Siber tehdit istihbarat raporu: amerika seçimleri

yazar: abdulsamet sunar   
rapor tarihi: 02/11/2024

Özet:   
Bu Rapor, 2024 ABD Başkanlık Seçimleri’ni tehdit eden potansiyel siber, hibrit ve manipülatif unsurlar analiz etmektedir. Tehditler, seçim güvenliği, kamu güvenliği, demokratik kurumlar ve ulusal güvenlik üzerinde etki faktörü oluşturmaktadır. Seçimke ilişkili kritik altyapılar, bilgi akışları ve kamusal algı hedef alınarak sosyal mühendislik, fidye yazılım ve gelişmiş psikolojik operasyon (PSYOP) teknikleri kullanıldığı gözlenmektedir. Rapor, Genel tehdit unsurlarını değerlendirerek kapsamlı şekilde ABD seçim sürecinin güvenliğini katkıda bulunabilecek stratejik önlemler sunmaktadır.

AMAÇ:

Bu raporun amacı ABD seçim sürecini tehdit eden çeşitli tehdit aktörlerini, motivasyonlarını, kullandıkları teknikleri ve potansiyel hedefleri analiz etmek. Amaç, seçim süreci boyunca seçmen güvenini koruma, kamuoyunu bilgilendirme ve kritik altyapıları tehdit eden unsurları erken aşamada belirleyip güvenlik önlemleri geliştirmektir.

Tehdit aktörleri ve Motivasyonları:

|  |  |  |
| --- | --- | --- |
| Tehdit Aktörü | Motivasyon | MITRE Taktikleri ve Teknikleri |
| APT29 (Cozy Bear-Rusya-Devlet Destekli) | Toplumsal kutuplaşmayı artırmak, ABD'nin siyasi sürecine güvensizlik yaratmak ve uluslararası alanda ABD'nin imajını zayıflatmak. | TA0001- Initial Access,  T1566- Phishing TA0011- Command and Control,  T1071- Application Layer Protocol (HTTPS) TA0006- Credential Access,  T1555- Credentials from Password Stores |
| APT41 (Winnti Group-Çin-Devlet Destekli) | ABD'nin politik ve ekonomik çıkarlarını etkilemek, stratejik bilgi toplama ve endüstriyel casusluk yapmak. | TA0011- Command and Control,  T1095- Non-Application Layer Protocol TA0006- Credential Access,  T1071- Application Layer Protocol (Custom) TA0005- Defense Evasion,  T1027- Obfuscated Files or Information |
| Charming Kitten (İran-Devlet Destekli) | ABD’de siyasi ve toplumsal karışıklık yaratmak, adaylara karşı saldırılar düzenlemek. | TA0001- Initial Access,  T1566- Phishing TA0009- Collection, |
| Lazarus Group (APT38-Kuzey Kore-Devlet Destekli) | ABD’ye ekonomik zarar vermek, seçim sürecine müdahale ederek sosyal mühendislik ve dezenformasyon yaratmak. | TA0001- Initial Access,  T1566- Phishing TA0011- Command and Control,  T1071- Application Layer Protocol (HTTPS) TA0006- Credential Access,  T1558- Steal or Forge Web Session Cookie |
| APT10 (Stone Panda-Çin-Devlet Destekli) | ABD'nin endüstriyel ve ekonomik sırlarını elde etmek, seçim altyapılarına yönelik bilgi toplamak. | TA0001- Initial Access,  T1193- Spear Phishing Attachment TA0009- Collection,  T1083- File and Directory Discovery TA0011- Command and Control,  T1071- Application Layer Protocol |
| Sandworm Team (Rusya-Devlet Destekli) | Seçim altyapısını bozmak, toplumsal kaos yaratmak ve ABD seçim sistemine güvensizlik aşılamak. | TA0043- Manipulation,  T1566- Phishing TA0040- Impact,  T1485- Data Destruction TA0011- Command and Control,  T1071- Application Layer Protocol (DNS) |
| APT33 (Elfin Team) (İran-Devlet Destekli) | ABD’nin seçim sürecine müdahale ederek belirli adayları zayıflatmak, toplumsal karışıklık yaratmak. | TA0001- Initial Access, T1193- Spear Phishing Attachment TA0009- Collection, T1560- Archive Collected Data TA0011- Command and Control, T1071- Application Layer Protocol |
| APT28 (Fancy Bear) (Rusya-Devlet Destekli) | Seçim sürecine müdahale ederek dezenformasyon ve manipülasyonla toplumsal güveni sarsmak. | TA0043- Manipulation Tactics,  T1566- Phishing TA0011- Command and Control,  T1090- Proxy TA0009- Collection,  T1036- Masquerading |
| Volt Typhoon  (Çin- Devlet Deskteli) | ABD'nin kritik altyapısına sızma ve uzun süreli istihbarat toplama amacıyla hareket eder. Özellikle seçim süreçlerinde ABD’yi istikrarsızlaştırma ve Çin'in stratejik çıkarlarına hizmet etme amacı taşır. | T1078-TA0007- Reconnaissance and Credential Access,    TA0005-T1071.003- Defense Evasion and Encrypted Communication  TA0003- T1203- Persistence and Malicious Code Injection |
| FunkSec | Gizli bilgileri ifşa ederek ABD başkanlık makamına yönelik güvensizlik oluşturmayı ve kamuoyunda kaos yaratmayı hedefler. | TA0007, T1566- Collection and Social Engineering  TA0043, T1583.001- Impact Operations and Dark Web Data Leakage  TA0043, T1090- Disinformation Campaign and Proxy Usage |

devlet destekli aktörler:

ABD seçim sürecinde doğrudan veya dolaylı olarak müdahil olabilecek devlet destekli tehdit grupları seçim güvenliğii tehdit etmektedir. Bu ve bu tarz tehdit aktörleri ABD Seçim sürecine aşşağıdaki motivasyonlarla dahil olabilirler:

* Rusya: Toplumsal kutuplaşmayı artırmak için sosyal medya ve darknet’te dezenformasyon kampanyaları yürütmektedir. Özellikle, ABD'nin dış politikasını etkilemek amacıyla belirli adaylara karşı psikolojik operasyonlar düzenlemektedir.
* Çin: ABD'nin iç politikasına etkide bulunmak amacıyla sosyal mühendislik ve hedefli kimlik avı saldırılarına odaklanmıştır. Ayrıca, Volt Typhoon gibi gruplar kritik altyapılara yönelik tehdit oluşturur.
* İran: Siyasi istikrarsızlık yaratma amacıyla dezenformasyon ve kimlik avı saldırıları düzenlemektedir. Özellikle belirli adayların imajını zedelemeye yönelik dezenformasyon kampanyaları ve sahte haber siteleri aracılığıyla kamuoyunu manipüle etmektedir.

Paramiliter ve Örgütlü Suç Grupları:

Paramilitary Election İnterference makalesi, seçim süreçlerini etkiemek amacıyla Amerika’nın 2022 ara seçimlerinden itibaren organize olmuş paramiliter grupların faaliyetlerini ortaya koymaktadır. APII (American Patriot |||%) gibi gruplar, seçmenler korkutmak ve seçim güvenliğini zayıflatmak amacıyla “Ballot Box Watching” adı altında örgütlü gözetim faaliyetleri yürütmüştür. Bu gruplar, gözetim operasyonları organize ederken seçim merkezlerine yakın bölgelerde silahlı ve organize bir “gray man” olarak bilinen kişilerle desteklenmiştir.

* APII: Seçim gözlemcilerini organize eden ve gölge operasyonları yürüten APIII, “America First” hareketine bağlı bir ideoloji benimsemektedir.
* The People’s Movement ve Clean Elections USA: Bu gruplar, APIII ve diğer milislerin operasyonlarında lojistik destek sağlamış ve seçim gözlem faaliyetlerinde halka açık bir yüz görevi görmüştür.

HACKTİVİST GRUPLAR

Hacktivist gruplar, ABD seçim sürecini kamuoyu önünde itibarsızlaştırmak ve halkı yönlendirmek amacıyla kimlik avı saldırıları ve dezenformasyon kampanyaları yürütebilir. Bu gruplar, belirli adaylara destek sağlamak ya da karşıt grupları sindirmek için seçim sürecini hedef alabilir.

Hibrit Tehditler ve Fidye Yazılımı Tabanlı Saldırılar

**Lockbit**: Bu grup, eski ABD Başkanı Donald Trump’a destek verdiğini belirterek, ABD seçim sürecine karşı yeni bir tehdit oluşturabileceğini ima etmiştir. Grup, fidye yazılımı saldırılarıyla seçim sürecini doğrudan etkileme potansiyeline sahiptir.

SALDIRI TEKNİKLERİ VE TAKTİKLER

* **Kimlik Avı ve Oltama kitleri**: Darknet'te, başkan adaylarını ve kampanyalarını taklit eden kimlik avı ve oltalama kitlerinin yaygınlaştığı tespit edilmiştir. Bu oltalama kitleri, seçmenlerin kişisel bilgilerini toplamayı hedeflemektedir. "Paramilitary Election Interference" raporunda, bu tür dolandırıcılık yöntemlerinin 2022 seçimlerinde yaygın olarak kullanıldığı ve seçim sürecinde daha da organize hale geldiği belirtilmiştir. Olayda, Darknet’te yayılan kimlik avı kitleri kullanılarak seçmenler yanıltıcı sitelere yönlendirilmekte ve sosyal güvenlik numarası gibi hassas bilgileri toplanmaktadır. AP||| ve diğer milis grupları 2022 ara seçimlerinde uyguladıkları “**Ballot Box Watching**” adlı organize seçim gözetim faaliyetlerini 2024 için genişletmeyi hedeflemekte ve Telegram gibi sosyal medya platformları üzerinden bu operasyonlar, seçmenlerin özgürce oy kullanmalarını engellemeye yönelik çeşitli korkutma taktikler içermektedir.

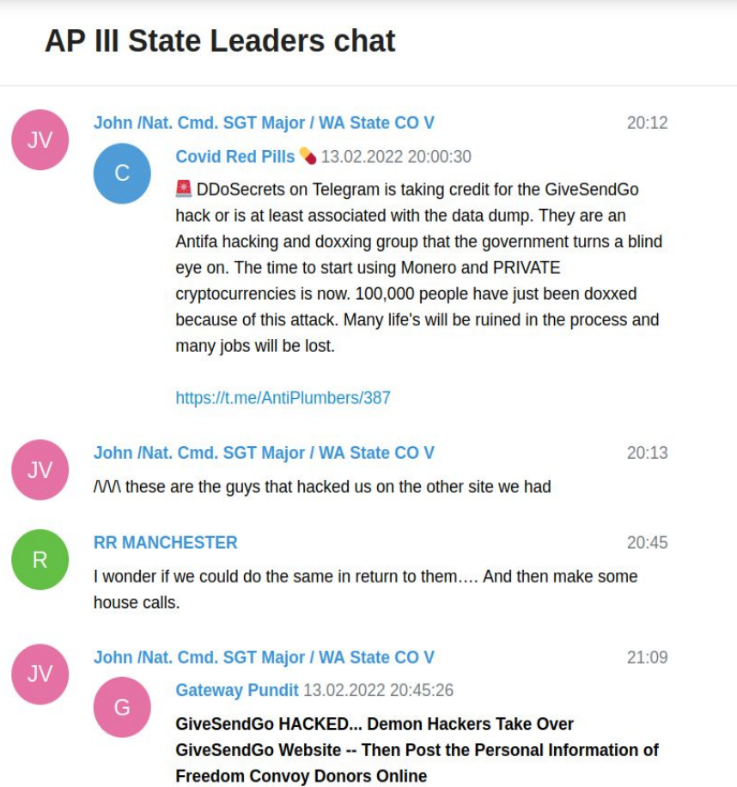
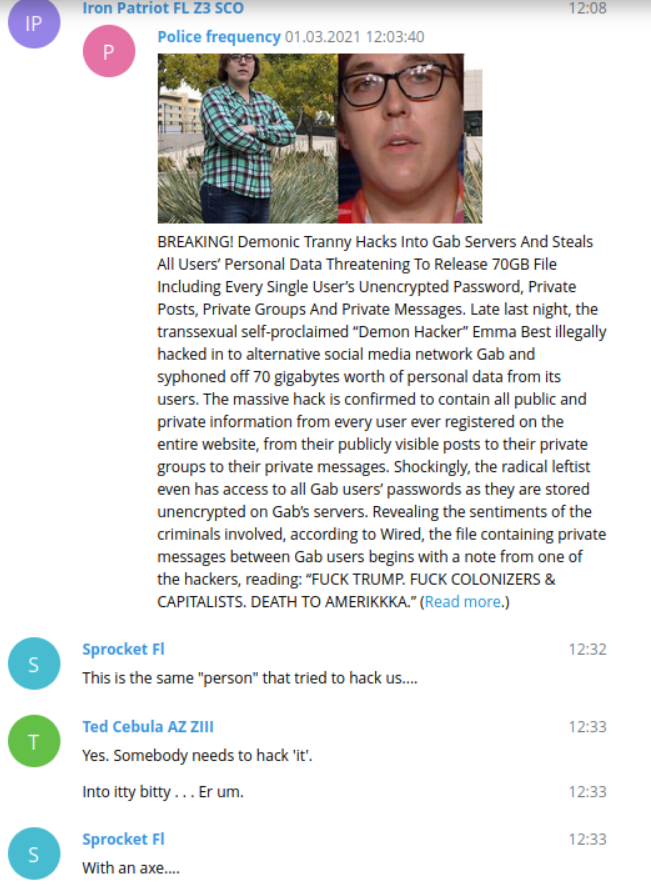
Bulgular incelendiğinde operasyon ve detayları şu şekildedir;

1. **Seçmen korkutma Taktikleri:** AP||| üyeleri, oy kutusu izleme görevini görünürde sıradan seçmenler olarak gerçekleştirmekte;

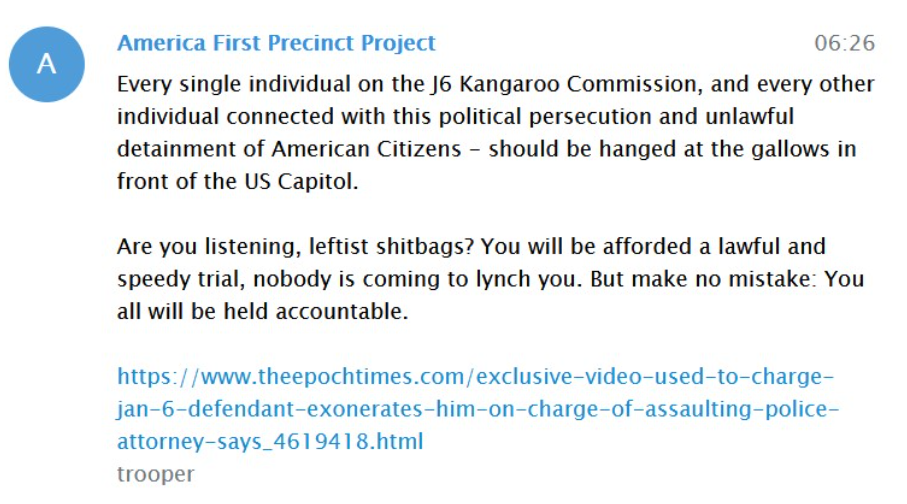
Ancak bu “seçmenlerin” çoğu milis grupların talimatlarıyla organize bir şekilde çalışmaktadır. Bu kişiler, kuralları belirleyen “**Rules of engagement”** adlı bir rehber üzerinde hareket etmekte, belirli bir vardiya sistemi ile alanları denetlemekte ve bölgedeki “**kaptanlar”**’a günlük raporlar göndermektedir. İçlerinde bazıları gizlice silah taşımakta ve gerektiğinde hızlı müdahale ekibi (QRF) olarak adlandırılan bir grubu harekete geçirmek üzere konumlanmaktadır.

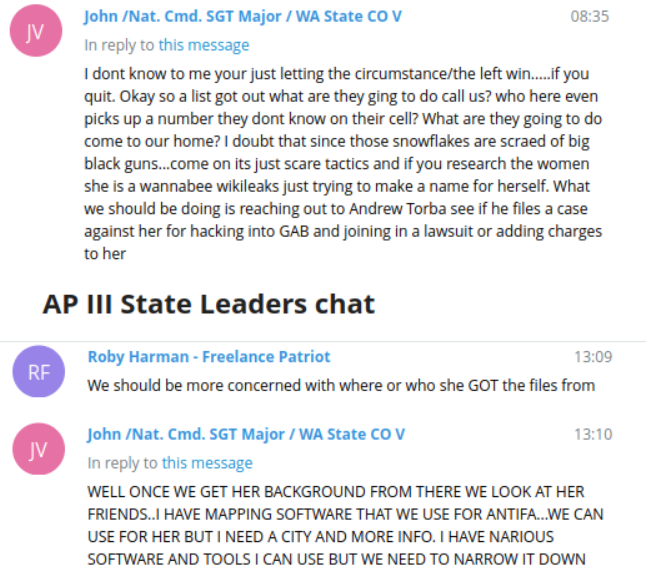
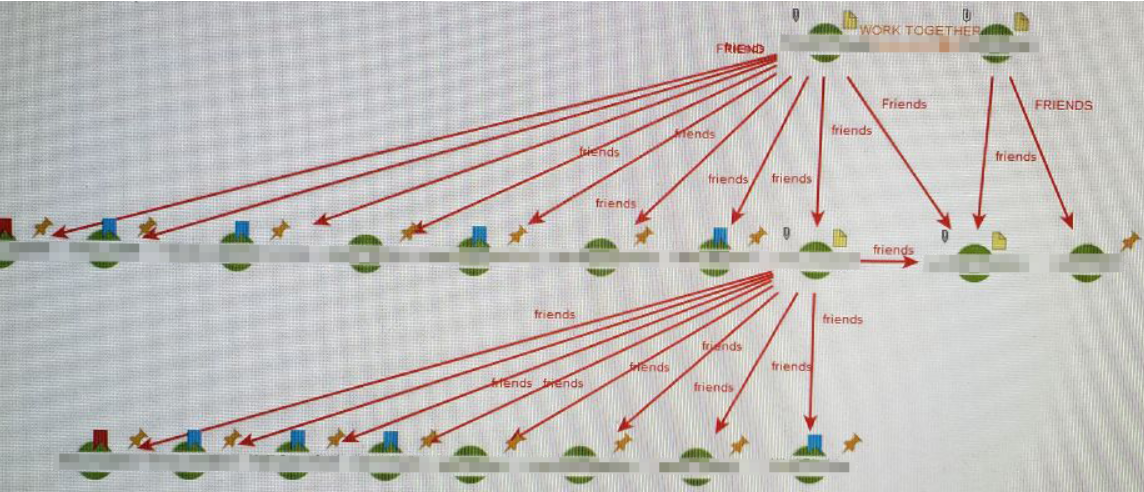
1. **Planlanan Koordinasyon ve “Gri Adam” Rolleri**: Sızıntı içerisinde incelediğimizde, bu operasyonların Telegram üzerinden organize edildiği ve AP|||, The People’s Movement, Clean Elections USA gibi grupların seçim izleme faaliyetlerini yönettiği belirtilmektedir. Özellikle “**Gri adam”** rolü taşıyan üst düzey liderler, izlemeye doğrudan katılmaksızın alanın çevresinde bulunarak, gerektiğinde operasyonu kontrol etmekte ve QRF ile iletişim halinde olmaktadır. Bu kişiler genellikle güvenlik, askeri veya kolluk kuvvetleri deneyimine sahiptir ve grupların kordinasyonunu sağlamaktadır.
2. **Konuşma kayıtları ve Deliller:** Rapora göre, sızıntının 2024 seçimleri öncesinde yaklaşık 570 GB’lık bir dosya halinde yayımlandığı ve bu dosyanın 2022 ara seçimlerinden başlayarak günümüze kadar yapılan planları ve konuşmaları içerdiği belirtilmiştir. Bu dosyalar, AP||| grubunun iç iletişimlerini, Telegram sohbetlerini ve çeşitli gözetim talimatlarını kapsamaktadır.   
   Sızıntı içeriğinde, milis üyelerinin seçim çalışanlarını ve oy taşıma araçlarını gözetlemeyi planladıkları dair kanıtlar yer almaktadır.

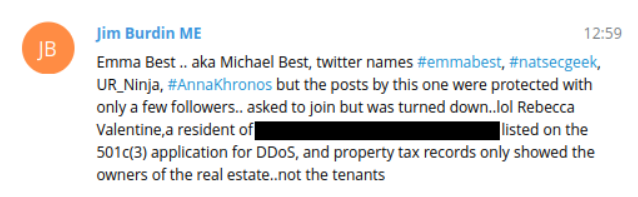
Raporda ve çeşitli haber kaynaklarında seçim sürecine dahil “yeni yöntemler geliştirdiklerini” ve 2022 seçimlerinden öğrendikleri taktikleri 2024 seçimlerinde daha gelişmiş bir şekilde uygulamaya koyduklarını göstermektedir. Bu durum, özellikle “**Bir sonraki seçim mühimmat kutusunda karar verilecek”** gibi tehditkâr mesajlarla güçlendirilmektedir ve potansiyel şiddet olaylarına yol açabileceği ön görülmektedir.











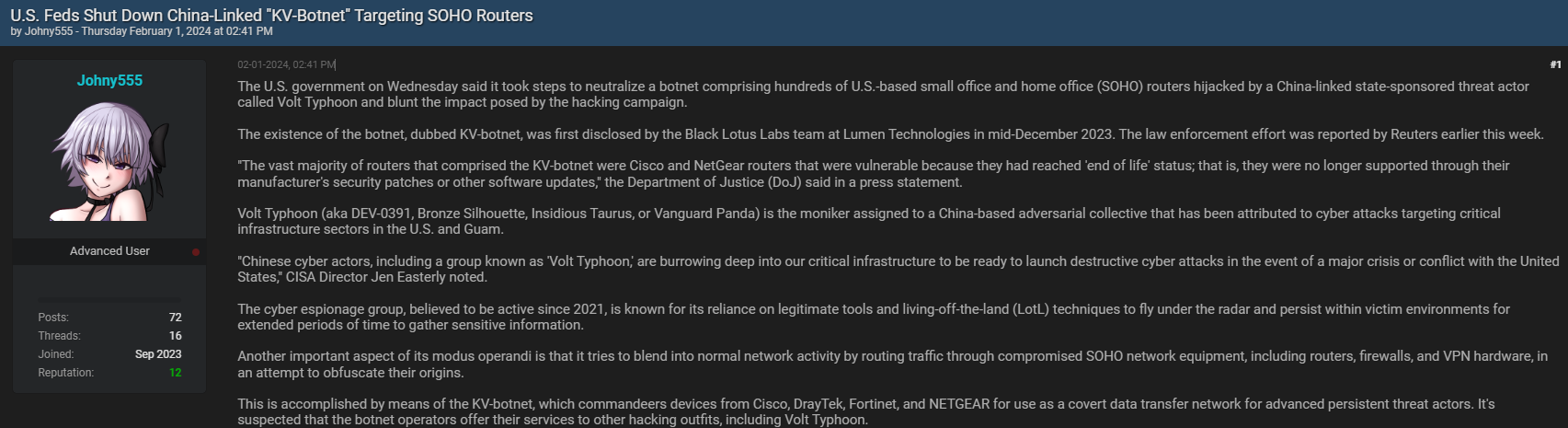
* **KV-Botnet ile Seçim Altyapısına Yönelik Hibrit Tehdit:** KV-Botnet, Çin destekli Volt Typhoon grubuna ait siber saldırı Vektörleriden biri olup, özellikle savunmasız SOHO yönlendiricilerini hedef alarak ABD’nin kritik altyapısına yönelik bir dizi istihbarat toplama, gizli veri aktarımı ve saldırı hazırlığı yapmaktadır. KV-botnet, seçim sürecinde kritik iletişim altyapısına, seçmen verilerine ve oylama sistemlerine yönelik potansiyel bir tehdit oluşturarak seçim güvenliğini doğrudan bir risk teşkil etmektedir.

İlk olarak Aralık 2023’te, Lumen Technologies’in Black Lotus Labs ekibi tarafından KV-botnet’in ABD içindeki savunmasız soho cihazları hedef aldığı tespit edilmiştir. Botnet’in ağ üzerindeki hareketleri gizlemek ve komuta & kontrol (C2) iletişimi için VPN ve şifreli bağlantılar kullanarak siber saldırı kapasitesine sahip olduğu belirlenmiştir.

Ocak 2024 tarihinde Cisco, NetGear gibi yönlendiricilere yayılmış olup seçim altyapısına yönelik keşif faaliyetleri yapmaya başlamış ve Cihazın kritik iletişim ağlarını bozma veya karşı tarafın bilgilerine müdahele etme riski taşışmaktadır.

Seçim güvenliğini sağlamak ve kritik verilerin çalınmasını veya manipüle edilmesini önlemek isteyen ABD hükümeti risk almak istemeyip ola el attı ve botnet’i devre dışı bırakarak bu riskleri azaltmak için harekete geçmiştir.

Çin hükümeti, bu olaya tepki göstererek ABD’nin suçlamalarını reddetmiştir ve bunun bir “**Dezenformasyon kampanyası”** olarak nitelendirmiştir. Çin’in açıklaması, ABD’nin suçlamalarını propaganda olarak gördüğünü ve bu tür faaliyetleri desteklemediğini vurgulamıştır.

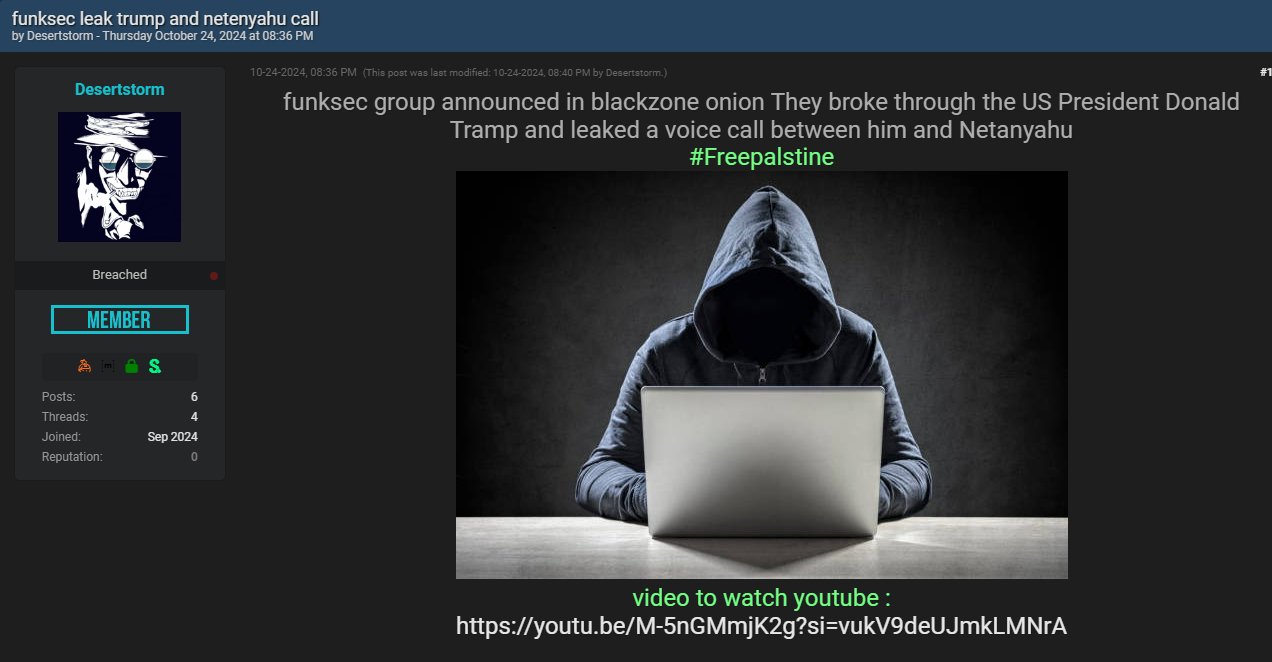
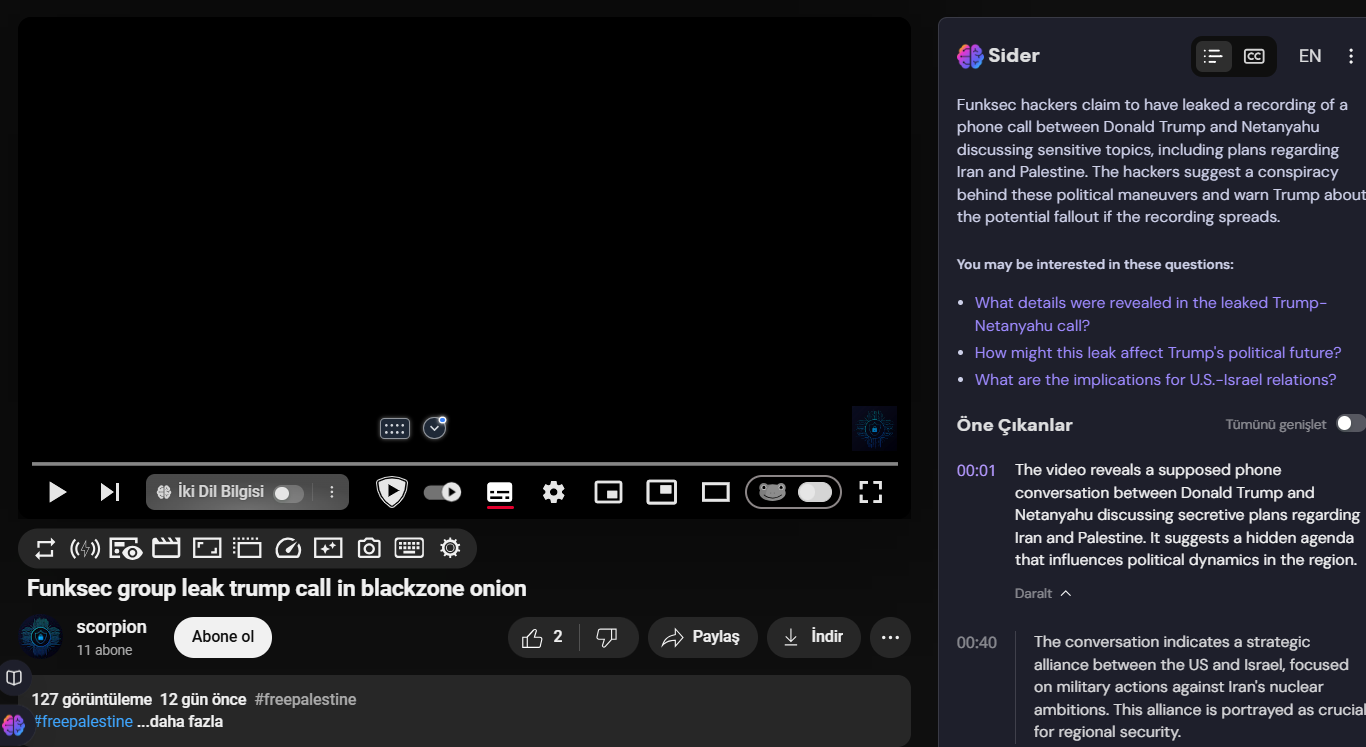




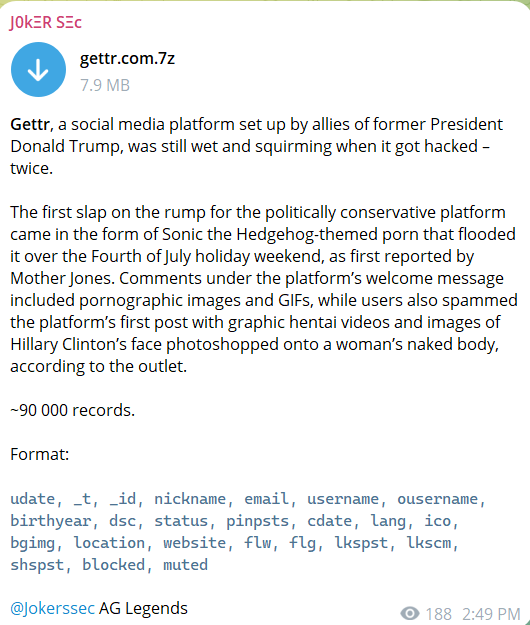
* **FunkSec Grubu ve BlackZone Üzerinden Yapılan Gizli İletişim Sızıntısı:** FunkSec adlı siber tehdit grubu, ABD Başkanı Donald Trump ile İsrail Başbakanı Benjamin Netanyahu arasında gerçekleşen gizli bir telefon görüşmesini ele geçirip sızdırdığını idda etti. Sızıntı, “**BlackZone**” adlı bir Dark Web platformu olan **Onion** üzerinden duyuruldu.   
  Video içeriğinde Başkan Donald Trump ile Benjamin Netanyahu arasında **İran’ın nükleer hakkında projesi ciddi endişeler** dile getiriliyor. Bu durum bölgedeki güvenlik dinamiklerini etkileyebileceğini vurguluyorlar.

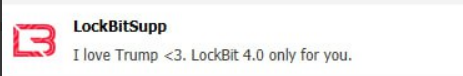
Video’nun devamında Filistin’in durumu ve İsrail’in politikası hakkında planlarını sürdürdüğüü belirtiyorlar. Bu, Orta Doğu’daki politikaların karmaşıklığını artırıyor.

Ekim 2024 yılında yayınlanan bu video da Günümüzde yapay zekâ desteği ile artık resimler, videolar, anılar tekrar canlanabiliyor ve üzerinde küçük oynamalar ile farkına bile varmadan yapmadığımız veya yapamadığımız şeyleri gösterebiliyoruz. Lakin söz konusu bu video olunca işin doğruluk kısmı ile alakalı delil yok.   
Ama bu Başkanlık adayı Donald Trump için bir tehdit faktörü oluşturmakta ve özellikle ABD seçim süreci sırasında ortaya çıkması nedeni ile siyasi manipülasyon amacına hizmet edebileceği düşünülmektedir.



* **Gettr** **Veri Sızıntısı ve İçerik Manipülasyonu:** Gettr, Donald Turmp’ın müttefikleri tarafından kurulan muhafazakâr bir platformdur. 2021 yılında piyasaya sürülen platfom, daha çok “**ifade özgürlüğüne”** odaklandığını vurgulayarak geleneksel sosyal medya devlerinden bağımsız ve sansüre karşı bir alternatif olarak konumlanmıştır.   
  Lakin platform, kurulduğu dönemde iki büyük saldırıya maruz kalmıştır. Platform, özellikle 4 Temmuz tatil haftasında, pornografik içeriklerle doldurularak manipüle edilmiştir. Saldırganlar, platformun açılış mesajının altına pornografik görüntüler ve GIF’ler ekleyip, ayrıca platformun ilk gönderisine hentai vidoları ve Hillary Clinton’ın yüzünün montajlandığı çıplak görsellerle spamlemiştir.   
    
  Saldırının ardından yaklaşık 90.000 kullanıcının kayıt bilgileri sızdırıldığı tespit edilmiştir. Sızdırılan veriler aşşağıdaki formatta ele geçirilmiştir.   
  - {udate, \_t, \_id, nickname, email, username, ousername, birthyear, dsc, status, pinpsts, cdate, lang, ico, bgimg, location, website, flw, flg, lkspst, lkscm, shspst, blocked, muted}  
    
  Bu bilgiler kullanıcıların kişisel kimlik bilgileri, doğum yolları, e-posta adresleri ve diğer profil bilgileri içermektedir. Bu veri sızıntısı, kullanıcıların kimlik avı saldırılarına karşı savunmasız kalmasına da vesile olmuştur.   
    
  Olay sonrası kullanıcılar, platfomun güvenliğine ve siyasi atmosferdeki belirli seçmen grubların görüşlerine olan güvenini sarsarak seçim sürecine dolaylı etkiler yaratmıştır.

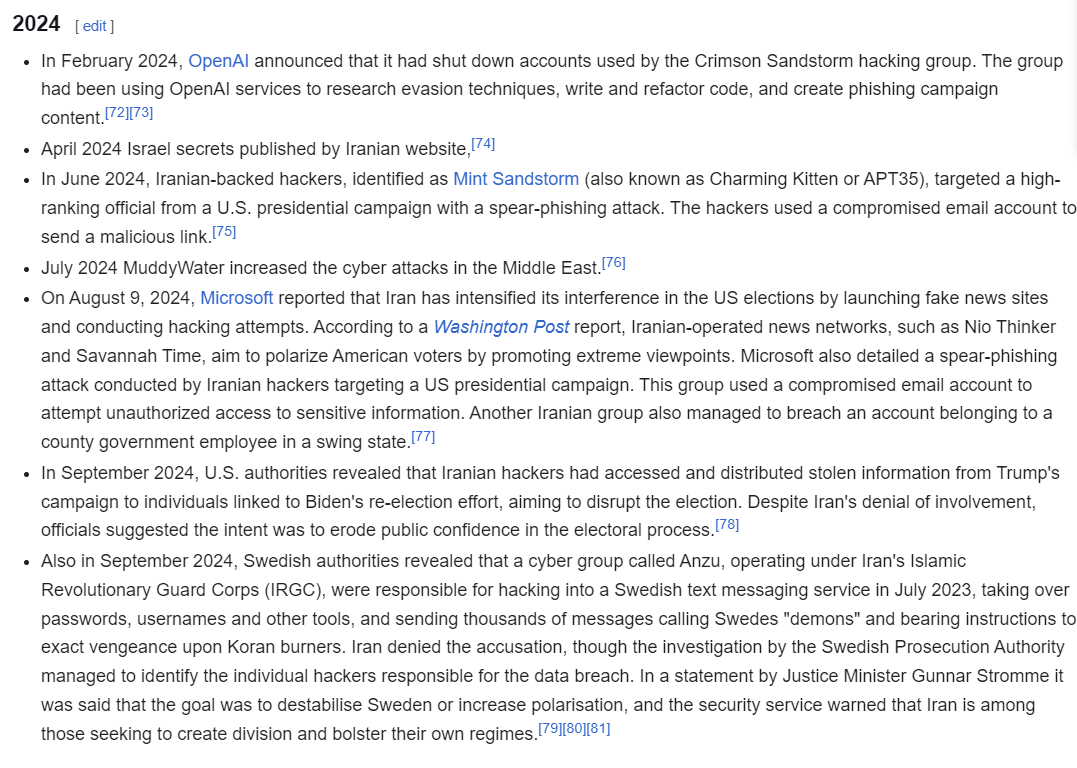


* **LockBit ve Sosyal manipülasyon:** Lockbit fidye yazılımı grubu, eski ABD Başkanı Donald J. Trump’a destek verdiğini açıkladı. Rusya bağlantılı bir siber suç örgütü olan Lockbit, 2024 Subatında altyapısının kolluk kuvvetleri tarafından kapatılmasının ardından, karanlık ağda yeniden ortaya çıkarak Trump’a desteğini belirten bir mesaj yayınladı.   
    
    
  Grup lideri, “Şahsen Trumpa oy vereceğim” ifadesini kullandı. Lakin ABD vatandaşı olup olmadıkları konusunda şüpheler bulunmaktadır.

Bu açıklamanın ardından, Trump veya yönetiminin Rusya merkezli siber suç faliyetleriyle herhangi bir ilgisi olduğuna dair hicbir kanıt bulunmadığını vurgulamak önemlidir.   
Şahsi olarak bu destek açıklamasının dikkat çekme veya kamuoyuna etkileme amacı taşıyan tek taraflı bir beyan olduğunu düşünüyorum.  
  
Ama yinede grubun siyasi bir figüre destek açıklması alışıkmadık bir durum ve bu tür bir hareket, faaliyetlerini politize etme ve siyasi bölünmeleri istismar etme girişimi olarak yorumlanabilir.

* **2024 Seçimleri: İran Destekli APT35’in (Mint Sandstorm) Siber Tehditleri:** İran bağlantılı Mint Sandstorm (APT35), ABD ve müttefiklerine yönelik hedefli saldırılar düzenleyen, İran hükümetiyle bağlantılı bir siber tehdit grubudur. Özellikle siyas, süreçlere müdahele etmek ve hassas verilere erişim sağlamak amacı ile güden bu grup, geçmişte ABD ve Batılı kurumlara karşı yoğun kimlik avı kampanyaları tanınmaktadır. 2024 ABD seçim sürecindede Mind Sandstorm, ABD’nin seçim güvenliğini tehdit eden öncelikli gruplardan biri olarak öne çıkmaktadır.   
    
  İran, Amerika 2024 seçim sürene müdehele etme stratejilerinden biri, Mint Sandstorum’un dezenformasyon kampanyalarıdır. Grup, “**Nio Thinker”** ve “**Savannah Time”** gibi sahte haber siteleri aracılığı ile ABD kamuoyuna yönelik manipülatif içerikler yaymaktadır. Bu platforlarda yayımlanan içerikler, ABD ‘deki siyasi kutuplaşmayı derinleştirerek seçmenlerin kararlarını etkilemeyi hedeflemektedir. Özellikle salıncak eyaletlerdeki dezenformasyon faaliyetleri, seçim güvenliğini tehdit eden kritik bir unsur olarak değerlendirilmektedir.   
  Sadece dezenformasyon la yetinmeyen iranlı APT grubu Mind Sandstorm, süreç içerisinde   
  Sosyal medya operasyonları, Kritik alt yapılara yaplan çeşitli ataklarla süreci kendi lehine çevirmeye odaklı siyasi, diplomatik ve seçmenlere büyük güven kırıklığına da sebeb olmuşlardır.   
    
  Microsoft Tehdit Analiz Merkezi (MTAC), üretici yapay zekanın (generative AI) kötü niyetli kullanımını incelemeye devam ettiğini ve bu çabaların, Microsoft’un 2024 seçimleri sırasında aldatıcı yapay zekâ kullanımı engelleme taahüdüyle uyumlu olduğunu belirtmiştir.   
    
  Sonuç olarak, MTAC'nin gözlemlerine göre, pek çok aktör geçmişte etkili olduğu kanıtlanmış tekniklere dönmeye başladı. Bu teknikler arasında basit dijital manipülasyonlar, içeriğin yanlış aktarımı, sahte bilgilerin güvenilir etiketler veya logolarla desteklenmesi gibi yöntemler yer alıyor.

SONUÇ VE ÖNERİLER

2024 ABD Başkanlık Seçimleri, çok sayıda devlet destekli aktör, organize suç grubu ve hacktivist grup tarafından hedef alınan karmaşık bir siber tehdit ortamında gerçekleşmektedir. Yabancı devletler, paramiliter gruplar ve siber suç örgütleri, ABD seçim sürecine müdahele ederek stratejik çıkarlarını korumaya ve ABD’nin iç istikrarını bozarak toplumsal kutuplaşmayo derinleştirmeye çalışmaktadır. Rapor boyunca ele aldığım tehdit aktörleri ve saldırı yöntemleri, bu grupların seçim sürecini hedef alarak seçim güvenliğini olabildiğince zedelemek ve yıpratmak için kapsamlı bir çaba içinde oldukları ortaya koymaktadır.   
  
Bundan dolayı Şahsi olarak düşünce fikirleri gelecek olası seçimlerde bu ve bu tür olayların engellenmesi/önlem alınabilmesi için;

* Seçim altyapılarına yönelik hibrit ve siber saldırılara karşı önlemler sıkılaştırılmalı ve monitoring sistemler geliştirilmelidir. Özellikle **KV-Botnet** gibi tehditler göz önüne alınarak SOHO yönlendiriciler ve IoT cihazları gibi zayıf noktalara karşı eksta güvenlik önlemleri alınmalıdır.   
  Bu, Rusya ve Çin gibi aktörlerin, bu sistemlere zarar vermek, verileri manipüle etmek veya seçmenlerin oylarının yanlış sayılmasına yol açabilecek müdahalelerde bulunmalarını engelleyecek ve fiziksel ve dijital erişim kanallarını seviyelerini arttırıcaktır.
* Yapay zekâ ile üretilen derin sahte videolar ve manipülatif içerikler, özellikle sosyal medyada hızla yayılabilir. Örneğin, adayları yanlış söylemlerle veya şiddet eğilimli davranışlarla gösteren sahte videolar seçmenleri yanıltarak seçmen algısını değiştirebilir. Rusya ve İran gibi devlet destekli grupların, bu tür içerikleri sosyal medya botları ve sahte hesaplar aracılığıyla yaygınlaştırması beklenmektedir. Bu tür içeriklerin hızla tespit edilmesi ve kaldırılması için sosyal medya platformları ile yakın iş birliği yapılmalı, içerikler için otomatik tespit ve raporlama mekanizmaları geliştirilmeli ve kamuya sahte içerikler hakkında farkındalık eğitimleri verilmelidir. Gelişmiş yapay zekâ tabanlı derin sahte tespit araçları uygulanmalıdır.
* Yabancı tehdit aktörleri, seçmenlerin kişisel bilgilerini ele geçirerek, kimlik avı saldırıları yoluyla onları kandırma veya yanıltma riski taşımaktadır. Özellikle seçim gününde seçmenlere yönelik sahte mesajlar veya e-postalar gönderilerek oy kullanmalarını engellemeye yönelik girişimlerde bulunulabilir. Bu tür saldırılar seçmenlerin özel bilgilerini ifşa ederek onları tehdit etmek için de kullanılabilir. Bundan ötürü, Seçmen bilgileri hassas bir şekilde korunmalı, güvenlik protokolleri sıkılaştırılmalı ve seçmenlere yönelik kimlik avı saldırılarına karşı farkındalık artırılmalıdır.
* Seçim merkezlerinde paramiliter grupların varlığı, fiziksel tehditler ve seçmenlerin sandıklardan uzak durmasına neden olabilir. Özellikle "Ballot Box Watching" gibi eylemlerle, belirli grupların seçim merkezlerinde seçmenleri gözdağı verici bir şekilde izlemeye çalışması, toplumsal güvenliğe yönelik riskleri artırabilir. Bu tür gruplar, seçim günü protesto ve gösteriler düzenleyerek şiddet olaylarını tetikleyebilir. FBI ve CISA bu olaylardan ders çıkararak seçim merkezlerinde güvenliği sağlamak için güvenlik güçleri hazır bulunmalı ve seçmenlerin güvenliğini sağlamak adına güvenli oy kullanma alanları oluşturulmalıdır.   
  Halkın bu ve bu tarz olaylara tekrar baş kaldırmaması adına da yasa dışı hareket edenler için yasal yaptırımlar uygulanmalıdır.   
    
  2024 ABD Başkanlık Seçimleri, ABD demokrasisi ve ulusal güvenlik için kritik bir test niteliği taşımaktadır. Devlet destekli siber tehdit aktörleri, seçim sürecine olan güveni zedelemek, toplumsal kutuplaşmayı artırmak ve ABD’nin uluslararası imajını sarsmak amacıyla tüm imkanlarını seferber etmektedir. Bu raporun sunduğu analiz ve öneriler doğrultusunda ABD İstihbarat Topluluğu ve ilgili tüm kurumlar, seçim sürecinin güvenliğini sağlamak için kapsamlı bir koordinasyon ve iş birliği içerisinde hareket etmelidir. Unutulmamalıdır ki, **seçim güvenliği sadece siber bir mesele değil, aynı zamanda bir demokrasi meselesidir.**