Kayseri üniversitesi Siber Güvenlik Uygulama ve Araştırma Merkezi

Analiz sonuçları-II

DRIDEX

Haziran 2014'te ortaya çıkan Dridex, 2010 ve 2013 yılları arasında aktif olan bankacılık truva atı Bugat'ın beşinci çeşitidir ve 2014 yılına kadar aktif olan GameOverZeuS'a (GoZ) özgü özelliklerle zenginleştirilmiştir. Genelde Word makroları üzerinden ilerlemesini sürdüren bir yazılımdır.

Bugat ve Cridex olarak da bilinen bankacılık türünün birincil işlevi hırsızlıktır, yani çevrimiçi bankacılık erişim kodlarını çalmak ve tehdit aktörlerinin ele geçirilmiş banka hesaplarından hileli transferler yapmasına olanak tanımaktır.

Bu amaçla, Dridex en az üç yöntem kullanır. Bu yöntemler aşağıda belirtilmiştir:

- Daha önce ele geçirilmiş çevrimiçi bankaların yasal web sayfalarına, erişim kodlarını isteyen müşterilere kötü amaçlı formlar görüntüleyen bir HTML komut dosyasının enjekte edilmesi;
- Bankaların web sayfaları gibi görünen kötü niyetli bir sayfaya yönlendirme;
- Bankanın web sitesinden sunucu yanıtının kesilmesi ve oradaki kodu enjekte eden tehdit aktörlerinin PHP sunucusuna iletilmesi.

Dridex'in Yapısı

Dridex modüler bir mimariye sahiptir; temelde yükleyici (loader) ve ana işlevlerini yerine getirmek için kullanılan bir dizi çekirdek modülünden (core module) oluşmaktadır. Çekirdek modülüne ek modüller entegre edilebilmektedir.

İlk enfeksiyondan sonra Dridex ek modülleri indirebilir ve kurabilir. Bu durum, Truva Atı'nı oluşturanların özelliklerini eklemesi ve iyileştirmesi için nispeten basit hale getirir.

Aynı zamanda çekirdek modülü, tümleşik işlevleri içeren ve işlevselliğini genişletmek için başka modüllerin eklenebileceği bir yük olarak da bilinmektedir.

Loader Module (Yükleyici Modülü)

Yükleyici modülü, Çekirdek modülün indirilmesinden ve kurulmasından sorumludur. Yükleyici, HTTPS aracılığıyla iletişim kurar ve yerleşik yapılandırmada bulunan kontrol sunucularıyla değiş tokuş edilen XML mesajlarını şifrelemek için RC4'ü kullanır.

Yükleyici modülü, Çekirdek modül için bir yükleme noktası görevi görecek bir kayıt defteri anahtarı oluşturur. Ayrıca indirilen Çekirdek modül için yapılandırma bilgilerini içeren kayıt defteri anahtarını da oluşturur.

Son olarak Yükleyici, yerleşik yapılandırmasındaki sunucuların birinden Çekirdek modül ikili dosyasını ve Çekirdek modül yapılandırmasını istemektedir.

Core Module (Çekirdek Modülü)

Çekirdek modül, Dridex'in işlevselliğinin çoğundan sorumludur. Eşler ve uzak sunucularla ağ iletişimi için HTTPS veya ham TCP kullanır. Ağ üzerinden gönderilen veriler RC4 ile şifrelenir, asimetrik şifreleme kullanır ve Gzip kullanılarak sıkıştırılır. Çekirdek modül kendi genel ve özel anahtar çiftini oluşturmaktadır.

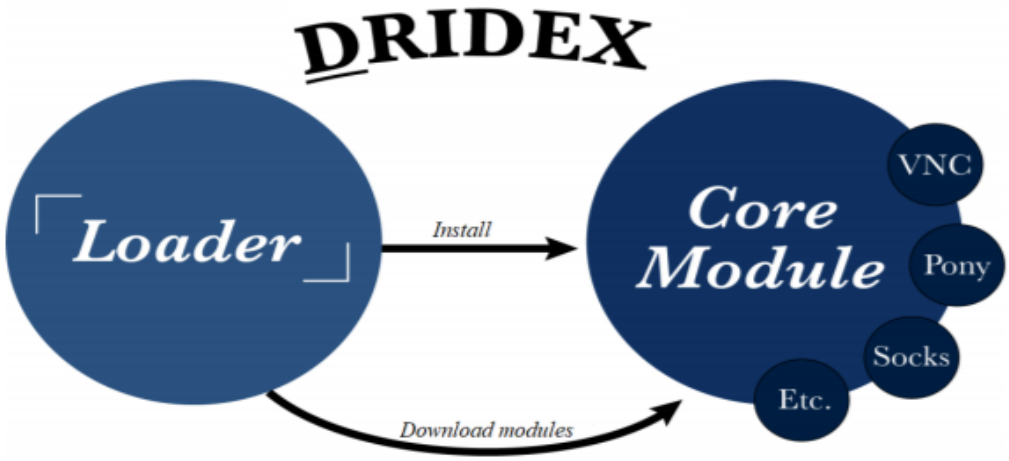
- Formlardan bilgi çalma
- Ekran görüntüsü alma
- HTTP isteklerini yeniden yönlendirme
- Web uygulamalarına kod enjekte etme
- Tuş vuruşlarını günlüğe kaydetme
- Şifreleri çalma
- Sanal ağ bilgi işlemi (VNC)
- Geri bağlantı oluşturma
- Mini sunucu olarak hareket etme (eş düğüm)
- Dosyaları silme
- Diğer modülleri indirme
- Çerezleri çalma

Çekirdek modül, explorer.exe işlemine eklenir. Modül ayrıca (Man In The Browser) MITB saldırılarını gerçekleştirmek için kendisini web tarayıcı süreçlerine enjekte etmektedir.

Çekirdek modülü aşağıdaki temel işlevleri gerçekleştirebilir:

Çekirdek modülü, bu işlevleri P2P (Peer to Peer) ağı üzerinden komutlar, modüller ve yapılandırma bilgileri gönderip alarak gerçekleştirmektedir. XML mesajları, P2P ağı üzerinden iletişim kurmak için kullanılır. Çekirdek modülü, ağ trafiğini CryptGenKey API kullanılarak çalışma zamanında oluşturulan bir anahtarla şifrelemek için RC4'ü kullanır.

Dridex'in eski versiyonları, ağ trafiğini şifrelemek için RC4 yerine XOR kullanıyordu.



Dridex'in genel yapısı

Dridex'in işlevsellikleri aşağıdaki modüllerle genişletilebilir:

VNC Modülü

VNC modülü, bir sanal ağ bilgi işlem (VNC) sunucusu görevi görür. Her ikisi de benzer işlevsellik içeren bir x86 ve x64 modülü mevcuttur.

Modül, bilgisayarı uzaktan kontrol etmek için bir grafik kullanıcı arabirimi (GUI) sağlar ve VNC sunucusunu başlatmak ve durdurmak olmak üzere iki temel işlevi içerir. Bağlanılacak etki alanı ve bağlantı noktası, VncStartServer işlevine giriş bağımsız değişkenleri olarak iletilir.

VNC Modülü ile kurbanın bilgisayarında aşağıdaki işlevlere ulaşılabilmektedir.

- Komut İstemi
- Olay Görüntüleyici
- Bilgisayar Yönetimi
- Dosya Gezgini
- Kontrol Paneli
- Görev Yöneticisi
- Aygıt Yöneticisi
- Programlar ve Özellikler
- Disk Yönetimi
- Güç Seçenekleri

Kısaca Dridex üzerinden VNC Modülü ile sistem kontrolünü sağlamak mümkündür.

SOCKS Modülü

SOCKS modülü, güvenliği ihlal edilmiş bilgisayarda uzaktan komut yürütme, arama ve indirme işlevlerini desteklemektedir. Her ikisi de benzer işlevsellik içeren bir x86 ve x64 modülü mevcuttur.

Ayrıca güvenliği ihlal edilmiş bilgisayarı uzaktan kontrol etmek için komutları HTTP istekleri olarak yorumlayan bir sunucu görevi görür. Uzak adres, modüle argüman olarak iletilir.

SOCKS modülü, güvenliği ihlal edilmiş bir bilgisayarda aşağıdaki işlevleri sağlar:

- Uzaktan komut yürütme
- Dosya indirme
- Dosya sistemi arama
- Komut ve kontrol

Pony Modülü: Pony yazılımına dayalı olarak erişim kodlarını çalabilir.

Kill OS (İşletim Sistemini Öldür): Bulaşmış iş istasyonunu sabote etmek amacıyla ana önyükleme kaydını (MBR) sabit sürücüden siler.

Mod4 Modülü: Yeni bir süreç oluşturmak için kullanılan ek bir modüldür.

Mod6 Modülü: Outlook kullanarak e-posta göndermek için kullanılır. Mevcut kişilere e-posta göndermek için Outlook'u kullanarak bir spam modülü olarak işlev görür.

Dridex Enfeksiyon Süreci

Dridex, Windows web tarayıcıları her açıldıklarında kendisini enjekte etme ve çevrimiçi bankacılık oturumları için izleme yeteneğine sahiptir.

Kimlik bilgileri, öncelikle tarayıcıdaki adam (MITB) saldırıları yoluyla çalınır.

Truva atı daha sonra çevrimiçi bankacılık oturumları için tarayıcı etkinliğini izler. Kullanıcı, yaklaşık 300 web sitesinden (çoğunlukla bankalar) oluşan yapılandırılmış bir listeden birinde oturum açarsa, Dridex, çevrimiçi formlara veri girişi yakalama, tuş vuruşlarını kaydetme veya ekran görüntüsü alma gibi çeşitli yöntemler kullanarak kimlik bilgilerini çalmaya çalışır.

Çalınan veriler, şifreli iletişimler kullanılarak saldırgan tarafından kontrol edilen C&C sunucularına geri iletilir.

Dridex enfeksiyon süreci

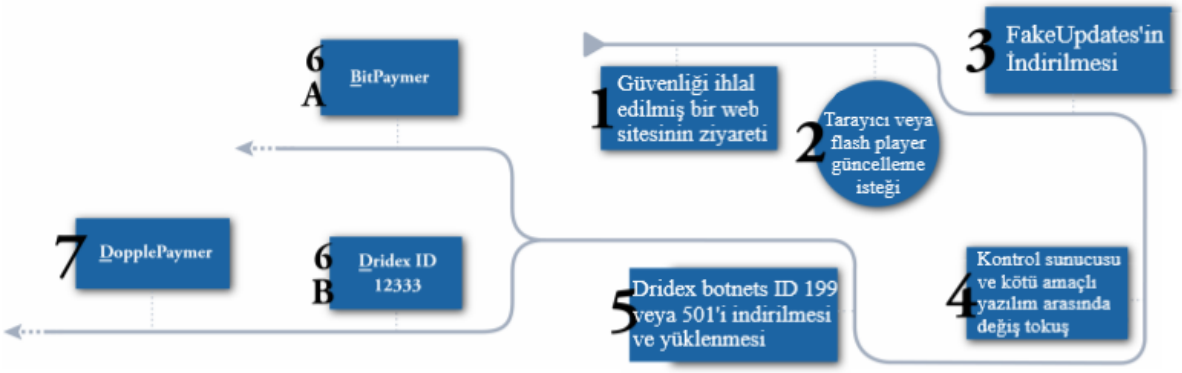
Dridex'in BitPaymer ve FakeUpdates Üzerindeki Etkisi

BitPaymer yazılımı, Dridex aracılığıyla sisteme girmektedir.

BitPaymer (FriedEx), Temmuz 2017'de fidye yazılımı olarak keşfedilmiştir. Bu fidye yazılımı ikili dosyadır, yani dağıtılamaz veya kendi isteğiyle bir C2 sunucusuna (kontrol sunucusu) giriş yapılamaz. Operatörleri bu nedenle manuel olarak yürütür.

Bitpaymer'ın Dridex'i içeren enfeksiyon zinciri

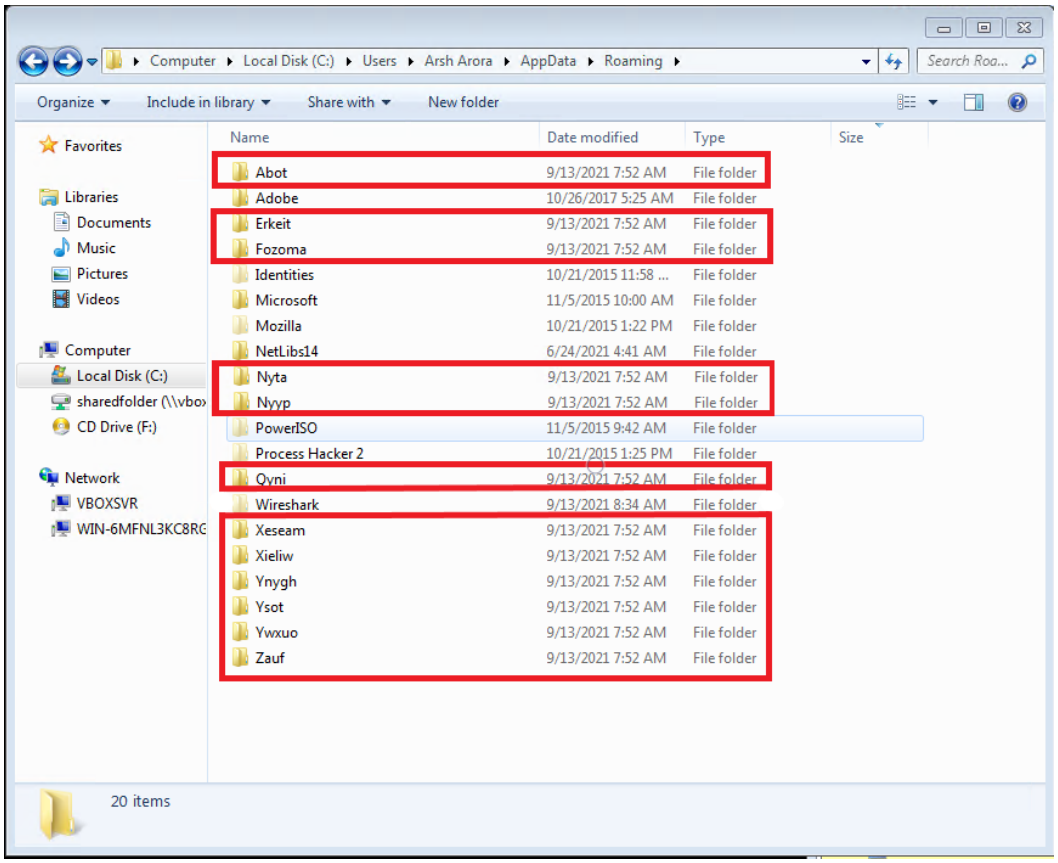
2019'dan beri Dridex v4 botnet'lerinin (ID 199 ve 501'in), FakeUpdates (takma adı SocGholish) aracılığıyla dağıtıldığı düşünülmektedir. Watering Hole (Sulama deliği) saldırıları veya kötü amaçlı bir URL'ye işaret eden kimlik avı e-postaları, FakeUpdates'in yükleneceği yanlış bir tarayıcı güncellemesinin görüntülenmesini ardından sisteme Dridex ve BitPaymer veya DoppelPaymer'in yayılmasını getirmektedir.

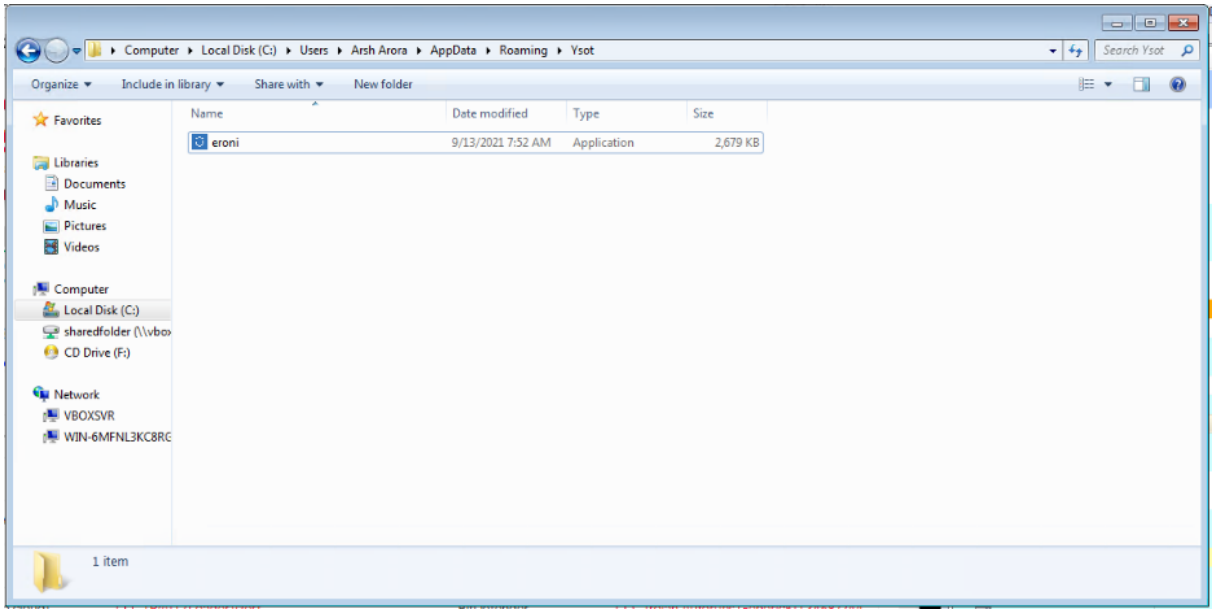


FakeUpdates aracılığıyla Dridex enfeksiyon zinciri

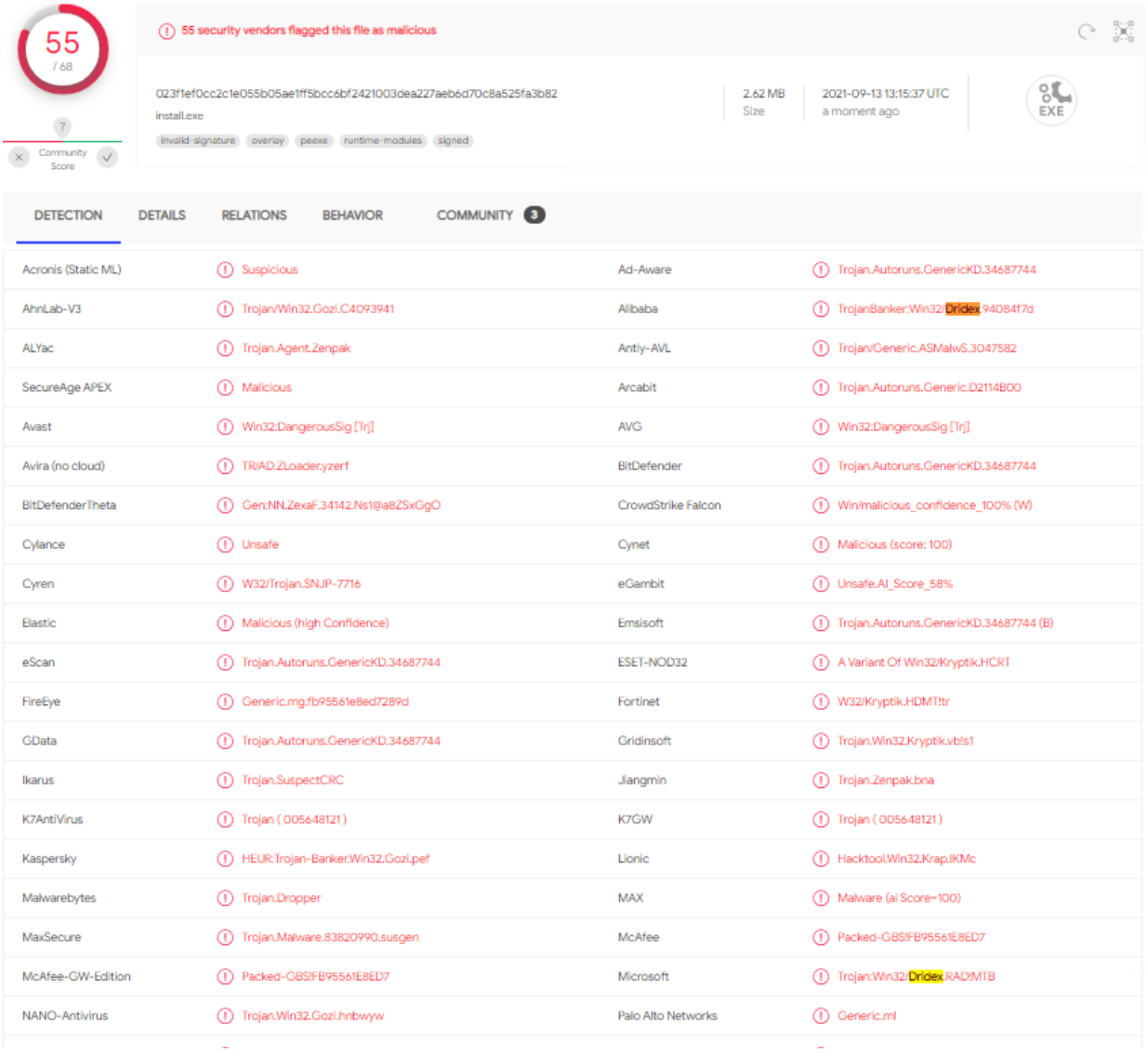
Dridex Analizleri

Dridex virüsünün çalıştırıldıktan sonra C:\Users\Arsh Arora\AppData\Roaming dizinine oluşturulan klasörler ve bu klasörlerin arasında "Ysot" isimli klasöre indirilen dosya aşağıda görülmektedir.





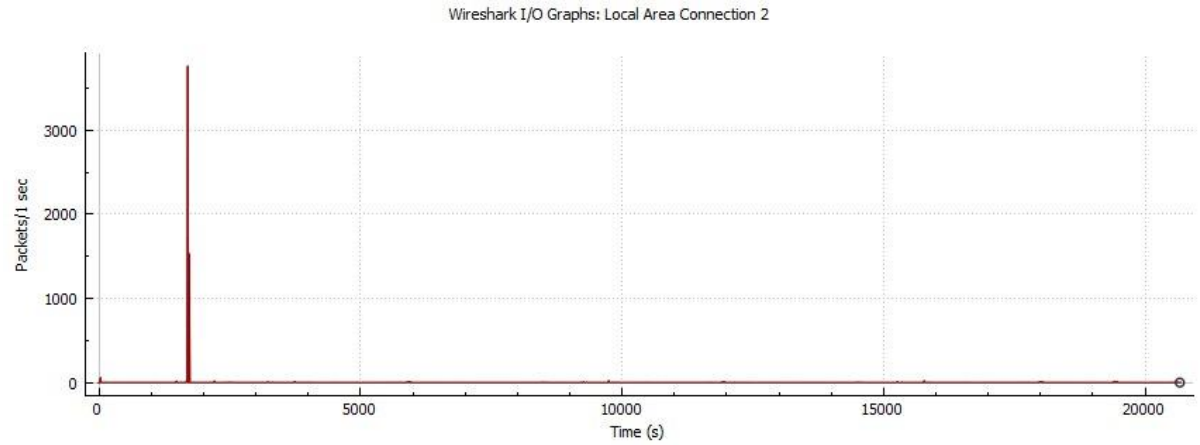
Dridex virüsünün indirdiği dosyanın VirusTotal üzerindeki analiz sonuçları aşağıdaki şekilde gösterilmiştir.



Dridex virüsünün çalışmadan önceki temiz ağ trafiği aşağıdaki grafikde verilmiştir.

= All Packets

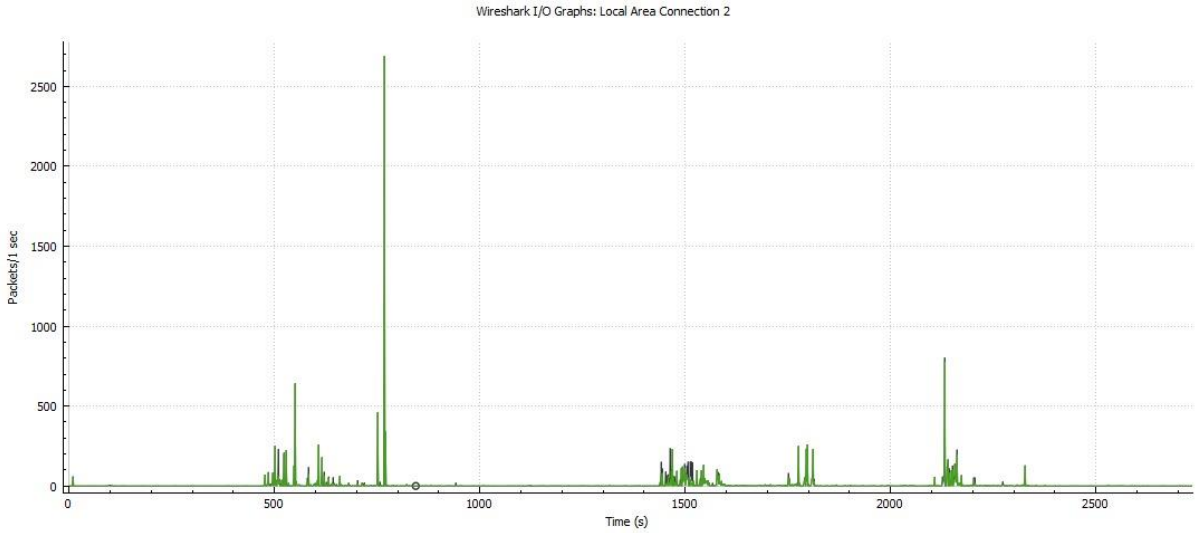
= TCP



Dridex virüsünün çalıştıktan sonraki oluşan ağ trafiği aşağıdaki grafikde verilmiştir.

= All Packets

= TCP



ICEDID

14 Kasım 2017'de IBM X-Force araştırması, IcedID adlı bir bankacılık Truva Atı'nın Emotet Truva Atı'nın yardımıyla yayıldığını ve bankalarla birlikte finans sektöründe kullanılan sistemleri de hedef aldığını tespit etmiştir.

IcedID, kullanıcının finansal bilgilerini hedefleyen ve diğer kötü amaçlı yazılımlar için bir damlalık görevi görebilen modüler bir bankacılık truva atıdır. Yani kendi spamlarına ek olarak, başta Emotet olmak üzere diğer kötü amaçlı yazılımlardan ikincil bir yük olarak bırakılır.

Çevrimiçi bankacılık oturumları için oturum açma kimlik bilgileri de dahil olmak üzere finansal bilgileri çalmak için tarayıcıdaki adam saldırısını kullanır. İlk saldırısını başarıyla tamamladıktan sonra, çalınan bilgileri banka hesaplarını ele geçirmek ve dolandırıcılık işlemlerini otomatikleştirmek için kullanmaktadır.

IcedID, kendisini işletim sistemi belleğine ve normal işlemlere enjekte etmek gibi virüsten koruma ve diğer kötü amaçlı yazılım algılama yöntemlerinden kaçınmak için birden çok enjeksiyon yöntemi kullanır.

Bunun yanında virüs, bankaları, ödeme kartı sağlayıcılarını, cep telefonu servis sağlayıcılarını, web postalarını, e-ticaret web sitelerini hedef almaktadır.

IcedID Enfeksiyon Süreci

İlk enfeksiyonun ardından, IcedID antivirüsü sisteme bulaşır ve süreç içi boş bırakma (İlk başta aktiflik sağlamıyor) yoluyla kalıcılık sağlar.

IcedID, çeşitli Uygulama Programlama Arabirimi (API) işlevlerini bağlar ("ntdll!ZwCreateUserProcess" ve "ntdll!RtlExitUserProcess" gibi).

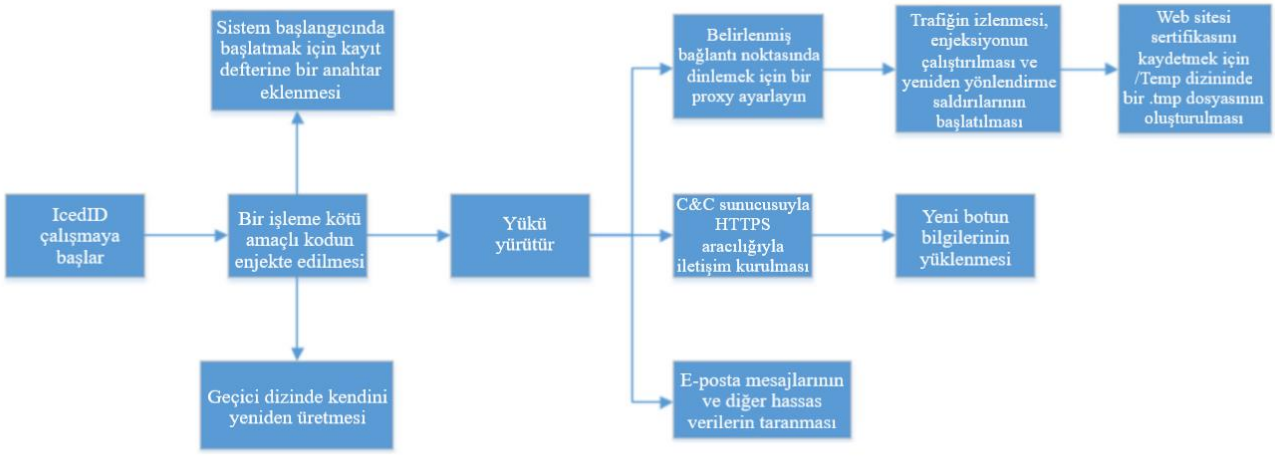
Çalıştırıldıktan sonra takma kodunu kaldırır ve "svchost.exe" adlı bir hizmet ana bilgisayar işlemi oluşturur. Bu işlem, IcedID'nin kendisini "KERNEL32.DLL" ve "SHLWAPI.DLL" olmak üzere iki Dinamik Bağlantı Kitaplığına (DLL) yazmasına olanak tanır.

"svchost.exe" oluşturulduktan sonra, kurbanın hesap ayrıcalıklarına bağlı olarak yükü "%ProgramData%" veya "%AppData%" klasörüne yazar.

Ek olarak, sistem her yeniden başlatıldığında kötü amaçlı yazılımın ikili dosyasını yürütmesine izin veren zamanlanmış bir görev oluşturulur.

Son olarak, kabuk kodunu tutmak için üç ek "svchost.exe" alt işlemi oluşturur.

IcedID, daha sonra ana modülünü başlatmadan önce sistemin yeniden başlatılmasını bekler. Bu adımlar, IcedID'nin kötü niyetli işlemlerinin başarıyla çalışmasını ve sistem her yeniden başlatıldığında işletim sistemi üzerinde meşru işlemler gibi görünmesini sağlar.



IcedID Üzerinde Tarayıcıdaki Adam Saldırısı

IcedID, ağ genelinde yayılma yeteneğine sahip olup, virüslü sistemdeki tüm etkinlikleri izlemesine, verileri sızdırmasına ve tarayıcıda adam saldırısı gerçekleştirmesine olanak tanır.

Spesifik olarak, tarayıcıdaki adam saldırısı üç adımdan oluşur:

- Web-enjeksiyon
- Proxy Kurulumu
- Yeniden Yönlendirme

Web enjeksiyonu

IcedID, kullanıcının Firefox, Google Chrome veya Internet Explorer gibi bir web tarayıcısını açmasını bekler. Bir tarayıcı başlatıldığında, IcedID tarayıcının türünü tanımlar ve uygulamaya kabuk kodunu enjekte eder.

Algılama ve güvenlik uygulamalarından daha fazla kaçınmak için, hedef sürece bellek ayırır ve kabuk kodunu enjekte eder. Kabuk kodunun enjeksiyonundan sonra IcedID, tarayıcının koruma durumunu değiştiren bir yama uygular.

Bu tarayıcı enjeksiyon işlemi, başka bir tarayıcı uygulaması açıldığında sürekli olarak tekrarlanır. Web enjeksiyon saldırısı, kurbanın etkinliğinin görünmesine, tarayıcının davranışına müdahale edilmesine ve ilişkili bilgilerin toplanmasına olanak tanır.

Proxy kurulumu

IcedID'nin tarayıcı işlevlerinden bir diğeri ise trafiği bir IcedID proxy sunucusuna yönlendirir.

Proxy sunucusu yeniden yönlendirmesi, ek bir "svchost.exe" oluşturularak ayarlanır. Ek "svchost.exe", IP adresini yeni bir bağlantı noktası numarasıyla ayarlamak için talimatlar oluşturmak için kullanılır.

Proxy sunucusu daha sonra tüm tarama trafiğini almaya başlar. Bu proxy, oturum açma kimlik bilgileri, bankacılık bilgileri ve ödeme kartı ayrıntıları gibi belirli bilgileri tanımlamak için tarama trafiğini izlemek için kurulmuştur.

Tanımlama üzerine, bu veriler kurbanın ağından saldırganın Komuta ve Kontrol (C2) sunucusuna aktarılır.

Bir proxy kurulduktan sonra, trafiği izler ve trafiği yeniden yönlendirmeye hazırlanmaya başlar.

Yeniden yönlendirme

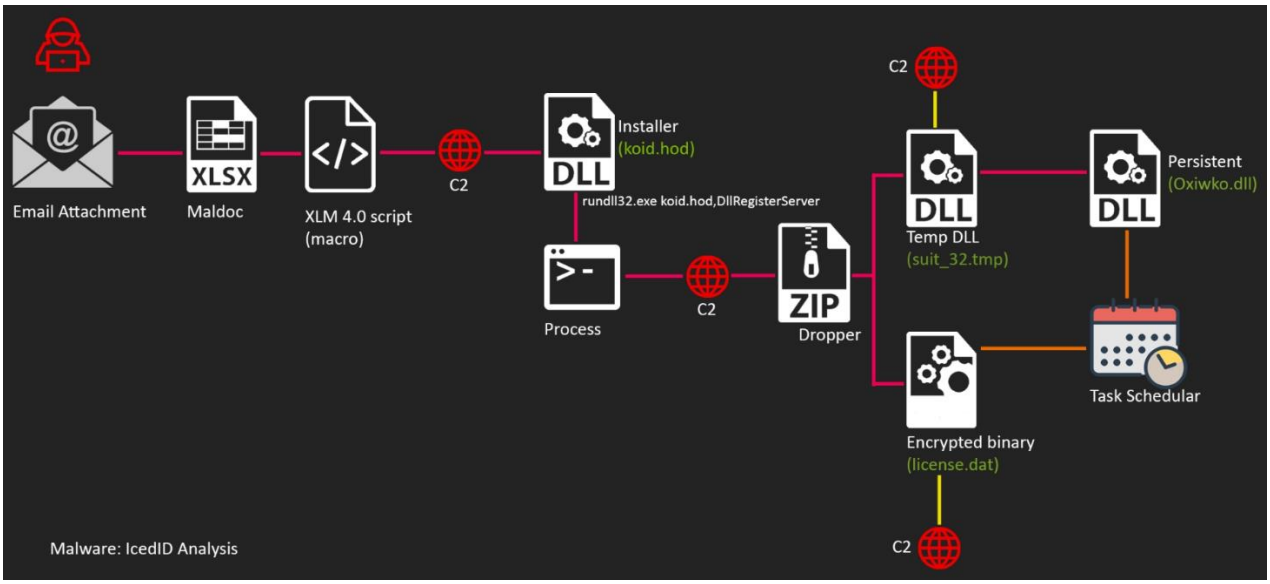
Tüm kullanıcı trafiği proxy'de durdurulur. Proxy, kurbanı, daha sonra oturum açma kimlik bilgilerini ve ilgili bilgileri gerçek web sitesine ileten yansıtılmış web sitelerine yönlendirir.

Bu yöntemi kullanarak IcedID, çok faktörlü kimlik doğrulamayı (MFA) başarıyla atlatır. Örneğin, bir kurban bir e-postadan veya kısa mesajdan kötü amaçlı web sitesine MFA kodunu girdiğinde, hemen yakalanır, yönlendirilir ve gerçek bankacılık oturum açma sayfasında kullanılır.

IcedID Komuta ve Kontrol İletişimi

IcedID komuta ve kontrol sunucusuyla, proxy'si aracılığıyla Güvenli Köprü Metni Aktarım Protokolü (HTTPS) kullanarak iletişim kurar. Dosyaları virüslü istemciye indirir ve ayrıca bilgileri kontrol ve komuta sunucusuna geri sızdırır.

Etkilenen sistemden C2 sunucusuna giden trafik, diğer sızan verilerle birlikte virüslü ana bilgisayar hakkında istemci kimlikleri içerir. Bu kimlikler, IcedID yazılım operatörünün kötü amaçlı yazılımın bulaşma aşamasını belirlemesine yardımcı olan bir bot, proje veya kampanya kimliği aracılığıyla bireysel istemciyi tanımlamak için kullanılmaktadır.



IcedID Gizleme ve Şifreleme

IcedID üzerinde kod analizini zorlaştırmak için farklı gizleme yöntemleri kullanılmaktadır.

DAT dosyaları, gerektiğinde şifre çözme ile birlikte hareketsiz halde şifrelenir. Şifreleme anahtarını oluşturmak için benzersiz istemci kimliği ve belirli dosya kimlikleri kullanılmaktadır.

İkinci olarak, IcedID, önemli dizeleri bir kayan anahtar algoritması aracılığıyla bir XOR şifresiyle kodlamak için dize gizlemeyi kullanmaktadır.

Ek olarak, komuta ve kontrol sunucusunun URL'lerinin güncellenmesi gerektiğinde imza doğrulamasını kullanır.

Son olarak, kötü amaçlı yazılım polimorfiktir, bu da algılamayı ve analizi daha zor hale getirir. Kötü amaçlı yazılımın ".text" bölümünün ikili kodu, sisteme her yüklendiğinde değiştirilir.

Değişiklikten sonra sanal boyut güncellenir ve doğrulama için yeni bir sağlama toplamı oluşturulur.

IcedID Ağ Yayılımı

X-Force araştırmacılarına göre IcedID, güvenlik açıklarından ziyade Emotet Truva Atı yardımıyla yayılmaktadır. Yani Emotet, IcedID'yi enfeksiyon için kurban ana bilgisayarına yeni bir yük olarak indirir.

IcedID, yaygın Truva atı işlevlerinin dışında, kendisini ağlar arasında da yayabilir. Yukarıda da belirtildiği üzere, sistemde Emotet varsa Emotet'in mevcut ağ erişiminden yararlanacaktır.

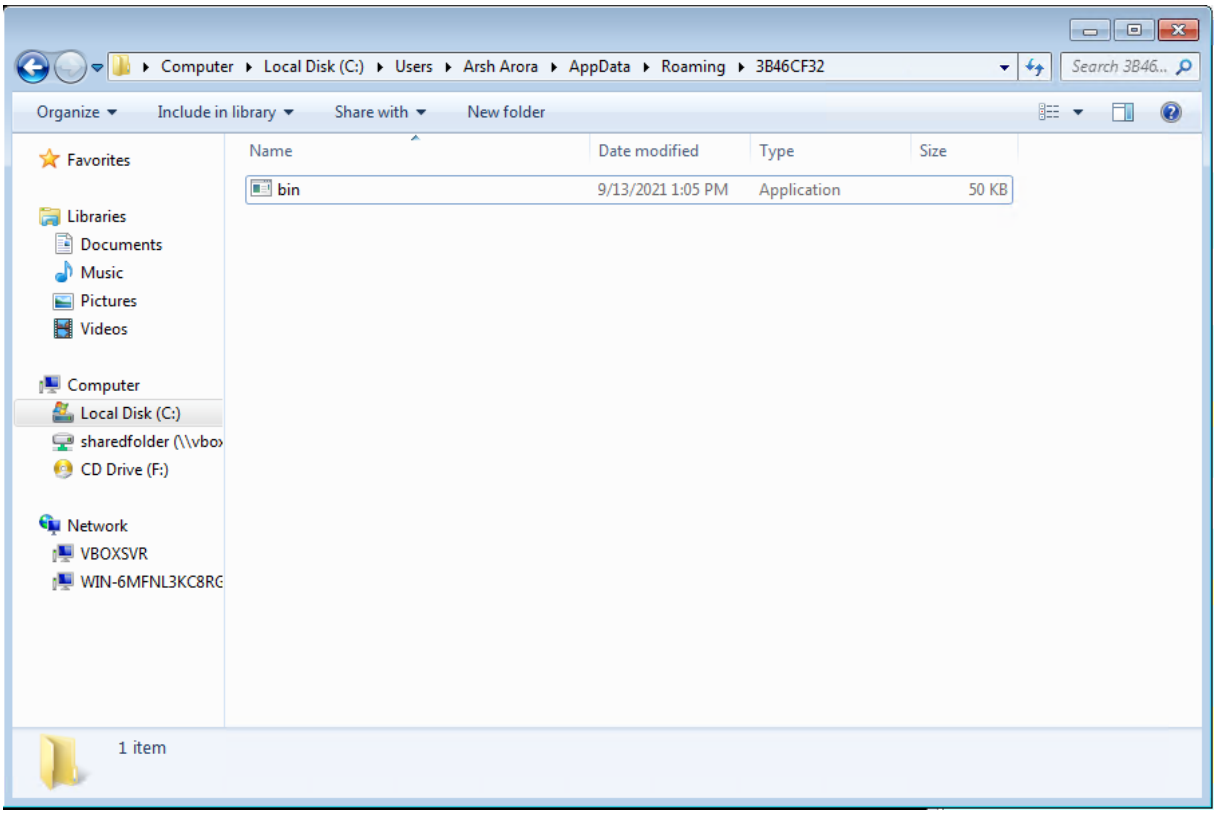
IcedID, Basit Dizin Erişim Protokolü'nü (LDAP) sorgulayarak bulduğu kullanıcı hesaplarına karşı bir kaba kuvvet sözlüğü saldırısı kullanarak bir ağ boyunca yayılmaya çalışır.

Yerel bir proxy kurarak kurbanın çevrimiçi etkinliklerini izler. Saldırı araçları, Dridex ve TrickBot tarafından kullanılan şemaya benzer web sitesi enjeksiyonlarını ve karmaşık yönlendirmeleri içermektedir.

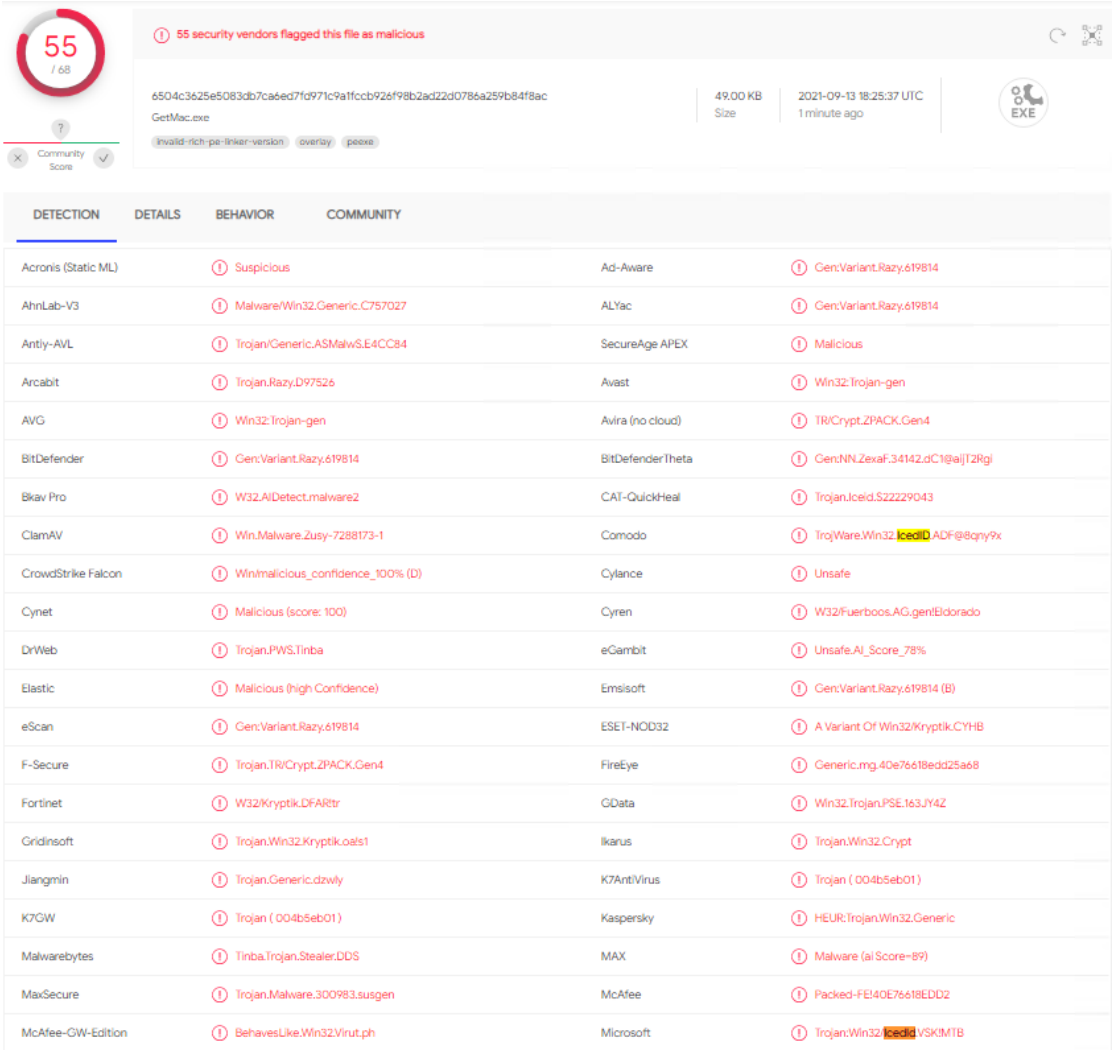
Bu yöntemleri kullanarak, orijinal ana bilgisayardan diğer uç noktalara ve terminal sunucularına geçmeyi amaçlar. Bu sunucular, iş istasyonları, yazıcılar ve diğer paylaşılan ağ cihazları gibi çeşitli uç noktalara hizmet vermektedir.

IcedID Analizleri

IcedID virüsünün çalıştırıldıktan sonra C:\Users\Arsh Arora\AppData\Roaming dizinine oluşturulan klasör "3B46CF32" ve bu klasöre indirilen dosya aşağıda görülmektedir.



IcedID virüsünün indirdiği dosyanın VirusTotal üzerindeki analiz sonuçları aşağıdaki şekilde gösterilmiştir.



55 / 68

55 security vendors flagged this file as malicious

6504c3625e5083db7ca6ed7fd971c9a1fccb926f98b2ad22d0786a259b84f8ac
GetMac.exe
invalid-rich-pe-linker-version overlay peexe

49.00 KB Size
2021-09-13 18:25:37 UTC 1 minute ago
EXE

Community Score

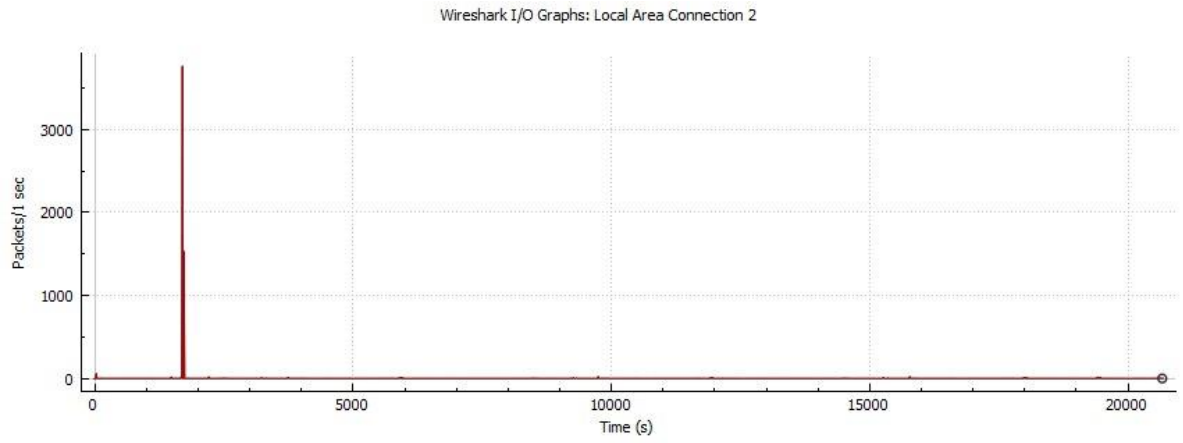
DETECTION DETAILS BEHAVIOR COMMUNITY

Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Variant.Razy.619814
AhnLab-V3	Malware/Win32.Generic.C757027	ALYac	Gen:Variant.Razy.619814
Antiy-AVL	Trojan/Generic.ASMalwS.E4CC84	SecureAge APEX	Malicious
Arcabit	Trojan.Razy.D97526	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	TR/Crypt.ZPACK.Gen4
BitDefender	Gen:Variant.Razy.619814	BitDefenderTheta	Gen:NN.ZexaF.34142.dC1@aijT2Rgi
Bkav Pro	W32.AIDetect.malware2	CAT-QuickHeal	Trojan.Iceid.S22229043
ClamAV	Win.Malware.Zusy-7288173-1	Comodo	TrojWare.Win32.IcedID.ADF@8qny9x
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Fuerboos.AG.gen!Eldorado
DrWeb	Trojan.PWS.Tinba	eGambit	Unsafe.AI_Score_78%
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Razy.619814 (B)
eScan	Gen:Variant.Razy.619814	ESET-NOD32	A Variant Of Win32/Kryptik.CYHB
F-Secure	Trojan.TR/Crypt.ZPACK.Gen4	FireEye	Generic.mg.40e76618edd25a68
Fortinet	W32/Kryptik.DFAR!tr	GData	Win32.Trojan.PSE.163JY4Z
Gridinsoft	Trojan.Win32.Kryptik.oa!s1	Ikarus	Trojan.Win32.Crypt
Jiangmin	Trojan.Generic.dzwly	K7AntiVirus	Trojan (004b5eb01)
K7GW	Trojan (004b5eb01)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Tinba.Trojan.Stealer.DDS	MAX	Malware (ai Score=89)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Packed-FE!40E76618EDD2
McAfee-GW-Edition	BehavesLike.Win32.Virut.ph	Microsoft	Trojan:Win32/Icedid.VSK!MTB

IcedID virüsünün çalışmadan önceki temiz ağ trafiği aşağıdaki grafikde verilmiştir.

= All Packets

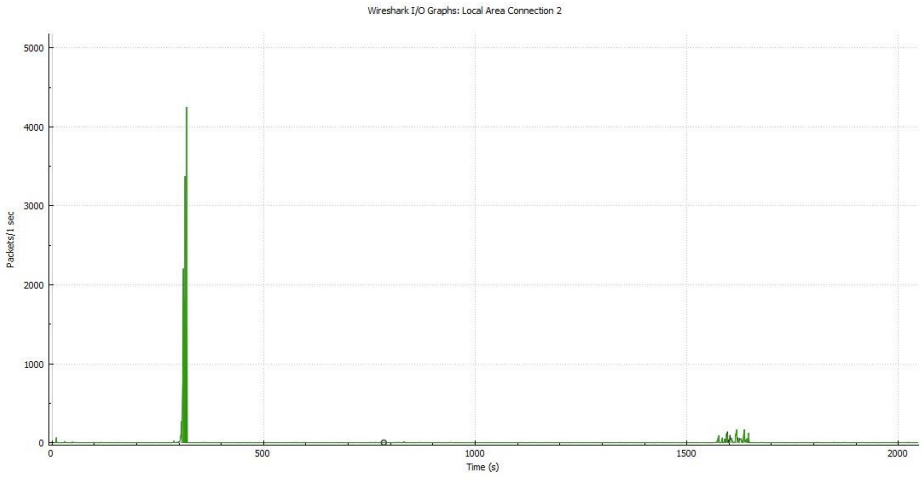
= TCP



IcedID virüsünün çalıştıktan sonraki oluşan ağ trafiği aşağıdaki grafikde verilmiştir.

= All Packets

= TCP



ZEUS

Zeus veya diğer bir adıyla Zbot, var olan Truva atları arasında en eski ve en yaygın olarak kullanılan yazılımlardan birisidir. Kullanıcıların çevrimiçi bankacılık kimlik bilgilerini çalmak için tasarlanmış bir suç yazılımı kitidir. Öncelikle finansal veri hırsızlığını hedef alır.

Kit tarafından oluşturulan botlar, güvenliği ihlal edilmiş bilgisayarlarda arka planda sessizce çalışarak, bilgileri toplar ve Truva atının sahibine geri göndermekle görevlidirler.

Ana odak noktası, çevrimiçi bankacılık ayrıntılarını ve diğer oturum açma kimlik bilgilerini çalmaktır ancak farklı veri hırsızlığı türleri de mevcuttur.

Zeus kitinin kullanımı çok basittir ve çok az teknik bilgi gerektirir. Sonuç olarak, hepsi kendi kontrolörlerine sahip, Zeus tarafından oluşturulmuş çok sayıda bağımsız botnet mevcuttur.

Geçmişten Günümüze Zeus

Zeus'un genel amacı ilk ortaya çıktığından beri aynı kalsa da, bu amaca nasıl ulaştığı konusunda yol boyunca birkaç gözle görülür değişiklik olmuştur.

En eski sürümler, hedef sistemde ilk çalıştırıldığında bot, yürütülebilir dosyasının verildiği tutarlı dosya adıyla ve veri dosyalarına verilen dosya adlarıyla dikkat çekiciydi.

- İlk örnekler, yürütülebilir dosyalar için aşağıdaki dosya adlarını kullanırdı:

ntos.exe, oembios.exe, twext.exe

Veri dosyaları aşağıdaki dizinlerde saklanırdı:

<System>\wsnpoem

<System>\sysproc64

<System>\twain_32

- Bir sonraki ana sürüm, yürütülebilir ad için ağırlıklı olarak “sdra64.exe”yi kullandı ve veri

dosyalarını “<System>\lowsec” içerisinde depolamıştır.

- Zeus’un günümüzdeki sürümü, rastgele bir dosya adıyla yürütülebilir dosyayı, yürüten kullanıcının

Uygulama Verileri klasöründe yeni oluşturulan, rastgele adlandırılmış bir klasörde saklamaya başlamıştır.

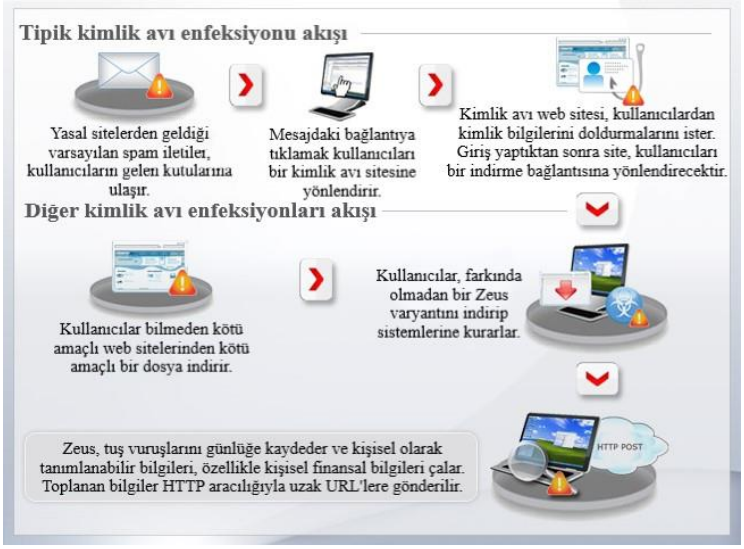
Zeus Nasıl Çalışır?

1. Doğrudan indirme veya kimlik avı yoluyla rastgele oluşturulmuş bir dosya adı kullanarak APPDATA klasörüne kendisinin bir kopyasını yazarak kullanıcıların makinesine bulaşır.
2. Zeus botnetine bağlanır.
3. Truva atının sahibi, sağlanan PHP ve SQL şablon dosyalarını kullanarak onu uzak bir konumdan kontrol eder.
4. Sahibinin truva atını nasıl özelleştirdiğine bağlı olarak banka hesap bilgilerini çalar.
5. Çalınan veriler aynı dizinde (APPDATA) şifreli olarak saklanır.
6. Zeus son olarak çalınan verileri komuta ve kontrol sunucusuna gönderdiğinde yerel kopyayı siler.

Bilgi toplamanın birincil kaynağı, tarayıcıdaki adam tuş vuruşu günlüğü ve form yakalamadır.

Kredi/banka kartı numaraları ve banka hesap bilgileri genellikle işe yarasa da, esas olarak giriş kimlik bilgilerini toplar.

Zeus Enfeksiyon Zinciri



Zeus Bileşenleri

Zeus botnet'in üç temel bileşeni vardır:

1. Zeus Truva Atı
2. Zeus yapılandırma dosyası (configuration)
3. Çalınan kimlik bilgilerinin gönderildiği Zeus bırakma bölgesi

Zeus botnet, ilk aşamada Truva Atı'nda birkaç teslimat yöntemi kullanır.

Zeus Truva Atı yürütüldükten sonra, önceden belirlenmiş bir konumdan yapılandırma dosyasını indirir ve kurbanın, genellikle bankaların seçimini, oturum açma URL'lerini ve benzerlerini içeren yapılandırma dosyasının tanımladığı belirli bir hedefe oturum açmasını bekler.

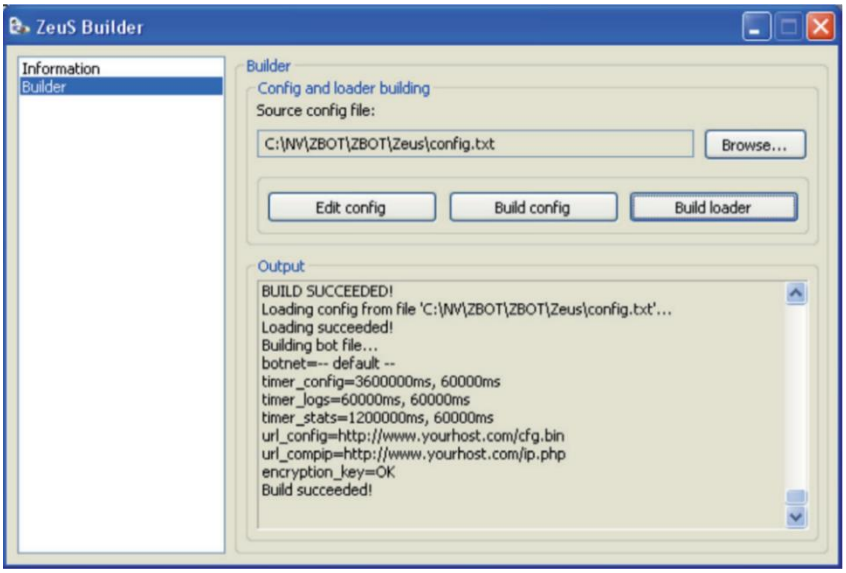
Geleneksel tuş kaydedicilerin aksine, Zeus Truva Atları, çevrimiçi bankacılık oturumu gibi bir tarayıcı oturumundan değişkenleri alan "tarayıcıdaki adam saldırları" aracılarıdır. Bu, Zeus'u özellikle tehlikeli hale getirir, çünkü yasal bir Web oturumuna ek form alanları enjekte etme yeteneğine de sahiptir.

The Builder(İnşaatçı)

ZeuS Builder, Zeus araç setinin en önemli parçalarından biridir. Botnet'i yapmak için kullanılan ikili dosyanın yanı sıra botnet'in tüm ayarlarını saklayan yapılandırma dosyasını oluşturmaktan sorumludur.

Tüm Zeus botnet'leri, çok yönlü bir yapılandırma dosyasına dayalı olarak oluşturulmuştur. Bu dosya, botnet'in adı, çalınan bilgileri ne sıklıkla geri göndereceği ve kötü amaçlı yazılımın bağlanması gereken sunucu gibi ayarları içerir. Ancak daha da önemlisi, Zeus'un hedefleyebileceği bankaların bir listesini içerir.

ZeuS, yalnızca kullanıcıların girdiği tüm bankacılık oturum açma kimlik bilgilerini ve şifrelerini toplamakla kalmaz, aynı zamanda daha önce bahsedildiği gibi kullanıcıların bankacılık web sitesi görünümüne doğrudan ek form bileşenleri enjekte etme yeteneğine de sahiptir.



Yapılandırma Dosyası

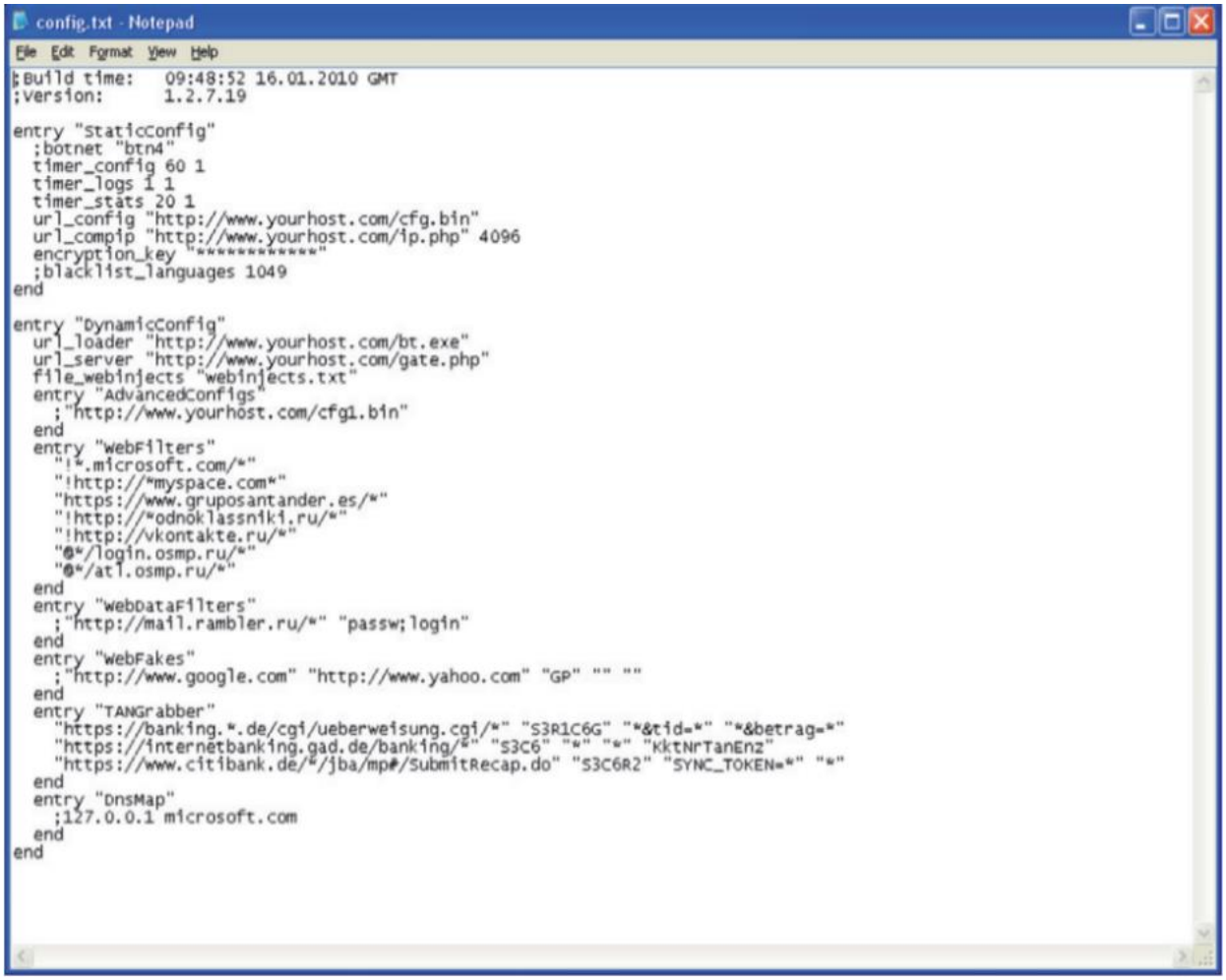
Bu dosya çalınan tüm verilerin gönderildiği adresi içerir. Yapılandırma dosyası alınamazsa, bot çalınan verileri nereye göndereceğini bilemez.

Dosyanın aldığı biçim, Zeus'un sunduğu çeşitli işlevleri etkinleştiren ve özelleştiren bir dizi bloktur.

İki ana “entry 'StaticConfig'” ve “entry 'DynamicConfig'” olmak üzere “giriş” ile başlayan bölümlere ayrılmıştır. Bu iki bölüm, ikili dosyaya sabit kodlanacak ayarlarla ve yapılandırma dosyasına yazılacak ve çalışma zamanında indirilecek ayarlarla ilgilenir.

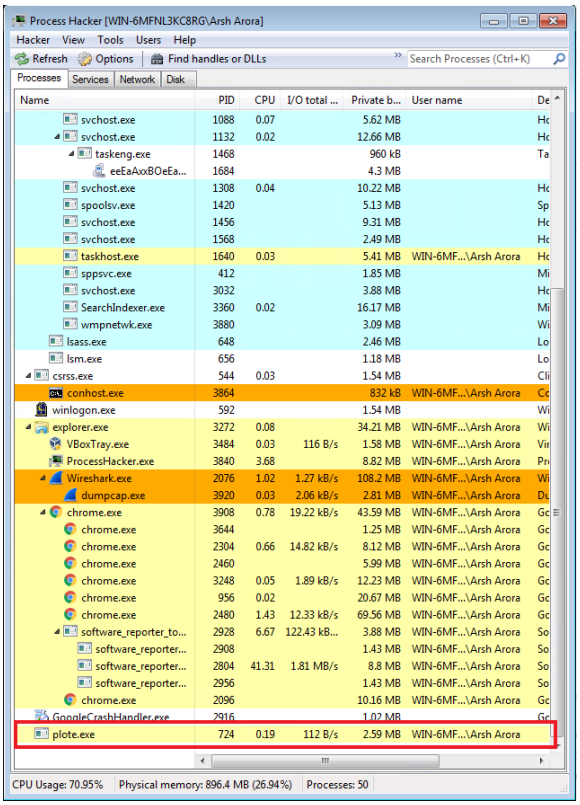
ZeuS Builder ve ZeuS Server, minimum teknik bilgiye sahip birinin bile çok kısa bir sürede tamamen işlevsel ve son derece profesyonel bir botnet yapılandırmasına ve kurmasına olanak tanıdığından, kötü amaçlı yazılım araç setini siber suçlar için fiili standart haline getirdi.

Zeus'un kullanım kolaylığı, en önemli satış noktasıdır.

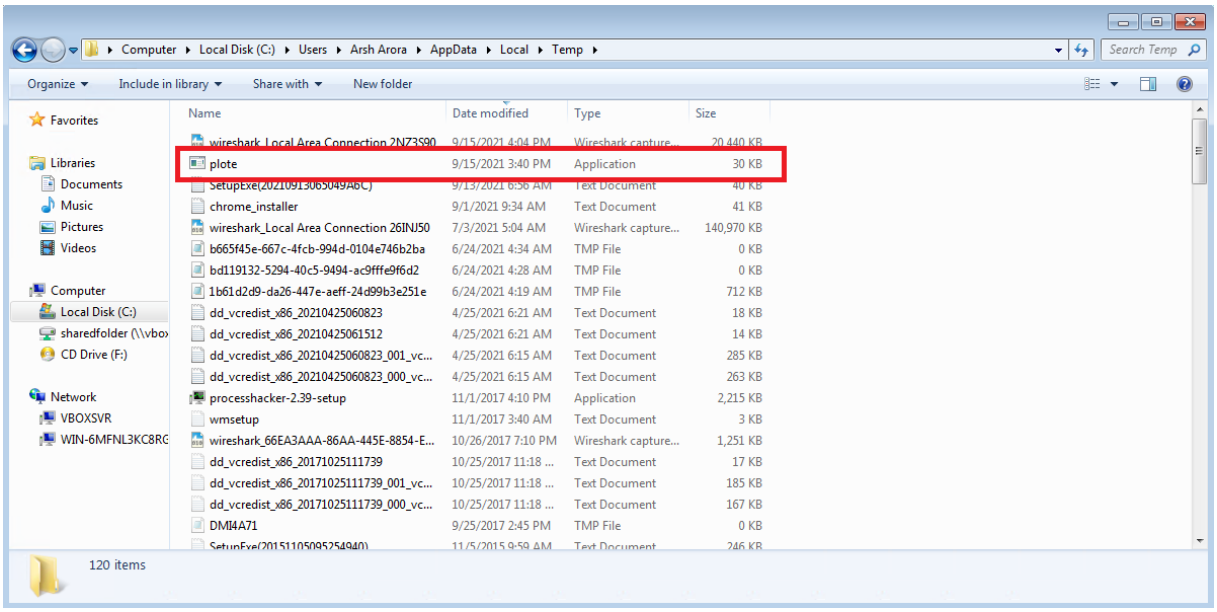


Zeus Analizleri

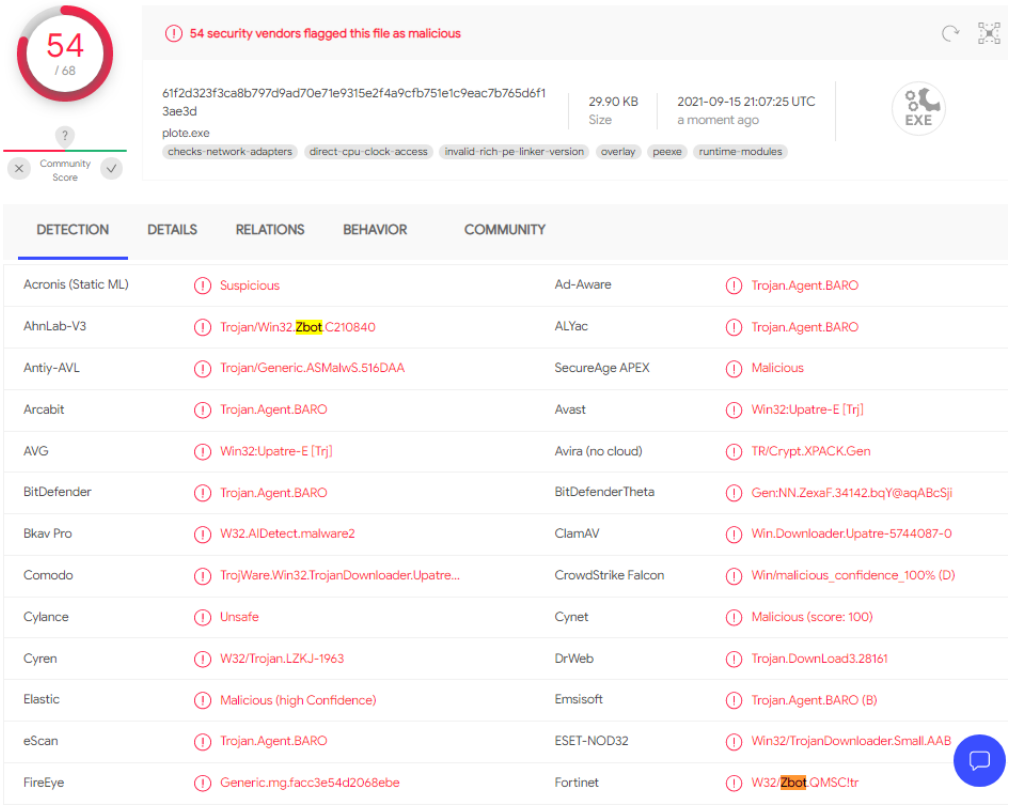
Zeus virüsünün çalıştırıldıktan sonra Process Hacker programı üzerinde aktif çalışan uygulamalar arasında ‟plote” isimli uygulama görülmektedir. Bu durum aşağıdaki şekilde gösterilmektedir.



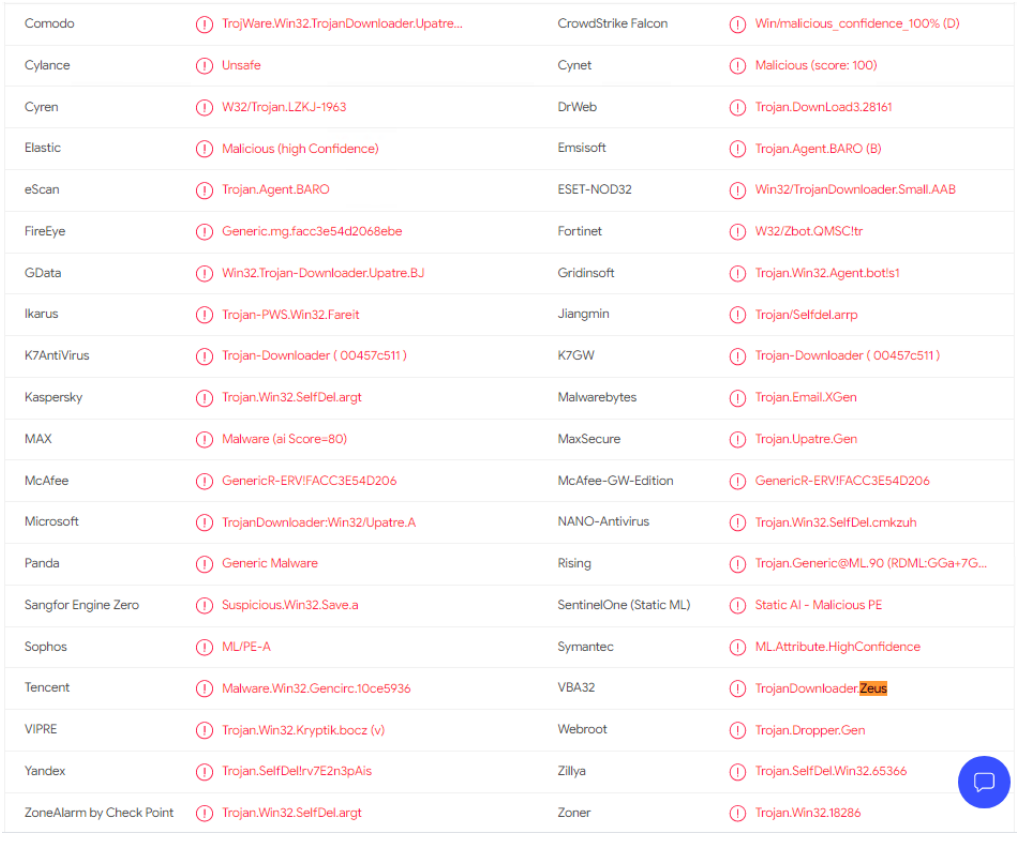
Zeus virüsünün çalıştırıldıktan sonra C:\Users\Arsh Arora\AppData\Local\Temp dizinine indirilen ‟plote” isimli dosya aşağıda görülmektedir.



Zeus virüsünün indirdiği dosyanın VirusTotal üzerindeki analiz sonuçları aşağıdaki şekilde gösterilmiştir. Virüs bu şekilde Zbot adıyla geçmektedir.



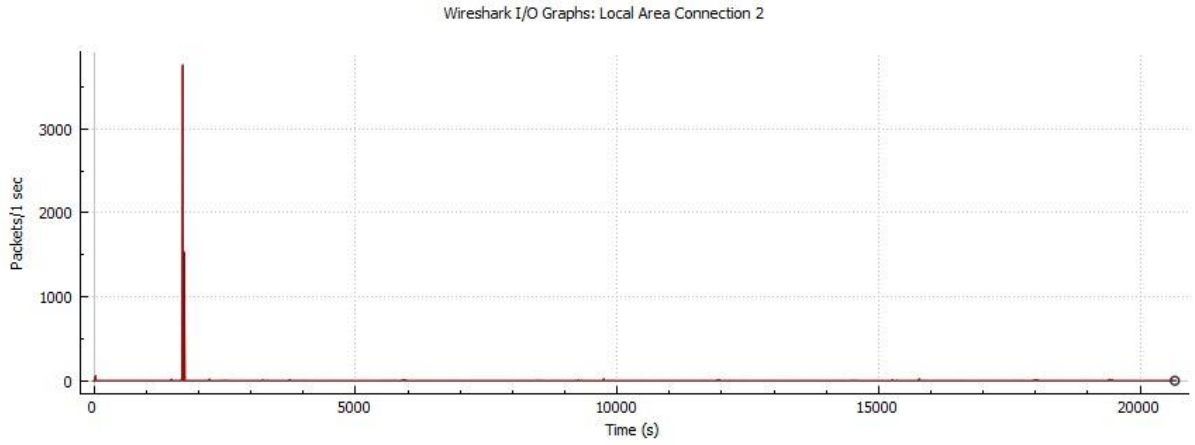
Zeus virüsünün indirdiği dosyanın VirusTotal üzerindeki analiz sonuçları aşağıdaki şekilde gösterilmiştir. Virüs burada Zeus adıyla geçmektedir.



Zeus virüsünün çalışmadan önceki temiz ağ trafiği aşağıdaki grafikte verilmiştir.

= All Packets

= TCP



Zeus virüsünün çalıştıktan sonraki oluşan ağ trafiği aşağıdaki grafikte verilmiştir.

= All Packets

= TCP