باسمه تعالی

تحلیل فنی باج‌افزار

TFlower

فهرست مطالب

۱. مقدمه :

در تاریخ ۳۰ ژوئیه سال ۲۰۱۹ میلادی، باج‌افزاری با عنوان TFlower مشاهده شد. بر اساس مشاهدات صورت‌گرفته، تمرکز اصلی این باج‌افزار بر روی سازمان‌ها و شرکت‌ها می‌باشد. طبق بررسی‌های انجام‌شده، باج‌افزار TFlower هیچ پسوندی را به فایل‌های رمزگذاری شده اضافه نمی‌کند و تنها نشانه اولیه آلودگی به این باج‌افزار، قرارگرفتن پیغام باج‌خواهی آن با عنوان !_Notice_!.txt در سیستم قربانی می‌باشد. باج‌افزار TFlower از الگوریتم AES جهت رمزگذاری فایل‌های مورد نظر خود در سیستم قربانی استفاده می‌کند. براساس اخبار منتشر شده، این باج‌افزار معمولاً از طریق پروتکل RDP به اهداف خود نفوذ کرده و مبلغ بسیار بالای ۷۰ بیت‌کوین باج را درخواست می‌دهد.

۲. مشخصات فایل اجرایی :

نام فایل	chilli.exe
MD5	0643324fa7f74a3c5288cde9d26c19a8
SHA-1	b8d671d96d49b8ed29a52919a77aeadf07ea74f0
SHA-256	bfb57cfbb7a887a81d3c8f5cff587f94ac0a60a3b6b0ef904653bf08aca21fa4
نوع فایل	Win32 EXE
اندازه فایل	۲.۱۵ مگابایت

فایل اجرایی این باج‌افزار دارای ٦ بخش است :

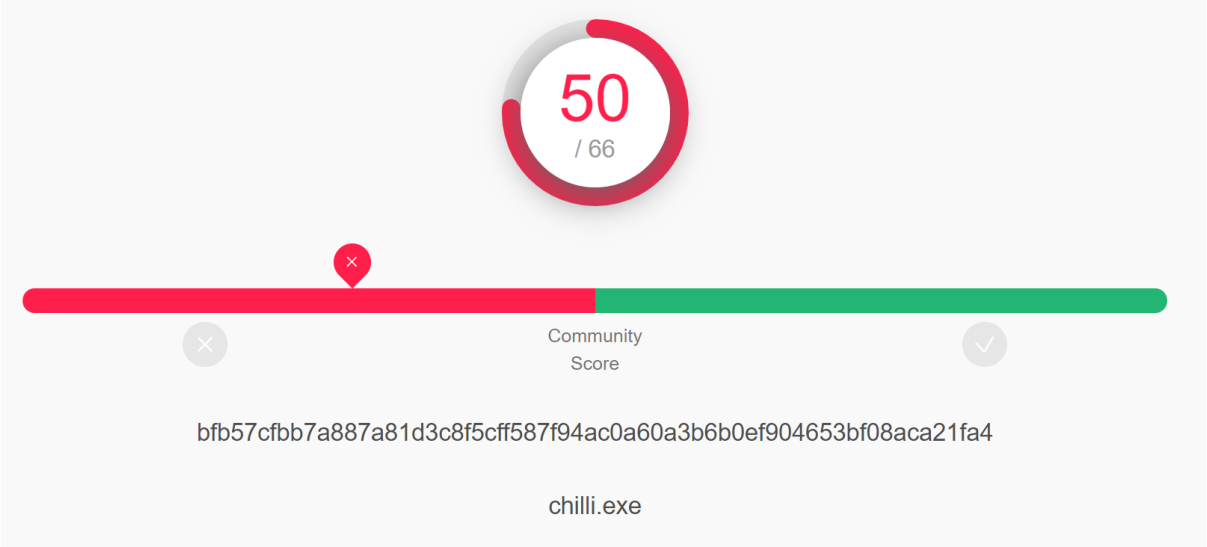
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
-	7.98	4096	1101824	523776
.rsrc	0	1105920	4096	0
.idata	1.31	1110016	4096	512
-	0.26	1114112	2924544	512
yeaqrpjm	7.95	4038656	1728512	1725952
hckhuela	3.42	5767168	4096	512

۳. شجره‌نامه

تاکنون والدی برای این باج‌افزار مشاهده نشده و به نظر می‌رسد باج‌افزار Tflower با هیچ باج‌افزاری ارتباط و یا شباهت ندارد.

٤. میزان تهدید فایل باج‌افزار

درحال حاضر تعداد ۵۰ مورد از ٦٦ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.

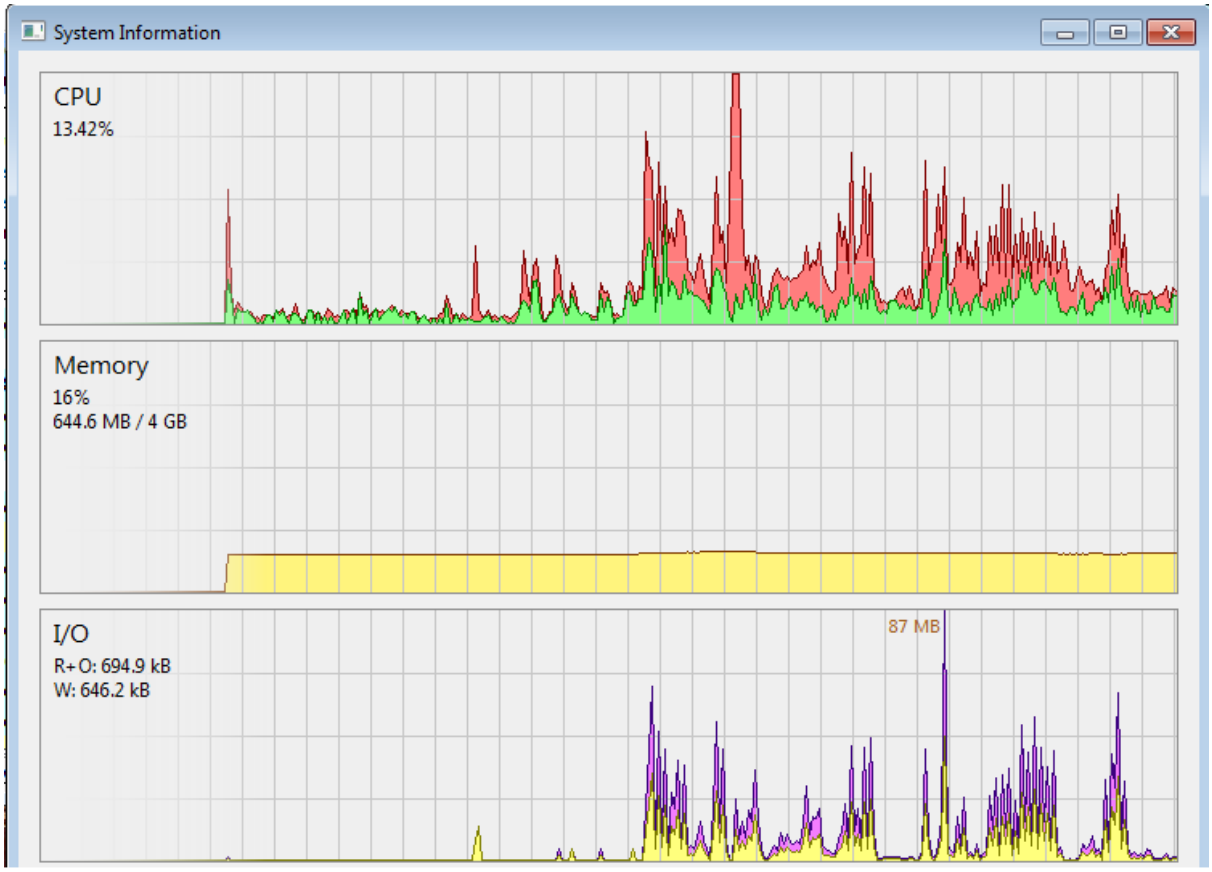


۵. تحلیل پویا

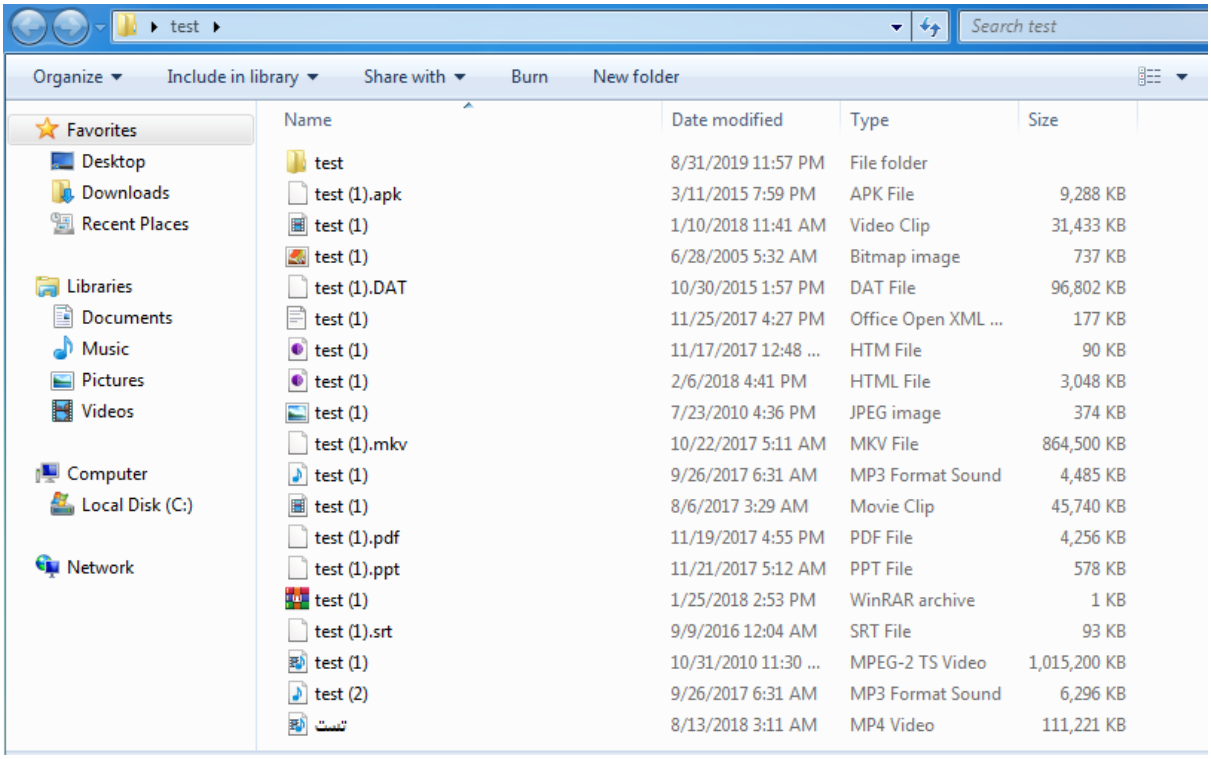
۵-۱ آناتومی حمله:

طبق بررسی‌های صورت گرفته، باج‌افزار TFlower به محض شروع فعالیت در سیستم قربانی، تمام دایرکتوری‌ها را اسکن نموده و سپس شروع به رمزگذاری فایل‌ها می‌نماید. فرآیند رمزنگاری بسته به منابع سیستم قربانی، بین ۲۰ الی ۳۰ دقیقه طول می‌کشد.

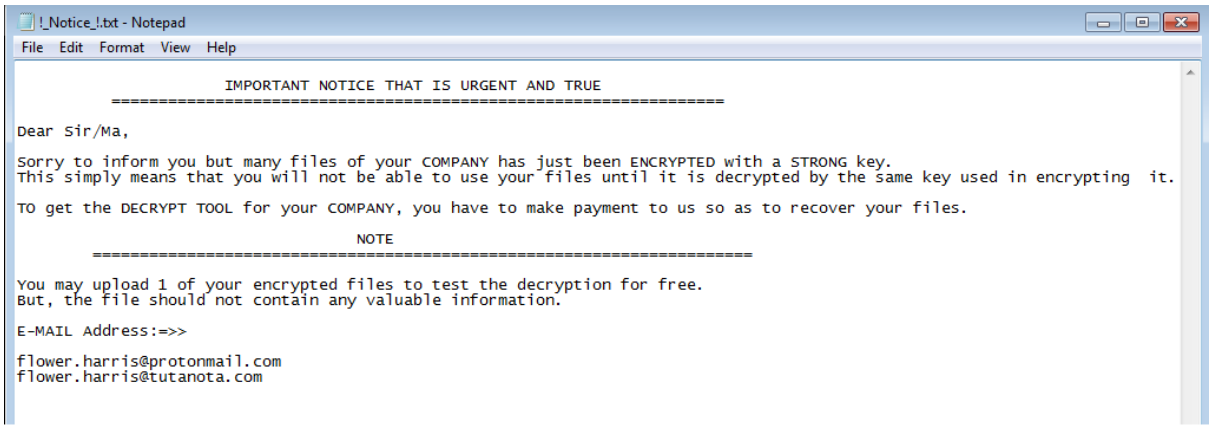
باج‌افزار با بهره‌گیری از منابع سیستم قربانی (CPU، Disk و I/O) فرآیند رمزنگاری را تکمیل می‌کند. همانطور که مشاهده می‌کنید حافظه RAM در یک مقدار ثابت باقی مانده است. بنابراین هرچه توان پردازشی پردازنده سیستم قربانی بالاتر بوده و سرعت خواندن/نوشتن دیسک نیز بیشتر باشد، رمزگذاری نیز سریعتر اتفاق می‌افتد.



در فرآیند رمزنگاری، این باج‌افزار هیچ پسوندی را به فایل‌های رمزگذاری شده اضافه نمی‌کند.



باج‌افزار TFlower فایل‌های با پسوند exe. را نیز رمزگذاری می‌کند. بنابراین نرم‌افزارهای نصب شده بر روی سیستم‌عامل پس از رمزگذاری دیگر قابل اجرا نمی‌باشند. این باج‌افزار سه فرآیند دیگر به نام‌های mscorsvw، sppsvc و svchost را نیز اجرا می‌کند. پیغام باج‌خواهی باج‌افزار TFlower نیز با نام !_Notice_!.txt بر روی دسکتاپ قرار می‌گیرد که محتوای آن در تصویر زیر قابل مشاهده است.



همانطور که در پیغام باج‌خواهی این باج‌افزار مشخص است، ابتدا به قربانی اطلاع داده شده که تمام فایل‌های موجود در سیستم وی رمزگذاری شده است و تنها راه بازیابی آن‌ها، انجام دستورالعمل‌های ارایه شده در پیغام باج‌خواهی می‌باشد. سپس عنوان شده است که فایل‌ها با همان کلیدی که رمز شده‌اند قابل رمزگشایی هستند که این مورد نشان می‌دهد مهاجم از الگوریتم رمزنگاری متقارن در فرآیند رمزگذاری استفاده کرده است. در ادامه، به قربانی پیشنهاد داده شده است تا یک فایل رمز شده که فاقد اطلاعات ارزشمندی است را برای راستی آزمایی به آدرس‌های ایمیل flower.harris@protonmail.com و flower.harris@tutanota.com ارسال کند تا به صورت رمزگشایی شده تحویل بگیرد. فایل باج‌افزار پس از اتمام فرآیند رمزگذاری همچنان به صورت فعال در سیستم باقی میماند.

تغییرات رجیستری ایجاد شده توسط باج‌افزار در طول فعالیت در سیستم قربانی نیز، به صورت زیر می‌باشد:

کلیدهای اضافه شده:

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASAPI32

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASMANCS

HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\F373B387065A28848AF2F34ACE192BDDC78E9CAC

مقادیر اضافه شده:

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASAPI32\EnableFileTracing: 0x00000000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASAPI32\EnableConsoleTracing: 0x00000000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASAPI32\FileTracingMask: 0xFFFF0000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASAPI32\ConsoleTracingMask: 0xFFFF0000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASAPI32\MaxFileSize: 0x00100000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASAPI32\FileDirectory: "%windir%\tracing"

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASMANCS\EnableFileTracing: 0x00000000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASMANCS\EnableConsoleTracing: 0x00000000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASMANCS\FileTracingMask: 0xFFFF0000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASMANCS\ConsoleTracingMask: 0xFFFF0000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASMANCS\MaxFileSize: 0x00100000

HKLM\SOFTWARE\Microsoft\Tracing\sample_RASMANCS\FileDirectory: "%windir%\tracing"

HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\F373B387065A28848AF2F34ACE192BDDC78E9CAC\Blob: 03 00 00 00 01 00 00 00 14 00 00 00 F3 73 B3 87 06 5A 28 84 8A F2 F3 4A CE 19 2B DD C7 8E 9C AC 1D 00 00 00 01 00 00 00 10 00 00 00 95 B4 47 5F EF 63 CA F7 45 2D 10 FA A6 F6 36 2B 14 00 00 00 01 00 00 00 14 00 00 00 52 D8 88 3A C8 9F 78 66 ED 89 F3 7B 38 70 94 C9 02 02 36 D0 53 00 00 00 01 00 00 00 20 00 00 00 30 1E 30 1C 06 06 2B 81 1F 01 11 01 30 12 30 10 06 0A 2B 06 01 04 01 82 37 3C 01 01 03 02 00 C0 62 00 00 00 01 00 00 00 20 00 00 00 55 92 60 84 EC 96 3A 64 B9 6E 2A BE 01 CE 0B A8 6A 64 FB FE BC C7 AA B5 AF C1 55 B3 7F D7 60 66 09 00 00 00 01 00 00 00 34 00 00 00 30 32 06 08 2B 06 01 05 05 07 03 01 06 08 2B 06 01 05 05 07 03 02 06 08 2B 06 01 05 05 07 03 04 06 08 2B 06 01 05 05 07 03 08 06 08 2B 06 01 05 05 07 03 03 0B 00 00 00 01 00 00 00 3E 00 00 00 41 00 63 00 74 00 61 00 6C 00 69 00 73 00 20 00 41 00 75 00 74 00 68 00 65 00 6E 00 74 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 20 00 52 00 6F 00 6F 00 74 00 20 00 43 00 41 00 00 00 20 00 00 00 01 00 00 00 BF 05 00 00 30 82 05 BB 30 82 03 A3 A0 03 02 01 02 02 08 57 0A 11 97 42 C4 E3 CC 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 30 6B 31 0B 30 09 06 03 55 04 06 13 02 49 54 31 0E 30 0C 06 03 55 04 07 0C 05 4D 69 6C 61 6E 31 23 30 21 06 03 55 04 0A 0C 1A 41 63 74 61 6C 69 73 20 53 2E 70 2E 41 2E 2F 30 33 33 35 38 35 32 30 39 36 37 31 27 30 25 06 03 55 04 03 0C 1E 41 63 74 61 6C 69 73 20 41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 52 6F 6F 74 20 43 41 30 1E 17 0D 31 31 30 39 32 32 31 31 32 32 30 32 5A 17 0D 33 30 30 39 32 32 31 31 32 32 30 32 5A 30 6B 31 0B 30 09 06 03 55 04 06 13 02 49 54 31 0E 30 0C 06 03 55 04 07 0C 05 4D 69 6C 61 6E 31 23 30 21 06 03 55 04 0A 0C 1A 41 63 74 61 6C 69 73 20 53 2E 70 2E 41 2E 2F 30 33 33 35 38 35 32 30 39 36 37 31 27 30 25 06 03 55 04 03 0C 1E 41 63 74 61 6C 69 73 20 41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 52 6F 6F 74 20 43 41 30 82 02 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 02 0F 00 30 82 02 0A 02 82 02 01 00 A7 C6 C4 A5 29 A4 2C EF E5 18 C5 B0 50 A3 6F 51 3B 9F 0A 5A C9 C2 48 38 0A C2 1C A0 18 7F 91 B5 87 B9 40 3F DD 1D 68 1F 08 83 D5 2D 1E 88 A0 F8 8F 56 8F 6D 99 02 92 90 16 D5 5F 08 6C 89 D7 E1 AC BC 20 C2 B1 E0 83 51 8A 69 4D 00 96 5A 6F 2F C0 44 7E A3 0E E4 91 CD 58 EE DC FB C7 1E 45 47 DD 27 B9 08 01 9F A6 21 1D F5 41 2D 2F 4C FD 28 AD E0 8A AD 22 B4 56 65 8E 86 54 8F 93 43 29 DE 39 46 78 A3 30 23 BA CD F0 7D 13 57 C0 5D D2 83 6B 48 4C C4 AB 9F 80 5A 5B 3A BD C9 A7 22 3F 80 27 33 5B 0E B7 8A 0C 5D 07 37 08 CB 6C D2 7A 47 22 44 35 C5 CC CC 2E 8E DD 2A ED B7 7D 66 0D 5F 61 51 22 55 1B E3 46 E3 E3 3D D0 35 62 9A DB AF 14 C8 5B A1 CC 89 1B E1 30 26 FC A0 9B 1F 81 A7 47 1F 04 EB A3 39 92 06 9F 99 D3 BF D3 EA 4F 50 9C 19 FE 96 87 1E 3C 65 F6 A3

18 24 83 86 10 E7 54 3E A8 3A 76 24 4F 81 21 C5 E3 0F 02 F8 93 94 47 20 BB FE D4 0E D3 68 B9 DD C4 7A 84 82 E3 53 54 79 DD DB 9C D2 F2 07 9B 2E B6 BC 3E ED 85 6D EF 25 11 F2 97 1A 42 61 F7 4A 97 E8 8B B1 10 07 FA 65 81 B2 A2 39 CF F7 3C FF 18 FB C6 F1 5A 8B 59 E2 02 AC 7B 92 D0 4E 14 4F 59 45 F6 0C 5E 28 5F B0 E8 3F 45 CF CF AF 9B 6F FB 84 D3 77 5A 95 6F AC 94 84 9E EE BC C0 4A 8F 4A 93 F8 44 21 E2 31 45 61 50 4E 10 D8 E3 35 7C 4C 19 B4 DE 05 BF A3 06 9F C8 B5 CD E4 1F D7 17 06 0D 7A 95 74 55 0D 68 1A FC 10 1B 62 64 9D 6D E0 95 A0 C3 94 07 57 0D 14 E6 BD 05 FB B8 9F E6 DF 8B E2 C6 E7 7E 96 F6 53 C5 80 34 50 28 58 F0 12 50 71 17 30 BA E6 78 63 BC F4 B2 AD 9B 2B B2 FE E1 39 8C 5E BA 0B 20 94 DE 7B 83 B8 FF E3 56 8D B7 11 E9 3B 8C F2 B1 C1 5D 9D A4 0B 4C 2B D9 B2 18 F5 B5 9F 4B 02 03 01 00 01 A3 63 30 61 30 1D 06 03 55 1D 0E 04 16 04 14 52 D8 88 3A C8 9F 78 66 ED 89 F3 7B 38 70 94 C9 02 02 36 D0 30 0F 06 03 55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 1F 06 03 55 1D 23 04 18 30 16 80 14 52 D8 88 3A C8 9F 78 66 ED 89 F3 7B 38 70 94 C9 02 02 36 D0 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 01 06 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 03 82 02 01 00 0B 7B 72 87 C0 60 A6 49 4C 88 58 E6 1D 88 F7 14 64 48 A6 D8 58 0A 0E 4F 13 35 DF 35 1D D4 ED 06 31 C8 81 3E 6A D5 DD 3B 1A 32 EE 90 3D 11 D2 2E F4 8E C3 63 2E 23 66 B0 67 BE 6F B6 C0 13 39 60 AA A2 34 25 93 75 52 DE A7 9D AD 0E 87 89 52 71 6A 16 3C 19 1D 83 F8 9A 29 65 BE F4 3F 9A D9 F0 F3 5A 87 21 71 80 4D CB E0 38 9B 3F BB FA E0 30 4D CF 86 D3 65 10 19 18 D1 97 02 B1 2B 72 42 68 AC A0 BD 4E 5A DA 18 BF 6B 98 81 D0 FD 9A BE 5E 15 48 CD 11 15 B9 C0 29 5C B4 E8 88 F7 3E 36 AE B7 62 FD 1E 62 DE 70 78 10 1C 48 5B DA BC A4 38 BA 67 ED 55 3E 5E 57 DF D4 03 40 4C 81 A4 D2 4F 63 A7 09 42 09 14 FC 00 A9 C2 80 73 4F 2E C0 40 D9 11 7B 48 EA 7A 02 C0 D3 EB 28 01 26 58 74 C1 C0 73 22 6D 93 95 FD 39 7D BB 2A E3 F6 82 E3 2C 97 5F 4E 1F 91 94 FA FE 2C A3 D8 76 1A B8 4D B2 38 4F 9B FA 1D 48 60 79 26 E2 F3 FD A9 D0 9A E8 70 8F 49 7A D6 E5 BD 0A 0E DB 2D F3 8D BF EB E3 A4 7D CB C7 95 71 E8 DA A3 7C C5 C2 F8 74 92 04 1B 86 AC A4 22 53 40 B6 AC FE 4C 76 CF FB 94 32 C0 35 9F 76 3F 6E E5 90 6E A0 A6 26 A2 B8 2C BE D1 2B 85 FD A7 68 C8 BA 01 2B B1 6C 74 1D B8 73 95 E7 EE B7 C7 25 F0 00 4C 00 B2 7E B6 0B 8B 1C F3 C0 50 9E 25 B9 E0 08 DE 36 66 FF 37 A5 D1 BB 54 64 2C C9 27 B5 4B 92 7E 65 FF D3 2D E1 B9 4E BC 7F A4 41 21 90 41 77 A6 39 1F EA 9E E3 9F D0 66 6F 05 EC AA 76 7E BF 6B 16 A0 EB B5 C7 FC 92 54 2F 2B 11 27 25 37 78 4C 51 6A B0 F3 CC 58 5D 14 F1 6A 48 15 FF C2 07 B6 B1 8D 0F 8E 5C 50 46 B3 3D BF 01 98 4F B2 59 54 47 3E 34 7B 78 6D 56 93 2E 73 EA 66 28 78 CD 1D 14 BF A0 8F 2F 2E B8 2E 8E F2 14 8A CC E9 B5 7C FB 6C 9D 0C A5 E1 96

HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\23\52C64B7E\@C:\Windows\system32\notepad.exe,-469: "Text Document"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\HO-PREG\Qrfxgbc\fnzcyr.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 80 6E CB 4D 85 73 D5 01 00 00 00 00

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Run\proxycap: "C:\Users\UB-CERT\Desktop\sample.exe"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\MuiCache\23\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042: "Peer to Peer Trust"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local Settings\MuiCache\23\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103: "Domain Name System (DNS) Server Trust"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\MuiCache\23\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042: "Peer to Peer Trust"

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local Settings\MuiCache\23\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103: "Domain Name System (DNS) Server Trust"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\23\52C64B7E\@C:\Windows\system32\notepad.exe,-469: "Text Document"

کلیدهایی که مقادیر آن‌ها تغییر پیدا کرده است:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\CurrentLanguage\Counter

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}ComputeIgnorableProduct (Enter)

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}ComputeIgnorableProduct (Leave)

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter)

HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave)

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}ComputeIgnorableProduct (Enter)

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}ComputeIgnorableProduct (Leave)

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Enter)

HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-806e6f6e6963}DeleteProcess (Leave)

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{645FF040-5081-101B-9F08-"00AA002F954E}\DefaultIcon\: "C:\Windows\System32\imageres.dll,-54

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{645FF040-5081-101B-9F08-"00AA002F954E}\DefaultIcon\: "C:\Windows\System32\imageres.dll,-55

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{7P5N40RS-N0SO-4OSP-874N-P0S2R0O9SN8R}\Ertfubg 1.8.3\i5_ertfubg_1.8.3_orgn1_jva32_k64_fep_ova_i5\ertfubg.rkr

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

۵-۲ روش انتشار:

براساس اخبار منتشر شده از قربانیان، این باج‌افزار اغلب از طریق پروتکل‌های RDP آسیب‌پذیر و محافظت نشده در بستر اینترنت به اهداف خود نفوذ می‌کند.

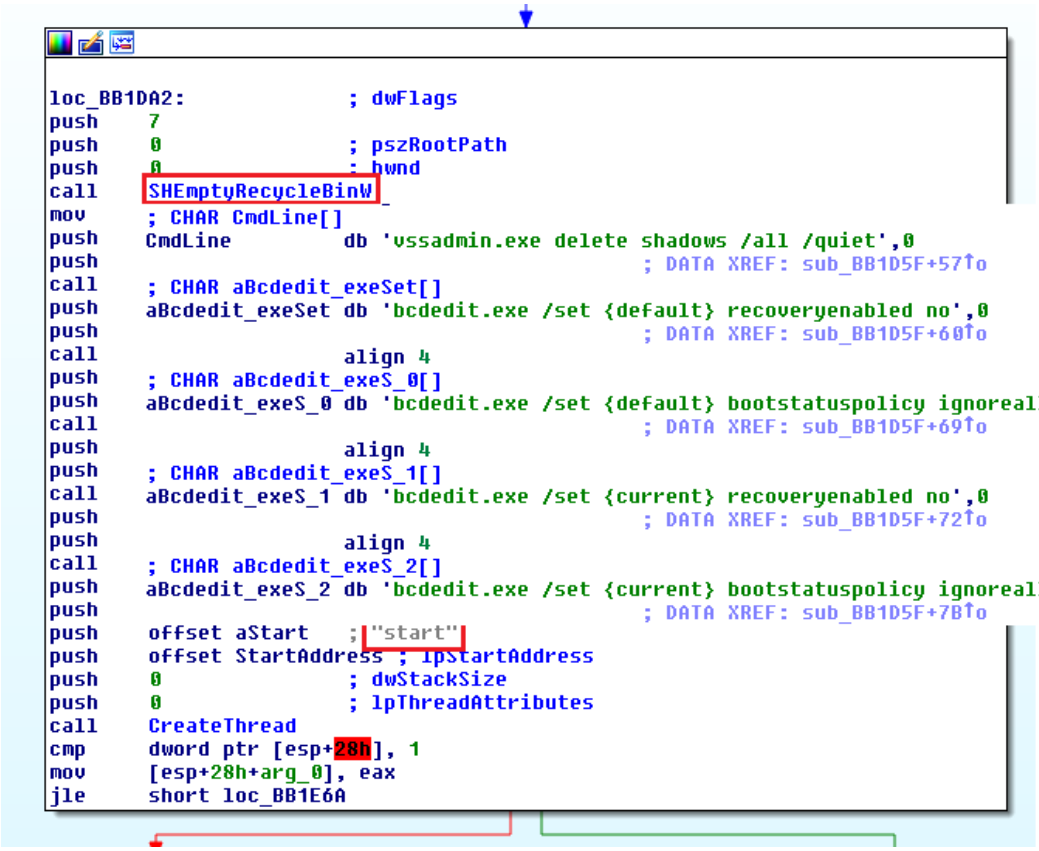
۵-۳ روش جلوگیری:

با توجه به روش رایج نفوذ این باج‌افزار، اکیداً توصیه می‌شود در صورتی که جهت ارتباطات خود از پروتکل RDP استفاده می‌نمایید، اقدامات مربوط به امن‌سازی این پروتکل نظیر رمزعبور پیچیده، احراز هویت دوعاملی و ... را انجام دهید.

٦. تحلیل ایستا

٦-١ تحلیل کد:

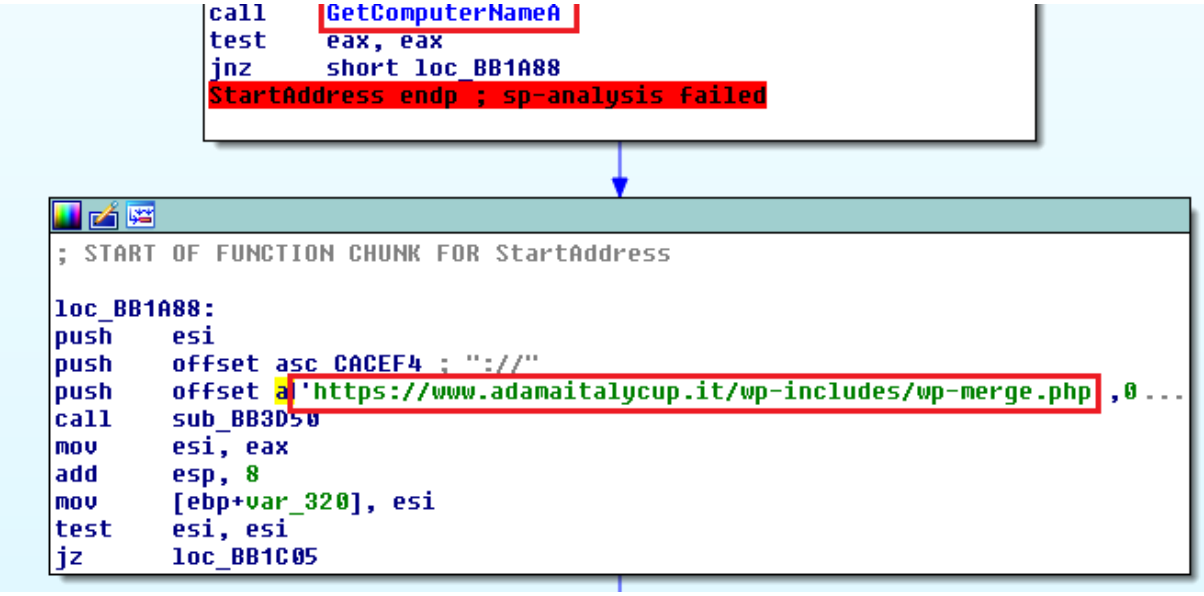
پس از تحلیل کد باج‌افزار، نتایج زیر حاصل گردید. این باج‌افزار درابتدای فعالیت خود محتوای تمام فضاهای Recycle Bin درون سیستم قربانی را پاک می‌کند.



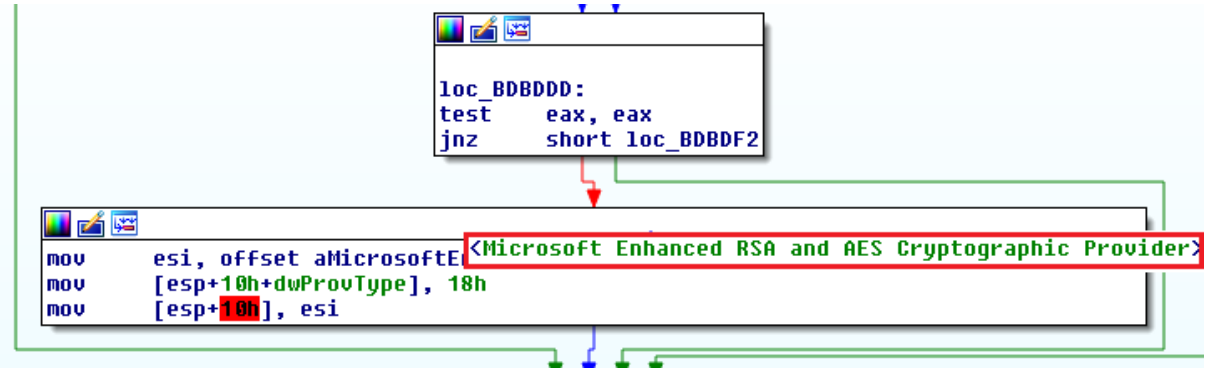
سپس همانطور که در تصویر بالا مشخص است، دستورات زیر را اجرا می‌کند.

vssadmin.exe delete shadows /all /quiet	حذف فضای VSS
bcdedit /set {default} recoveryenabled No	غیرفعال سازی قابلیت Automatic Startup Repair
bcdedit /set {default} bootstatuspolicy ignoreallfailures	غیرفعال سازی قابلیت Windows Error Recovery در هنگام بوت شدن ویندوز
bcdedit /set {current} recoveryenabled No	غیرفعال سازی قابلیت Automatic Startup Repair
bcdedit /set {current} bootstatuspolicy ignoreallfailures	غیرفعال سازی قابلیت Windows Error Recovery

در طول فعالیت باج‌افزار در سیستم قربانی، اطلاعات سیستم قربانی به آدرس مشخص شده در تصویر زیر ارسال می‌شود.

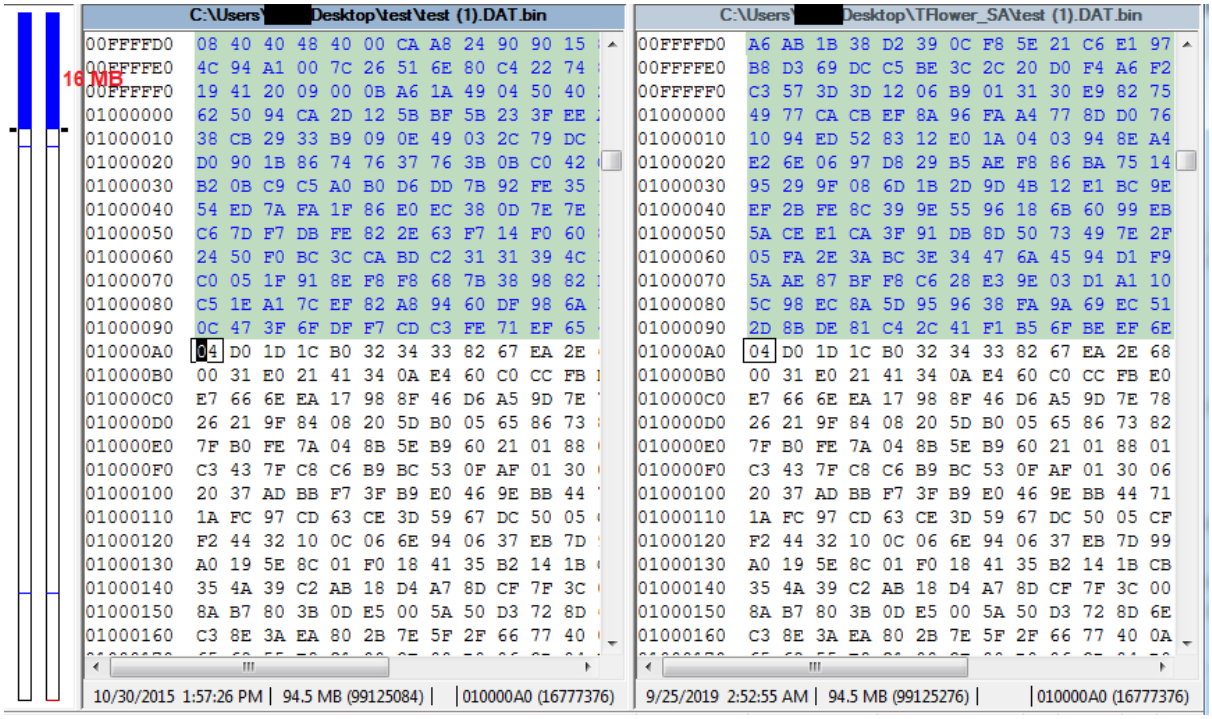


همانطور که در ابتدا اشاره شد، باج‌افزار TFlower از الگوریتم AES جهت رمزگذاری فایل‌های مورد نظر خود در سیستم قربانی استفاده می‌کند.

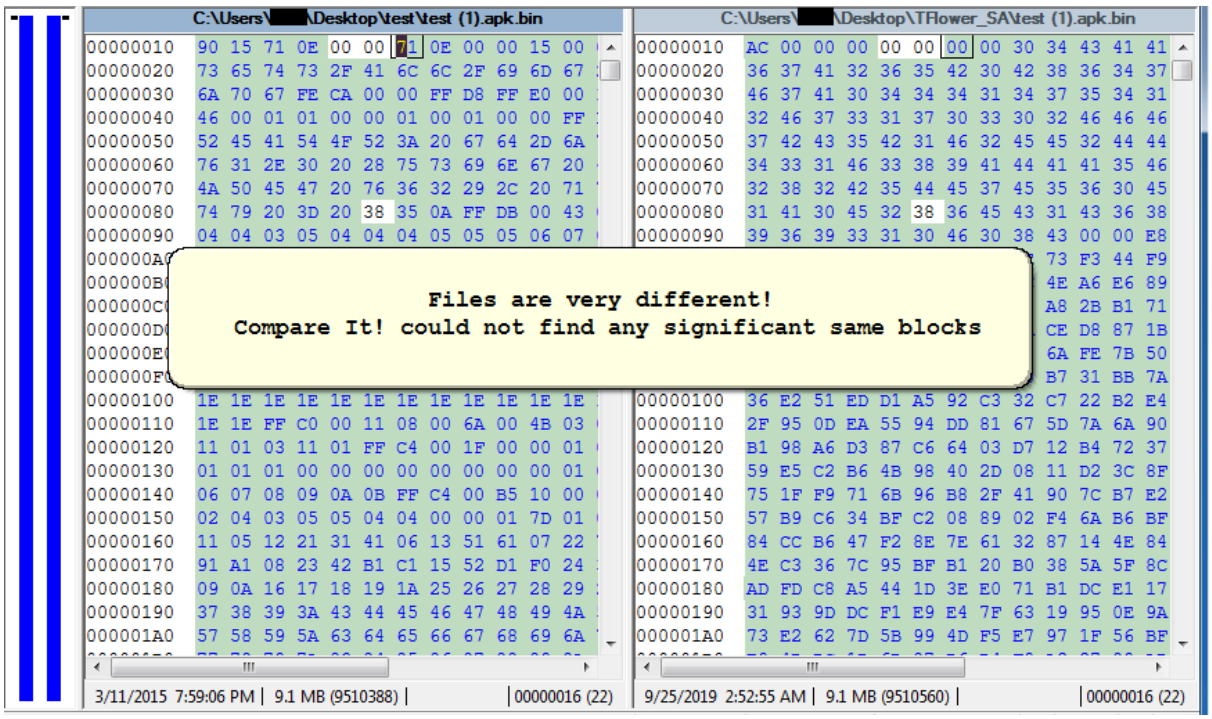


ضمناً این باج‌افزار از الگوریتم نامتقارن RSA نیز، در فرآیند رمزنگاری خود بهره می‌برد که در تصویر بالا مشخص شده است. کلید عمومی تولید شده توسط این الگوریتم جهت رمزگذاری کلید AES استفاده شده در رمزگذاری فایل‌ها و کلید خصوصی تولید شده به سرور فرمان و کنترل باج‌افزار، ارسال می‌شود.

طبق بررسی‌ها و مقایسه‌های انجام شده بر روی چند نمونه فایل سالم با نسخه رمزشده آن، باج‌افزار TFlower، ۱۶مگابایت اول هر فایل را رمزگذاری می‌کند.



این موضوع بدان معناست که تمام فایل‌های با حجم کمتر از این مقدار کاملا رمزگذاری خواهند شد.

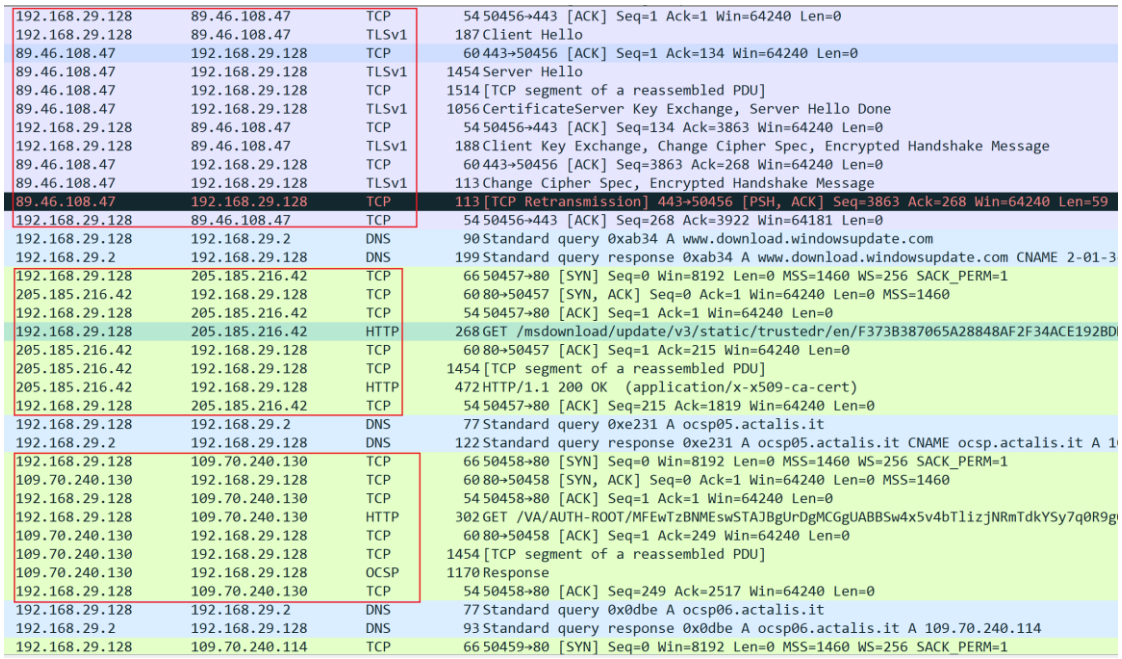


۶-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه ایجاد شده حین اجرای باج‌افزار، نتایج زیر مشاهده شد.

ارتباطات:

کشور	پروتکل	شماره پورت	آدرس میزبان	آدرس آی‌پی
ایتالیا	TCP,TLSv1	۸۰	ocsp06.actalis.it	۸۹.٤٦.۱۰۸.٤۷
ایتالیا	TCP,OCSP,HTTP	۸۰،٤۳۳	www.adamaitalycup.it	۱۰۹.۷۰.۲٤۰.۱۱٤
آمریکا	TCP,HTTP	۸۰،٤٤۳	www.download.windowsupdate.com	۲۰۵.۱۸۵.۲۱٦.٤۲



192.168.29.128	89.46.108.47	TCP	54	50456→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	89.46.108.47	TLSv1	187	Client Hello
89.46.108.47	192.168.29.128	TCP	60	443→50456 [ACK] Seq=1 Ack=134 Win=64240 Len=0
89.46.108.47	192.168.29.128	TLSv1	1454	Server Hello
89.46.108.47	192.168.29.128	TCP	1514	[TCP segment of a reassembled PDU]
89.46.108.47	192.168.29.128	TLSv1	1056	CertificateServer Key Exchange, Server Hello Done
192.168.29.128	89.46.108.47	TCP	54	50456→443 [ACK] Seq=134 Ack=3863 Win=64240 Len=0
192.168.29.128	89.46.108.47	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
89.46.108.47	192.168.29.128	TCP	60	443→50456 [ACK] Seq=3863 Ack=268 Win=64240 Len=0
89.46.108.47	192.168.29.128	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
89.46.108.47	192.168.29.128	TCP	113	[TCP Retransmission] 443→50456 [PSH, ACK] Seq=3863 Ack=268 Win=64240 Len=59
192.168.29.128	89.46.108.47	TCP	54	50456→443 [ACK] Seq=268 Ack=3922 Win=64181 Len=0
192.168.29.128	192.168.29.2	DNS	90	Standard query 0xab34 A www.download.windowsupdate.com
192.168.29.2	192.168.29.128	DNS	199	Standard query response 0xab34 A www.download.windowsupdate.com CNAME 2-01-3
192.168.29.128	205.185.216.42	TCP	66	50457→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
205.185.216.42	192.168.29.128	TCP	60	80→50457 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.29.128	205.185.216.42	TCP	54	50457→80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	205.185.216.42	HTTP	268	GET /msdownload/update/v3/static/trustedr/en/F373B387065A28848AF2F34ACE192BD
205.185.216.42	192.168.29.128	TCP	60	80→50457 [ACK] Seq=1 Ack=215 Win=64240 Len=0
205.185.216.42	192.168.29.128	TCP	1454	[TCP segment of a reassembled PDU]
205.185.216.42	192.168.29.128	HTTP	472	HTTP/1.1 200 OK (application/x-x509-ca-cert)
192.168.29.128	205.185.216.42	TCP	54	50457→80 [ACK] Seq=215 Ack=1819 Win=64240 Len=0
192.168.29.128	192.168.29.2	DNS	77	Standard query 0xe231 A ocsp05.actalis.it
192.168.29.2	192.168.29.128	DNS	122	Standard query response 0xe231 A ocsp05.actalis.it CNAME ocsp.actalis.it A 1
192.168.29.128	109.70.240.130	TCP	66	50458→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
109.70.240.130	192.168.29.128	TCP	60	80→50458 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.29.128	109.70.240.130	TCP	54	50458→80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.29.128	109.70.240.130	HTTP	302	GET /VA/AUTH-ROOT/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSw4x5v4bTlizjNRmTdkYSy7q0R9g
109.70.240.130	192.168.29.128	TCP	60	80→50458 [ACK] Seq=1 Ack=249 Win=64240 Len=0
109.70.240.130	192.168.29.128	TCP	1454	[TCP segment of a reassembled PDU]
109.70.240.130	192.168.29.128	OCSP	1170	Response
192.168.29.128	109.70.240.130	TCP	54	50458→80 [ACK] Seq=249 Ack=2517 Win=64240 Len=0
192.168.29.128	192.168.29.2	DNS	77	Standard query 0x0dbe A ocsp06.actalis.it
192.168.29.2	192.168.29.128	DNS	93	Standard query response 0x0dbe A ocsp06.actalis.it A 109.70.240.114
192.168.29.128	109.70.240.114	TCP	66	50459→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

محتوای زیر مربوط به آدرس آی‌پی ۸۹.٤٦.۱۰۸.٤۷ می‌باشد.

```
GET /VA/AUTH-ROOT/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSw4x5v4bTlizjNRmTdkYSy7q0R9gQUUtiIOsifeGbtifN7OHCUyQICNtACEEXnjKX1%2B9NeCmwXM
%2FgYu1Q%3D HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.1
Host: ocsp05.actalis.it
```

محتوای زیر مربوط به آدرس آی‌پی ۲۰۵.۱۸۵.۲۱٦.٤۲ می‌باشد.

```
GET /msdownload/update/v3/static/trustedr/en/F373B387065A28848AF2F34ACE192BDDC78E9CAC.crt HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.1
Host: www.download.windowsupdate.com

HTTP/1.1 200 OK
Cache-Control: public,max-age=172800
Content-Type: application/x-x509-ca-cert
Last-Modified: Thu, 23 Jul 2015 23:16:35 GMT
Accept-Ranges: bytes
ETag: "80b4b9e9dc5d01:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 1471
Date: Wed, 25 Sep 2019 10:30:25 GMT
Connection: keep-alive
X-CCC: UA
X-CID: 2
```

همانطور که درتصاویر بالا قابل مشاهده است، باج‌افزار TFlower از دو آدرس بالا با آدرس میزبان‌های متفاوت، جهت استفاده از API رمزنگاری مایکروسافت برای انجام فعالیت‌های رمزگذاری خود در سیستم قربانی، بهره برده است.

٦-٣ رمزگشایی:

تاکنون، هیچ‌گونه ابزاری جهت رمزگشایی این باج‌افزار ارایه نشده است.