CryptXXX \ CrypMIC – intensywnie dystrybuowany ransomware w ramach exploit-kitów

Archived: 2026-04-05 13:02:41 UTC

W ostatnim czasie otrzymujemy zgłoszenia związane z infekcją ransomware znanym jako CryptXXX i jego naśladowcą CrypMIC.

Kampania

Zagrożenie pojawiło się kilka miesięcy temu jako moduł exploit-kita Neutrino. Infekcja następuje po wejściu na stronę na której publikowane są złośliwe reklamy (malvertising).

Celem ataku jest głównie nieaktualna wtyczka Adobe Flash Player (wersje do 21.0.0.213, podatność CVE-2016-4117). Złośliwe oprogramowanie dystrybuowane jest zamiennie z ransomware takim jak CryptoWall, TeslaCrypt, CryptoLocker i Cerber.

W ciągu dwóch tygodni czerwca twórcom CryptXXX udało się zarobić 70 BTC (na dzień wpisu jest to około 160 000 PLN / 41 000 USD). Lukratywność tego przedsięwzięcia spowodowała pojawienie się naśladowców, szukających szybkiego zarobku za pomocą malware określanego jako CrypMIC.

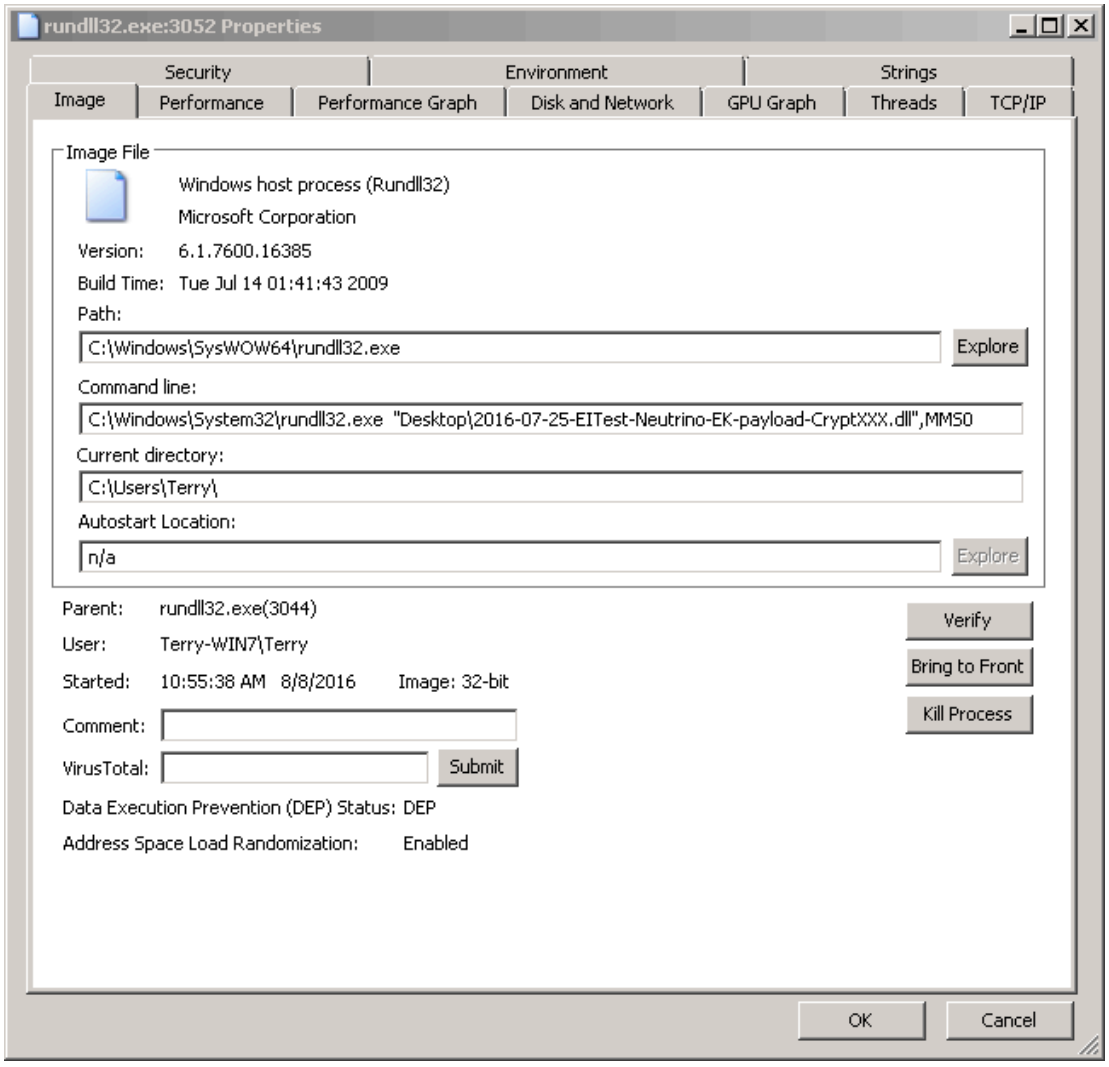
Bardzo rzadko zdarza się tyle podobieństw pomiędzy niespokrewnionymi rodzinami malware:

- Dostarczane jako biblioteki .DLL (w niektórych wersjach ten sam entry-point: XMS0\MMS0)
- Schemat nazewnictwa pliku w postaci: rad[losowy_ciąg_znaków].tmp.dll
- Żądany okup w wysokości 1,2 – 2,4 BTC
- Nazwy plików z informacją o okupie różnią się jedynie jedną literą (‚!’ na początku) i mają takie same rozszerzenia (.TXT, .BMP)
- Własny protokół komunikacji po TCP (port 443)
- Takie same stringi, mające identyfikować (prawdopodobnie) kampanię
- Szyfrowanie udziałów sieciowych oraz dysków wymiennych podłączonych do komputera w momencie infekcji
- Zbliżony układ graficzny i tekst na bitmapach z żądaniem okupu, ustawianych jako tapeta na pulpicie

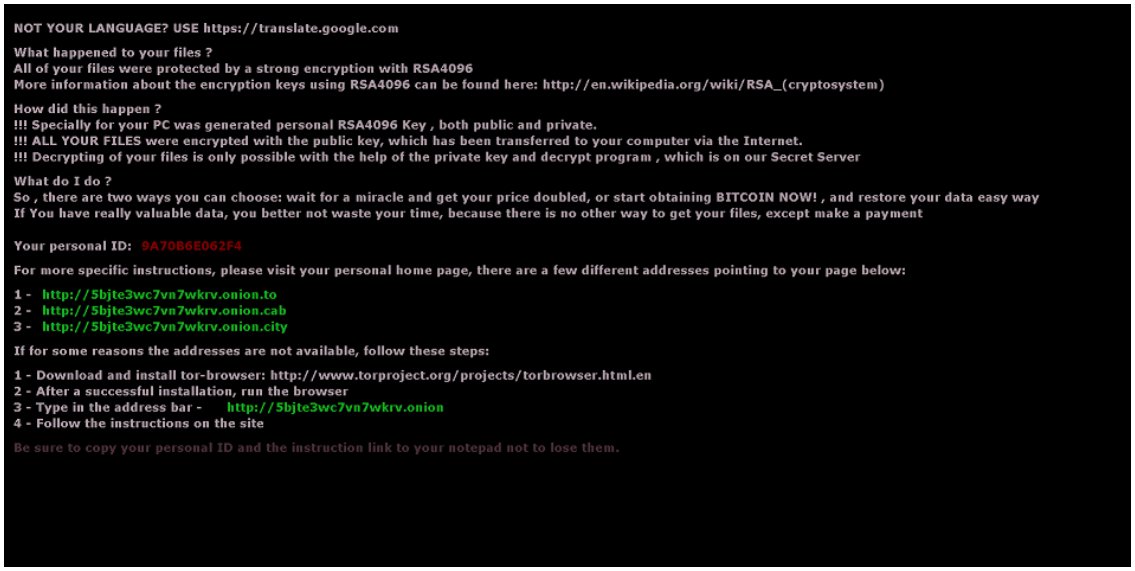
Szczegóły techniczne CryptXXX

CryptXXX jest napisany w Delphi i dystrybuowany, jak już wcześniej było wspomniane, jako biblioteka DLL. Uruchamiany jest w systemie ofiary za pomocą rundll32.exe lub regsvr32.exe.

Poniższy opis dotyczy wersji oznaczonej przez programistów jako 5.003 z dnia 25.07.16 (MD5: fb43d0a186f9952523a7e9ac1202da2a).



Po infekcji do folderu autostart użytkownika dodawany jest skrót o nazwie [12_znakowy_identyfikator_użytkownika].lnk, który wyświetla po uruchomieniu systemu żądanie okupu. Malware ma również funkcję przesłonięcia pulpitu z wiadomością o okupie, co skutkuje niemożnością korzystania z systemu operacyjnego.



Stringi, które odpowiadają za realizację funkcjonalności CryptXXX są zaciemnione za pomocą operacji bitowej XOR ze stałą wartością 0xEh (widoczne na zrzucie ekranowym poniżej). Malware korzysta jedynie z packera oraz niestandardowego protokołu komunikacji w celu utrudnienia analizy. Nie ma natomiast funkcjonalności wykrywania i blokady analizy w debuggerach czy środowiskach wirtualnych.

```
push    offset loc_100335B3
push    dword ptr fs:[eax]
mov     fs:[eax], esp
lea     ecx, [ebp-0Ch]
mov     edx, offset encypted_NOT_YOUR_LANGUAGE
mov     eax, 0Eh
call    DecryptString
push    dword ptr [ebp-0Ch]
push    offset off_10033668
lea     ecx, [ebp-10h]
mov     edx, offset encrypted_What_happened_to_your_files
mov     eax, 0Eh
call    DecryptString
push    dword ptr [ebp-10h]
push    offset off_100336C8
lea     ecx, [ebp-14h]
mov     edx, offset encrypted_All_of_your_files_were_protected
mov     eax, 0Eh
call    DecryptString
push    dword ptr [ebp-14h]
push    offset off_100336C8
lea     ecx, [ebp-18h]
mov     edx, offset encrypted_More_information_about_the_encryption_keys
mov     eax, 0Eh
call    DecryptString
push    dword ptr [ebp-18h]
```

Na chwilę obecną szyfrowane są pliki o 933 rozszerzeniach (pełna lista rozszerzeń znajduje się tutaj). Programiści postarali się i na liście rozszerzeń, oprócz tych najpopularniejszych, znajdziemy również takie jak: mobilne formaty wideo, aplikacje Android APK czy projekty środowiska programistycznego Apple Xcode. Szyfrowanie następuje za pomocą kombinacji algorytmów RSA i RC4. Po infekcji domeny do opłacenia okupu otrzymywane są od C&C.

W wersji 5.001 wysyłany jest również moduł o nazwie fx100.dll, służący do wykradania danych z przeglądarek internetowych, klientów poczty, klientów VPN czy komunikatorów. Niestety nie udało się go pozyskać z ostatniej wersji próbki.

Szczegóły techniczne CrypMIC

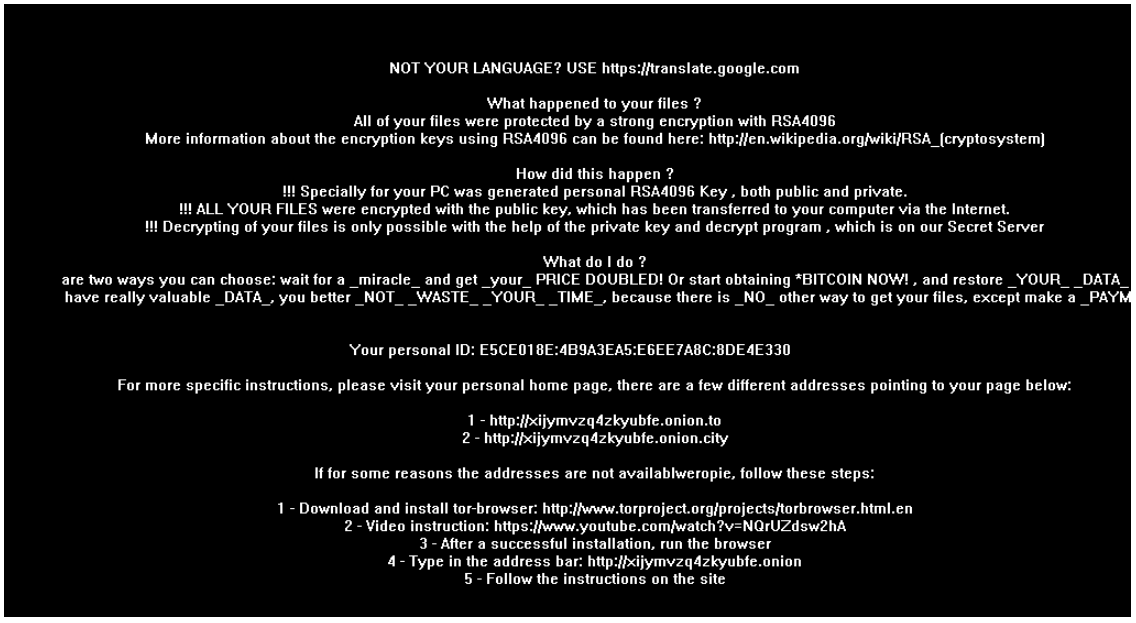
W przeciwieństwie do swojego pierwowzoru CrypMIC wyróżnia sie dużo mniejszym skomplikowaniem – stringi nie są zaciemnione oraz nie jest wykorzystywany moduł służący do kradzieży danych. Również ilość rozszerzeń szyfrowanych plików jest mniejsza – jest ich „zaledwie” 901 (pełna lista rozszerzeń znajduje się tutaj). Pliki szyfrowane są za pomocą algorytmu AES-256. Opis dotyczy wersji z dnia 05.08.16 (MD5: 584a2227d62e9e29b770d98c4b83844d).

```
a_pdn:
                unicode 0, <*.PDN>,0
a_pds:                                  ; DATA XREF: sub_100172A0+A↓o
                unicode 0, <*.PDS>,0
a_pdt:
                unicode 0, <*.PDT>,0
a_pe4:
                unicode 0, <*.PE4>,0
a_pef:                                  ; DATA XREF: sub_10016976+1B↓o
                unicode 0, <*.PEF>,0
a_pem:
                unicode 0, <*.PEM>,0
a_pff:                                  ; DATA XREF: sub_1001A6EC+93↓o
                unicode 0, <*.PFF>,0
a_pfi:
                unicode 0, <*.PFI>,0
a_pfs:
                unicode 0, <*.PFS>,0
a_pfv:                                  ; DATA XREF: sub_1001BC11+17↓o
                unicode 0, <*.PFV>,0
a_pfx:                                  ; DATA XREF: sub_1002A211+15↓o
                unicode 0, <*.PFX>,0
a_pgf:                                  ; DATA XREF: sub_100212D7+16↓o
                unicode 0, <*.PGF>,0
a_pgm:                                  ; DATA XREF: sub_10022D6A+1C↓o
                unicode 0, <*.PGM>,0
a_phm:                                  ; DATA XREF: sub_1001C1B5+F↓o
                unicode 0, <*.PHM>,0
```

Co ciekawe, CrypMIC potrafi wykryć uruchomienie w środowisku wirtualnym, jednak nie przeszkadza mu to w szyfrowaniu plików. Warto wspomnieć również o kasowaniu kopii plików wykonanych za pomocą mechanizmu Volume Shadow Copy – operacja wymaga podniesienia uprawnień, co spowoduje wyświetlenie okienka z User Account Control. Nie udzielenie zgody w tym oknie spowoduje zablokowanie operacji i ciągłe jego wyświetlanie do momentu udzielenia uprawnień.

Aktualizacja 01.09.16

Firma Fortinet odnotowała również ataki CrypMIC (błędnie rozpoznany we wpisie jako CryptXXX) w wersji .exe (MD5: 7bb58c27b807d0de43de40178ca30154). Poza zmianą sposobu uruchamiania nie odnotowaliśmy żadnych zmian w logice działania ransomware.



Jak sobie poradzić z ransomware?

W chwili obecnej najpewniejszym sposobem odzyskania plików po zaszyfrowaniu, jest posiadanie ich aktualnej kopii zapasowej. W przypadku CrypMIC programiści udostępnili niedziałający program deszyfrujący o nazwie Microsoft Decryptor – nawet po zapłaceniu okupu, odzyskanie plików było niemożliwe. Oczywiście należy również pamiętać o aktualizacjach zainstalowanego oprogramowania, systemu operacyjnego oraz sygnatur malware.

Dla zaawansowanych użytkowników, godne polecenia są dwa programy: honeypot AntiRansom, który tworzy i monitoruje fałszywe pliki pakietu Office, wykrywa procesy próbujące je modyfikować i je zamyka (dodatkowo tworzy zrzut pamięci procesu do późniejszej analizy), oraz ProcFilter wykorzystujący reguły YARA do wykrywania niepożądanych procesów.

W przypadku CryptXXX \ CrypMIC infekcji są w stanie zapobiec blockery reklam i skryptów (uBlock Origin, NoScript, uMatrix), włączenie w przeglądarce funkcji click-to-play oraz aktualna przeglądarka i komponent Adobe Flash Player.

Hashe próbek i reguły YARA

CrypMIC (05/08/16) SHA256:
52611b0c008fe84ecd68f89b9223c4a644935e42d7b8638dffe2e27552c2321e
CrypMIC (wersja EXE) SHA256:
eb72bef17b4f62a3cef6e36385cbdd65cf916f36b28d86b37b2990e2fc9e5330
CryptXXX (25/07/16) SHA256:
dc527934c6b26e65ce9cfdcd026795e978a53b7ee9a672551990ee583ed2a083

```
rule cryptxxx : ransomware
{
```

```
meta:
author="kamilf"

strings:
$string_decryption_loop = { 8B 55 FC 0F B7 54 5A FE 33 D7 66 89 54 58 FE 43 4E 75 E5 }
$dll_entry_point = { ( 4D | 58 ) 4D 53 ( 30 | 31 | 32 ) }
$file_encryption_loop = { 8B 45 E4 50 8D 45 E0 50 8D 85 5F FF FF FF 50 6A ?? 6A ?? 6A ?? }
$ransom_wallpaper_creation = { 8D 45 ?? 50 6A ?? 8D 85 [4] 50 8B [2] 50 E8 [4] 89 45 ?? 33 D2
55 68 [4] 64 FF 32 64 89 22 8B 45 ?? 50 }

condition:
3 of ($string_decryption_loop, $dll_entry_point, $file_encryption_loop,
$ransom_wallpaper_creation)
}

rule crypmic : ransomware
{
meta:
author="kamilf"

strings:
$vss_removal_tool = "vssadmin" wide
$ransom_note_loop = { 8A 8A [4] 88 0C 10 42 81 FA [4] 72 EE }
$readme_file_loop = { 8D 40 01 66 89 0C 17 8D 14 00 33 DB 0F B7 8A [4] 66 3B D9 }
$victim_id = { F3 0F 7E 05 [4] A0 [4] 8B 96 [4] 66 0F [4] F3 0F 7E 05 [4] 66 0F [4] }

condition:
2 of ($ransom_note_loop, $vss_removal_tool, $readme_file_loop, $victim_id)
}
```
