Orange Polska S.A.
Bezpieczeństwo Systemów Teleinformatycznych / Wydział Operacji Bezpieczeństwa

Warszawa, 17.07.2017

Raport z analizy porównawczej rodzin ransomware JAFF i Cry

Próbka

Analizowana próbka to moduł PE32 o następujących skrótach kryptograficznych.

Md5	f5ebb00e1fb9bbcfe5ae742082e2002f
Sha256	41bce3e382cee06aa65fbee15fd38f7187fb090d5da78d868f57c84197689287
Sha512	295df12f3399ae468091029dbaea4574c864021f6e5ee00ce0a7480a1ed599ce7b72d5d04d105e751f61c61e417d9757805acfaa8c1f130e07cc04551f480dc4

Próbka została uzyskana w trakcie analizy powłamaniowej w systemie jednego z klientów Orange Polska. Klient otrzymał ją w postaci pliku .docm, załączonego do wiadomości e-mail, udającej informację z fakturą. Opisywany plik zawierał skrypt pobierający i usiłujący uruchomić właściwą próbkę.

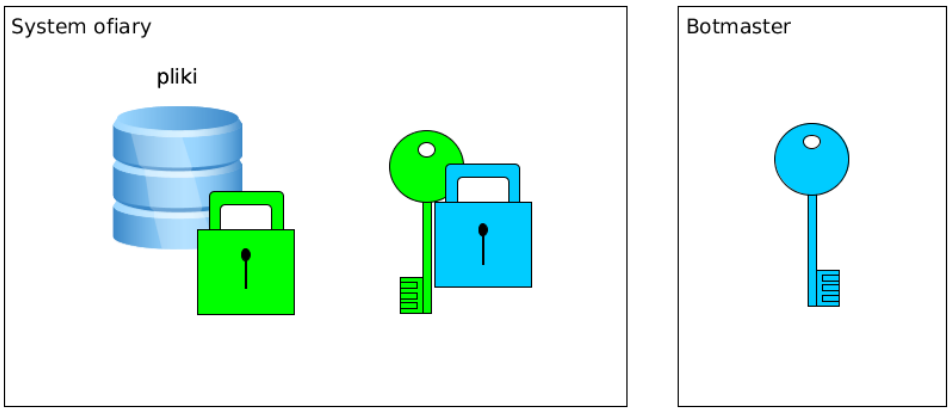
Działanie

Próbka przeszukuje dysk w systemie ofiary oraz odnalezione w sieci udostępnione zasoby w poszukiwaniu potencjalnie ważnych dokumentów. Po zlokalizowaniu szyfruje je i przedstawia ofierze żądanie okupu. Notatka od twórcy złośliwego oprogramowania sugeruje, że po uiszczeniu okupu ofierze zostanie udostępniony klucz, umożliwiający odzyskanie zaszyfrowanej zawartości.

Powiazania JAFF z Cry

W trakcie analizy próbki gatunku znanego pod nazwą JAFF ransomware, analitycy CERT Orange Polska natrafili na szereg poszlak wiążących ją z opisywanym wcześniej gatunkiem CryLocker. Według szacunków obie rodziny ransomware pokrywają się co najmniej w 70% funkcjonalności kodu (szczegóły znajdziecie w grudniowej analizie ransomware Cry, opublikowanej na naszej stronie). Poniżej przedstawiamy najważniejsze podobieństwa i różnice zidentyfikowane w tych dwóch próbkach.

Oba gatunki stosują mechanizm dwóch par kluczy asymetrycznych. Jedna z par kluczy jest identyczna dla wszystkich zainfekowanych maszyn (przy czym częścią prywatną dysponuje jedynie przestępca/botmaster), zaś druga jest unikalna dla każdej infekcji. Dzięki temu schematowi ransomware nie wymaga kontaktu z infrastrukturą C&C w celu wygenerowania klucza **przed** zaszyfrowaniem danych. Jest to niepokojący kierunek rozwoju oprogramowania klasy ransomware, który utrudni zapobieganie tego typu atakom w przyszłości.



Rysunek 1: Schemat zastosowania dwóch par kluczy

Zarówno Cry jak i JAFF wykorzystują do komunikacji z ofiarą o kanał C&C oparty na sieci TOR, która uniemożliwia lub znacznie utrudnia zlokalizowanie infrastruktury. Oba gatunki przedstawiają ofierze instrukcje, w której opisują, w jaki sposób korzystać z tego kanału w celu uiszczenia okupu.

Rysunek 2: Notatka z żądaniem okupu wygenerowana przez Cry

Rysunek 3: Notatka z żądaniem okupu wygenerowana przez JAFF

Zanim złośliwe oprogramowanie przystąpi do ataku na system ofiary, sprawdza, czy klawiatura posiada układ typowy dla Rosji (w obu przypadkach) oraz części krajów Europy Wschodniej (tylko Cry). Po wykryciu tych układów klawiatury, malware odstępuje od infekcji.

```
.text:00402EA9 push    0Ah
.text:00402EAB call    ds:user32_GetKeyboardLayoutList
.text:00402EB1 test    eax, eax
.text:00402EB3 jle     short loc_402EF8
.text:00402EB5 xor     edx, edx
.text:00402EB7 test    eax, eax
.text:00402EB9 jle     short loc_402EF8
.text:00402EBB jmp     short loc_402EC0
.text:00402EBD ; ---------------------------------------
.text:00402EBD lea     ecx, [ecx+0]
.text:00402EC0
.text:00402EC0 loc_402EC0:
.text:00402EC0
.text:00402EC0 mov     cx, [esp+edx*4+2Ch+var_28]
.text:00402EC5 mov     esi, 3FFh
.text:00402ECA and     cx, si
.text:00402ECD movzx   ecx, cx
.text:00402ED0 cmp     ecx, 23h
.text:00402ED3 jz      short loc_402EFF
.text:00402ED5 cmp     ecx, 3Fh
.text:00402ED8 jz      short loc_402EFF
.text:00402EDA cmp     ecx, 19h
.text:00402EDD jz      short loc_402EFF
.text:00402EDF cmp     ecx, 22h
```

Rysunek 4: Sprawdzenie układu klawiatury w Cry

```
.text:00405125 jnz     short near ptr unk_40516D
.text:00405127 call    ds:kernel32_GetSystemDefaultLangID
.text:0040512D mov     ecx, 3FFh
.text:00405132 and     ax, cx
.text:00405135 cmp     ax, 19h
.text:00405139 jz      short loc_405168
.text:0040513B call    ds:kernel32_GetUserDefaultLangID
.text:00405141 mov     edx, 3FFh
.text:00405146 and     ax, dx
.text:00405149 cmp     ax, 19h
.text:0040514D jz      short loc_405168
.text:0040514F call    ds:kernel32_GetUserDefaultUILanguage
.text:00405155 mov     ecx, 3FFh
.text:0040515A and     ax, cx
.text:0040515D cmp     ax, 19h
.text:00405161 jz      short loc_405168
.text:00405163 call    near ptr dword_401E6C+4
```

Rysunek 5: Sprawdzenie układu klawiatury w JAFF

Uderzająco podobne są do siebie również fragmenty protektorów pozyskanych do analizy obu próbek – to poszlaka najsilniej przemawiająca za powiązaniem pomiędzy tymi dwoma gatunkami.

```
.text:0040C0A5 add     eax, ecx
.text:0040C0A7
.text:0040C0A7 ; =============== S U B R O U
.text:0040C0A7
.text:0040C0A7
.text:0040C0A7 sub_40C0A7 proc near
.text:0040C0A7
.text:0040C0A7
.text:0040C0A7 arg_0= dword ptr  4
.text:0040C0A7
.text:0040C0A7 push    ecx
.text:0040C0A8 push    edx
.text:0040C0A9 mov     edx, [esp+8+arg_0]
.text:0040C0AD mov     ecx, [esp+8]
.text:0040C0B1 add     ecx, 0FFh
.text:0040C0B7 sub     ecx, edx
.text:0040C0B9 inc     ecx
.text:0040C0BA inc     ecx
.text:0040C0BB mov     [esp+8], ecx
.text:0040C0BF pop     edx
.text:0040C0C0 pop     ecx
.text:0040C0C1 retn    4
.text:0040C0C1 sub_40C0A7 endp
```

Rysunek 6: Mechanizm antidebug - fragment protektora oprogramowania Cry

```
.text:00419DB3 sub_419DB3 proc near
.text:00419DB3
.text:00419DB3
.text:00419DB3 arg_0= dword ptr  4
.text:00419DB3
.text:00419DB3 push    edx
.text:00419DB4 push    ecx
.text:00419DB5 mov     ecx, [esp+8]
.text:00419DB9 add     ecx, 0FFh
.text:00419DBF inc     ecx
.text:00419DC0 inc     ecx
.text:00419DC1 mov     edx, [esp+8+arg_0]
.text:00419DC5 sub     ecx, edx
.text:00419DC7 mov     [esp+8], ecx
.text:00419DCB pop     ecx
.text:00419DCC pop     edx
.text:00419DCD retn    4
.text:00419DCD sub_419DB3 endp
```

Rysunek 7: Fragment kodu protektora JAFF ransomware

Nowości w JAFF

Nowością w stosunku do Cry jest implementacja przeszukiwania sieci pod kątem udostępnionych zasobów, które próbka może zaszyfrować. Podobnie jak w Cry, szyfrowanie jest przeprowadzane w dedykowanym wątku, jednak w przeciwieństwie do poprzednika lista plików nie jest tworzona i następnie przekazywana do wątku. Malware tworzy za to specjalny obiekt IoCompletionPort, który służy do przekazywania zleceń dla dedykowanego wątku rekurencyjnego przeszukania i zaszyfrowania konkretnych zasobów.

```
.text:00401F19 mov     [ebp-1Ch], eax
.text:00401F1C call    ds:kernel32_CreateIoCompletionPort
.text:00401F22 lea     edx, [ebp-8Ch]
.text:00401F28 push    edx
.text:00401F29 mov     [ebp-90h], eax
.text:00401F2F call    ds:ntdll_RtlInitializeCriticalSection
.text:00401F35 push    ebx
```

Rysunek 8: Dedykowany wątek kolejno odbiera z kolejki IoCompletionPort zlecenia i przeprowadza szyfrowanie.

Ostatnią nowością jest poprawienie błędu (z punktu widzenia przestępcy) w próbce Cry, umożliwiającego częściowe lub całkowite odzyskanie zaszyfrowanej zawartości.

Podsumowanie

Powyższe informacje wskazują, że JAFF stanowi kolejny etap rozwoju ransomware Cry. Autorzy wykorzystali podobne techniki zabezpieczania próbki przed analizą, opóźnianie kontaktu z botmasterem i zastosowanie sieci TOR, jak również unikają infekowania ofiar posiadających rosyjski układ klawiatury.

W ramach działań mających na celu powstrzymanie rozprzestrzeniania się zagrożenia JAFF Orange zablokował możliwość pobierania szkodliwych załączników z rozpoznanych serwerów, powiązanych z tym złośliwym oprogramowaniem.

Jednocześnie przypominamy, że niezwykle istotne dla bezpieczeństwa danych użytkownika jest posiadanie aktualnego oprogramowania antywirusowego oraz unikanie otwierania załączników do maili nieoczekiwanych, dziwnie wyglądających, budzących nasz niepokój, gdy nie znamy osoby nadawcy, bądź mamy jakiekolwiek podejrzenie, czy wiadomość została wysłana przez deklarowanego nadawcę.