YILDIZ

SİBER TEHDİT İSTİHBARATI TAKIMI

APT32

Mart 2025

İÇİNDEKİLER

BÖLÜM 1: ÖZET

Advanced Persistent Threat (Gelişmiş Devamlı Tehdit) genellikle hükümet destekli bir grup bilişim suçlusu tarafından hazırlanan ve devam eden özel ve sistematik saldırı mimarisidir. İlgili grupların saldırılardaki motivasyonları para, şöhret vb. olabileceği gibi espiyonaj, sabotaj, karşı istihbarat faaliyetleri gibi olgularda da kendini bulabilmektedir.

APT saldırıları iyi kurgulanmış ve zaman içerisinde devam eden bir dizi saldırı adımının sonuçlandırılmasıdır. Bu saldırı adımları sırasıyla:

1-) İlgili grubun hedef ağa sızması (Genellikle kötü amaçlı yazılımlar kullanılır)

2-) Kullanılan kötü amaçlı yazılımın sistem üzerinde faaliyete geçme/faaliyet sahasını artırma gibi sebepler neticesinde grubun komuta kontrol sunucuları ile iletişim kurması

3-) Sistemde etkin ve yeterli dinleme yapılabilmesi için kalıcılığın sağlanması

4-) Zarar verme, veri ihlaline sebebiyet verme, casusluk faaliyetleri ile süreci sonuçlandırma adımlarından oluşur.

OceanLotus, SeaLotus, Cobalt Kitty, BISMUTH, TIN WOODLAWN gibi çeşitli isimler ile bilinen potansiyel saldırı tehditleri taşıyan bir grup olan APT32, 2014 yılından bu yana faaliyetlerine devam eden Vietnam menşeii bir APT grubudur.

Devlet destekli olduğu düşünülen ve genllikle siber espiyonaj faaliyetleri gösteren bu grubun hedefleri arasında hükümetler, şirketler, medya kuruluşları ve iç siyaset muhalifleri yer almaktadır.

BÖLÜM 2: APT32'YE GENEL BAKIŞ

APT32	OceanLotus
Takma Adlar	Cobalt Kitty, APT-C-00, SeaLotus, POND LOACH, Canvas Cyclone
Menşei	 Vietnam
Saldırı Hedefleri	Hükümetler, Aktivistler, Siyasi Muhalifler, Medya Kuruluşları vb.

Vietnam Hükümeti çıkarlayıla uyumlu hedeflere yönelik operasyonlar düzenleyen; sıklıkla OceanLotus takma adıyla bilinen APT32 grubunun başta yabancı hükümetler olmak üzere; iç siyaset muhalifleri, gazeteciler

aktivistler ve medya kuruluşları gibi kritik yapılara saldırılar düzenlediği tespit olunmuştur.

Grubun faaliyet sahası Vietnam ve Filipinler dahil olmak üzere genel olarak Asya Kıtası üzerinde kendini bulmaktadır.

APT32 grubunun saldırı motivasyonu değerlendirildiğinde Vietnam Hükümeti'nin siyasi varlığının devamlılığını sağlamak için siber dünyada varlık göstermek ve Vietnam'lı şirketlere yardım amaçlı espiyonaj faaliyetleri göze çarpmaktadır.

Grubun saldırı tarihçesine bakıldığında ise:

- **2014**: İlk faaliyetlerinin Vietnam'daki yabancı menşeili enerji ve inşaat şirketlerine yönelik olduğu tespit olunmuştur.
- **2019-2020**: Grup ilerleyen yıllarda COVID-19 pandemisini fırsat bilen bir phising saldırısı ile Dünya Sağlık Örgütü e-postalarını taklit ederek pek çok kullanıcıya virüs ve zararlı yazılım içeren dosyalar göndermiştir.
- **2021-2023**: Zaman içinde saldırı sahasını genişleten grup hedefleri arasına Güneydoğu Asya Hükümet Destekli kuruluşları, bölgenin önemli teknoloji ve otomotiv şirketlerini ekleyerek ransomware saldırılarında bulunmuştur

Grup ile ilgili yukarıda sayılan operasyonlar göze çarpmaktadır.

APT32 tarafından kullanılan taktikler, teknikler ve prosedürler değerlendirildiğinde MITREATT&CK çerçevesinde geliştirilmiş çeşitli yöntemlere başvurulduğu tespit olunmuştur. Bu bağlamda grubun operasyon adımlarının sırasıyla hedef ile ilk temas, hedefe zararlı yazılım bulaştırma, hedef üzerinde yetki yükseltme ve hedef sisteme zarar verme, veri sızıntıları oluşturma olduğu görülmüştür.

APT32 grubu gerçekleştirdiği operasyonlarda genel itibariyle AWS, DigitalOcean vb. Bulut Hizmetleri ve kiralık sunucular kullanmaktadır. Yine bu sunucular ve phising amaçlı oluşturdukları alan adlarını özelleştirilmiş sosyal mühendislik şablonları ile zenginleştirdikleri tespit olunmuştur.

BÖLÜM 3: APT32 MITRE ATT&CK TEKNİKLERİ

Domain (Alan)	ID	Teknik Adı ve Kullanımı
Kurumsal	T1087.001	**Hesap Keşfi: Yerel Hesaplar** APT32, net localgroup administrators komutunu kullanarak yönetici hesaplarını listelemiştir.
Kurumsal	T1583.001	**Altyapı Edinme: Alan Adları** APT32, bilgi toplamak ve kötü amaçlı yazılım dağıtmak için web siteleri kurup işletmiştir.
Kurumsal	T1583.006	**Altyapı Edinme: Web Hizmetleri** APT32, kötü amaçlı dosyaları barındırmak için Dropbox, Amazon S3 ve Google Drive kullanmıştır.
Kurumsal	T1071.001	**Uygulama Katmanı Protokolü: Web Protokolleri** APT32, HTTP/HTTPS üzerinden iletişim kuran JavaScript kullanarak ek framework'ler indirmiştir. Ayrıca şifrelenmiş yükleri HTTP ile aktarmıştır.
Kurumsal	T1071.003	**Uygulama Katmanı Protokolü: E-posta Protokolleri** APT32, Office makroları aracılığıyla C2 (komuta-kontrol) için e-posta kullanmıştır.
Kurumsal	T1560	**Toplanan Veriyi Arşivleme** APT32'nin arka kapısı, verileri sızdırmadan önce LZMA sıkıştırma ve RC4 şifreleme kullanmıştır.
Kurumsal	T1547.001	**Önyükleme veya Oturum Açma Sırasında Çalıştırma: Kayıt Defteri Çalıştırma Anahtarları** APT32, PowerShell/VBS betiklerini ve arka kapılarını çalıştırmak için Kayıt Defteri Run anahtarlarını kullanmıştır.
Kurumsal	T1059	**Komut ve Betik Yorumlayıcıları** APT32, Cobalt Strike beacon'larını indirmek için COM scriptlet'leri kullanmıştır.

Kurumsal	T1059.001	**PowerShell** APT32, PowerShell tabanlı araçlar, tek satırlık komutlar ve shellcode yükleyiciler kullanmıştır.
Kurumsal	T1059.003	**Windows Komut Kabuğu** APT32, cmd.exe ile komut çalıştırmıştır.
Kurumsal	T1059.005	**Visual Basic** APT32, makrolar, COM scriptlet'leri ve VBS betikleri kullanmıştır.
Kurumsal	T1059.007	**JavaScript** APT32, drive-by indirmeler ve C2 iletişimi için JavaScript kullanmıştır.
Kurumsal	T1543.003	**Sistem Süreci Oluşturma/Değiştirme: Windows Hizmetleri** APT32, PowerShell betiklerini yüklemek ve kalıcılık sağlamak için Windows Hizmetlerini değiştirmiştir.
Kurumsal	T1189	**Drive-by Bulaşma** APT32, kurbanları güvenliği ihlal edilmiş "watering hole" web sitelerine yönlendirerek bulaşma sağlamıştır.
Kurumsal	T1585.001	**Hesap Oluşturma: Sosyal Medya Hesapları** APT32, sahte web siteleriyle eş zamanlı sahte Facebook sayfaları oluşturmuştur.
Kurumsal	T1048.003	**Alternatif Protokol ile Veri Sızdırma: Şifrelenmemiş Protokoller** APT32'nin arka kapısı, verileri DNS paketlerinin alt alan adına kodlayarak sızdırmıştır.
Kurumsal	T1041	**C2 Kanalı Üzerinden Veri Sızdırma** APT32'nin arka kapısı, C2 sunucusuyla açılan kanal üzerinden veri sızdırmıştır.
Kurumsal	T1203	**İstemci Yürütme için Sömürü** APT32, kötü amaçlı kod çalıştırmak için RTF belgelerinde CVE-2017-11882 açığından yararlanmıştır.

BÖLÜM 4: APT32 IOC LİSTESİ

Hash Değerleri Tablosu

MD5	SHA-256	SHA1
9602d1e23d8f32f31f475beb057da271	8b1b20dc5f0b9fda45aa888cd3c298a52d5a923d84e5fcddc6e64d3f042f9a67	274efe297fd708fcb5a6d086eb045e316f91ccbe
3273dde8b51915160ababbe6092bfce2	8f031098e3722d2662203fafc57bafc927a6deb7424982102f45a1da6964806b	1495285a07f9e55c04efc5c380b5ab201ac94f7c
fc164ff402e76ec692c38fa568d4e7bd	4991093dbb8e839785abff95058b1e577c75160b9576a68e4ed84337eeed9335	a9c88aa6d725fef2aea04e40becffa926ac6a6fa
e785b68a4a0502f3abeeba137db8f9cd	e2fba9178320650553a41a2494ed2607d1923eef38f7e9d01a82ebac0865caf3	440460e49af5d3bfa55bf781d72d4de12f128e0a

Domain, Hostname ve IP Adresleri Tablosu

DOMAIN	HOSTNAME	IPv4
urnage.com	zone.apize.net	158.69.100.199
ucairtz.com	yii.yiihao126.net	164.132.45.67
ucaargo.com	worker.baraeme.com	176.107.176.6
tulationeva.com	utitled.po9z.com	176.107.177.216
tsworthoa.com	tops.gamecourses.com	184.95.51.179
traveroyce.com	support.chatconnecting.com	184.95.51.181
tonholding.com	stack.inveglob.net	184.95.51.190
vphelp.net	ssl.zin0.com	185.157.79.3
volver.net	share.codehao.net	192.121.176.148
vitlescaux.com	seri.volveri.net	198.50.191.195

BÖLÜM 5: KULLANILAN ZARARLI YAZILIMLAR

Ad	Açıklama
Arp	ARP önbelleğini görüntüleme/değiştirme aracı.
Cobalt Strike	Hedefli saldırı simülasyonu ve APT taklidi yapan ticari bir saldırı aracı.
Denis	Soundbite ve Goopy ile benzerlik gösteren bir Windows backdooru.
Ipconfig	TCP/IP, DNS, DHCP bilgilerini görüntüleme aracı.
Kerrdown	Ağ içine casus yazılım sızdırmak için kullanılan özel indirme aracı.
Komprogo	İşlem, dosya ve kayıt yönetimi yapabilen backdoor.
Mimikatz	Sistemden hash/parola çalmak için kullanılan kimlik bilgisi hırsızlığı aracı.
Net	Kullanıcı, grup, hizmet ve ağ bağlantılarını yöneten komut satırı aracı.
Netsh	Ağ bileşenlerini yapılandırma ve izleme aracı.
OSX_OCEANLOTUS.D	APT32 tarafından kullanılan Mac OS backdooru.
Phoreal	APT32'nin kullandığı imzalı bir backdoor.
Soundbite	APT32'nin kullandığı diğer bir imzalı backdoor.
WINDSHIELD	APT32'ye özel gelişmiş backdoor.

BÖLÜM 6: APT32'YE KARŞI ÖNERİLER

Kategori	Açıklama
E-posta Güvenliği	Gelişmiş phishing filtreleri ve DMARC/DKIM protokolleri.
Ağ İzleme	Anormal C2 trafiğini tespit etmek için SIEM çözümleri.
Yama Yönetimi	Kritik güvenlik açıklarının (özellikle Office ve macOS) zamanında kapatılması.
Kullanıcı Eğitimi	Sosyal mühendislik senaryolarına karşı farkındalık eğitimleri.

Kategori	Açıklama
Endpoint Koruma	Davranış tabanlı tespit (EDR) ve imzasız tehditlere odaklanan çözümler.

BÖLÜM 7: SONUÇ

Hükümet destekli yapısı, kaynakları ve teknik donanımı nedeniyle küresel çapta risk oluşturan APT32, yabancı hükümetler, şirketler ve kurumlar için potansiyel bir risk oluşturmaktadır. Bu kapsamda APT32'nin saldırılarına karşı kendilerini korumak isteyen şirketler ve kurumlar, proaktif istihbarat tabanlı savunma stratejilerine başvurmalı ve diğer güvenlik yapıları ile iş birliklerinde bulunmalıdır.

BÖLÜM 8: KAYNAKLAR

- Malpedia APT32
- MITRE ATT&CK: APT32
- InfinitumIT APT32
- FireEye, CrowdStrike Raporları
- ThreatBook CTI

YILDIZ

SİBER TEHDİT İSTİHBARATI TAKIMI

Mart 2025