Tyupkin’in Anatomisi

written by Mert SARICA | 2 February 2015

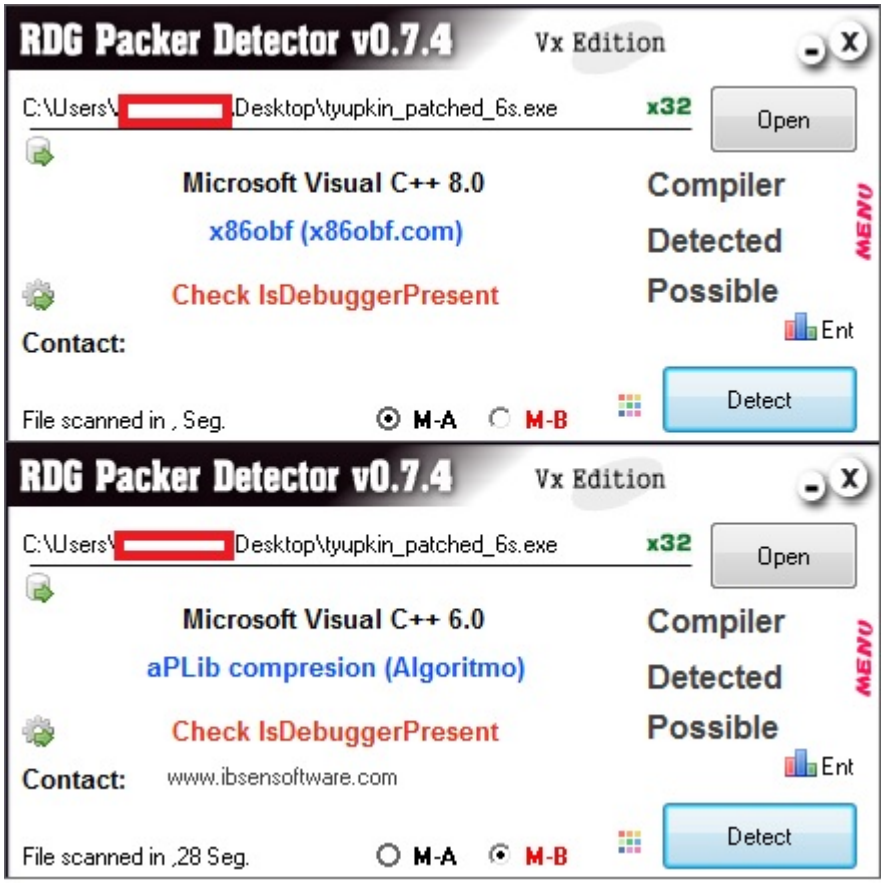
2 Ekim 2014 tarihinde Malezya’da, 18 tane NCR marka ATM’den bir zararlı yazılım yardımı ile yaklaşık 1 milyon dolar çalındığı haberlere yansıdı. İşin ilginç yanı ise bankalar bu konuda 4 ay önce uyarılmış olmalarına rağmen gerekli önlemleri almamıştı. Ardından 7 Ekim 2014 tarihinde Kaspersky firması, Tyupkin adını verdikleri bu zararlı yazılım ile art niyetli kişilerin ATMlerden yüklü miktarda para çaldığını teknik detayları ile birlikte duyurdu. Bu duyuruda zararlı yazılımın Batı Avrupa’da yaklaşık 50 tane ATM’de tespit edildiği bilgisi de yer alıyordu. VirusTotal’a bu zararlı yazılımın hangi ülkelerden yüklendiği bilgisine bakıldığında ise Rusya başta olmak üzere, ABD, Hindistan, Çin, İsrail, Fransa ve Malezya’da da bu zararlı yazılımın tespit edildiği görülüyordu.

Merak edenleriniz için Tyupkin ATM zararlı yazılımının ATMlere nasıl yüklendiğine ve paranın nasıl çalındığını kısaca açıklamak gerekirse;

- Art niyetli kişi, ATM’ye fiziksel olarak eriştikten sonra önyüklenebilir (bootable) cd veya usb’yi ATM’ye takıyor, ATM’yi yeniden başlatıyor ve oradan uzaklaşıyor.
- İşletim sistemi yeniden başladıktan sonra Tyupkin zararlı yazılımı işletim sisteminde çalışmaya ve komut beklemeye başlıyor.
- Sadece Pazar ve Pazartesi günleri komut kabul eden bu zararlı yazılıma erişmek için gelen kurye, tuş takımına (pin pad) zararlı yazılımın beklediği rakamları (misal 22222) giriyor.
- Tuşlanan bu rakamlar sonrasında ekranda bir oturum kodu (session code) beliriyor. Bu kodu cep telefonu ile operatöre ileten kurye, doğru oturum anahtarını (session key) tuşladıktan sonra zararlı yazılımın özel menüsüne erişiyor.
- Bu menüde ATM’nin hangi bölmesinde ne kadar para olduğunu öğrenen kurye, parayı çektikten sonra kayıplara karışıyor. (Video)

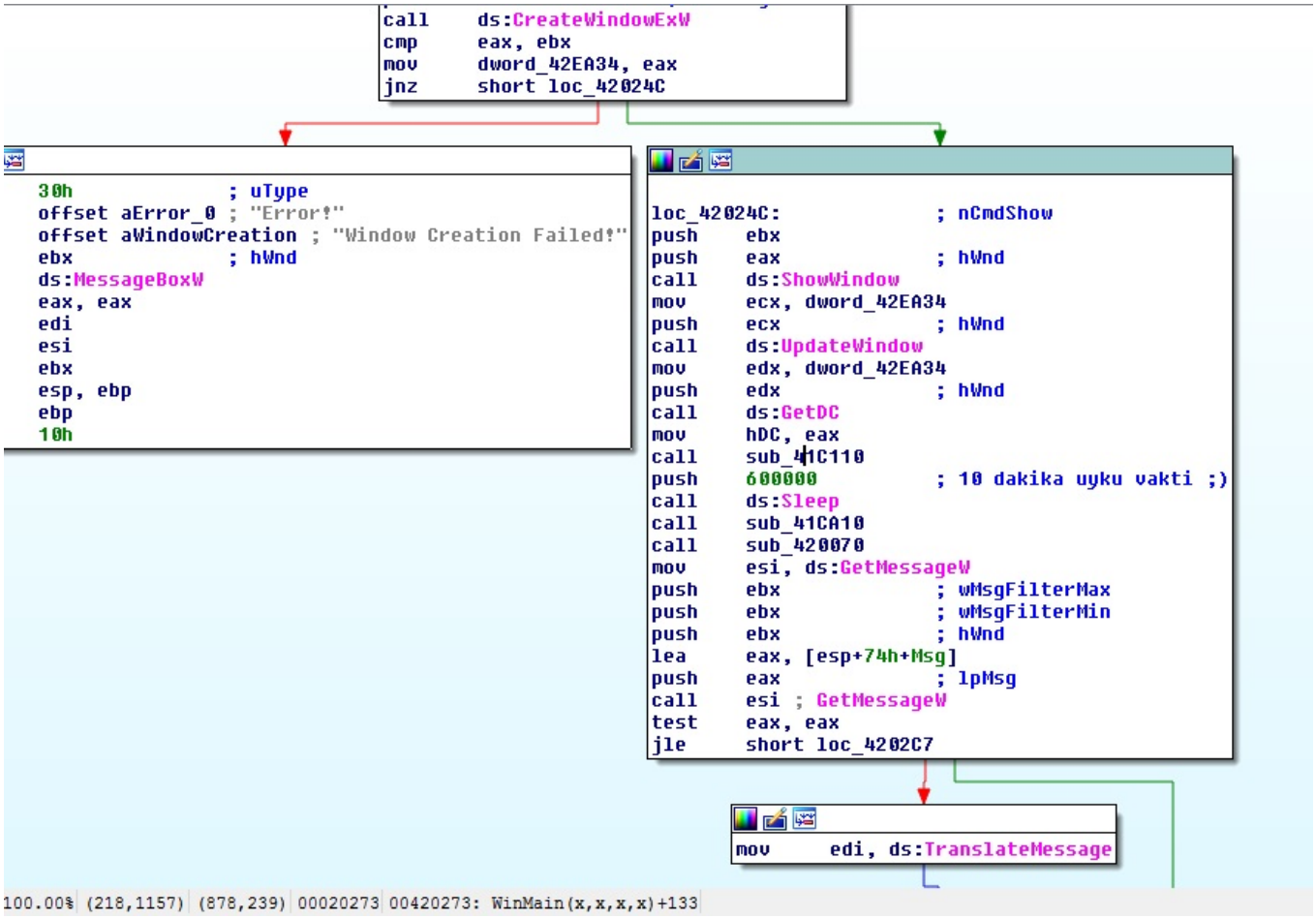
Ocak 2015 itibariyle Tyupkin zararlı yazılımına Türkiye’de de rastlandığı söylentileri kulaktan kulağa yayılmaya başladı. Kimi vakada, art niyetli kişilerin Tyupkin zararlı yazılımını ATM’nin kasasını anahtarla açarak, ki vakada ise kart okuyucunun altını matkapla delerek bulaştırdıkları söyleniyordu. Bu söylentilerin tamamında ise önyüklenebilir CD yerine önyüklenebilir USB kullanıldığı söyleniyordu. Söylentilerde gerçeklik payı

olup olmadığını araştırmaya başladıktan kısa bir süre sonra, Türkiye'de tespit edilen Tyupkin zararlı yazılımına (Aralık 2014 tarihinde derlenmiş sürüm) VirusTotal üzerinden ulaşmayı başardım.

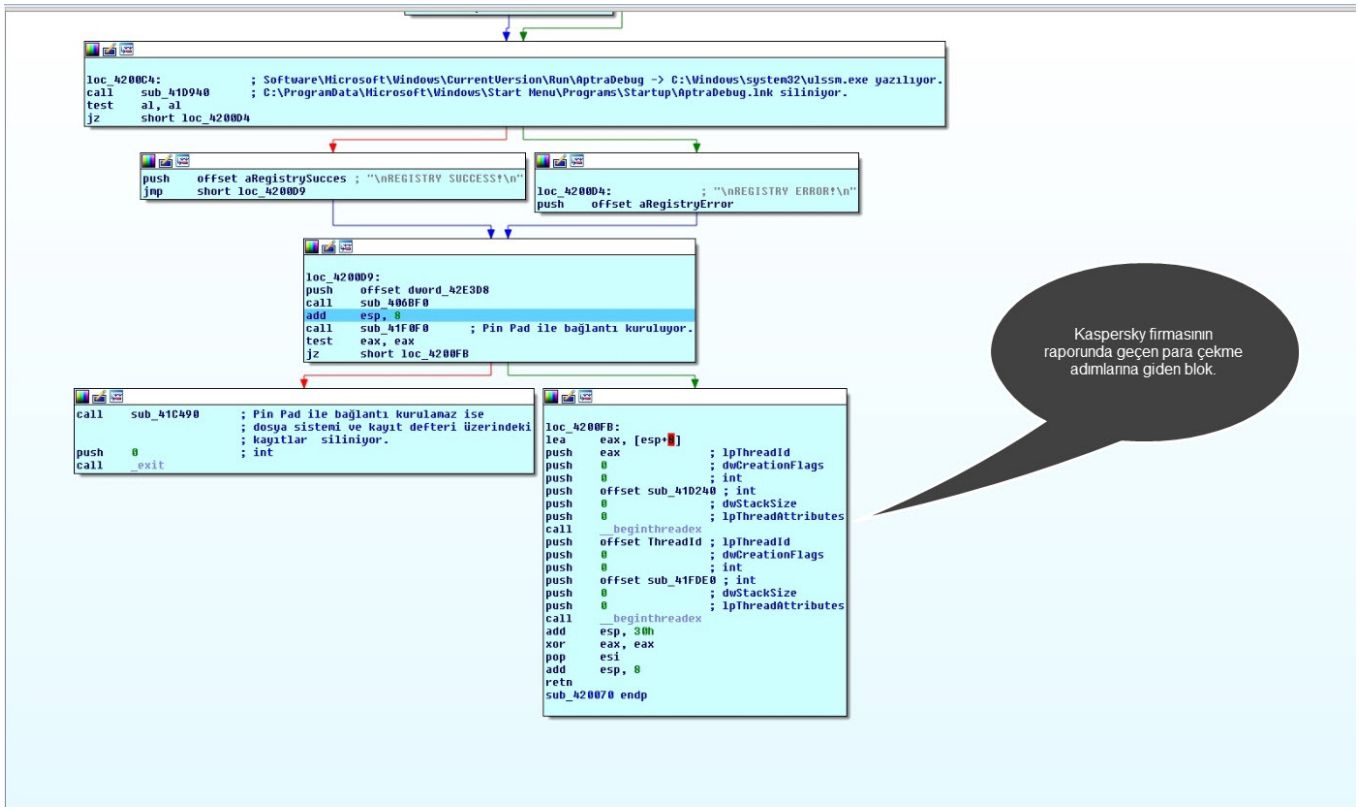


Hali hazırda Kaspersky tarafından detaylı bir şekilde analiz edilmiş bu zararlı yazılımı tekrar analiz etmek yerine, sisteme bulaştığının nasıl anlaşılabileceğine dair kilit noktalara hızlıca göz atmaya karar verdim. (Analizi ATM üzerinde gerçekleştirmediğim için analiz esnasında Pin Pad ile bağlantı kurulamamış ve bu nedenle Tyupkin'in tüm izleri sildiği, işlemleri geri aldığı senaryo üzerinden ilerlenmiştir.)

İlk olarak Tyupkin'in dinamik analizi atlatma adına çalıştıktan sonra 10 dakika uykuya geçmesine müdahale ederek (patch) bunu kısalttım.



Analize başladıktan kısa bir süre sonra Tyupkin'in çalışmak ya da çalışmamak işte bütün mesela bu dediği ana kontrol adımına geldim. Burada ATM'nin Pin Pad'i ile bağlantı kurmaya çalışan Tyupkin, bağlantı kuramadığı taktirde hem önyüklenebilir aygıt (cd, usb) üzerinden hem de kendi üzerinden yaptığı değişiklikleri geri almaya başlıyordu. Bu adımlar sayesinde zararlı yazılımın hangi güvenlik yazılımlarını devre dışı bıraktığı da anlaşılabiliyordu. (Kaspersky'nin raporuna göre Tyupkin, McAfee'nin Application Control (SolidCore) yazılımını devre dışı bırakıyordu.)



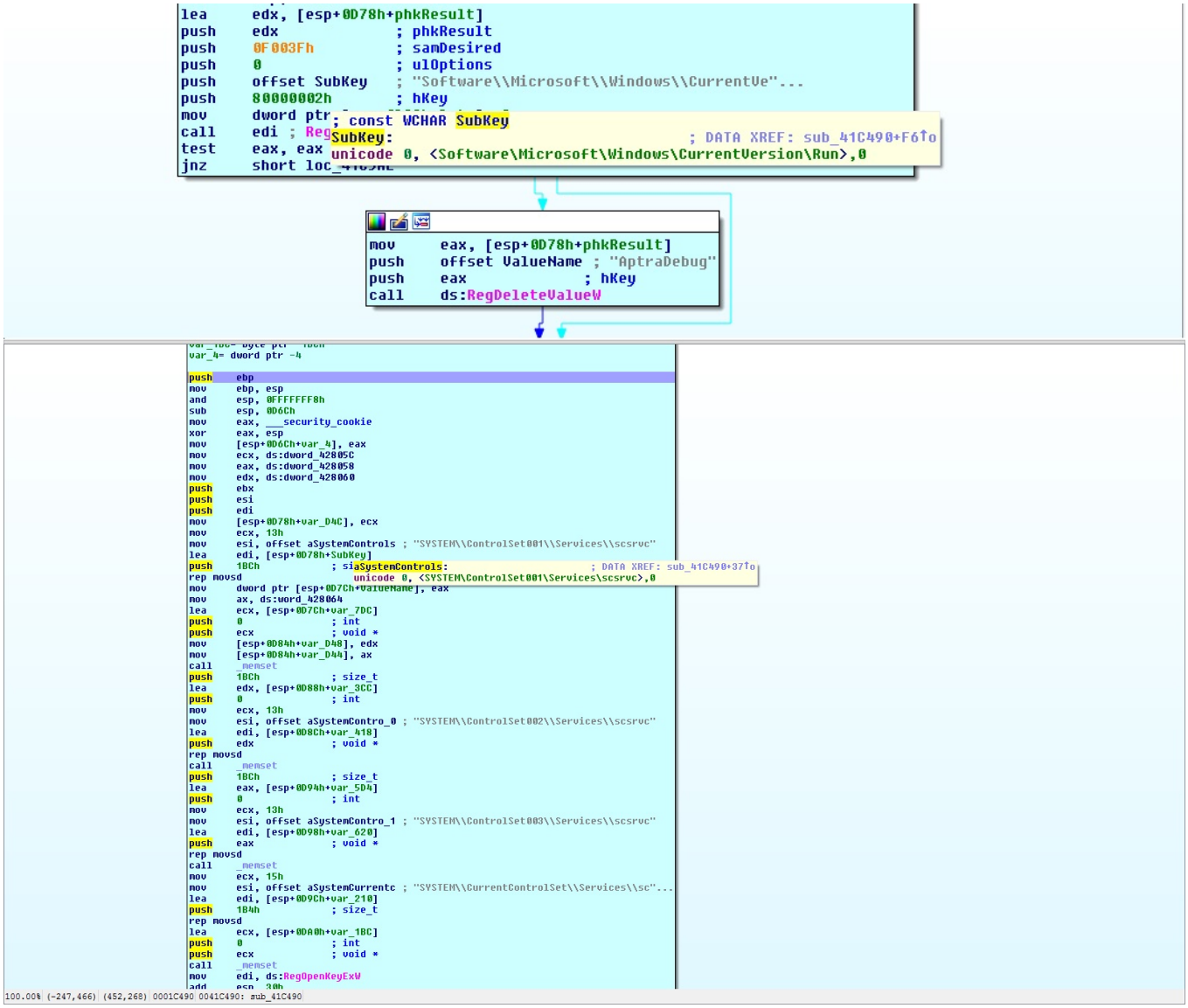
Zararlı yazılımın çalıştıktan ancak Pin Pad'e bağlanamadıktan sonra hangi adımlardan geçtiğini kısaca açıklamam gerekirse;

Sistem başladıktan sonra çalışabilmesi adına kayıt defterindeki (registry) Software\Microsoft\Windows\CurrentVersion\Run\AptraDebug anahtarına C:\Windows\system32\ulssm.exe değerini yazıyor. (sub_41D940)

Önyüklenebilir aygıt üzerinden oluşturulduğunu tahmin ettiğim C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\AptraDebug.lnk dosyasını (muhtemelen bu da system32\ulssm.exe dosyasını işaret ediyor.) siliyor. (sub_41D750)

Tyupkin, Pin Pad ile bağlantı kuramaz ise daha önce oluşturduğu Software\Microsoft\Windows\CurrentVersion\Run\AptraDebug anahtarını siliyor. Ardından yine önyüklenebilir aygıt üzerinden devre dışı bıraktığı McAfee Application Control'un (SolidCore) servislerinin, sistem yeniden başladığında tekrar çalışabilmesi adına aşağıdaki değişiklikleri gerçekleştiriyor. (sub_41C490)

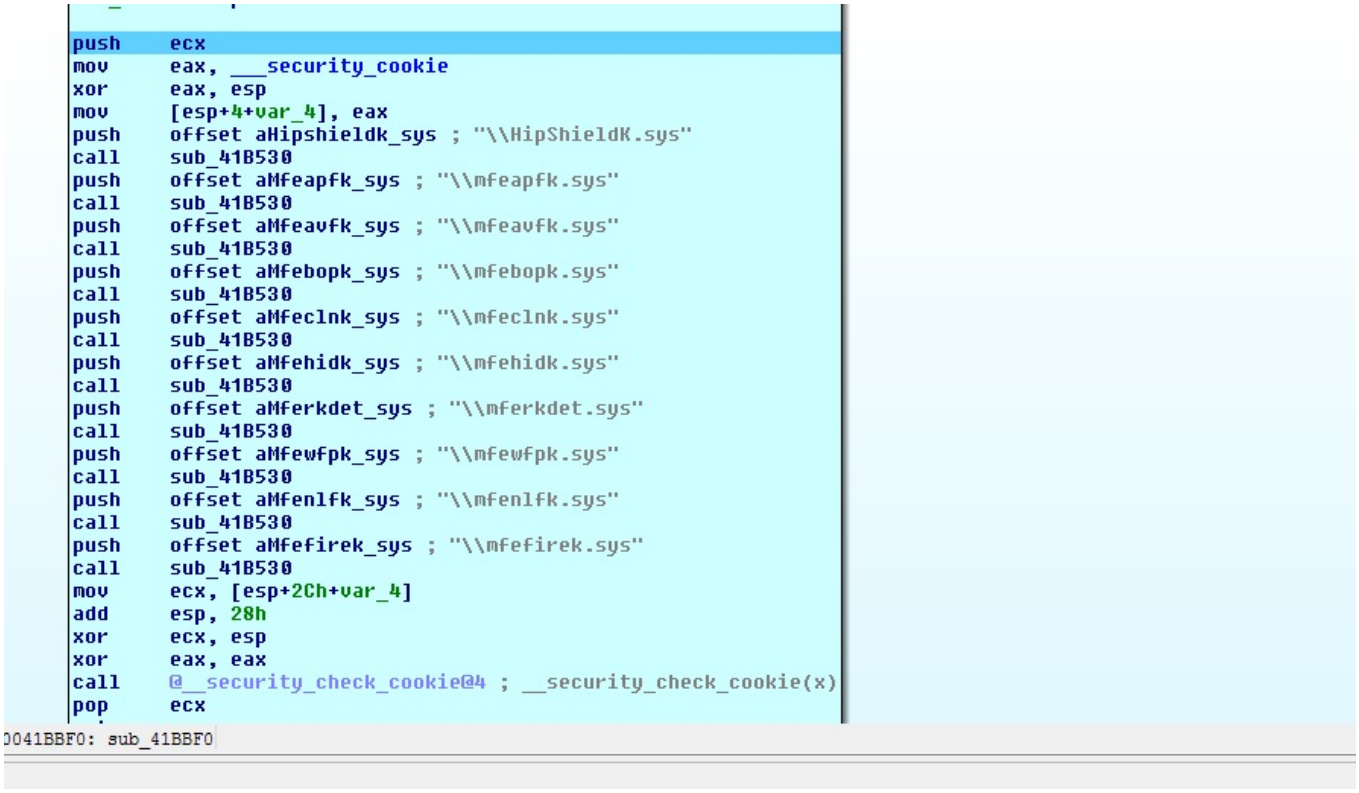
HKLM\System\CurrentControlSet\services\scsrvc\Start değerini 2 olarak değiştiriyor.
HKLM\System\CurrentControlSet002\services\scsrvc\Start değerini 2 olarak değiştiriyor.
HKLM\System\CurrentControlSet003\services\scsrvc\Start değerini 2 olarak değiştiriyor.



Yine önyüklenebilir aygıt (bootable usb, cd) üzerinden gerçekleştirildiğini tahmin ettiğim bu işlemde, McAfee Application Control (SolidCore), Mcafee Host IPS ve Mcafee Antivirüs yazılımlarına ait olan aşağıdaki dosyaları C:\windows\system32\config klasöründen alıp, C:\windows\system32\drivers klasörüne kopyalıyor. (En başta config klasörüne kopyalamasının sebebi, u dosyaları bulamayan güvenlik yazılımlarının sistem başlangıcında çalışmasını engellemektir.) (sub_41BBF0)

HipShieldK.sys (Mcafee Host IPS sürücüsü),
mfeapfk.sys (Mcafee Antivirüs sürücüsü),
mfeavfk.sys (Mcafee Antivirüs sürücüsü),
mfebopk.sys (Mcafee Antivirüs sürücüsü),
mfehidk.sys (Mcafee Antivirüs sürücüsü),
mfeclnk.sys (Mcafee Antivirüs sürücüsü),
mferkdet.sys (Mcafee Antivirüs sürücüsü),
mfewfpk.sys (Mcafee Antivirüs sürücüsü),
mfenlfk.sys (Mcafee Host IPS sürücüsü),

mfefirek.sys (Mcafee Host IPS sürücüsü)

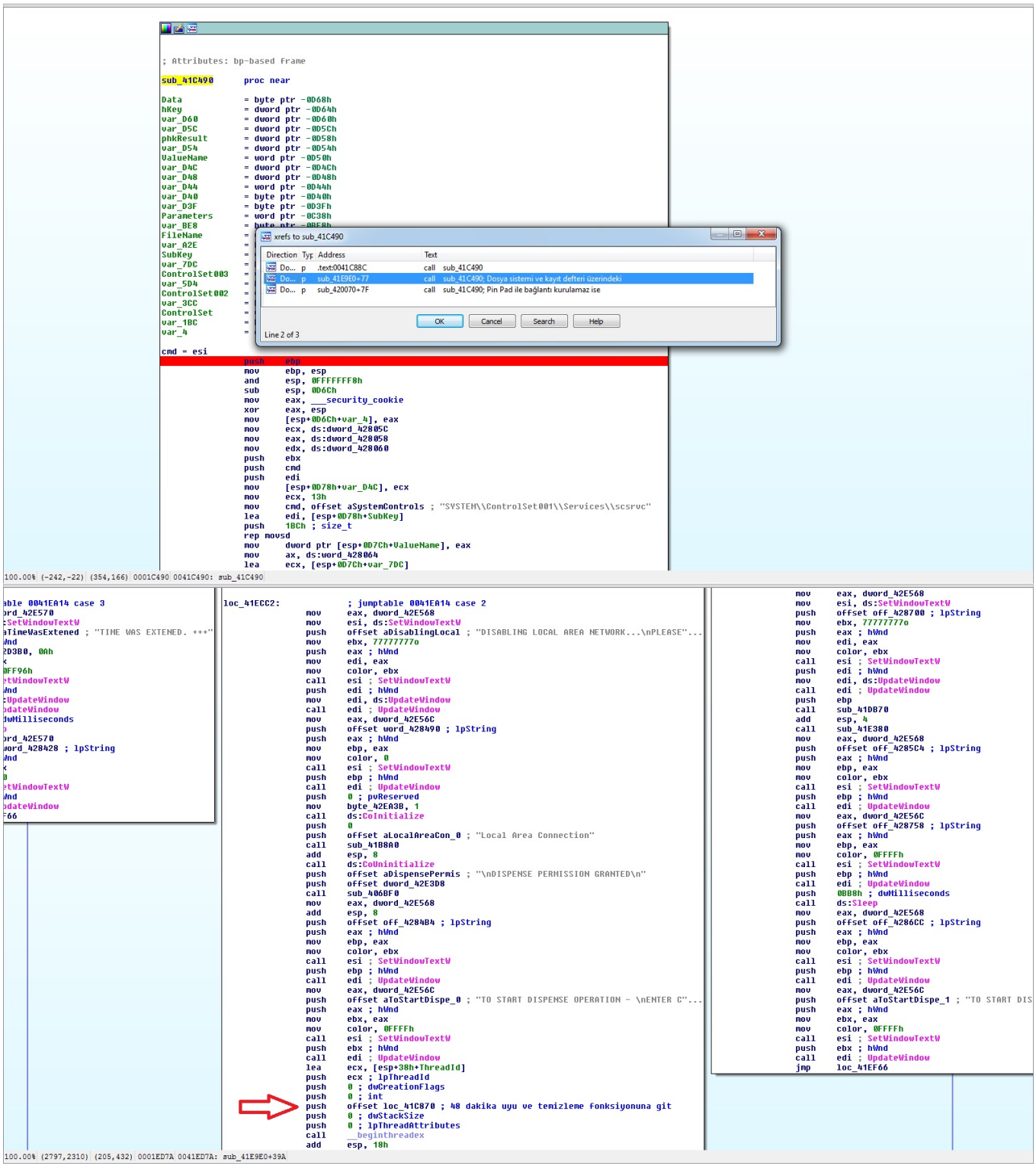


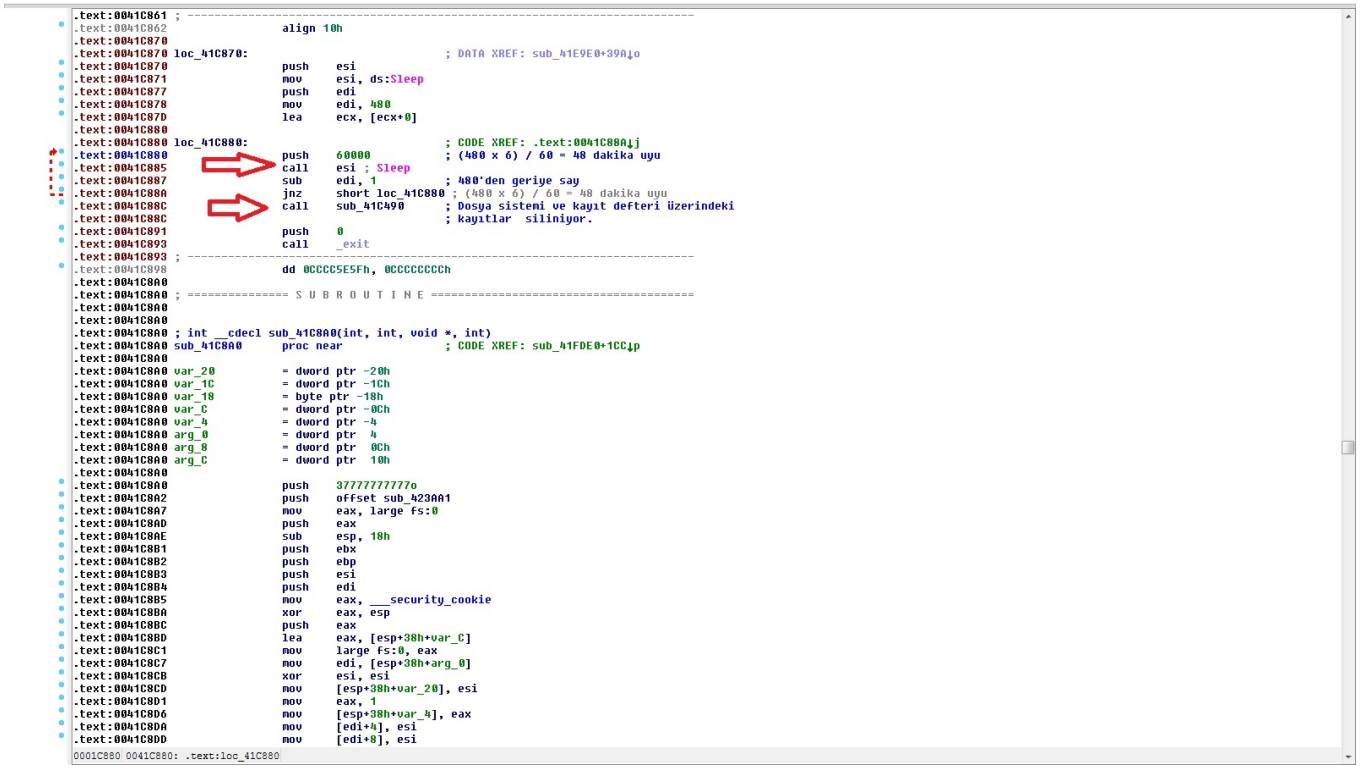
NCR firmasının Aptra uygulaması ile birlikte dağıttı özelleştirilmiş Solidcore yazılımına ait kayıtları (solidcore.log ve s3diag.log) C:\program files\ncr aptra\Solidcore for APTRA\Logs klasöründen siliyor. (sub_41B450)

Yine önyüklenebilir aygıt üzerinden kopyalandığını tahmin ettiğim Windows\System32\kbd110.dll dosyasını siliyor. (sub_41C490)

Son olarak ise “C:\Windows\System32\cmd.exe” /C ping 127.0.0.1 -n 8 & del /F /S /Q C:\Windows\system32\ulssm.exe komutunu çalıştırarak ulssm.exe dosyasını siliyor. (sub_41C490)

Analizi tamamlamadan önce bu iz silme ve yapılan işlemleri geri alma fonksiyonunun (sub_41C490) başka hangi fonksiyonlardan çağrıldığına (xfref) baktığımda, karşıma çıkan iki fonksiyondan biri dikkatimi çekti. Bu fonksiyonda öncelikle yerel ağ bağlantısı durduruluyor ardından para çekme için izin veriliyor ve ardından 48 dakika sonra izleri silme, işlemleri geri alma (sub_41C490) fonksiyonu çağrılıyor.


; Attributes: bp-based frame
sub_41C490 proc near
xrefs to sub_41C490
Direction Typ Address Text
Do... p .text:0041C88C call sub_41C490
Do... p sub_41E9E0+77 call sub_41C490; Dosya sistemi ve kayıt defteri üzerindeki
Do... p sub_420070+7F call sub_41C490; Pin Pad ile bağlantı kurulamaz ise
OK
Cancel
Search
Help
Line 2 of 3
loc_41ECC2:
; jumptable 0041EA14 case 2
aDisablingLocal ; "DISABLING LOCAL AREA NETWORK...\nPLEASE"...
aLocalAreaCon_0 ; "Local Area Connection"
aDispensePermis ; "\nDISPENSE PERMISSION GRANTED\n"
aToStartDispe_0 ; "TO START DISPENSE OPERATION - \nENTER C"...
aToStartDispe_1 ; "TO START DIS
loc_41C870 ; 48 dakika uyu ve temizleme fonksiyonuna git
loc_41EF66



Gerçekleştirdiğim bu kısa analiz sonucunda, Türkiye'de görülen Tyupkin ile Kaspersky'nin raporunda yer alan sürüm arasında bazı farklar olduğu görülüyor.

Birincisi, Türkiye sürümünde sadece Mcafee Application Control (Solidcore) değil bunun dışında sürücü dosyalarına bakılacak olursa Mcafee Antivirüs ve Mcafee Host IPS de devre dışı bırakılıyor gibi görünüyor.

İkincisi ise yine Kaspersky'ın raporunda para çekme işlemi gerçekleştirildikten sonra Tyupkin'in kendini sildiğine yer verilmemiş ancak mevcut sürümde böyle bir işlev bulunuyor. (Bu işlev nedeniyle, kurye tarafından ATM'den para çalınmadan önce Tyupkin bulaşmış bir ATM'yi tespit etmek isteyenlerin yapması gereken işlerden ikisi, sistem üzerinde ulssm.exe adlı bir yazılımın çalışıp çalışmadığını kontrol etmek ve bu dosyanın Windows\system32 klasörü altında olup olmadığını kontrol etmek yerinde olacaktır.)

Bu zararlı yazılıma karşı çözüm olarak ATM üzerinde disk şifreleme, fiziksel erişimde ve bağlantı noktalarında iş akışını dahi etkileyebilecek düzeyde radikal kısıtlamalar düşünülebilir.

Kısıtlı zaman ve teknik imkanlar dahilinde (eksikler veya hatalar olabilir) gerçekleştirdiğim bu analizin, Tyupkin'e karşı verilen mücadeleye katkısı olması dileğiyle bir sonraki yazıda görüşmek üzere herkese güvenli günler dilerim.