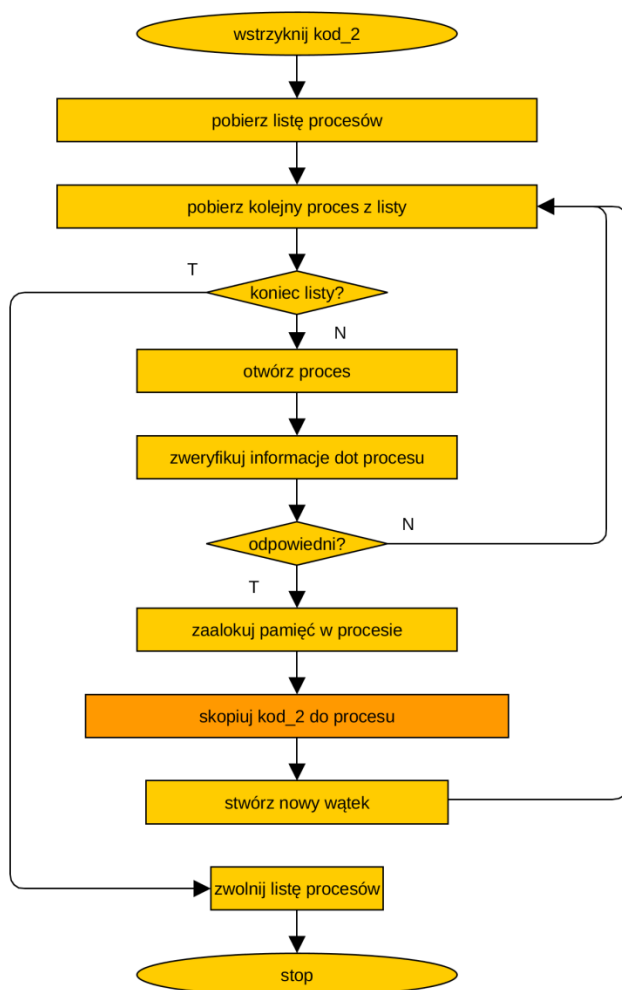
0012E888	34 30 33 34 61 35 00 00 00 00 00 00 00 00 00 00	4034a5.....	0012E848	00000000
0012E898	0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E84C	0012E888
0012E8A8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		0012E850	0012EAAF

UNKNOWN 0012E898: Stack[000008F0]:0012E898

0012E988	43 3A 5C 57 69 6E 64 6F 77 73 5C 73 79 73 74 65	C:\Windows\sys	0012E864	0012E988
0012E988	6D 33 32 5C 64 72 69 76 65 72 73 5C 34 30 33 34	m32\drivers\4034	0012E868	00000000
0012E988	61 35 2E 73 79 73 00 00 00 00 00 00 26 00 32 00	a5.sys.....&.2.	0012E86C	00000000
0012E988	07 00 00 00 00 00 00 00 64 EA 12 00 67 7F C6 77	dř..g.Åw	0012E870	00000000
0012E9C8	C4 00 2A 00 27 00 26 00 07 00 00 00 00 00 2A 00	!.*.'.&.....*	0012E874	00000000

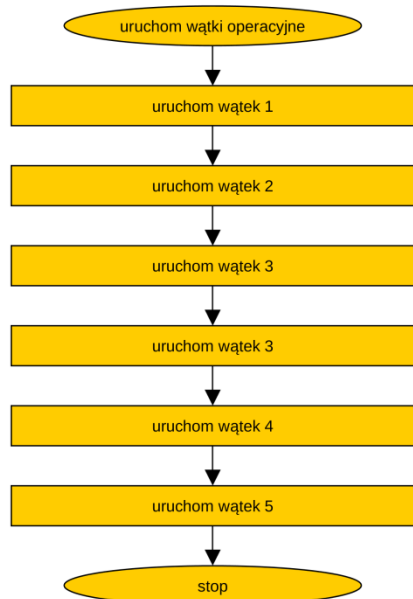
Rysunek 11: Załadowanie rootkita do jądra systemu ofiary

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.