



APT31 TEKNİK ANALİZ RAPORU



@echocti



@echocti



echocti.com

İçindekiler

01

Yönetici Özeti

- Giriş
- Rapor İçeriği
- Raporun Önemi

02

APT31 Grup Profili

- APT31 Kimdir?
- Hedef Alınan Ülke ve Sektörler
- En Çok Karşılaşılan Saldırı Türleri Neler?

03

APT31 Grubuya İlişkilendirilen Siber Saldırılar

- İlişkilendirilen Siber Saldırılar ve Detaylar

04

Hedef Alınan Ülke ve Sektörler

- APT31'in Hedef Aldığı Ülkeler
- APT31'in Hedef Aldığı Sektörler

05

APT31 Tarafından Hedef Alınan Kurumlar

- APT31 Teknik Analizinden Kurumları Hedef Alan
Distributed Denial-of-Service Saldırıları

06

APT31 Grubuya İlişkilendirilen Siber Saldırılar

07

APT31'in Saldırı Taktiği

- APT31 Saldırı Zinciri
- Mitre Attack Tablosu
- IOC's

08

Siber Saldırılara Karşı Nasıl Önlemler Alınmalı?

Yönetici Özeti

APT31, Çin hükümeti tarafından desteklendiği düşünülen bir siber tehdit aktörüdür ve dünya çapında birçok ülkeye ve sektörde yönelik geniş çaplı siber casusluk operasyonları gerçekleştirmektedir. Bu grup, Zirconium ve Judgment Panda gibi isimlerle de bilinir ve özellikle hassas devlet bilgilerini, stratejik endüstriyel sırları ve yenilikçi teknolojileri ele geçirmeyi hedefler. APT31, gelişmiş kimlik avı saldıruları, tedarik zinciri saldırıları ve kötü amaçlı yazılım kullanımında uzmanlaşmıştır.

Bu raporda, APT31'in kimliği, hedef aldığı ülkeler ve sektörler, ilişkilendirilen kampanyalar, kullanılan saldırı yöntemleri ve IoC'ler kapsamlı bir şekilde ele alınmıştır. Grub, Amerika Birleşik Devletleri, Avrupa Birliği ve Asya-Pasifik bölgesindeki stratejik sektörlerde yönelik saldırular düzenleyerek, bu bölgelerdeki ekonomik ve ulusal güvenliği tehdit etmektedir.

APT31'in faaliyetleri, özellikle savunma sanayi, hükümet kurumları, teknoloji firmaları ve enerji sektöründe önemli hasarlar bırakmıştır. Grubun kullandığı zararlı yazılımlar ve teknikler, saldıruların tespit edilmesini zorlaştırarak, uzun süreli erişim ve veri sızdırma operasyonlarına imkan tanımaktadır. Ayrıca, APT31'in tedarik zinciri saldırılarında gösterdiği yetkinlik, onun siber casusluk operasyonlarındaki başarısını artırmaktadır.

Bu raporda sunulan Mitre ATT&CK tablosu, APT31'in kullandığı taktik ve teknikleri kapsamlı bir şekilde analiz etmektedir. Ayrıca, belirlenen IoC'ler, APT31'in siber saldırularına karşı alınacak önlemler ve savunma stratejileri için önemli bilgiler sunmaktadır. Bu rapor, güvenlik ekiplerine, APT31'e karşı daha etkili güvenlik tedbirleri almaları için gerekli olan bilgileri sağlamayı amaçlamaktadır.

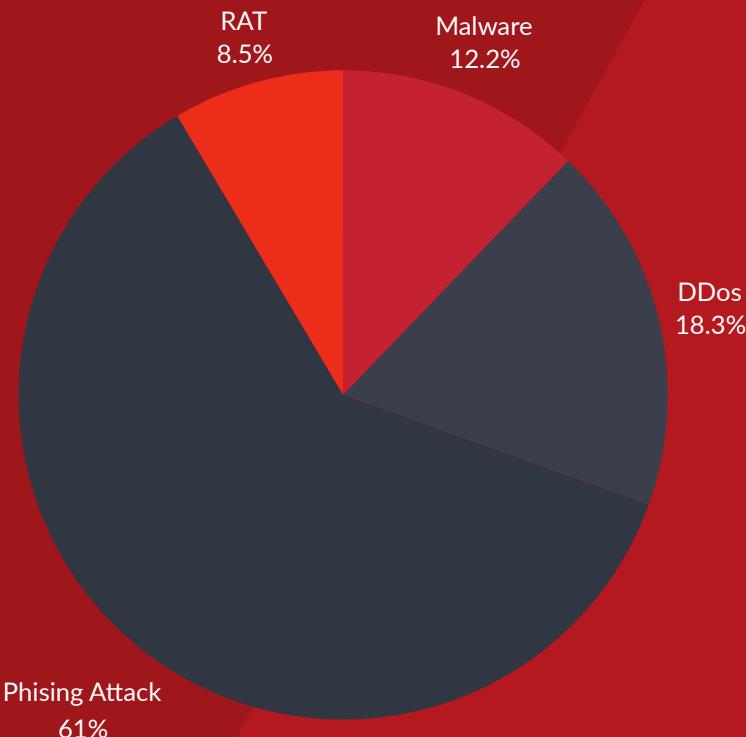
Sonuç olarak, APT31'in faaliyetleri, sadece hedef alınan ülkeler için değil, aynı zamanda küresel siber güvenlik için de ciddi bir tehdit oluşturmaktadır. Bu raporda sunulan bulgular ve öneriler, bu tehdide karşı alınacak önlemler konusunda rehberlik etmektedir.

Grup Profili

Bu bölümde, APT31'in genel profili, kim olduğu, hedef aldığı ülkeler ve sektörler hakkında detaylı bilgi verilmektedir.

APT31 Kimdir?

APT31, Çin merkezli bir devlet destekli tehdit aktörü olarak bilinmektedir. Grubun ana faaliyetleri arasında siber casusluk ve istihbarat toplama yer almaktadır. APT31, hükümetler, askeri kuruluşlar ve stratejik sektörlerde faaliyet gösteren kurumlara yönelik uzun vadeli saldırılar düzenlemektedir. Zirconium ve Judgment Panda gibi diğer isimlerle de bilinen bu grup, gelişmiş teknikler kullanarak sizdiği sistemlerde kalıcılık sağlamayı amaçlamaktadır. Bu tehdit aktörü, özellikle hassas bilgilere erişim ve endüstriyel sırları çalmak için gelişmiş kimlik avı teknikleri, kötü amaçlı yazılımlar ve tedarik zinciri saldırıları kullanılmaktadır.



APT31, Çin hükümeti adına istihbarat toplama görevi olan bir Gelişmiş Sürekli Tehdit grubudur. Diğer ulus-devlet aktörlerine benzer şekilde, grup belirli dikeyler yerine Çin Halk Cumhuriyeti ve onun stratejik ve jeopolitik hırsları için ilgi çekici verilere odaklanmaktadır. Çinli rakipler dünyadaki en üretken devlet destekli siber aktörlerden bazıları olarak kabul ediliyor.

Hedef Alınan Ülke ve Sektörler



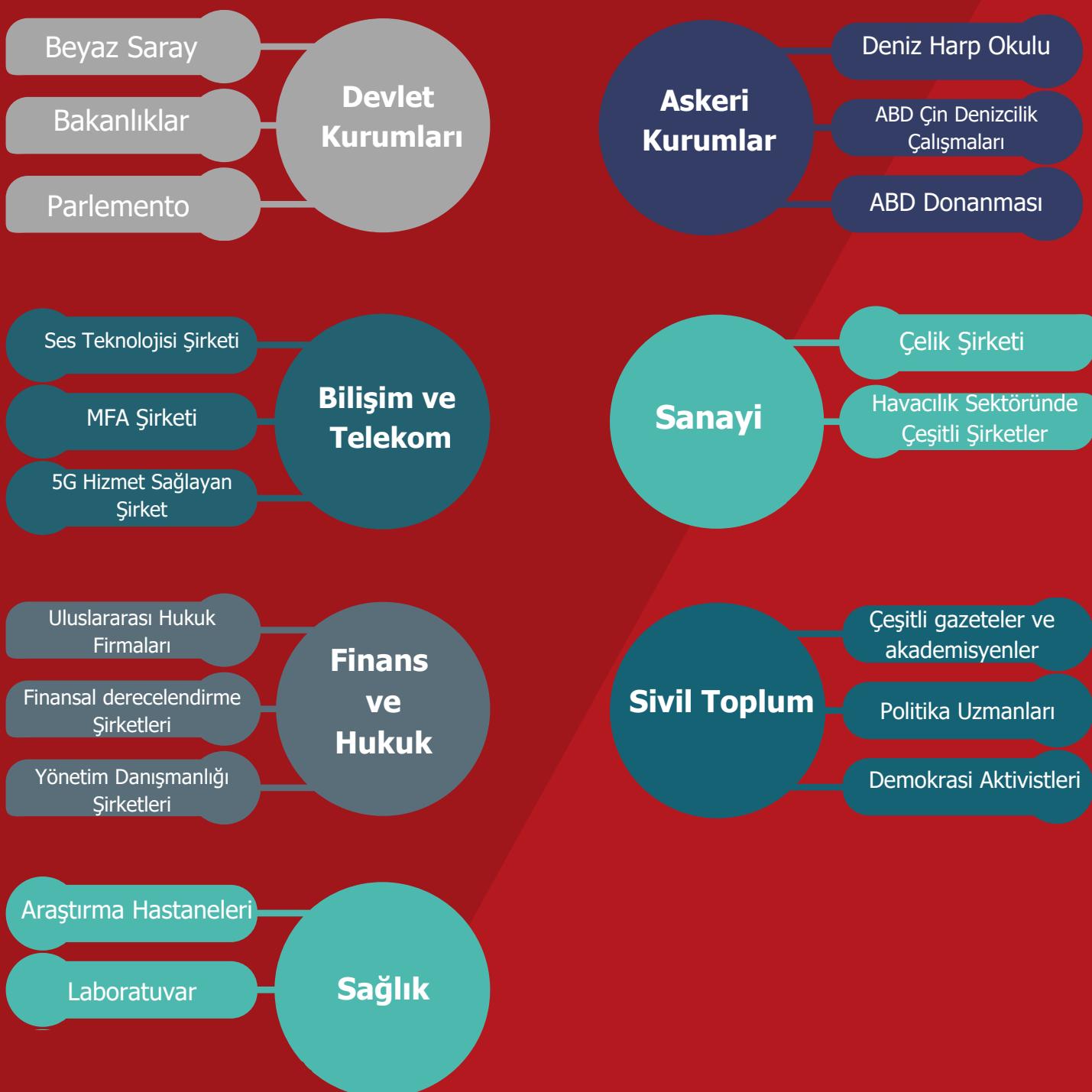
APT31'in Hedef Aldığı Ülkeler:

1. Amerika Birleşik Devletleri
2. Avrupa Birliği ülkeleri (özellikle Fransa, Almanya, Birleşik Krallık, Finlandiya)
3. Asya-Pasifik bölgesi ülkeleri (Japonya, Güney Kore, Hindistan)
4. Avustralya olmak üzere dünya genelinde birçok ülkeyi hedef almaktadır.

APT31'in Hedef Aldığı Sektörler:

1. Savunma ve Havacılık: Askeri teknoloji, araştırma ve geliştirme faaliyetleri.
2. Hükümet Kurumları: Diplomatik ve ulusal güvenlik ile ilgili bilgiler.
3. Teknoloji ve Telekomünikasyon: Yenilikçi teknolojiler, iletişim ağları.
4. Enerji ve Altyapı: Stratejik enerji verileri ve kritik altyapılar.
5. Sağlık Sektörü: Biyoteknoloji ve ilaç araştırmaları.

APT31 Tarafından Hedef Alınan Kurumlar



APT31 Grubuya İlişkilendirilen Siber Saldırılar

- Mart 2021'de Finlandiya parlamentosuna düzenlenen saldırı Çin bağlantılı APT31 grubu ile ilişkilendirildi.
- Temmuz 2021'de APT31 siber casusluk grubu tarafından çok sayıda Fransız kuruluşuna yönelik devam eden saldırılar gerçekleştirildi.
- 2021 ve 2022 yıllarında İngiliz parlamenterlerin e-postalarını hedef aldı.
- Şubat 2022'de APT31 grubu ABD hükümetiyle bağlantılı Gmail kullanıcılarını hedef alan kimlik avı kampanyası gerçekleştirdi.
- Temmuz 2023'te Doğu Avrupa'daki Hava Boşluğu Sistemlere Yapılan Saldırılar APT31 Grubuya ilişkilendirildi.
- Mart 2024'te ABD'nin kritik altyapı sektörlerinde faaliyet gösteren ABD kuruluşlarını hedef aldı.
- Temmuz 2024'te Rusya'daki hükümet kuruluşlarına yönelik yeni CloudSorcerer saldırıları APT31 ile ilişkilendirildi.

Mart 2021'de Finlandiya parlamentosuna düzenlenen saldırı Çin bağlantılı APT31 grubu ile ilişkilendirildi



Mart 2021'de Finlandiya Parlamentosu'na düzenlenen siber saldırı, Finlandiya Polisi tarafından Çin bağlantılı APT31 grubuna atfedildi.

Finlandiya makamları, saldırıyla ilgili olarak ağır casusluk, bilgi sistemine yasadışı erişim ve iletişim gizliliğinin ihlali gibi bir dizi suçu araştırdı. Suçların 2020 sonbaharı ile 2021 başı arasında işlendiği belirtildi.

Polis, soruşturmanın erken aşamalarında Çin bağlantılı siber casusluk grubu APT31'in saldırıyla dahil olduğundan şüphelenmiş ve yapılan detaylı incelemeler sonrasında bu atılı doğrulamıştır. Ayrıca, polis yetkilileri bir şüpheliyi tespit ettilerini duyurmuştur.

Ulusal Soruşturma Bürosu'ndan Baş Dedektif Müfettiş Aku Limnell, bu uzun soluklu soruşturmanın, ulus-devlet aktörleri tarafından kullanılan karmaşık bir suç altyapısını ortaya çıkardığını açıklamıştır. Soruşturma sürecinde, Finlandiya Polis Teşkilatı uluslararası kuruluşlarla ve Finlandiya Güvenlik ve İstihbarat Servisi ile işbirliği yapmıştır.

Aynı dönemde ABD hükümeti, Çin bağlantılı APT31 grubunun üyeleri olduğu iddia edilen iki Çinli bilgisayar korsanına yönelik yaptırımlar duyurmuştur. Bu yaptırımlar, ABD'nin kritik altyapı sektörlerine yönelik kötü niyetli siber operasyonlar düzenleyen Zhao Guangzong ve Ni Gaobin adlı şahısları hedef almıştır. ABD Hazine Bakanlığı ayrıca, Çin Devlet Güvenlik Bakanlığı'nın ABD'nin kritik altyapı sektörlerine yönelik saldırılarda cephe olarak kullandığı Wuhan Xiaoruzhi Bilim ve Teknoloji Şirketi'ne (Wuhan XRZ) yaptırım uygulamıştır.

2021 ve 2022 Yıllarında İngiliz Parlmenterlerin e-postalarını hedef aldı

2021 yılında, Çin bağlantılı APT31 grubunun İngiliz parlmenterlerin e-posta hesaplarına yönelik bir siber saldırısından neredeyse kesin olarak sorumlu olduğu düşünülüyor. GCHQ Ulusal Siber Güvenlik Merkezi (NCSC) tarafından yapılan değerlendirmelerde, bu saldırıların özellikle Çin'in kötü niyetli faaliyetlerine dikkat çeken parlmenterleri hedef aldığı belirtilmiştir. Aynı dönemde, 2021 ve 2022 yılları arasında İngiltere Seçim Komisyonu'nun bilgisayar sistemlerinin tehlikeye atılması da Çin devletine bağlı bir aktöre atfedilmiştir. Bu saldırırlarda tehdit aktörlerinin, Seçim Komisyonu'ndan ve e-posta verilerinden önemli bilgileri ele geçirdiği ve bu bilgilerin Çin istihbarat servisleri tarafından casusluk faaliyetlerinde kullanılabileceği değerlendirilmiştir.



Şubat 2022'de APT31 grubu ABD Hükümetiyle bağlantılı Gmail kullanıcılarını hedef alan kimlik avı kampanyası gerçekleştirdi

Google, Çin bağlantılı siber casusluk grubu APT31 tarafından yürütülen bir kimlik avı kampanyasını engellediğini açıkladı. Bu kampanya, ABD hükümetiyle ilişkili Gmail kullanıcılarını hedef almıştır. Kimlik avı kampanyası Şubat ayında gerçekleşmiş olup, Google Tehdit Analizi Grubu tarafından tespit edilmiştir. Tehdit Analizi ekibi, kampanyanın Ukrayna'daki devam eden işgaliyle bağlantılı olmadığını belirtmiştir. Google TAG direktörü Shane Huntley, BT devinin tüm kimlik avı mesajlarını başarılı bir şekilde tespit edip engellediğini doğrulamıştır.



Temmuz 2023'te Doğu Avrupa'daki Hava Boşluklu Sistemlere Yapılan Saldırılar APT31 Grubuyla ilişkilendirildi

```
aCreateDir    db 'create dir',0Ah,0 ; DATA XREF: sub_452050+5A2To
aUploadHostInfo db 'upload host info',0Ah,0 ; DATA XREF: sub_452050+750To
align 4
aBeginExeccomma db 'begin execCommand',0Ah,0 ; DATA XREF: sub_452050+A82To
aSleeptimeD db 'sleepTime:$d',0Ah,0 ; DATA XREF: sub_452050+B85To
align 4
asc_627A48 db '/',0 ; DATA XREF: sub_452C30+78To
; .text:loc_45C9CfTo ...
aContent_0 db '/content/',0 ; DATA XREF: sub_452C30+110To
align 4
a1780 db '1780',0 ; DATA XREF: sub_452C30+102To
; sub_452C30+342To
align 10h
a1781 db '1781',0 ; DATA XREF: sub_452C30+20ETo
align 4
a1784 db '1784',0 ; DATA XREF: sub_452C30+3E0To
```

Doğu Avrupa'daki sanayi kuruluşlarına yönelik bir dizi siber saldırının arkasında, Çin bağlantılı bir grup olduğu düşünülüyor. Bu saldırılar, özellikle hava boşluklu sistemlerdeki verileri çalmak amacıyla geliştirilen karmaşık yöntemler içeriyordu.

Saldırılarda kullanılan kötü amaçlı yazılımlar üç ana kategoriye ayrıldı: Uzaktan kalıcı erişim sağlama, hassas bilgileri toplama ve toplanan verileri aktarma. Bu yazılımlar arasında, hava boşluklu sistemlerden veri sızdırma için taşınabilir sürücülerini enfekte eden modüler bir kötü amaçlı yazılım öne çıkıyor. Bu yazılım, taşınabilir sürücülerini profil çıkarma ve bu sürücüler aracılığıyla izole edilmiş ağlardan veri sızdırma yeteneğine sahip. Ayrıca, yerel bilgisayarlardan veri çalmak ve bu verileri bulut hizmetleri aracılığıyla aktarmak için kullanılan diğer türde kötü amaçlı yazılımlar da bu saldırılarda yer aldı.

Grup, saldırılarında farklı kötü amaçlı yazılım aileleri kullandı. Bu yazılımlar arasında, dosya yükleme ve indirme, komut çalıştırma, ters kabuk açma ve kendi izlerini silme gibi geniş bir yelpazede işlevler sunan yazılımlar bulunuyor. Ayrıca, uzaktan erişim ve ilk veri toplama için kullanılan yazılımlar, çalışan süreçleri listeleme, bağlı cihazları tanımlama, dosya işlemleri gerçekleştirme, ekran görüntülerini alma ve kendini güncelleme gibi yeteneklere sahip. Bulut hizmetlerinin komuta ve kontrol için kullanılması, bu tür hizmetlerin tehdit aktörleri tarafından giderek daha fazla suistimal edildiğini gösteriyor.

Grup, bu saldırılarında yalnızca Windows sistemlerini değil, aynı zamanda Linux sistemlerini de hedef aldı. Güney Kore'deki bazı şirketlere yönelik saldırılarında, basit yapısına rağmen, ağ paket algılamasından kaçınmak için şifreleme kullanan ve çeşitli kötü amaçlı işlevler gerçekleştiren bir arka kapı yazılımı kullanıldığı tespit edildi. Bu saldırılar, grubun hem Windows hem de Linux platformlarında karmaşık ve sofistik bir tehdit oluşturduğunu ortaya koyuyor.

Mart 2024'te ABD'nin kritik altyapı sektörlerinde faaliyet gösteren ABD kuruluşlarını hedef aldı



ABD Hazine Bakanlığı, APT31 grubunun ABD'nin kritik altyapı sektörlerine yönelik saldırılarda yer aldığı iddia edilen iki Çinli bilgisayar korsanına (Zhao Guangzong ve Ni Gaobin) yaptırım uygulayacağını duyurdu. Bu korsanların, Çin Devlet Güvenlik Bakanlığı ile bağlantılı olduğu ve Vuhan merkezli bir teknoloji şirketi olan Wuhan Xiaoruzhi Bilim ve Teknoloji Şirketi Limited'e ait paravan bir şirket aracılığıyla bu saldırıları gerçekleştirdikleri belirtilmiştir.

ABD Adalet Bakanlığı, APT31 grubunun iki üyesinin de aralarında bulunduğu yedi Çin vatandaşı hakkında, bilgisayarlara izinsiz girme ve elektronik dolandırıcılık yapma suçlamalarıyla iddianame düzenledi. Bu grup, yaklaşık 14 yıldır Çin'in ekonomik casusluk ve dış istihbarat hedefleri doğrultusunda ABD'de ve yurtdışında muhalifleri, şirketleri ve siyasi yetkilileri hedef almıştır.

APT31'in Çin Devlet Güvenlik Bakanlığı'nın bir parçası olarak yürütüdüğü siber casusluk programı, hem Çin içindeki hem de dışındaki siyasi muhalifleri, ABD'deki ve diğer yerlerdeki hükümet yetkililerini, adayları, kampanya personelini ve Amerikan şirketlerini hedef alıyor. Bu grup, binlerce birey ve şirketi hedef alan küresel bilgisayar korsanlığı kampanyaları yürütmüş ve hedeflerin ağlarına, e-posta hesaplarına ve telefon görüşmesi kayıtlarına uzun süreli erişim sağlamıştır.

EastWind kampanyası: Temmuz 2024'te Rusya'daki hükümet kuruluşlarına yönelik yeni CloudSorcerer saldırıları APT31 ile ilişkilendirildi



Temmuz 2024'ün sonlarında, Rus hükümet kuruluşları ve BT şirketlerine yönelik bir dizi devam eden hedefli siber saldırı tespit edildi. Bu saldırılar, zararlı kisayol ekleri içeren kimlik avi e-postaları aracılığıyla gerçekleştirildi. Saldırganlar, Dropbox bulut hizmetini kullanarak cihazlara komut gönderen kötü amaçlı yazılımlar yaydılar ve bu yazılımlar aracılığıyla ek yükler indirdiler. Bu saldırı kampanyası, EastWind olarak adlandırıldı ve saldırılarda APT31 grubu tarafından kullanılan araçlar ve güncellenmiş bir CloudSorcerer arka kapısı tespit edildi.

Saldırılarda kullanılan zararlı yazılımlar, özellikle APT31 grubu ile ilişkilendirilmiştir. EastWind kampanyasında tespit edilen önemli araçlardan biri, GrewApache olarak adlandırılan ve en az 2021'den beri kullanılan bir zararlı yazılımdır. Ayrıca, CloudSorcerer arka kapısının saldırıcılar tarafından güncellenerek LiveJournal ve Quora profilleri gibi popüler ağ hizmetlerini ilk C2 sunucuları olarak kullandığı tespit edilmiştir. Saldırılar sırasında, PlugY adlı yeni bir arka kapı da keşfedilmiştir; bu yazılım, DRBControl arka kapısının koduna benzerlik gösteren karmaşık bir komut setine sahiptir.

EastWind kampanyasında saldırıcılar, mızraklı kimlik avi e-postaları kuruluşlara sızmayı başardılar. Bu e-postalar, RAR arşivleri ile birlikte gönderildi ve kuruluşların e-posta adreslerini hedef aldı. Saldırganlar, kötü amaçlı etkinliklerini gizlemek için GitHub, Dropbox, Quora, LiveJournal ve Yandex.Disk gibi popüler ağ hizmetlerini C2 sunucuları olarak kullandı. Bu yöntemler, saldırı trafiğinin tespit edilmesini zorlaştırdı ve saldırılardan etkisini artırdı.

EastWind kampanyası, APT31'in Rusya'daki hükümet ve BT kuruluşlarını hedef alarak, gelişmiş siber casusluk tekniklerini kullanmaya devam ettiğini göstermektedir. Saldırılarda kullanılan araçların güncellenmiş ve karmaşık doğası, bu tehdit aktörlerinin sürekli olarak yöntemlerini geliştirdiğini ve hedeflerine yönelik tehdit seviyesini artırduğunu ortaya koymaktadır.

APT31'in Saldırı Taktiği

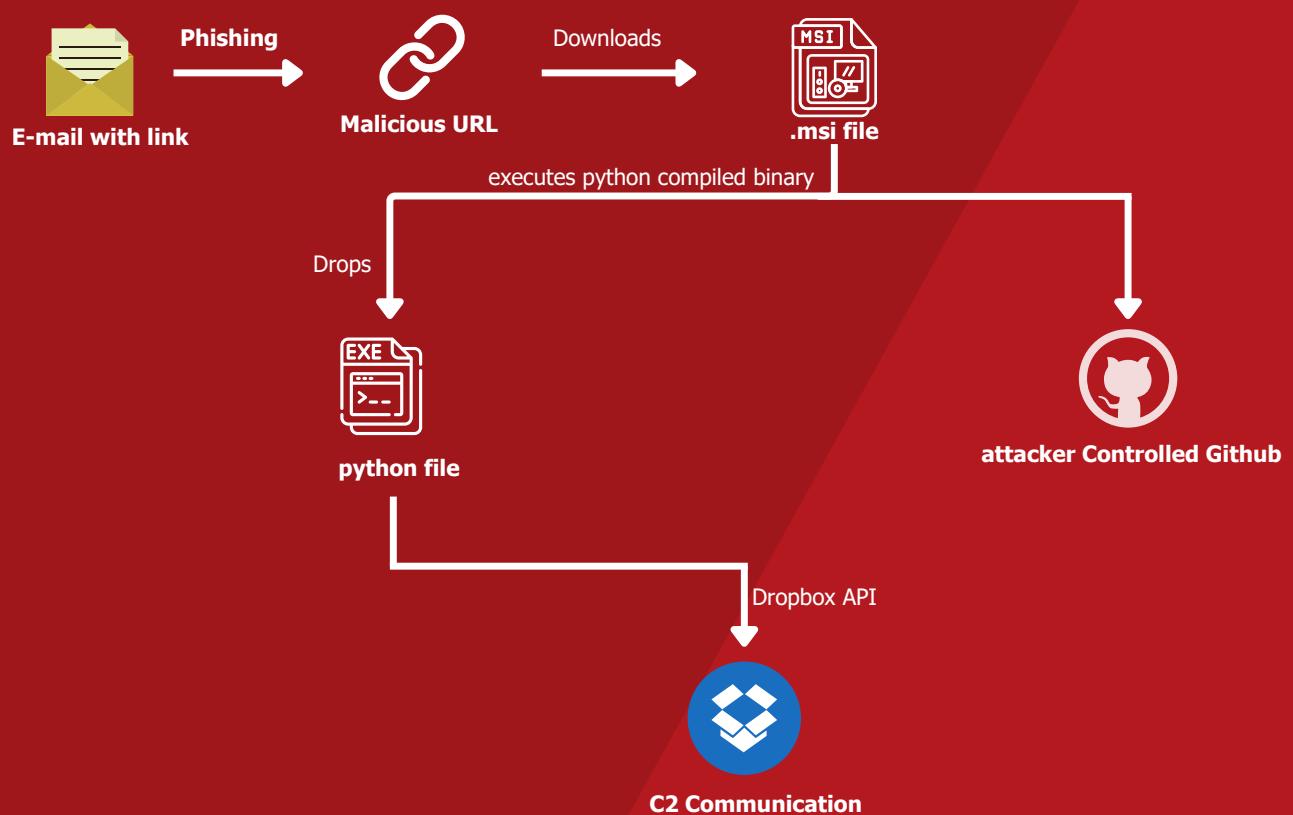
APT31, iki aşamalı bir strateji benimseyerek operasyonlarını gerçekleştirmiş gibi görünüyor. İlk aşamada, kurbanlara tanınmış ABD'li gazetecilerden geldiği izlenimi verilen e-postalar gönderiliyordu. Bu e-postalar, meşru haber makalelerinden alınmış alıntılar içeriyor ve takip bağlantılarıyla birlikte geliyordu. Bu bağlantılar, büyük olasılıkla orijinal makaleye yönlendirme amacıyla taşıyordu. Kurbanlar bu bağlantılara tıkladığında, saldırganlar, e-postanın hangi cihazda açıldığı ve alicının IP adresi gibi ön bilgi toplama imkanı buluyordu. Sadece 2018 yılının Haziran ve Eylül ayları arasında, bu tür 10.000'den fazla takip e-postasının gönderildiği kaydedildi.

Toplanan bilgiler, saldırganların kurbanların cihazlarına yönelik doğrudan saldırılar düzenlemelerine olanak tanıyordu. Özellikle, APT31'in kurbanların aile üyelerini hedef alarak, daha sıkı güvenlik önlemleriyle korunan kurumsal ağlar yerine ev yönlendiricilerine saldırmayı tercih ettiği vurgulanıyor. APT31'in ev kullanıcılarına yönelik bu tür saldırılar gerçekleştirdiği, 2021 yılının Aralık ayında yayımlanan bir raporda da doğrulanmıştır.

Araç olarak, APT31 ilk aşamada bir dizi kötü amaçlı yazılım ailesi kullandı. Bu yazılımlar, DLL side loading tekniğiyle sisteme sızdırıldı. Daha sonra saldırganlar, ticari bir penetrasyon testi aracı olan CobaltStrike'ın sürümlerine yöneldi. Örneğin, bir vakada saldırganlar, askeri uçuş simülatörleri üreten bir savunma yüklenicisinin yan kuruluşunu hedef alarak, bu noktadan ana ağa erişim sağladı. Bu saldırıda, bir yerel yetki yükseltme zeroday açığı kullanıldıktan sonra bir SQL injection kullanılmıştır.

APT31'in genellikle sunucu tarafı istismarları tercih ettiği ve kurbanla etkileşimi en aza indirdiği belirtilse de, Hong Kong'daki bir aktivist grubunu hedef alan diğer faaliyetler, saldırganların zararlı ekler veya bağlantılar içeren sahte e-postalar göndermeye de başvurduğunu gösteriyor. Ayrıca, saldırganların zararlı yazılım yüklemek için sahte Adobe Flash güncelleme sayfaları oluşturdukları da iddia ediliyor. Dikkat çekici bir diğer ayrıntı, APT31'in bazı kurbanlar için çift katmanlı enfeksiyonlar kullanarak, ilk kötü amaçlı yazılım tespit edilse bile ağa erişimlerini yeniden kazanma stratejisine başvurmuş olmasıdır.

APT31 Grubunun Saldırı Zinciri



Mitre ATT&CK Tablosu

Taktik	Teknik	Açıklama
Initial Access	Spear Phishing Attachment	Hedefli kimlik avı e-postalarıyla zararlı eklerin gönderilmesi.
Execution	PowerShell	PowerShell komutları kullanarak zararlı kod çalıştırma.
Persistence	Create Account	Hedef sisteme yeni kullanıcı hesapları oluşturma.
Privilege Escalation	Exploitation for Privilege Escalation	Sistem güvenlik açıklarını kullanarak yetki yükseltme.
Defense Evasion	Obfuscated Files or Information	Zararlı kodun algılanmasını zorlaştırmak için dosyaları gizleme.
Credential Access	Credential Dumping	Hedef sistemden kimlik bilgilerini toplama.
Discovery	System Information Discovery	Sistem bilgilerini toplama ve analiz etme.
Lateral Movement	Remote Services	Uzaktan erişim servislerini kullanarak sistemler arası hareket.
Exfiltration	Exfiltration Over C2 Channel	Komuta ve kontrol kanalı üzerinden veri sızdırma.

IoC's

IoC	Type
themicrosoftnow[.]com	URL
meeting[.]equitaligaiustizia[.]it	URL
137[.]74[.]76[.]92	IP
23[.]218[.]225[.]10	IP
28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd7a41e	SHA256
e024fe959022d2720c1c3303f811082651aef7ed85e49c3a3113fd74f229513c	SHA256
d6b348976b3c3ed880dc41bb693dc586f8d141fbc9400f5325481d0027172436	SHA256
c0f93f95f004d0afd4609d9521ea79a7380b8a37a8844990e85ad4eb3d72b50c	SHA256
caeca1933efcd9ff28ac81663a304ee17bbcb8091d3f9450a62c291fec973af5	SHA256
de19e0163af15585c305f845b90262aee3c2bdf037f9fc733d3f1b379d00edd0	SHA256

Siber Saldırılardan Nasıl Korunabilirsiniz?

Kurumunuzun siber alanda güvenliğini sağlamak istiyorsanız eğer, alınması gereken bazı önlemler bulunmaktadır.

Kullandığımız Yazılımlarda Zafiyet Var mı?

Zafiyetli olduğu açıklanan yazılımlar eğer kurumunuzda da kullanılıyorsa, bu yazılımların güncellenmesi gerekmektedir. Eğer kullandığınız yazılım uzun bir süredir güncelleme desteğini vermiyor ise, rakip bir ürünün kullanımına geçilmelidir. Aksi takdirde saldırganlar bu yazılım açıklarından faydalananarak kurum içerisindeki ağa erişebilir ve uç noktadaki cihazlar üzerinde zararlı davranışlarda bulunarak sisteme zarar verebilirler.

Çalışanlarımıza ait Kişisel Bilgiler Sızdırılmış mı?

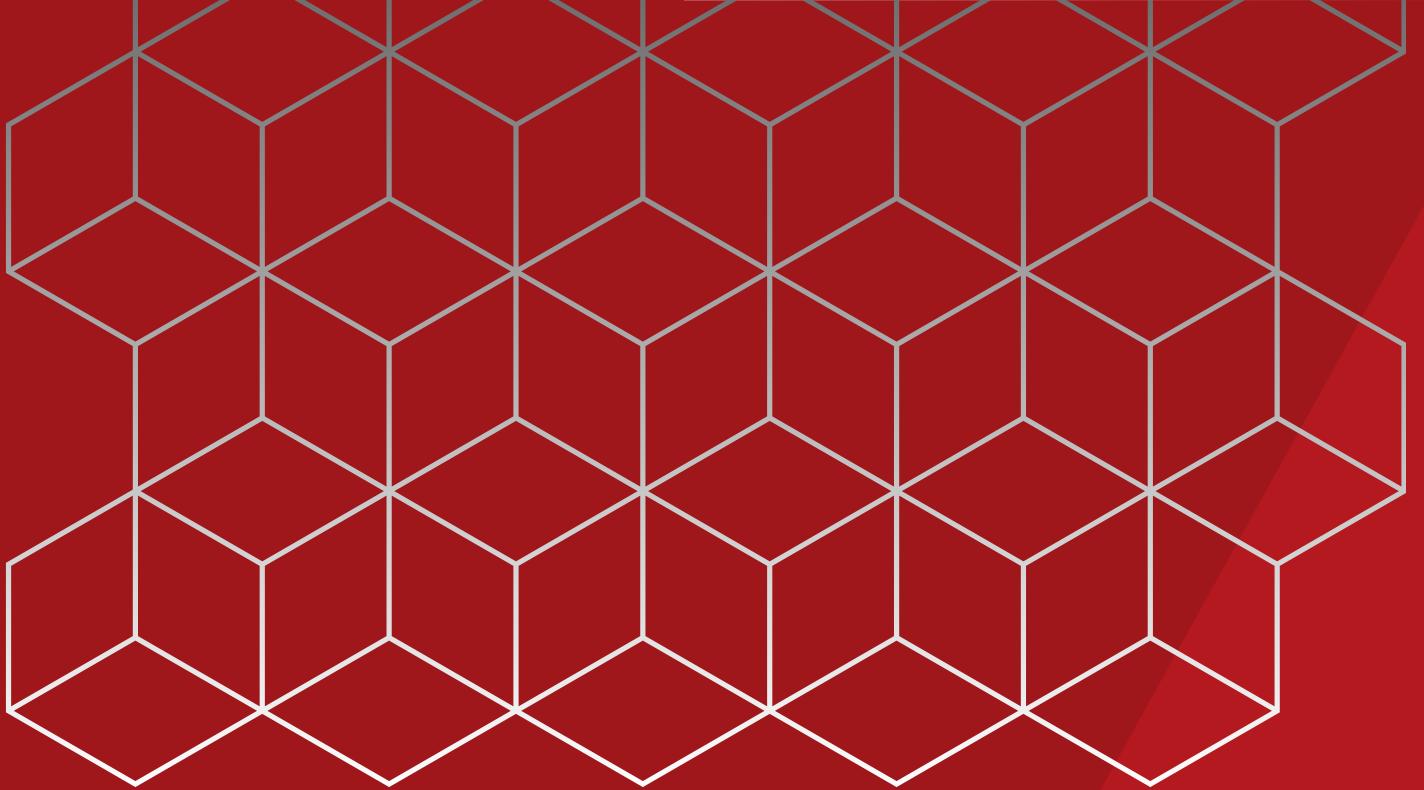
Özellikle kurum yöneticilerinin kurumsal hesap bilgileri üçüncü taraf yazılımlardan kaynaklı olarak sızdırılabilirmektedir. Sızdırılan bu hesap bilgileri kullanılarak phising kampanyaları gerçekleştirilebilir veya sızdırılan hesap bilgilerinin türüne ve önemine göre, şahıs üzerinden kuruma zarar verilebilir. Bu durumların önüne geçmek için belirli periyodlar ile personellerden kurumsal hesap şifrelerini değiştirmeleri istenebilir.

Çalışanlarımız Siber Güvenlik Konusunda Yeterli Farkındalık Sahipler mi?

Alınması gereken belki de en mühim önlem insan farkındalığıdır. Özellikle, bilişim alanına nispeten uzak kalan fakat aynı anda bulunan çalışanların siber güvenlik farkındalığı eğitimleri almaları elzemdir. Tanımlanan çalışan profili, siber saldırganlar tarafından ilk alınan hedeflerdir. Bu noktada farkındalık eğitimleri ile bu konunun önüne geçebilirsiniz.

Özetle,

Her türlü önlem alındığı bir durumda bile siber saldırıya uğrayabilir ve bu saldırılardan zarar alabilirsiniz. Önemli olan alınabilecek potansiyel zararı en aza indirebilmektir.



ECHO

CYBER THREAT INTELLIGENCE

