Kayseri üniversitesi Siber Güvenlik Uygulama ve Araştırma Merkezi

Analiz sonuçları-III

BANKACILIK VİRÜSLERİ TRİCKBOT EMOTET VE SYHLOCK

BANKACILIK VİRÜSÜ

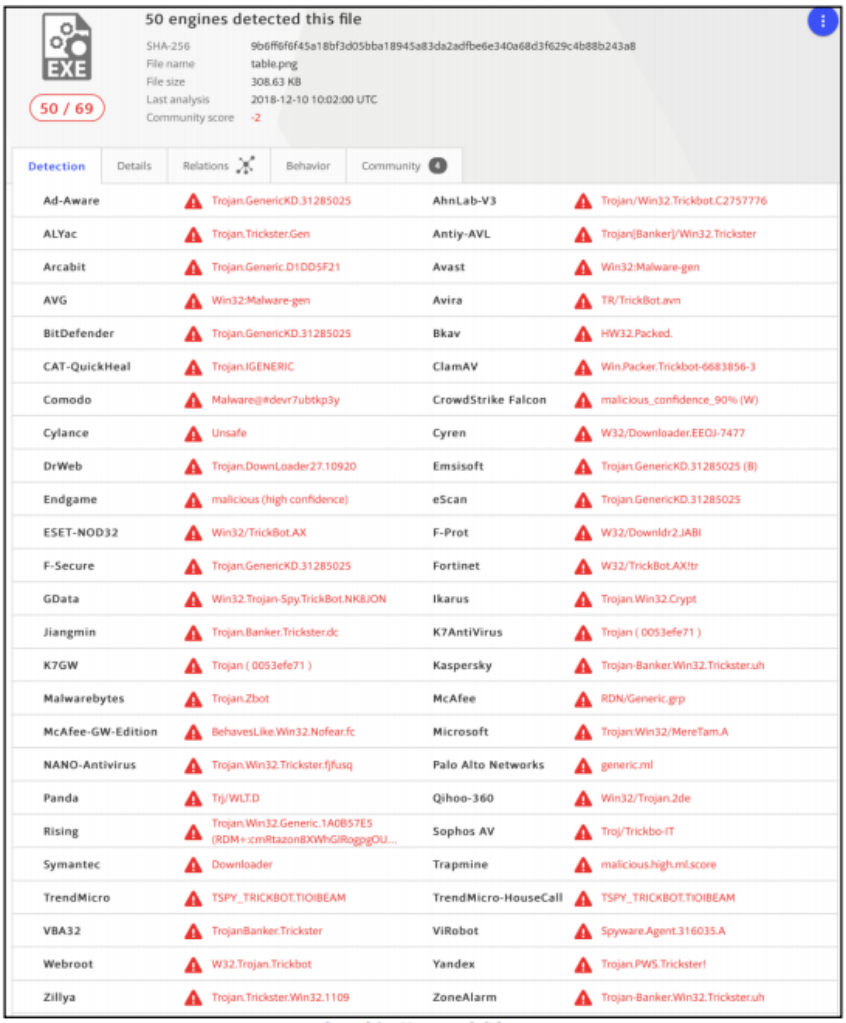
Son yıllarda mobil uygulamaların kullanımının yaygınlaşmasıyla birlikte Mobil Bankacılık kanalı ile yapılan işlemlerin de kullanımında büyük bir artış görülmektedir. Bu sebeple Mobil cihazlar üzerinden sunulan bankacılık hizmetlerinin güvenliği çok daha önemli hale gelmiştir. Online ve mobil bankacılık sistemlerini hedef alan farklı amaçlar ve özelliklerle oluşturulmuş virüslere bankacılık virüsü denir.

TRİCKBOT

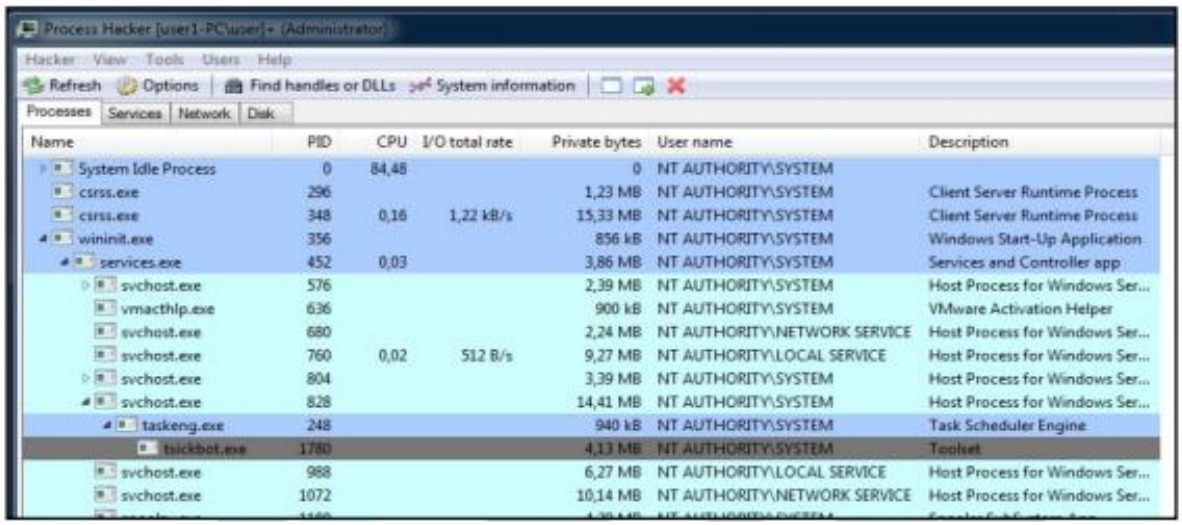
Trickbot isimli zararlı yazılımın farklı sürümleri bulunmaktadır. İncelenen zararlı yazılımın MD5 değeri 6ebd6dce92fb9add429d36f84c11148e olup incelenen dosyaya ait diğer ayırt edici özellikler aşağıdaki görselde listelenmiştir.

MD5	6ebd6dce92fb9add429d36f84c11148e
SHA-1	183881f00a69eb9e2b94e64c871e0dd197d722dd
Authentihash	ae0b9e56744f92fbbcee92ccecfb4430072ea13ef9f144737297f6003b2d2766
Imphash	5f9c0494ad15fdbf575716a7f38ae24f
File Type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
SSDeep	6144:kJKDVItC9xO/4judQqXrm2SgUz6XGJVuDFzcTl2:kiWC6XS2DUz6XGfud5
TRiD	Win64 Executable (generic) (61.7%) Win32 Dynamic Link Library (generic) (14.6%) Win32 Executable (generic) (10%) OS/2 Executable (generic) (4.5%) Generic Win/DOS Executable (4.4%)
File Size	308.63 KB

Virustotal ile yapılan ön incelemede farklı antivirüs programları tarafından özellikle Banker ve Spy isimleri ile birlikte ağırlıklı olarak Trojan ismi ile adlandırıldığını görmekteyiz. Dosyanın Virustotal'e ilk yüklenme tarihinin ise 15 Ekim 2018 olduğu görülmektedir.

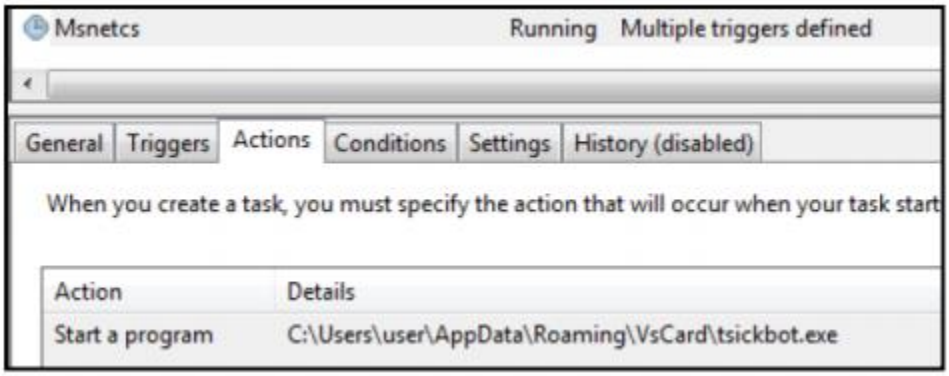


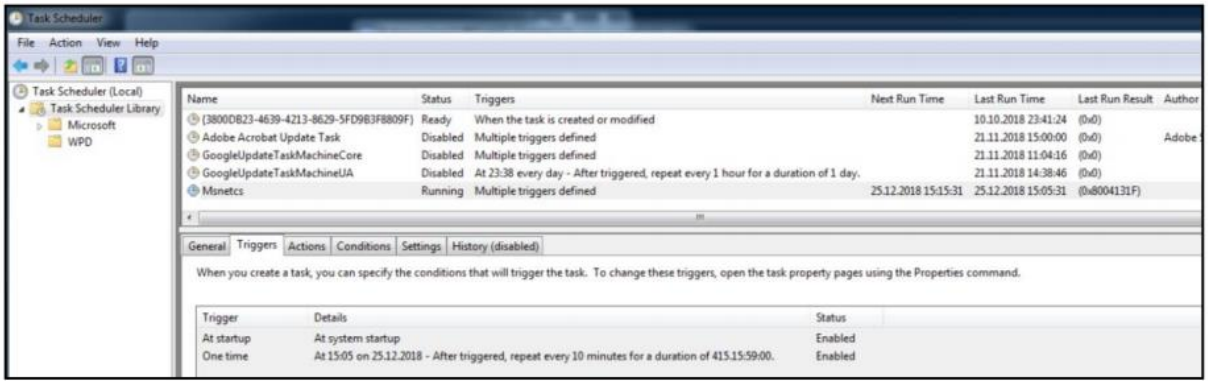
Söz konusu zararlı yazılımı çalıştırarak sistemde bıraktığı izler tespit edilmeye çalışılmıştır. Trickbot zararlı yazılımını kullanıcı hesabı ile çalıştırıp bir süre bekledikten sonra zararlı yazılımın farklı bir proses altında çalışmaya başladığını görülmektedir. Ayrıca analiz esnasında orijinal olarak çalıştırılan dosya ismindeki bazı harflerin değiştirilerek yeni isim ile prosesin oluşturulduğu görülmüştür.



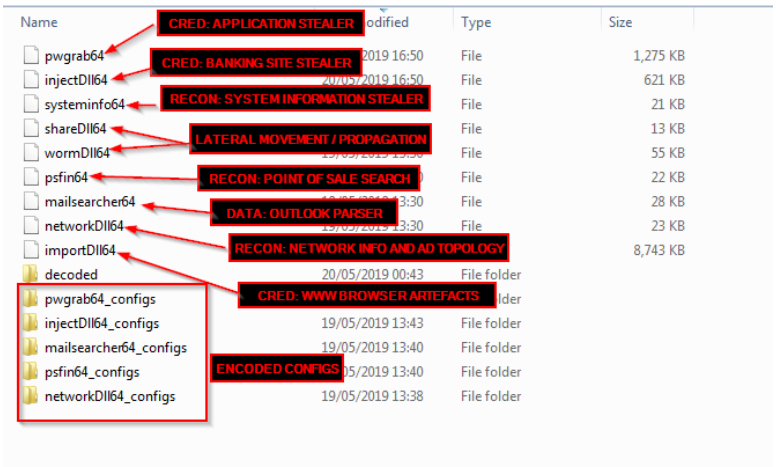
Dinamik analiz esnasında çalıştırılan trickbot.exe isimli zararlı yazılım ismi içerisinde bulunan r harfinin s harfi ile değiştirildiği gözlenmektedir.

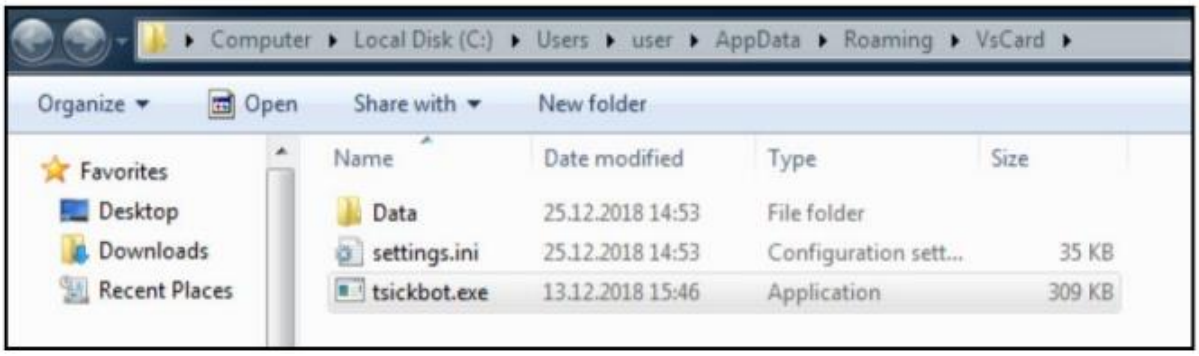
Çalıştırılan trickbot.exe isimli dosyanın bir süre sonra tsickbot.exe ismi ile çalışması zamanlanmış görev altında bir işlem olabileceğini de gösterebilmektedir. Zamanlanmış görevler incelendiğinde işletim sistemi başladığında ve her 10 dakikada bir tsickbot.exe ismi dosyanın çalıştırılması için ayarlandığı görülmektedir. Çalıştırılacak olan dosyanın da %APPDATA% altında VsCard klasöründe olduğu da görülmektedir. Zararlı yazılımın kendisini her açılışta veya görev yöneticisi tarafından kapatıldığında tekrar çalışmak için önlem aldığı anlaşılmaktadır.





Zamanlanmış görev ile çalıştırılan dosyanın %APPDATA% altında VsCard klasöründe olduğu önceki incelememizde görülmüştür. Söz konusu dosyanın içeriği hash değeri incelendiğinde orijinal dosya ile aynı hash değerine sahip olduğu görülmektedir. Zararlı yazılımın kendisini %APPDATA% altında VsCard klasörüne kopyalığı ve artık bu klasörden çalıştığı anlaşılmaktadır.

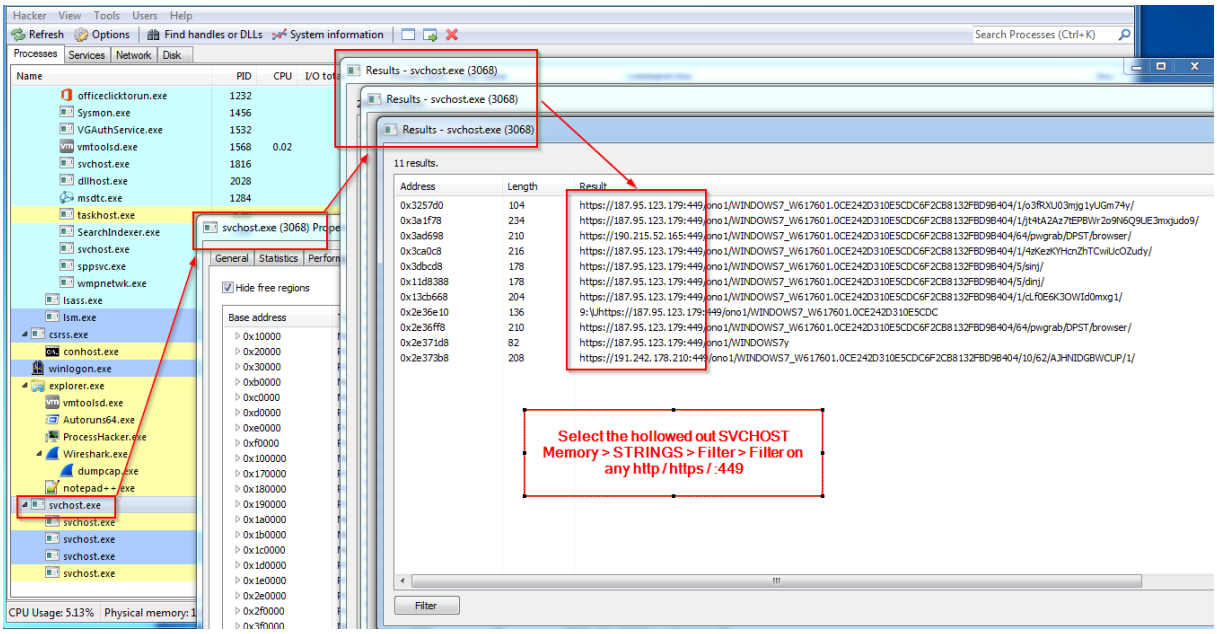




Zararlı yazılım %APPDATA% altında VsCard klasöründe çalışmaya başladıktan sonra ulaşmaya çalıştığı IP adresleri aşağıda listelenmiştir. Söz konusu IP adreslerine giden GET istekleri

https://IP/lib332/USER1-PC_W617601.60BA36xxxxxxxx1A5F1F3B5D8D699AE9/5/spk/ formatında olmaktadır.

5.104.41.188	31.179.162.86	42.115.91.177	47.49.168.50
54.39.167.242	62.141.94.107	68.109.83.22	69.57.26.30
71.13.140.89	71.94.101.25	91.235.128.186	94.232.20.113
107.175.127.147	115.78.3.170	149.154.71.206	158.69.177.176
185.251.39.106	187.190.249.230	195.54.163.91	197.232.50.85
198.100.157.163	207.140.14.141		



Tehdit Vektörü Göstergeleri (Indicator of Compromises) a) Zararlının iletişime geçtiği IP ve domain bilgileri:

5.104.41.188	62.141.94.107	71.94.101.25
68.109.83.22	69.57.26.30	71.13.140.89
91.235.128.186	94.232.20.113	07.175.127.147
115.78.3.170	149.154.71.206	158.69.177.176
185.251.39.106	187.190.249.230	195.54.163.91
197.232.50.85	198.100.157.163	207.140.14.141
31.179.162.86	42.115.91.177	47.49.168.50
54.39.167.242		

- Zararlının IP adresini elde etmek için bilgi aldığı web siteleri

· api.ipify.org

· api.ip.sb

· checkip.amazonaws.com

· icanhazip.com

· ident.me

· ip.anysrc.net

· ipecho.net

· ipinfo.io

· myexternalip.com

· wtfismyip.com

· myexternalip.com

TRİCKBOT'DAN NASIL KORUNURUZ

1. Web tarayıcısından banka hesaplarına veya şifre ile bir websiteye giriş yapıldıktan sonra tarayıcının çerezlerinin silinmesini öneriyoruz. Trickbot bu çerezlerin içindeki giriş bilgilerini çalıyor.

2. Web tarayıcısına kurduğunuz eklentilere (plug-in) çok dikkat etmenizi tavsiye ediyoruz en sağlıklısı ise tarayıcılarınızda hiç eklenti kullanmamanızdır.

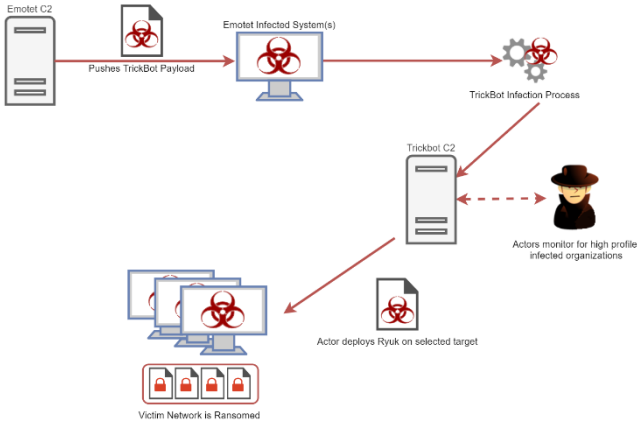
3. Eğer Anlamadığınız yada tanımadığınız mail adreslerinden bir e-posta aldıysanız Emin olmadığınız sürece sizi yönlendirdiği link'e yada resimlere tıklamayınız.

4. Gelen E-postalar tanıdıklarınızdan'da gelebilir. Size yaptığınız işle alakalı bir mutabakat fatura teklif gibi x bilgiler iletmiş olabilir. Tanıdığınız kişiye mailin doğruluğunu teyit etmenizi öneririm.

EMOTET

Emotet, orijinal olarak bankacılık Trojanı biçiminde geliştirilen, kötü amaçlı bir bilgisayar yazılım programıdır. Hedefi, yabancı cihazlara erişmek ve hassas özel verileri gözetlemektir. Emotet, temel antivirüs programlarını kandırması ve onlardan saklanmayı başarmasıyla tanınır. Kötü amaçlı yazılım sisteme girdiğinde bir bilgisayar solucanı gibi yayılır ve ağdaki diğer bilgisayarlara sızmaya çalışır.

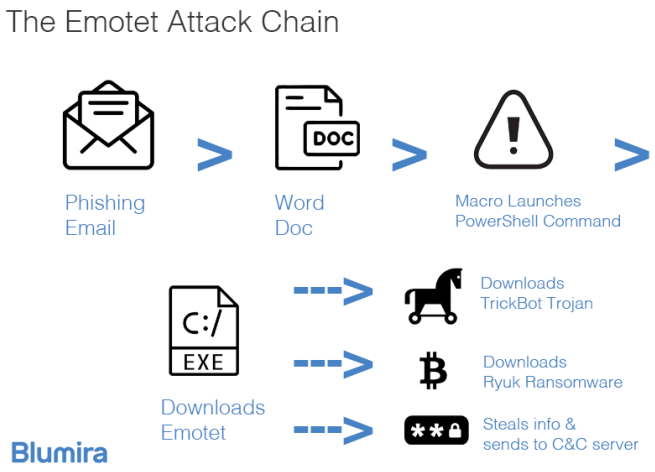
Emotet genellikle spam e-postalar yoluyla yayılır. İlgili e-postada kötü amaçlı bir bağlantı veya virüs taşıyan bir belge bulunur. Belgeyi indirdiğinizde veya bağlantıyı açtığınızda, kötü amaçlı yazılım otomatik olarak bilgisayarınıza indirilir. Bu e-postalar gerçeğe son derece yakın bir görünümle hazırlanır ve birçok kişi Emotet yüzünden zarar görmüştür.



EMOTET BANKACILIK VİRÜSÜ DAVRANIŞSAL ANALİZİ

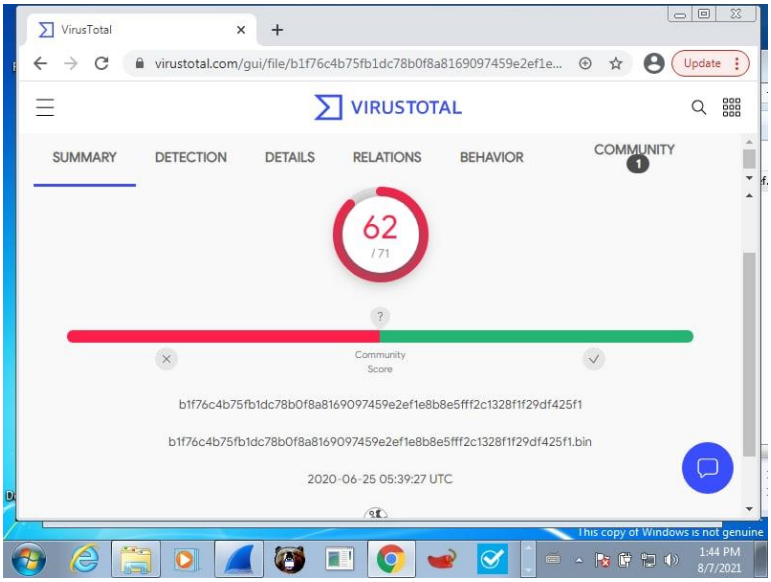
Emotet genellikle Outlook toplama adı verilen yöntemle yayılır. Trojan, zaten etkilenen kullanıcılardan gelen e-postaları okur ve yanıltıcı gerçek içerik oluşturur. Meşru ve kişisel bir görünüme sahip olan bu e-postalar bilindik spam e-postalarından farklıdır. Emotet, bu kimlik avı e-postalarını arkadaşlar, aile üyeleri ve iş arkadaşları gibi kaydedilen kişilere gönderir.

E-postalarda genellikle alıcının indirmesi gereken virüs taşıyan bir Word belgesi veya tehlikeli bir bağlantı bulunur. Gönderici olarak her zaman doğru bir adım görüntülenir. Böylece alıcı e-postanın güvenli olduğunu düşünür: Her şey meşru bir e-posta gibi görünmektedir. Birçok durumda alıcılar tehlikeli bağlantıya tıklar veya virüs içeren eki indirir.

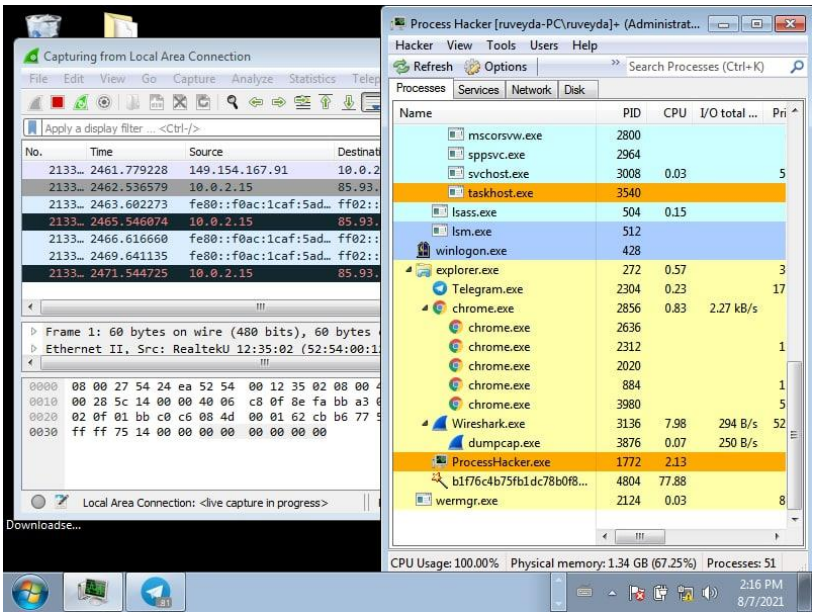


Emotet, ağa erişim sağladığında yayılabilir. Bu süreçte, kaba kuvvet yöntemini kullanarak hesapların parolalarını kırmaya çalışır. Emotet'in diğer yayılma yöntemi, Windows'da bulunan ve kötü amaçlı yazılımın insan müdahalesi olmadan yüklenmesine olanak sağlayan EternalBlue ve DoublePulsar güvenlik açıklarından yararlanmaktır. 2017'de, para sızdırmaya yönelik Trojan WannaCry, EternalBlue güvenlik açığından yararlanarak büyük bir siber saldırı gerçekleştirdi ve yıkıcı bir hasara neden oldu.

Virustotal ile yapılan ön incelemede farklı antivirüs programları tarafından incelendiğinde 62 tanesinin emoteti zararlı bir dosya olarak gördüğü ortaya çıkmıştır.Dosyanın Virustotal'e ilk yüklenme tarihinin ise 25 Haziran 2020 olduğu görülmektedir.

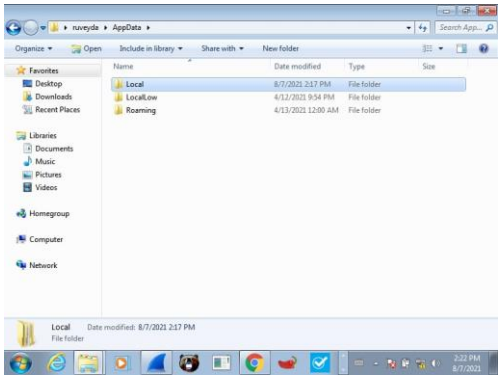


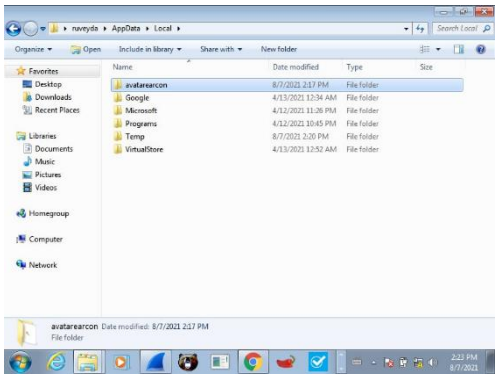
Emotet çalıştırıldıktan sonra Processhacker ve Wireshark üzerindeki değişimleri görülmektedir.

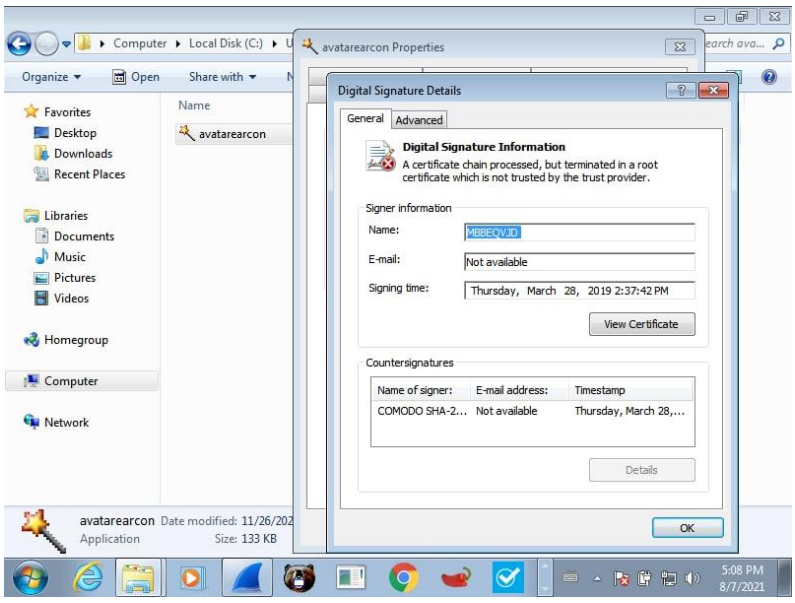


Çalıştırılan avataraercom isimli dosyanın bir süre sonra çalışması zamanlanmış görev altında bir işlem olabileceğini de gösterebilmektedir. Zamanlanmış görevler incelendiğinde işletim sistemi

başladığında ve her 10 dakikada bir avataraercom ismi dosyanın çalıştırılması için ayarlandığı görülmektedir. Çalıştırılacak olan dosyanın da %APPDATA% altında Local klasöründe olduğu da görülmektedir. Zararlı yazılımın kendisini her açılışta veya görev yöneticisi tarafından kapatıldığında tekrar çalışmak için önlem aldığı anlaşılmaktadır.







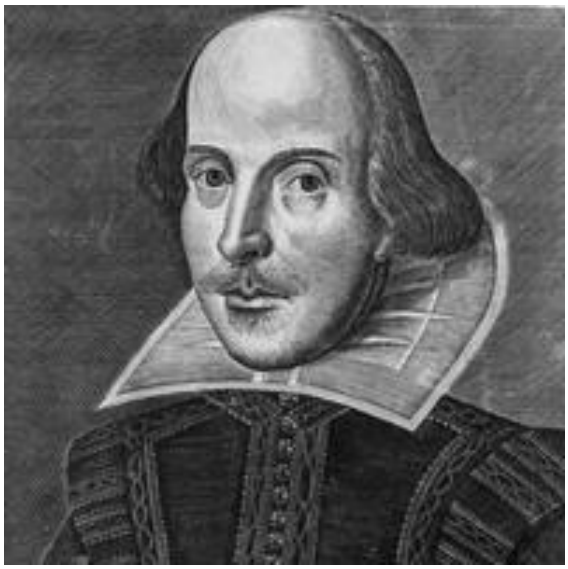
EMOTET'TEN KORUNMA YÖNTEMLERİ

- Güvenlik güncellemeleri olası güvenlik açıklarının kapatılması için üreticiler tarafından sağlanan güncellemelerin en kısa süre içinde yüklenmesi çok önemlidir.
- Virüs koruması kötü amaçlı yazılım koruması programı yüklediğinizden ve bilgisayarınızın güvenlik açıklarına karşı düzenli olarak taranmasını sağladığınızdan emin olun.
- E-postalardaki şüpheli ekleri indirmeyin veya kuşku uyandıran bağlantılara tıklamayın.
- Verilerinizi düzenli olarak bir harici depolama cihazına yedekleyin.
- Tüm oturum açma işlemlerinizde (çevrimiçi bankacılık, e-posta hesabı, çevrimiçi mağazalar) mutlaka güçlü parolalar kullanın.
- Dosya uzantıları: Bilgisayarınızın, dosya uzantılarını varsayılan olarak görüntülemesini sağlayın.

SYHLOCK

Shylock kötü amaçlı yazılımı, ağ veri trafiğini durdurmak ve finansal kurumların web sitelerine kod enjekte etmek için tarayıcı tabanlı saldırılara ve sahte dijital sertifikalara güvenmeleri ile karakterize edilen Shylock bankacılık Truva Atları ailesinin herhangi bir üyesini ifade eder.

Birincisi Şubat 2011'de keşfedildi. Kodunda William Shakespeare'in "Venedik Tüccarı" na yapılan çeşitli referanslar nedeniyle, vicdansız para ödünç veren Shylock karakteri olarak adlandırıldı.



SHYLOCK BANKACILIK VİRÜSÜ DAVRANIŞSAL ANALİZİ

Shylock, arka planda dolandırıcılık işlemlerini otomatik olarak başlatabilen otomatik işlem hizmeti (ATS) adı verilen bir teknik kullanır. Yetenekleri şunları içerir:

Shylock/Caphaw.D

File hash

```
$ rahash2 -a sha256 shylock_d.exe
shylock_d.exe: 0x00000000-0x00049000
sha256: 35ccf0e051fb0ff61e52ff4130eb3 \
    8521f954f90ad9c97be59af1e7901974557
$
```

Mitigations

```
$ rabin2 -k '*' shylock_d.exe
archs=0:0:x86:32
pe.seh=true
$
```

- Kullanıcı hesapları ve hesap bakiyeleri hakkında bilgi alma
- Arka planda hileli işlemler gerçekleştirme
- Kullanıcıyı bir Güvenli Anahtar ile bir işlemin kimliğini doğrulaması için kandırmak için sosyal mühendislik saldırıları
- İşlem kayıtlarındaki girişleri gizleme ve bakiyeleri değiştirme
- Bazı dolandırıcılık algılama mantığından kaçınmak için mevcut fonların yüzdelerini ve değerlerini ayarlama

SHYLOCK TARAFINDAN GELİŞTİRİLEN VE İNDİRİLMEKTE OLAN MODÜLLER ŞUNLARI İÇERİR:

•**Archiver(Arşivleyici):** Kaydedilmiş video dosyalarını uzak sunuculara yüklemeden önce sıkıştırır

•**BackSocks:** Güvenliği ihlal edilmiş bilgisayarın bir proxy sunucusu gibi davranmasını sağlar

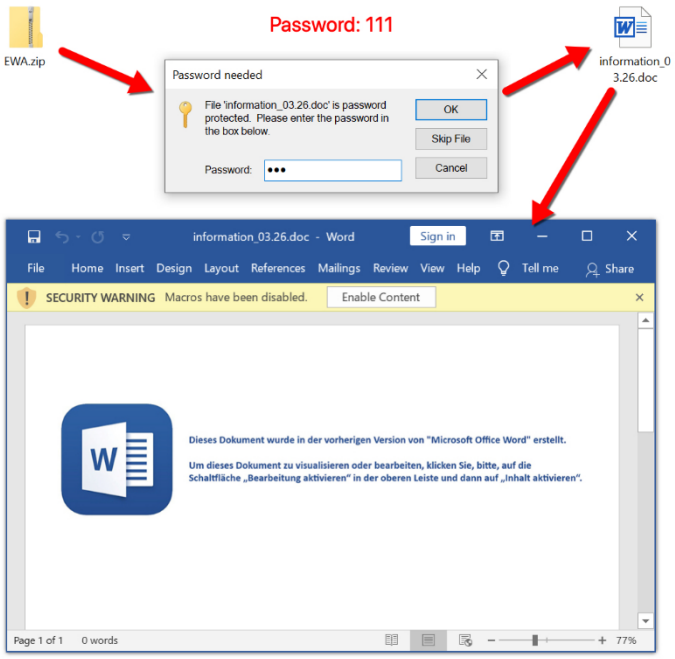
• **DiskSpread:** Shylock'un bağlı, sabit olmayan sürücülere yayılmasını sağlar

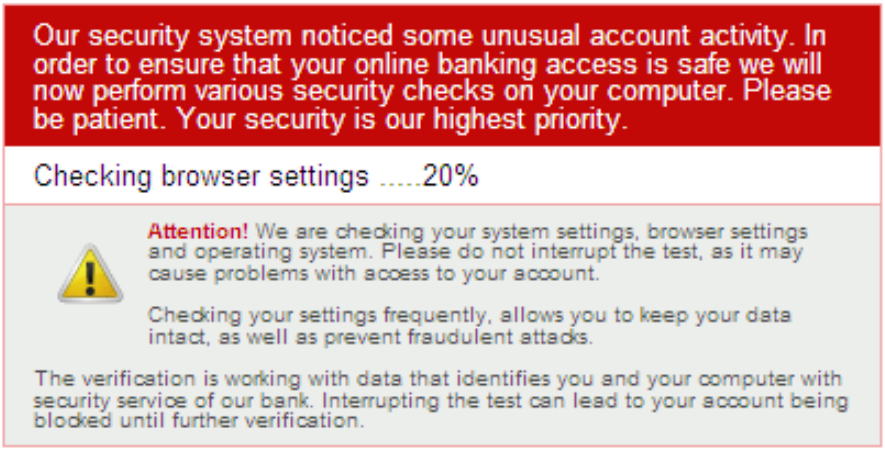
• **Ftpgrabber:** Çeşitli uygulamalardan kaydedilmiş şifrelerin toplanmasını sağlar

• **MsgSpread:** Shylock'un Skype anlık mesajları yoluyla yayılmasını sağlar

• **VNC:** Saldırgana, güvenliği ihlal edilmiş bilgisayara bir uzak masaüstü bağlantısı sağlar

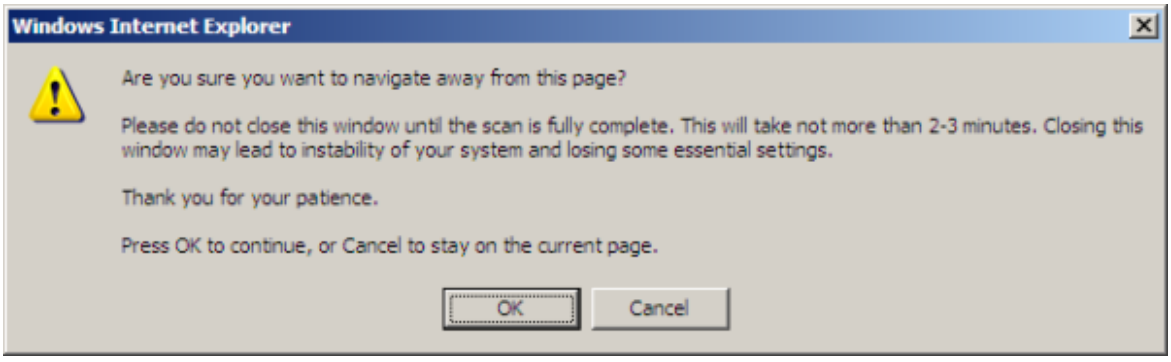
Bir kurban, virüslü bir makinede bankasına giriş yaptığında, kimlik bilgileri bankaya ve saldırganlara gönderilir. Bu, saldırganların hesabın kontrolünü ele geçirmesine ve sahte işlemler başlatmasına olanak tanır. Kullanıcının dikkatini dağıtmak için saldırganlar tarafından bir takım oyalama taktikleri kullanılmaktadır. Örneğin, müşterilere karşı kullanılan oyalama taktiği, bilgisayarda ek güvenlik kontrolleri yapıyormuş gibi görünen bir penceredir.





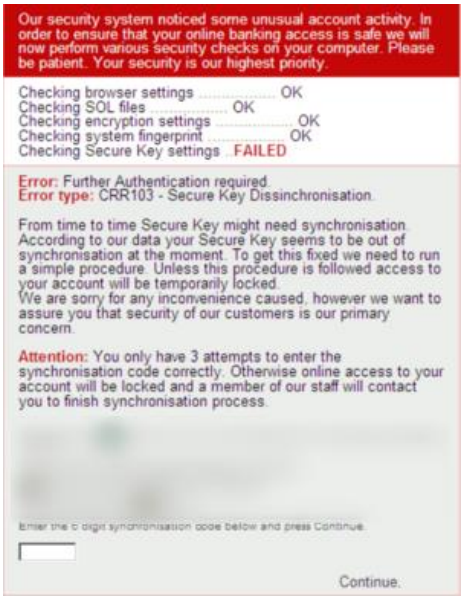
Şekil 1. Hileli bir işlem girişimi sırasında görüntülenen hata mesajı

Kullanıcı sabırsızlanır ve bu sayfadan uzaklaşmaya çalışırsa, onlara sosyal olarak tasarlanmış başka bir mesaj sunulur.



Şekil 2. Hileli bir işlem girişimi sırasında görüntülenen açılır hata mesajı

Hileli işlem ayarlandıktan sonra, son olarak kullanıcıdan, saldırgan tarafından sağlanan alanlara altı basamaklı güvenlik kodunu girerek sahte işlemi yetkilendirmesi istenir. Bu, mağduru yanlışlıkla sahte bir işleme izin vermesi için cezbedecektir.

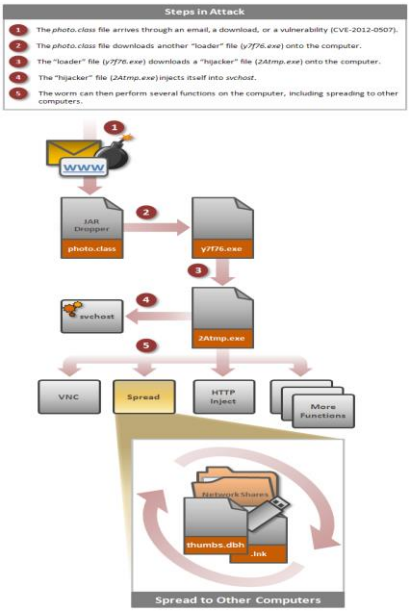


Şekil 3. Saldırganlar kurbanı bir güvenlik kodu sağlamaya ikna ediyor

Saldırganlar bir işlemi başarıyla yürüttükten sonra, kullanıcıyı ek işlem yetkileri sağlamak için daha fazla sosyal mühendislik yapabilirler. Alternatif olarak, Shylock, kullanıcının herhangi bir şüpheli aktiviteyi fark etmelerini önlemek için bir geciktirme taktiği olarak internet bankacılığını kullanmasını engelleyen bir bildirim görüntüleyebilir.

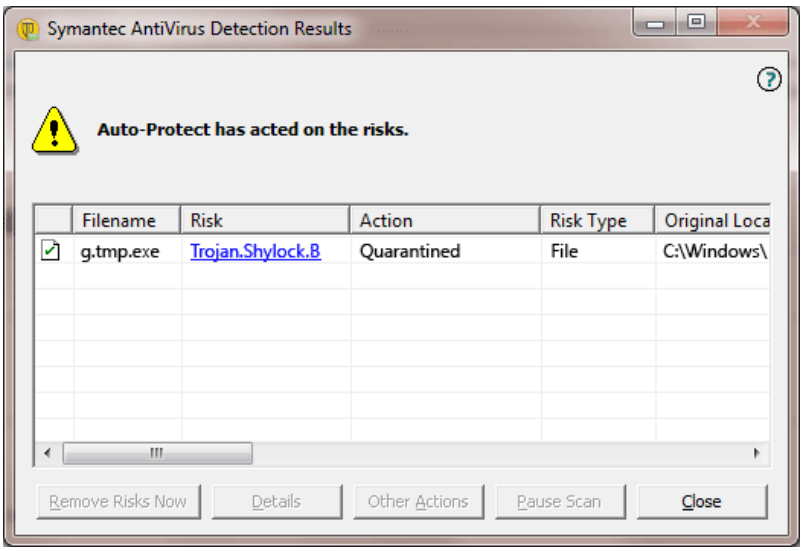
Shylock içeren virüslü istenmeyen e-postalar, PDF belgeleri gibi görünür ve genellikle önemli bir iş belgesi gibi görünecek şekilde tasarlanmıştır. Ek adları, aşağıdaki biçimi izledikleri için tanımlanabilir:

- 28-11 brevi statement_[DIGITS].pdf.exe
- copy #2 of invoice_[DIGITS].pdf.exe
- download_document_[DIGITS].pdf.exe
- f138-dec-12-2013-sorry_[DIGITS].pdf.exe
- invoice_[DIGITS].pdf.exe
- invoice_[DIGITS].pdf.exe
- luca[DIGITS].pdf.exe
- private_[DIGITS].pdf.exe
- servidor hpinvoice_[DIGITS].pdf.exe
- skype_update_december2013_patch[DIGITS].pdf.exe
- sorry_[DIGITS].pdf.exe
- statement_[DIGITS].pdf.exe



Shylock'un algılamadan kaçınmak için dosyalarını ve kayıt defteri girdilerini sildikten sonra (dahili bir pili olmadığı varsayılarak) makinenin güç kaynağının fiziksel olarak fişinin çekilmesinin, belleği ve ayrıca Shylock bulaşmasını temizleyeceğini bulunmuştur.

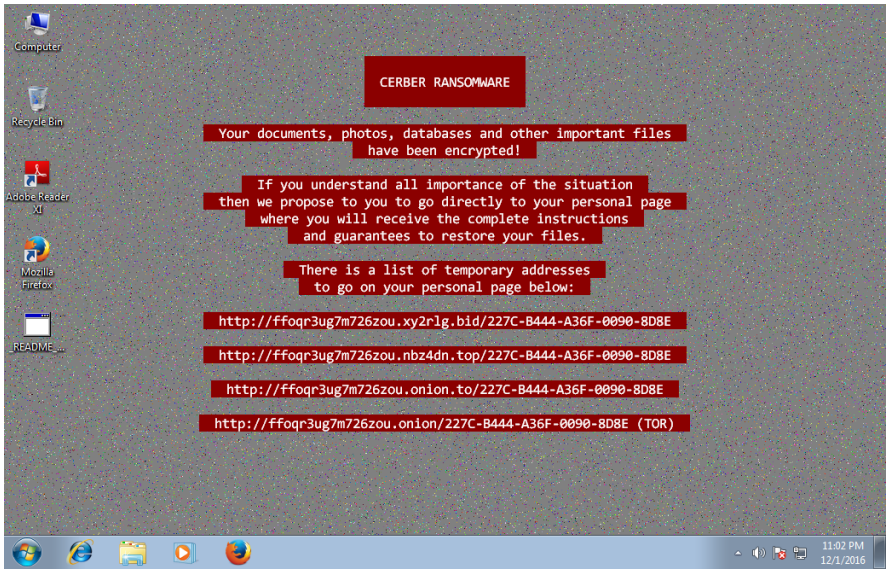
Shylock kötü amaçlı yazılımın ayırt edici özelliklerinden biri, kurulumdan sonra virüsten koruma tarayıcıları tarafından algılanmayı neredeyse tamamen önleme yeteneğidir. Shylock, tarayıcılardan kaçınmak için benzersiz bir üç adımlı süreç kullanır:



1. Adım: Mali Kötü Amaçlı Yazılım Bellekte Gizlenir

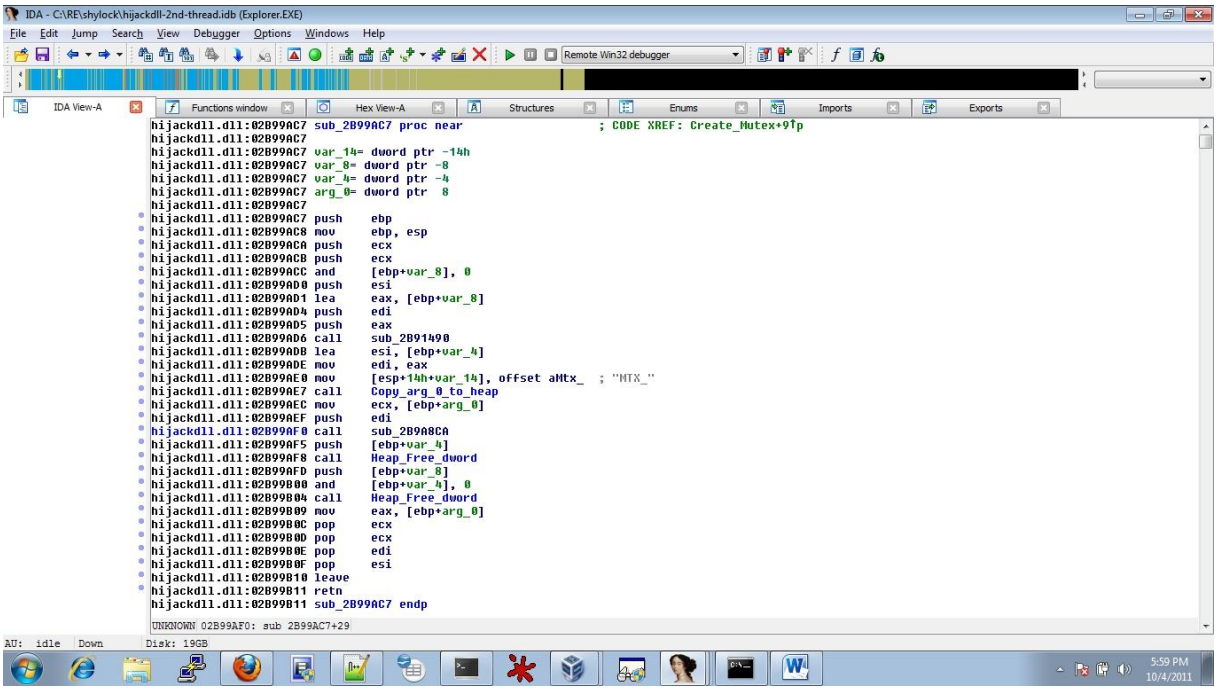
Shylock, kendisini bellekte çalışan tüm işlemlere (uygulamalara) enjekte eder. Her yeni uygulama başlatıldığında, Shylock uygulamanın bellekte çalışmasını askıya alır, kendisini uygulama sürecine enjekte eder ve ardından uygulamanın normal çalışmasına devam etmesine izin verir. Yüklendikten sonra, Shylock kodu ayrı bir işlem olarak çalışmaz; bunun yerine, kendisini bir makinede çalışan her gerçek uygulamanın içine yerleştirir. Bu, tespit edilmesini çok zorlaştırır. Üstelik Shylock algılansa

bile, çalışan birden fazla uygulamaya gömülü olması, durdurulmasını ve bellekten kaldırılmasını neredeyse imkansız hale getiriyor.



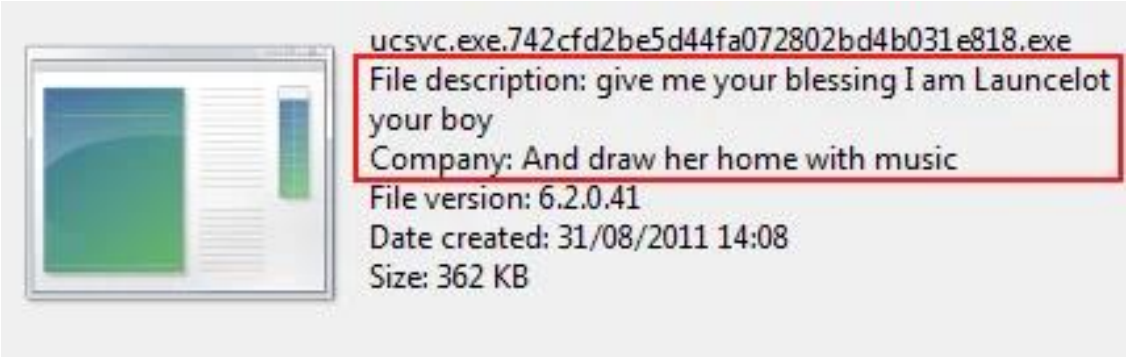
2. Adım: Watchdog Taramaları Algılar:

Shylock, bir virüsten koruma tarama işleminin devam ettiğini gösteren, dizin tarama ve kayıt defteri anahtarlarının numaralandırılmasıyla ilgili işlemleri arar ve durdurur. "Tarama" etkinliğini algıladığında, Shylock kendi dosyalarını ve kayıt defteri girdilerini siler ve onu algılanamaz hale getirir. Sadece hafızada aktif kalır.



3. Adım: Windows'un Kapatılmasını Korur:

İşletim sistemi kayıt defterindeki girişler, kötü amaçlı yazılımın (herhangi bir uygulama veya işlem gibi) dosyalarını başlatma işlemlerinin bir parçası olarak yürütmesine izin verir. Shylock, bir antivirüs taraması tarafından algılanmamak için dosyalarını ve kayıt defteri girdilerini kaldırdıktan sonra, sistemin kapanması/yeniden başlatılmasından kurtulamaz. Bu eylemlerden herhangi biri onu bellekten siler ve enfeksiyonu ortadan kaldırır. Hayatta kalmasını sağlamak için Shylock, Windows kapatma prosedürüne bağlanır ve sistem tamamen kapatılmadan hemen önce ve antivirüs uygulamaları da dahil olmak üzere tüm uygulamalar kapatıldıktan hemen sonra dosyaları ve kayıt defteri anahtarlarını eski durumuna getirir.



SYHLOCK'TAN KORUNMA YÖNTEMLERİ

- Bilinmeyen bir gönderenden aldığınız e-posta eklerini veya bağlantılarını açmayın. Bunlar kötü amaçlı yazılım içerebilir.
- Bir sosyal ağ veya messenger'da arkadaşınızdan bağlantı ya da ek içeren bir mesaj alsanız bile alternatif iletişim kanalları yoluyla mesajın meşruluğunu doğrulamaya çalışın. Ele geçirilen sosyal ağ ve messenger hesapları maalesef genellikle kötü amaçlı yazılım yaymak için kullanılır.
- Bankanızdan bir e-posta veya SMS aldığınızda bankaların asla hesapların PIN kodlarını veya parolalarını istemeyeceğini unutmayın. Bankaların müşteri postaları için her zaman kurumsal posta alanlarını kullandığını ve asla herkese açık e-posta servislerini kullanmadığını unutmamanız da faydalıdır.
- Kimlik avı web sitelerinden kaçınmaya çalışın: Bir sitenin güvenli bağlantı kullanıp kullanmadığını kontrol edin (adres çubuğunun başında https yazar)
- Herkese açık bir Wi-Fi ağı kullanırken hassas verileri girmekten kaçının
- Kötü amaçlı bankacılık faaliyetlerini engellemek için güvenilir bir güvenlik çözümü kullanın