# Kayseri üniversitesi Siber Güvenlik Uygulama ve Araştırma Merkezi

# Analiz sonuçları-I

# Danabot

Danabot son günlerde aktifliğini artırmış bir bankacılık virüsü çeşididir. Danabot, ilk olarak Mayıs 2018'de Proofpoint tarafından keşfedilen bir (bankacılık/hırsızlık) kötü amaçlı yazılımıdır. Bu yazılımın üç önemli sürümü vardır:

- Sürüm 1: Danabot - Down Under'da yeni bir bankacılık Truva Atı ortaya çıkıtı.
- Sürüm 2: Danabot Popülerlik Kazanıyor ve Büyük Kampanyalarda ABD Kuruluşlarını Hedefliyor.
- Sürüm 3: ESET'in Danabot'u yeni komut ve kontrol (C&C) iletişimi ile güncellenmişidir.

Mayıs 2018'den Haziran 2020'ye kadar Danabot, suç yazılımı tehdidin en önemlilerinden biriydi. Proofpoint araştırmacıları, sürüm 2'de en az 12 üye kimliği ve sürüm 3'te 38 üye kimliği olan birden fazla tehdit aktörünü gözlemledi. Bu üye kimlikleri(ID'ler), Danabot operatörlerinin hizmet verdiği tehdit aktörlerini temsil ediyor. Dağıtım, genellikle ağırlıklı olarak ABD, Kanada, Almanya, Birleşik Krallık, Avustralya, İtalya, Polonya, Meksika ve Ukrayna'da bulunan finansal kurumları hedef almıştır. Haziran 2020'den sonra, Proofpoint'in verilerinde ve halka açık tehdit istihbarat depolarında (Örneğin: MalwareBazaar ve Danabot) Danabot etkinliğinde keskin bir düşüş oldu. Açık bir neden olmadan tehdit ortamından kayboldu [1].

Danabot, Delphi programlama dilinde yazılmış, kimlik bilgilerini çalabilen ve virüslü sistemleri ele geçirebilen bir bankacılık truva atıdır. Faturalar gibi görünen spam e-postalar aracılığıyla dağıtılır. Kötü niyetli yürütüldüğünde, meşru bir sistem yönetim aracı olan PowerShell'i ve modüllerini almak ve çalıştırmak için BrushaLoader adlı Visual Basic komut dosyalarını (VBScript) kötü amaçlı kullanır.

Danabot ilk keşfedildiğinde, Word belgelerini gömülü olarak kullandı(makro). Kötü niyetli Etkinleştirildiğinde, Danabot'u PowerShell aracılığıyla indiren makro. Güvenlik araştırmacıları, BrushaLoader'ın son spam kampanyalarında kullanımının yakın zamanda ortaya çıktığını belirtti. Ve Danabot kendisi güncelledi.

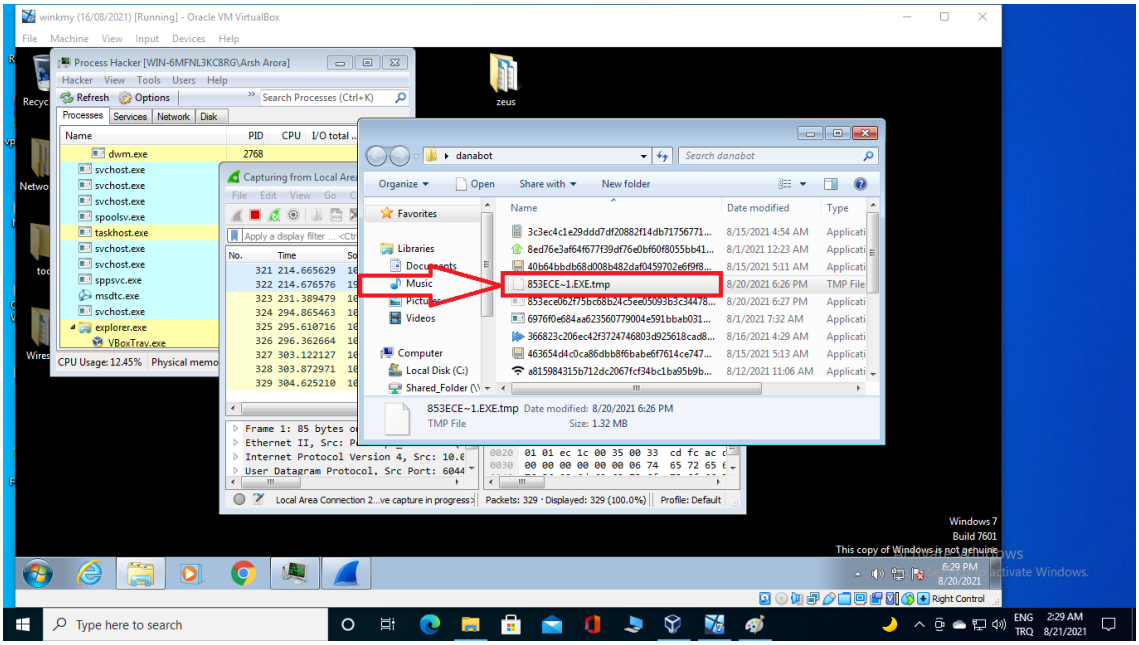
Danabot'un ilk olarak Avustralyalı kullanıcılara spam yoluyla, kullanıcının bir güvenlik şirketi tarafından "korunduğunu" iddia eden kötü niyetli bir Word belgesiyle dağıtıldığı görüldü. Danabot'un komut ve kontrol (C&C) sunucusu önce etkilenen sistemin IP'sini kontrol eder ve IP adresi Avustralya'da bulunuyorsa bankacılık truva atını bulaştırır.

Danabot'un operatörleri 2018'den beri hedeflerini genişletti. Son zamanlardaki spam kampanyaları şu anda başta Avusturya, Almanya, İtalya, Polonya ve Ukrayna olmak üzere Avrupa ülkelerine dağıtılıyor. Mesajlar hala fatura olarak görünse de, DanaBot'un çeşitli bileşenlerini indirmek için PowerShell ve BrushaLoader kullanılır.

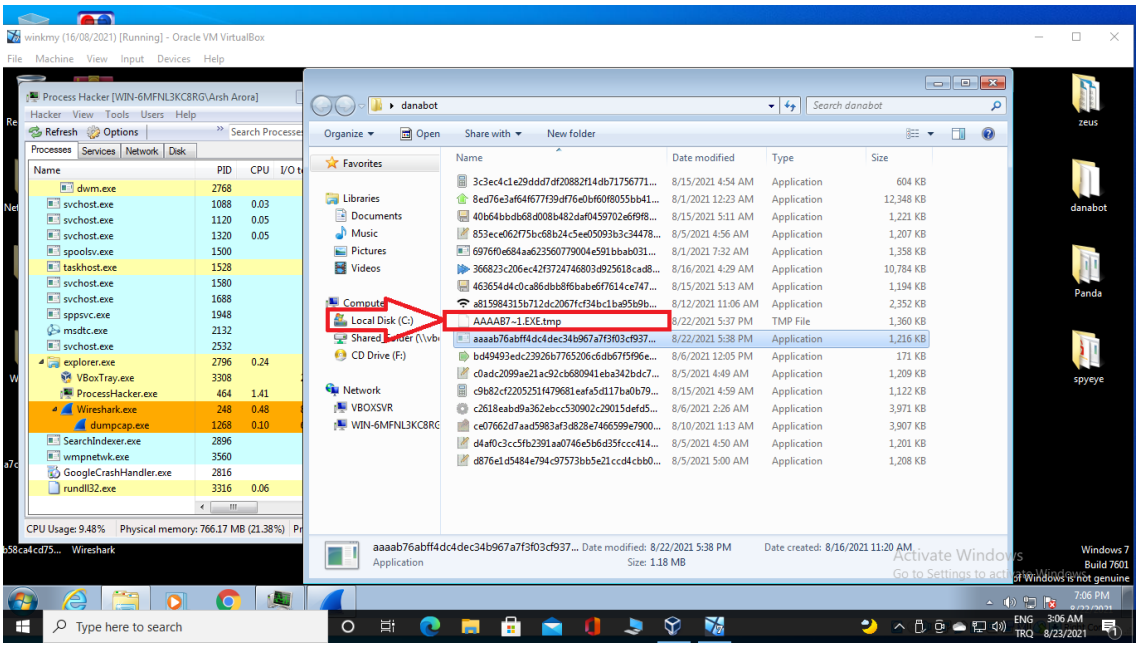
Danabot, çok aşamalı bulaşma zinciri ve modüler mimarisi ile dikkat çekiyor. Trustwave'in önceki araştırması ve ESET'in yeni araştırması, Danabot'un farklı işlevler gerçekleştiren - çoğunlukla dinamik bağlantı kitaplıkları (DLL) olarak - çeşitli bileşenler içerdiğini tanımlar. Tanımlanan eklentiler, çeşitli uygulamalardan kimlik bilgilerini çalar, diğer Windows tabanlı bilgisayarlara RDP (Uzak Masaüstü Protokolü) işlevi görür, diğerlerinin yanı sıra tarayıcılara komut dosyaları enjekte eder[2].

# Danabot analiz sonuçları

Yaptığımız analiz sonuçları danabot'un yeni tmp(TMP dosyaları, bilgisayarınızda kullandığınız herhangi bir program içinde düzenlemeler yaptığınızda, bu düzenlemelerin geri alınabilmesi için otomatik olarak oluşturulmuş dosyalardır.) uzantılı yeni dosya olşuturduğunu gözlemledik.




Şekil 1: Danabot virüsünün çalıştırdıktan sonra oluşturduğu dosya uzantısı

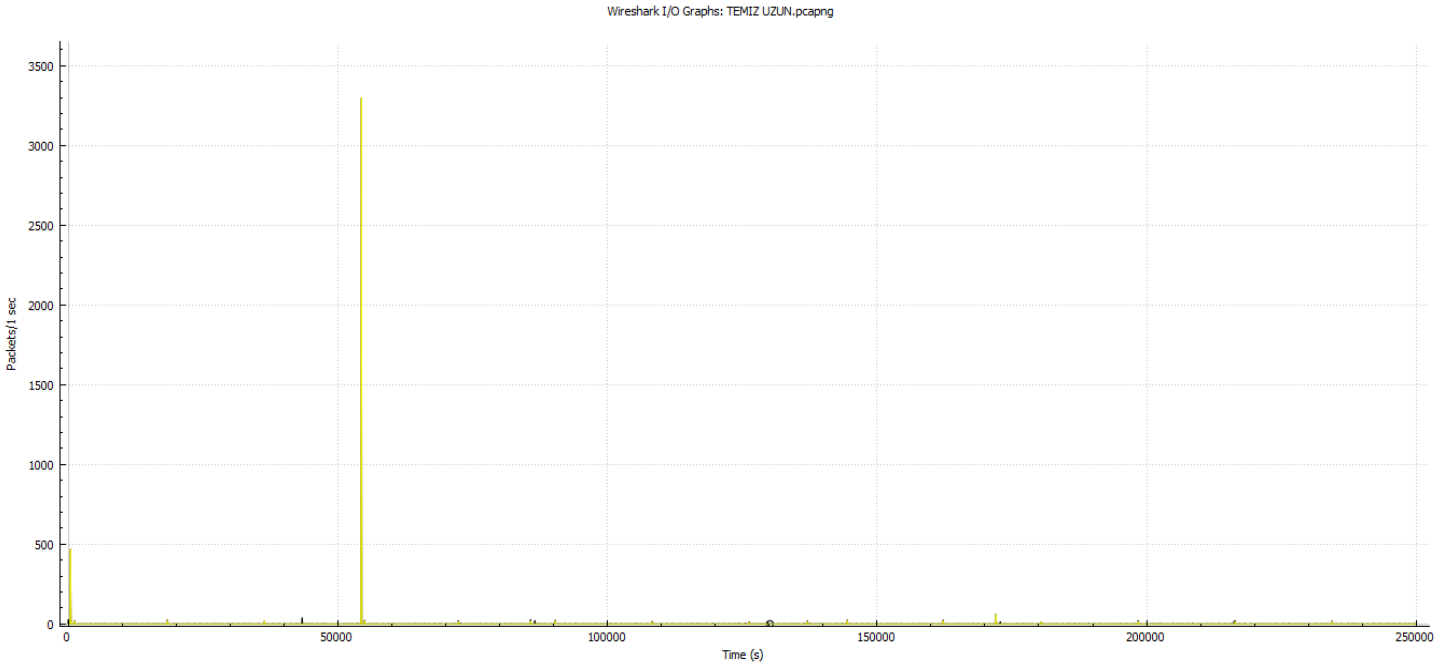



Şekil 2: Danabot virüsünün çalıştırdıktan sonra oluşturduğu dosya uzantısı

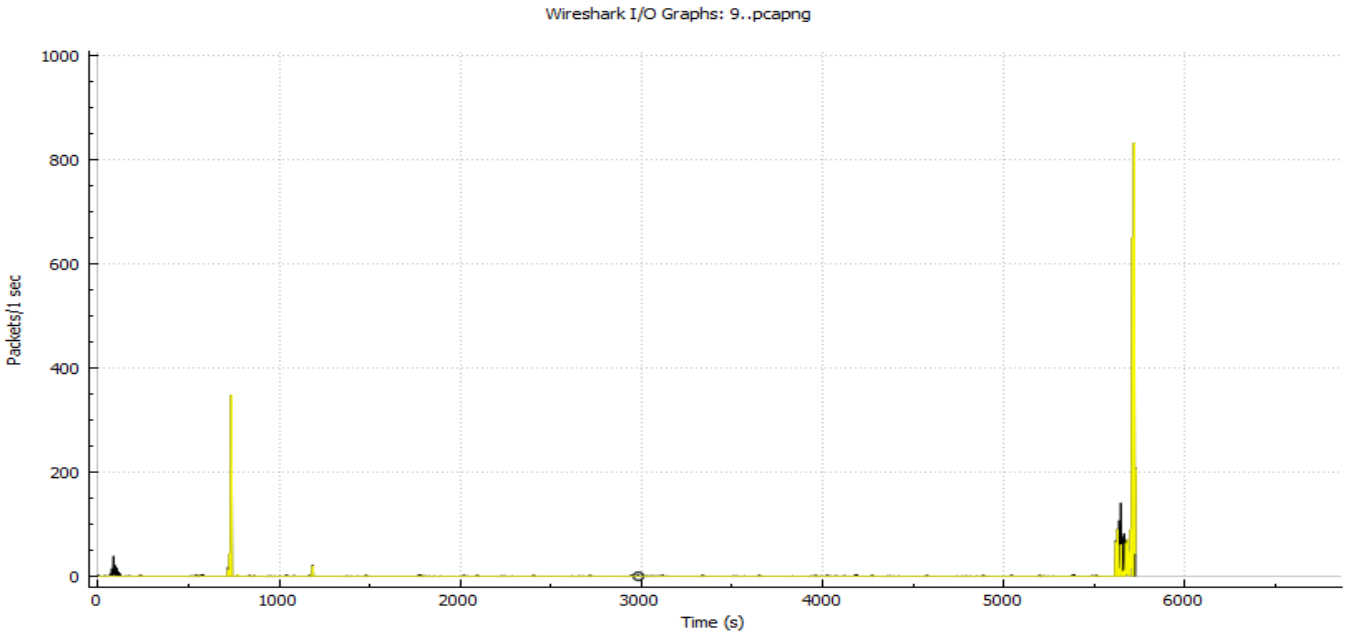
wireshark kullanarak yaptığımız trafik analiz sonuçları aşağıdaki gibi verilmiştir.

**=PC'ye gelen ve çıkan tüm paket çeşitleri**

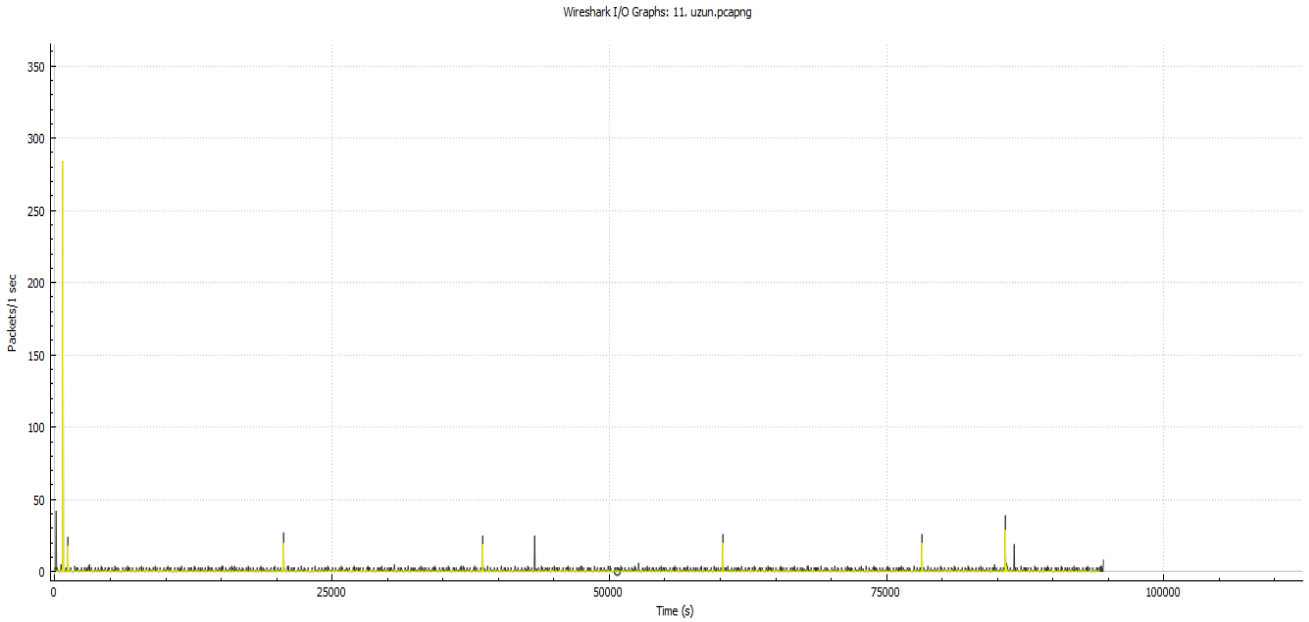
**=PC'ye gelen ve çıkan TCP paket çeşitleri**




Şekil 3: Temiz(virüsüz) bilgisayarın oluşturduğu trafik(her 1 saniyede PC gelen ve giden paket sayısı)




Şekil 4: Danabot virüsü çalışırken bilgisayarda oluşan trafik(her 1 saniyede PC gelen ve giden paket sayısı)




Şekil 5:Danabot virüsü çalışırken bilgisayarda oluşan trafik(her 1 saniyede PC gelen ve giden paket sayısı)

# Panda

Zeus Panda, Panda Banker veya Panda, bankacılık Truva Atı kategorisi altındaki orijinal Zeus'un (Truva atı) bir çeşididir. Keşfi, 2016 yılında Brezilya'da Olimpiyat Oyunları sırasında gerçekleşti. Kodun çoğu, orijinal Zeus truva atından türetilmiştir ve tarayıcıdaki kullanan kişinin tuş kaydını(keyloger) ve form kapma saldırıları gerçekleştirmek için kodlanmıştır. ZeuS Panda, çeşitli açıklardan yararlanma kitleri ve yükleyicilerle, doğrudan indirmeler ve kimlik avı e-postaları yoluyla saldırı kampanyaları başlatır ayrıca internet arama sonuçlarını virüslü sayfalara yönlendirir. Gizli yetenekler, kötü amaçlı yazılımın tespit edilmesini değil, aynı zamanda analiz edilmesini de zorlaştırır.

ZeuS Panda, Emotet, Smoke Loader, Godzilla ve Hancitor gibi çok sayıda yükleyicinin yeteneklerini kullanır. Yükleyicilerin yöntemleri değişir, ancak bir sisteme ZeuS Panda'yı kurmak için aynı nihai durum hedefi aynıdır. Yükleyicilerin çoğu, daha önce ZeuS Panda için bir dağıtım sistemi olarak yeniden donatılmadan önce orijinal olarak truva atıydı. Angler, Nuclear, Neutrino, Sundown gibi Exploit kitleri de kullanıldığından, dağıtım mekanizmaları yukarıda belirtilen yükleyicilerle zorunlu olarak durmaz. Zeus Panda bankacılık trojanının kodlayıcıları ve diğer truva atı kodlayıcıları, parasal kazançtaki daha yüksek potansiyel verim nedeniyle, istismar kitleri yerine yükleyicileri kullanmaya eğilimlidir. Yükleyiciler ayrıca, yeniden başlatma sırasında ve ayrıca silinmesi durumunda ZeuS Panda'nın kalıcı yeteneğini de ekler. Bir sistemde artık ZeuS Panda algılanmıyorsa ve yükleyici hala mevcutsa, kötü amaçlı kodu yeniden indirecek ve yeniden çalışmaya başlayacaktır.

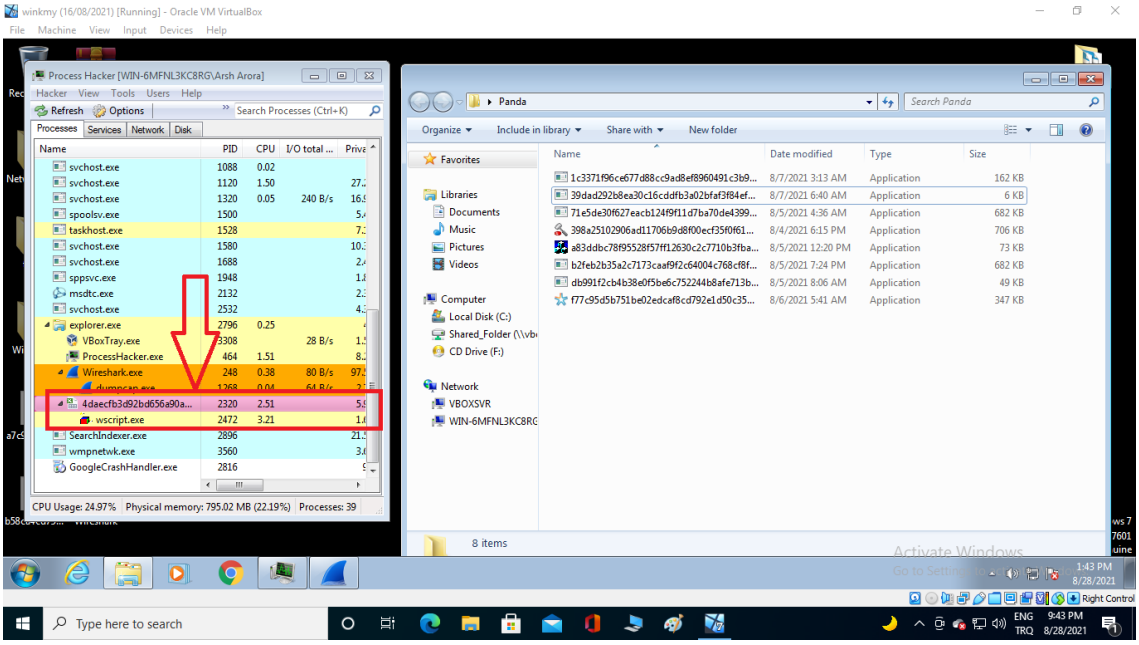
Zeus Panda'nın diğer bankacılık truva atlarına göre en önemli ayrımlarından biri, dünyanın belirli bölgelerindeki sistemleri hedefleyebilmesidir. Buna, bağlı olarak klavyedeki İnsan Arayüzü Aygıtı kodunu algıladığı ilkel bir işlemle yapar. Rusya (0x419), Beyaz Rusya (0x423), Kazakistan (0x43f) veya Ukrayna'dan (0x422) bir klavye kodu algılanırsa Zeus Panda kendini siler. Bu, Rus siber suçlularının tutuklanmaktan kaçınmak için uyguladıkları etik ile uyumludur: “Ruslar Rusları hacklememeli…”, ikincisi “Bir Rus İstihbarat servisi yardım isterse, siz sağlayın” ve son olarak “Tatil yaptığınız yere dikkat edin”.

Zeus Panda, indirme yoluyla sürücü, zehirli e-posta, word belgesi makrosu gibi birçok bulaşma yöntemi kullanır. İndirmelere göre sürücü, Bir kişinin yetkilendirdiği, ancak sonuçlarını anlamadan (örneğin, bilinmeyen veya sahte bir yürütülebilir program, ActiveX bileşeni veya Java uygulaması yükleyen indirmeler)

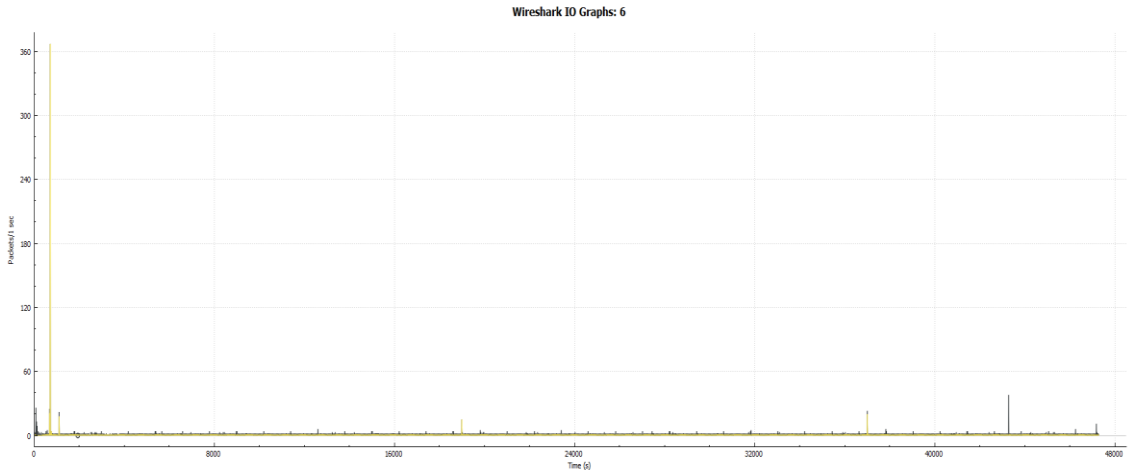
otomatik olarak indirilen indirmelerdir. Bir kişinin bilgisi dışında gerçekleşen herhangi bir indirme, genellikle bir bilgisayar virüsü, casus yazılım, kötü amaçlı yazılım veya suç yazılımı" dâhil. Zehirli e-posta, bir posta listesine çok sayıda geçersiz e-posta adresi enjekte edildiğinde oluşur, bu listeye mesaj göndermek için gereken kaynaklar, geçerli alıcıların sayısı artmamasına rağmen artmıştır. Komuta ve kontrol sunucuları, Zeus Panda'nın dünyanın uçsuz bucaksızlığına nasıl yayılabileceğini, aynı zamanda bir avuç operatör tarafından kontrol altında tutulabileceğini gösterir[3].

## Panda analiz sonuçları

Panda üzerinde yaptığımız analizler sonucunda yeni bir klasör oluşturmak yerine arka planda “wscript.exe” uzantısını çalıştırıyor ve çalıştığı klasörde kendini silmesi şeklindeki davranışlar gözlemledik.




Şekil 6: Panda virüsünün çalışma karakteristiği




Şekil 7: Panda virüsü çalışırken bilgisayarda oluşan trafik(her 1 saniyede PC gelen ve giden paket sayısı)

# Spyeye

Spyeye bir olan kötü amaçlı yazılım saldırıları kullanıcıların çalışan bu programın Google Chrome'u, Opera, Firefox ve Internet Explorer üzerinde Microsoft Windows işletim sistemleri. Bu kötü amaçlı yazılım, kötü amaçlı kullanım için kullanıcı kimlik bilgilerini çalmak için tuş kaydını(keyloger) ve form kapma kullanır. Spyeye, geçerli kullanıcılar banka hesaplarında oturum açmış olsa bile bilgisayar korsanlarının çevrimiçi banka hesaplarından para çalmasına ve işlem başlatmasına izin verir.

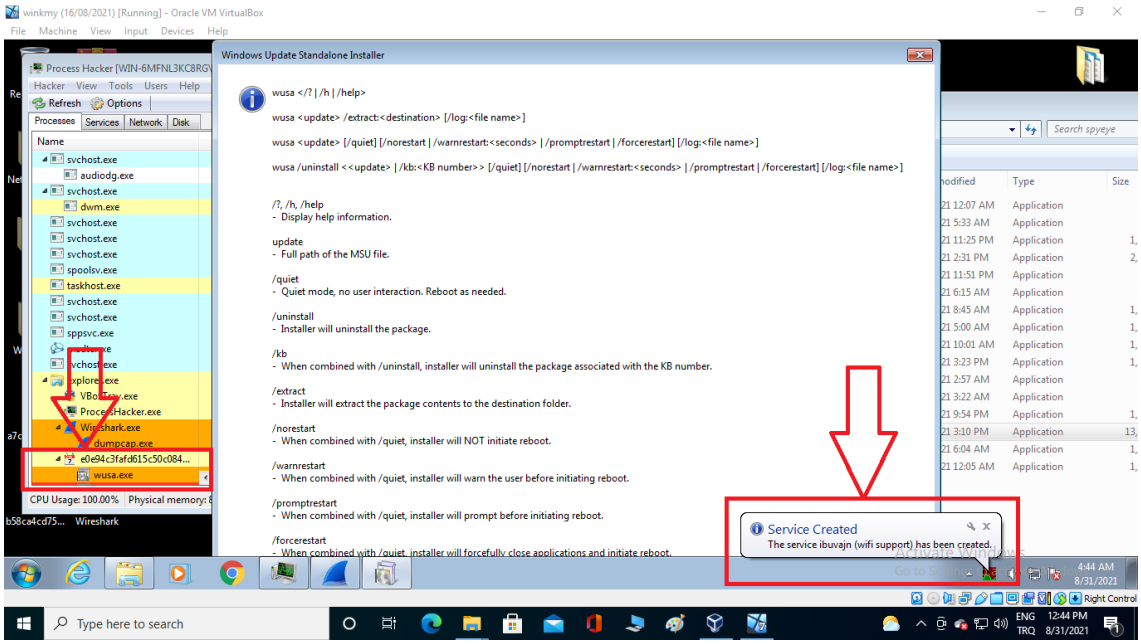
Spyeye, güvenliği ihlal edilmiş bir kullanıcının tarayıcısı bir web sayfası görüntülediğinde yeni alanlar ekleme ve mevcut alanları değiştirme yeteneğine sahiptir bu da kullanıcı adlarını, şifreleri veya kart numaralarını istemesine izin vererek bilgisayar korsanlarına para çalmalarına olanak tanıyan bilgiler verir. Kullanıcının sahte bakiyesini (sahte işlemler gizlenerek) kaydedebilir, böylece kullanıcı bir sonraki oturum açtığında, sahte işlemler ve gerçek bakiye kullanıcının tarayıcısında görüntülenmez (banka sahte işlemleri görse bile)

Spyeye 2009'da Rusya'da ortaya çıktı ve yer altı forumlarında 500$+'a satıldı ve Spyeye keylogger'lar, otomatik doldurma kredi kartı modülleri, e-posta yedeklemeleri, yapılandırma dosyaları (şifreli), Zeus katili, HTTP erişimi, POP3 yakalayıcılar ve FTP gibi özelliklerin reklamını yaptı.

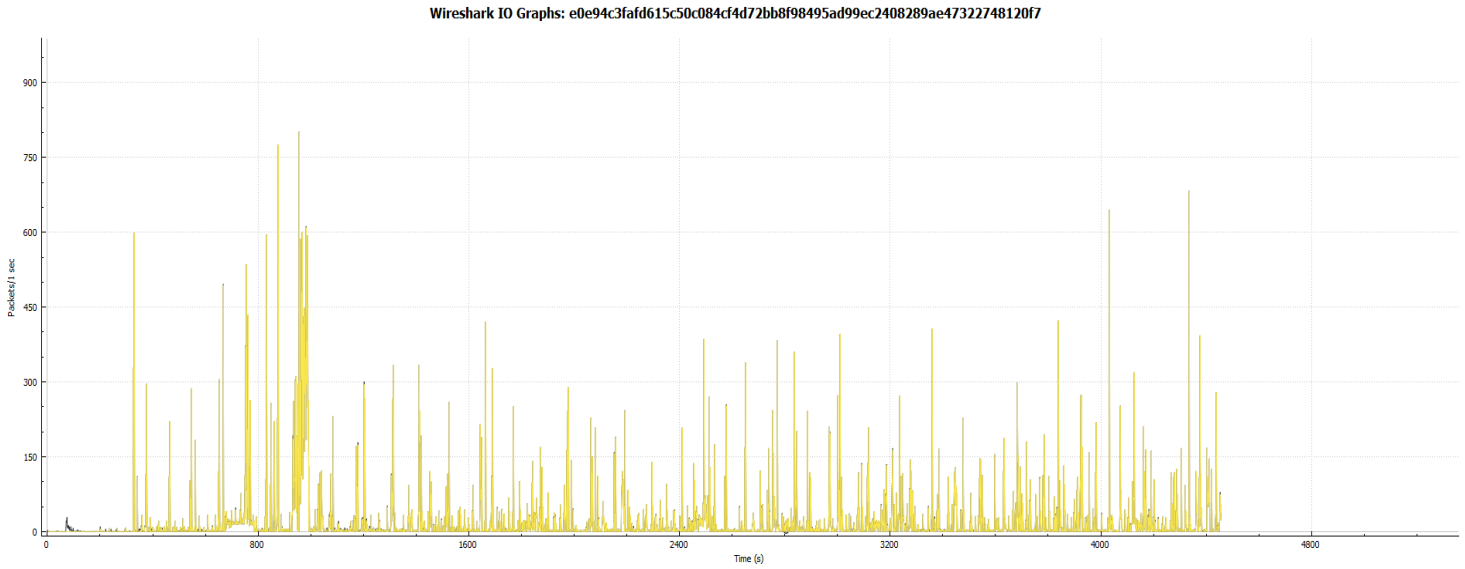
Amerika Birleşik Devletleri, Birleşik Krallık, Meksika, Kanada ve Hindistan'daki hedef kullanıcılar ve kurumlar Spyeye'ın en büyük kurbanlarıydı; Amerika Birleşik Devletleri, bu kötü amaçlı yazılımın kurbanı olan kurumların %97'sini oluşturuyordu[4].

# Spyeye analiz sonuçları

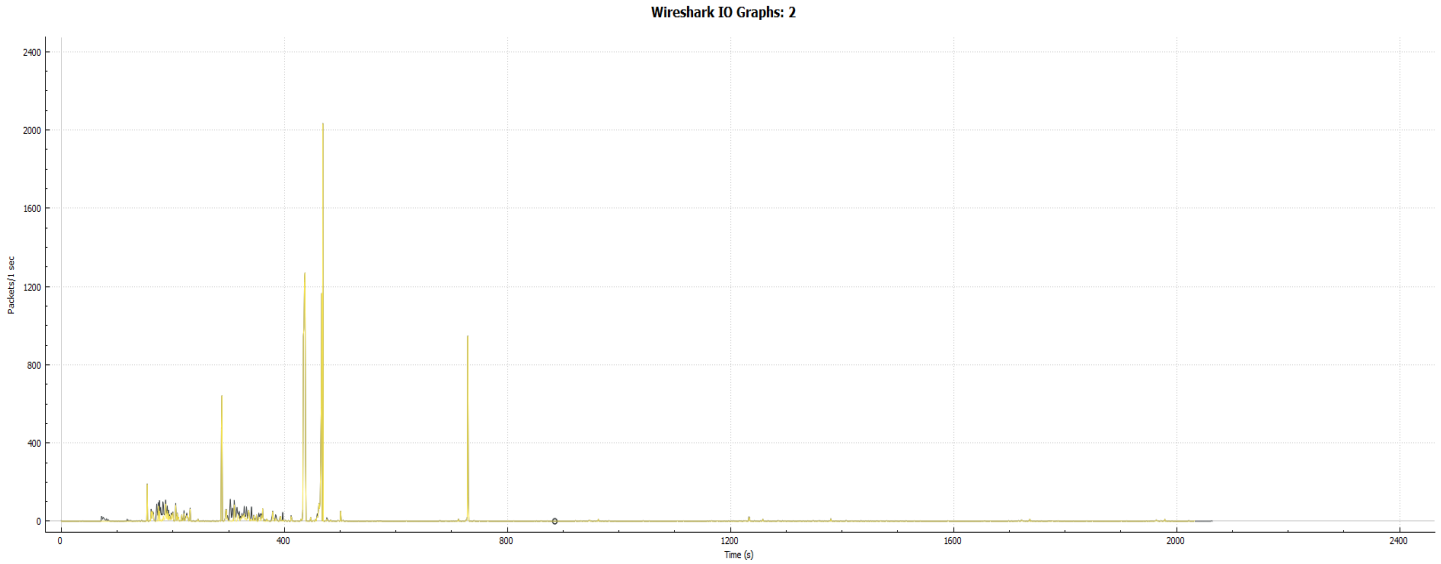
Spyeye dinamik analizinde Panda zararlı yazılımına benzer bir davranış sergiliyor. Çalıştığında kendini gizliyor(yani tıkladığınız exe uzantılı dosyayı siliyor ama arka planda çalışıyor). Ayrıca ağa içerisinde başka bilgisayarlara bulaşabilmesi için wifi support (kablosuz ağ desteği) oluşturuyor.




Şekil 8: Spyeye virüsünün çalışma karakteristiği




Şekil 9: Spyeye virüsü çalışırken bilgisayarda oluşan trafik(her 1 saniyede PC gelen ve giden paket sayısı)




Şekil 10: Spyeye virüsü çalışırken bilgisayarda oluşan trafik(her 1 saniyede PC gelen ve giden paket sayısı)

**Kaynakça**


- https://www.proofpoint.com/us/blog/threat-insight/new-year-new-version-danabot[1].
- https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/danabot-banking-trojan-found-targeting-european-countries[2].
- https://en.wikipedia.org/wiki/ZeuS_Panda[3].
- https://en.wikipedia.org/wiki/SpyEye[4].