infoblox

DECOY DOG SIRADAN BİR PUPY DEĞİL:

Sinsi bir DNS Kötü Amaçlı Yazılımını Paketten Ayırma

İÇERİK TABLOSU

GÖSTERGELER 33

Yönetici Özeti

Decoy Dog, Infoblox tarafından keşfedilen ve komut ve kontrol (C2) gerçekleştirmek için alan adı sistemini (DNS) kullanan bir kötü amaçlı yazılım araç setidir. Güvenliği ihlal edilmiş bir istemci, DNS sorguları aracılığıyla bir denetleyiciyle iletişim kurar ve ondan talimat alır. Bu denetleyici, sorguların normal çözümleme işlemiyle iletildiği bir DNS ad sunucusuna entegre edilmiştir. Decoy Dog'un varlığını Nisan 2023'te açıkladık ve 23 Nisan'da ilk bulgularımızın ayrıntılı bir raporunu yayınladık. Keşif, DNS verilerinin izlenmesine dayanıyordu. O sırada yapılan analizler, araç setinin Pupy olarak bilinen bir uzaktan erişim truva atına (RAT) dayalı olarak oluşturulduğunu doğruladı, ancak hangi sistemlerin istismar edildiği, araç setinin nasıl dağıtıldığı veya Pupy'nin değiştirilip değiştirilmediği bilinmiyordu.[1] Sağladığımız ayrıntılarla, topluluktaki diğer kişilerin güvenliği ihlal edilmiş makineleri bulmasını ve tüm hikayenin bilinmesini bekliyorduk. Ancak, Decoy Dog'u çevreleyen gizem daha da büyüdü.

Nisan ayından bu yana Infoblox, Decoy Dog ve Pupy hakkında daha fazla araştırma yaptı. Bu rapor o araştırmanın sonucudur. Decoy Dog'un Pupy için genel depoda olmayan komutları ve yapılandırmaları kullanan büyük bir yükseltme olduğunu öğrendik. Decoy Dog istemci iletişimlerini ayırmak ve her denetleyici hakkında bir dizi başka özellik çıkarmak için algoritmalar geliştirdik. Bu da araç setinin yayıldığı ve en az üç saldırganın kontrolü altında olduğu sonucuna yüksek bir güvenle varmamızı sağlıyor. Gözlemlediğimiz faaliyetler Rusya ve Doğu Avrupa ile sınırlı kalırken, denetleyiciler arasında birden fazla aktörle tutarlı farklı teknik, taktik ve prosedür (TTP) grupları bulunmaktadır.

Her Decoy Dog aktörü Nisan ayındaki açıklamalarımıza bir şekilde yanıt verdi ve varyasyonlar birden fazla operatör olduğuna ilişkin değerlendirmemizi destekliyor. Sosyal medyadaki ilk duyurunun hemen ardından bazı ad sunucuları kapatıldı. Geri kalanların tümü, ilk makalemizde vurguladığımız davranışları ortadan kaldırmak için değiştirildi, ancak bu, denetleyiciye bağlı olarak farklı şekillerde gerçekleştirildi. Bir dizi denetleyici, coğrafi sınırlama adı verilen bir teknikle sorguların geldiği ülkeye bağlı olarak yanıtları kısıtlamaya başlarken, diğerleri ping alt alanı için sorgulara verdikleri yanıtları değiştirdi.

Bir aktör, LinkedIn'deki açıklamamıza o kadar hızlı yanıt verdi ki, başlangıçta yeni alanların güvenlik araştırmacıları tarafından yapılmış taklit kayıtlar olduğunu düşündük. Ancak daha ileri analizler bunların yedek alanlar olduğunu gösterdi. Aktör, faaliyetlerini durdurmak yerine, mevcut tehlikeye atılmış müşterileri yeni denetleyicilere aktardı. Bu, aktörün mevcut kurbanlarına erişimini sürdürme ihtiyacı hissettiğini gösteren olağanüstü bir tepki. Decoy Dog alanlarının bir setinin TTP'leri ile diğerleri arasında net bir ayrım yarattı.

Duyurumuzu takip eden haftalarda, Decoy Dog'un faaliyet göstermesini sağlayan temel kötü amaçlı yazılımı ve güvenlik açığını tespit etmek için kimsenin ortaya çıkmamasına şaşırdık. Ancak araştırmamız ilerledikçe, iletişimin neden bir yılı aşkın bir süre boyunca tespit edilemediği anlaşıldı. Decoy Dog kullanılarak yapılan saldırılar son derece hedefe yöneliktir ve her bir denetleyicinin az sayıda aktif istemcisi var. Bazı sunucular, aylarca sürekli olarak dört ila sekiz aktif istemciyi sürdürmüştür. Diğerlerinde zaman içinde aynı anda aktif olan istemci sayısında artış görülürken, herhangi bir zamanda gözlemlenen etkilenen cihaz sayısı 100'den az olmuştur. Küçük bir kurban grubu genellikle mali motivasyonu olan aktörler ihtimalini ortadan kaldırır ve bir cihazda uzun süre kalma ihtiyacı son derece gelişmiş aktörlerle tutarlıdır.

Kendi Pupy trafiğimizdeki imzaları tespit ederek Decoy Dog iletişiminin bazı bölümlerini yeniden yapılandırabildik. İnternette bir Pupy sunucusu kurduk, bu da kodun seçici tersine mühendisliği ile birleştirildiğinde, DNS sorgularını ve yanıtlarını belirli Pupy komutlarıyla ilişkilendirmemizi sağladı. Bu sayede a) Decoy Dog'un Pupy'de bulunmayan komutlar içerdiğini tespit edebildik ve b) iletişimlerin çoğunun karakterini belirledik. Ek olarak, görünüşe göre Decoy Dog aktörleri anahtar değişimi gibi işlevler için DNS dışındaki

1 https://github.com/n1nj4sec/pupy

diğer taşıma katmanlarını kullanmak üzere Pupy'den yararlanıyor. Tehdit aktörleri muhtemelen bunu Pupy'nin bir uzaktan erişim truva atı (RAT) olarak avantajlarından biri olarak görmektedir.

Decoy Dog araç setinin bilinen ilk dağıtımı Mart ayı sonlarında veya Nisan 2022'nin başlarında gerçekleşti. Mayıs ortasına kadar aktif olan farklı TTP'lere sahip ikinci bir denetleyicinin ortaya çıkmasından da anlaşılacağı üzere, kısa bir süre sonra satılmış ya da çalınmıştır. Temmuz 2022'de üçüncü bir alan adı kaydedildi ve stratejik olarak Eylül ayına kadar yaşlandırıldı. Bu son iki denetleyicinin, Rus IP alanında barındırma da dahil olmak üzere birçok özelliği paylaşmaları nedeniyle aynı aktöre ait olması mümkün. Ancak aralarında bazı farklılıklar var. Birkaç ay sonra, yine önceki denetleyicilerden farklı özelliklere sahip iki alan adı daha kaydedildi. Bu alan adlarını kaydeden aktör, açıklamamızın hemen ardından istemcileri yeni alan adlarına taşıdı. Infoblox şu anda toplamda 21 Decoy Dog alan adını izliyor ve bunlardan bazıları geçen ay içinde tescil edilip kullanılmaya başlandı.

DNS günlüklerinin analizimiz aracılığıyla Decoy Dog'un Pupy'den önemli ölçüde farklı olduğunu belirledikten sonra, yürütülebilir dosyalarda farklılıklar olup olmadığını görmek için VirusTotal'da mevcut olan ilgili ikili örnekleri inceledik. Bu örneklerin ters mühendisliği, Pupy olarak tespit edilmelerine rağmen, açık kaynak sürümünden çok daha gelişmiş olduklarını gösterdi. Örnekler arasında a) istemcide keyfi Java kodu çalıştırma yeteneği, b) birkaç yeni taşıma mekanizması ve c) kalıcılığı sağlamak için yeni DNS mekanizmaları bulunmaktadır. Mekanizmalardan biri geleneksel DNS alanı oluşturma algoritmasına (DGA) benzer ve sözde acil durum denetleyicilerine bağlanmak için ücretsiz dinamik DNS sağlayıcıları kullanıyor. Tüm örnekler aynı temel güncellemeleri paylaşsa da örneklerden biri, akış aktarımlarının kullanımıyla ilgili olarak diğerlerinde görülmeyen benzersiz yeteneklere sahip.

Belirsizliğini koruyan nedenlerden ötürü Decoy Dog, genellikle içeriğin bir düşman tarafından tespit edilmesini ve kurtarılmasını önlemeyi amaçlayan gizli iletişimin temel ilkelerini ihlal etmektedir. Normal Pupy sunucuları güvenliği ihlal edilmiş istemcilerden tekrarlanan iletişim sorgularını reddederken, Decoy Dog sunucuları yalnızca tekrarlanan DNS sorgularına yanıt vermekle kalmaz, aynı zamanda iyi hazırlanmış herhangi bir sorguya da yanıt verir. Bu davranış, DNS'deki joker karakter yapılandırmalarına benzer ve Infoblox tarafından Decoy Dog'un algılanmasında önemli bir faktördü. Decoy Dog'un karmaşıklığı göz önüne alındığında, tekrar oynatma ve joker karakter davranışının tasarımdan kaynaklandığını tahmin ediyoruz; niyet ne olursa olsun, DNS'nin yaygın şekilde tekrarlanması, sektörün Decoy Dog'u yeni bir kötü amaçlı yazılım olarak görememesinin kısmen sorumlusuydu.

Bir güvenlik satıcısı tarafından yapılan agresif internet taraması, müşterilerimizin birçoğu da dahil olmak üzere küresel ağlar aracılığıyla milyonlarca Decoy Dog iletişiminin yeniden iletilmesine yol açtı. Bu da araç setini keşfetmemizi sağladı. Satıcının sorguları tekrar oynatmaktan kaçınmak için trafiği kötü amaçlı yazılım olarak tanımlayamaması, virüs bulaşmamış ağlardan Decoy Dog denetleyicilerine DNS bağlantılarını tetikledi. Hiçbir Infoblox müşterisine virüs bulaşmadığından ve çözümleyicilerimize yapılan sorguların hepsinin anormal satıcı taramasının bir sonucu olduğundan eminiz. Müşteri ağlarımız için acil tehdit olmamasına rağmen, Decoy Dog, kökenleri belirsiz olan sofistike bir araç seti olmaya devam ediyor ve yayılmaya devam edebilir.

Decoy Dog sadece vahşi doğada yeni gözlemlenmekle kalmıyor, aynı zamanda bildiğimiz kadarıyla, Pupy'nin DNS C2 bileşeninin kötü amaçlı bir işlemde ilk kullanımı. Bunun nedeni kısmen depodaki yazılımı değiştirmeyi ve DNS'yi düzgün bir şekilde yapılandırmayı gerektiren bir Pupy ad sunucusu kurmanın zorluğu. Bu durumun açığa çıkmaması, güvenlik sektörünün hem Pupy hem de Decoy Dog'u algılamasını ve bunlara karşı savunma yapmasını zorlaştırmaktadır. Bu C2 sistemlerini kullanan operasyonları bozmaya yardımcı olmak için, topluluğa kendi sunucumuzdan yakalanan Pupy DNS trafiğini ve yazılımın iç işleyişinin ayrıntılarını içeren bir araştırma veri kümesi sağlıyoruz. Bu dokümantasyon türünün ilk örneğidir ve başkalarının da tespit algoritmaları oluşturmasına ve bulgularımızı yeniden üretmesine olanak tanıyacaktır.

Decoy Dog'un hikayesi, bir tehdit tespit ve müdahale kaynağı olarak DNS'nin gücünü ortaya koymaktadır. Ayrıca, güvenlik sektörüne hakim olan kötü amaçlı yazılım merkezli istihbarat ekosisteminin doğasında var olan bir zayıflığı da ortaya koyuyor. Araç seti, DNS tehdit tespit algoritmaları tarafından keşfedildi ve bugün buna karşı tek savunma DNS'dir. Üstelik, birkaç denetleyici alanını şüpheli olarak işaretlemiştik ve hepsinin ortak bir kötü amaçlı yazılım kullandığını fark etmeden önce bunları çözümleyicilerimizde engelliyorduk. Kötü niyetli faaliyetleri henüz tespit edilmeden ve çoğu zaman faaliyete geçmeden engelleyen bu koruma türü, DNS tespit ve yanıt sistemlerine özgüdür.

Bu makalede savunuculara Pupy ve Decoy Dog'u tanımlamak için bilgi sağlıyoruz. DNS C2'yi derinlemesine tanımlayacak olsak da, kötü niyetli kişilerin Pupy'yi dağıtmasına yardımcı olacak bilgiler sağlamayacak ve Decoy Dog DNS imzasının tamamını ifşa etmeyeceğiz. Orijinal makalemizde tanımladığımız bazı davranışları açıklıyor ve Decoy Dog'un Pupy'den nasıl farklı olduğunu vurguluyoruz. Ayrıca, kötü amaçlı yazılımın kendisine sahip olmadan veya ad sunucusunu kontrol etmeden istemci sayısını ve komut trafiğini tahmin etmemizi sağlayan büyük hacimli Decoy Dog DNS trafiği analizimizi açıklayacağız. Decoy Dog örneklerinin Pupy örneklerinden nasıl farklı olduğunu açıklıyoruz. Son olarak, Decoy Dog operatörlerinin açıklamalarımıza nasıl tepki verdiklerini tartışıyor ve denetleyicilerin alt grupları arasındaki ortak özellikleri gösteriyoruz. Ekler, ilave destekleyici teknik bilgiler içermektedir.

ARKA PLAN

Infoblox, Nisan 2023'ün başlarında alan adı sistemini (DNS) kullanan bir komuta ve kontrol (C2) araç seti olan Decoy Dog'u keşfetti. Bu araç seti Pupy[2] adlı açık kaynaklı bir uzaktan erişim truva atına (RAT) dayanmaktadır ve istemciler ile sunucular veya denetleyiciler arasındaki şifreli iletişimi alan adı sorguları ve IP adresi yanıtları aracılığıyla aktarır. Keşif, anormal davranışlar için Infoblox çözümleyicilerine pasif DNS sorgularını izleyen algoritmalardan kaynaklandı. Decoy Dog alanları için sorgular, az sayıda müşteri ağındaki güvenlik cihazlarından yapılmıştı. Bu sorgular kalıcı, düşük profilli kötü amaçlı yazılım işaretleriyle tutarlı bir imza oluşturdu. İnsanların faaliyeti incelemesi endişe vericiydi çünkü DNS açıkça gizli bir iletişim kanalı olarak kullanılmasına rağmen, alan adları kamuya açık herhangi bir istihbarat verisinde C2 olarak tanımlanmamıştı. Hatta bazıları çevrimiçi itibar denetleyicilerinde "saygın" olarak etiketlendi. Topluluğun trafiği engellemesine ve tehlikenin niteliğini belirlemesine yardımcı olmak için 13 Nisan'da bir dizi alan adı yayınladık.

Orijinal araştırmamız sırasında Infoblox, Pupy yazılımından bağımsız benzersiz bir DNS imzası belirledi. Aktörler C2 sistemlerini çok özel bir şekilde konuşlandırmış ve işletmişlerdi; bu nedenle Decoy Dog'u farklı bir araç seti olarak tanımladık. Dünya çapında yalnızca az sayıda alan adı bu imzayı paylaşıyordu ve bunların hepsi Decoy Dog ad sunucularıydı.

23 Nisan'da imzanın bir kısmını, pasif DNS'in ilk analizini ve denetleyici alanlarının bir alt kümesini "Dog Hunt: Finding Decoy Dog Toolkit in Anomalous DNS Traffic"[3] adlı raporumuzda yayınladık. Bu makale, 'ping' içeren belirli alt alan adlarına. yönelik sorgulara bir dizi localhost yanıtı döndüren Pupy'nin belirli bir davranışını vurguladı. Ayrıca, DNS iletişiminde o sırada tam olarak açıklayamadığımız bir dizi eğilimi de tanımladı. Özellikle, yanıtlarda döndürülen IP adreslerinde ve sunucuların gizli bir iletişim sistemi için beklenmedik bir şekilde tekrarlanan sorgulara yanıt vermesinde şaşırtıcı modeller belirledik.

Duyuruların ardından, satıcılar ve diğer kuruluşlar da dahil olmak üzere güvenlik topluluğunun çok çeşitli üyeleri bizimle iletişime geçti. Birçoğu kendi ağlarında veya müşteri ağlarında ilgili trafiği görmüş, ancak hiç kimse tehlikeye atılmış cihazları tanımlamamış veya faaliyetin kapsamını fark etmemişti. Bu kuruluşlardan bazıları, DNS'nin kendi ağlarımızda nasıl

2 https://malpedia.caad.fkie.fraunhofer.de/details/win.pupy

3 https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/dog-hunt-finding-decoydog-toolkit-via-anomalous-dns-traffic/

oluşturulduğunu izole etmemizi ve doğrulamamızı sağlayan bilgiler verdi. Diğerleri faaliyetin kapsamının doğrulanmasına ve hipotezlerin test edilmesine yardımcı oldu. Bu gayriresmi işbirliği çok yararlıydı ve minnettarız.

Basitlik açısından, bu makalede Pupy terimini genel olarak Pupy'ye değil, özel olarak Pupy DNS C2'ye atıfta bulunmak için kullanıyoruz.

Pupy

NADİR BİR TÜR

Pupy, karmaşık bir modüler taşıma sistemine sahip açık kaynaklı bir istismar sonrası uzaktan erişim truva atıdır (RAT).[4] Birincil Pupy kod tabanı 2015 yılında GitHub'da kullanıma sunulmuş olsa da DNS C2 mekanizması 2019 yılına kadar eklenmemiştir. Bu makale Pupy C2'nin halka açık ilk belgelendirmesidir. Ayrıca, başkalarının hem çalışmalarımızı yeniden üretmesi hem de gelecek için savunmalar oluşturması için GitHub'da bir veri kümesi sağlıyoruz.

Pupy açık kaynak olmasına rağmen DNS C2 protokolünün kullanımı nadirdir; Decoy Dog dışında vahşi doğada kullanımını tespit edemedik.[5] ünyanın dört bir yanındaki kuruluşlara ve kurumlara hizmet veren kendi çözümleyicilerimizde, tarihsel olarak Pupy DNS C2 kullanımına ilişkin hiçbir kanıt bulamadık. Pupy için geliştirdiğimiz DNS algılayıcılarını kullanarak 2023'ün ilk altı ayı için küresel pDNS içinde, Decoy Dog dışında yazılımın kullanılmadığını tespit ettik. Son olarak, çok çeşitli satıcılara özel olarak sorduk; hiçbiri de kullanıldığını görmedi. Pupy'nin gelişmiş kalıcı tehdit (APT) aktörleri tarafından kullanıldığının rapor edildiği yerlerde, görünüşe göre DNS C2 bileşenleri kullanılmamıştır.[6]

Pupy'nin nadir kullanımı, muhtemelen, en azından kısmen, sistemi çalıştırmadaki zorluktan kaynaklanıyor. Küresel DNS üzerinden Pupy iletişimi kurmak kolay değil. Ad sunucusunu doğru bir şekilde yapılandırmayı ve GitHub deposundaki kodu değiştirmeyi gerektiriyor. Ek olarak, DNS'de Pupy yazılımının doğru şekilde işlemediği özyinelemeli çözümleyiciler arasında değişen karmaşıklıklar var. Bu zorluklar, oldukça sık gördüğümüz Cobalt Strike gibi popüler araçların aksine, hem kırmızı ekipler hem de bilgisayar korsanları tarafından benimsenmesini muhtemelen engelledi.[7]

Pupy DNS C2 bugün nadir olmasına rağmen, Decoy Dog kullanımı yayılıyor ve savunucuların bir şekilde Pupy ile karşılaşma olasılığı artıyor. Topluluğun hazırlanmasına yardımcı olmak için Infoblox, hem Decoy Dog hem de Pupy üzerinde önemli araştırmalar yaptı. Infoblox, davranışını Decoy Dog ile karşılaştırmak için İnternet'te bir Pupy sunucusu dağıttı. Daha sonra Infoblox çözümleyicilerinden paket verilerini (pcap) ve pasif DNS günlüklerini yakaladık. Decoy Dog'un benzersiz doğasını daha iyi anlamak için Pupy dağıtımımızı kodun seçici olarak ters mühendisliği ile birlikte kullandık. Bu bölümde, Pupy'nin araştırmamızla ilgili bileşenlerini açıklıyoruz. Basitlik için, bu makaleyi IPv4 (A kaydı) yanıtlarını kullanan iletişimlerle sınırlıyoruz, ancak mevcut olduğunda Pupy IPv6 (AAAA) yanıtlarını kullanacaktır. Makalede açıklanan sorgu kodlaması, Pupy sürüm 2 için geçerli varsayılandır (aksi belirtilmedikçe).[8]

---

4 https://github.com/n1nj4sec/pupy

5 "Vahşi doğada" ifadesi, siber güvenlik dilinde, izole penetrasyon testi veya araştırmanın bir parçası olmayan operasyonel olarak konuşlandırılmış anlamına gelmek için kullanılır.

6 https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/

7 https://www.esecurityplanet.com/threats/how-cobalt-strike-became-a-favorite-tool-of-hackers/

8 Pupy C2'nin önceki bir sürümü her sorguda ana bilgisayar bilgilerini içermiyordu. Artık Decoy Dog'un istemcinin 3. sürümü olduğunu biliyor olsak da sorgu kodlaması sürüm 2 ile aynı görünüyor.

PUPY'NİN İŞLEYİŞ ŞEKLİ

Bir önceki makalemizde Pupy hakkında genel bir bilgi vermiş ve Decoy Dog'un bazı olağandışı özelliklerini vurgulamıştık.[9] Bu makalede, Pupy iletişim protokolünün Decoy Dog ile bağlantılarını ve devam eden bir operasyonu anlamak için pasif olarak toplanan Pupy DNS'lerinden nasıl yararlanılacağını göstermek için daha ayrıntılı olarak inceleyeceğiz.

Pupy, virüs bulaşmış istemciler ve sunucu arasında sürekli iletişim sağlamak üzere tasarlanmıştır. Böylece aktör istemciye uzaktan erişmek istediğinde bağlantı zaten kurulmuş olur. Aktör, bağlı istemcileri izleyebilir ve onlara çok çeşitli işlemler sunmaları için seçici olarak komut verebilir. DNS yalnızca C2 iletişimleri için kullanılır. İstemciden sızan tüm önemli veriler Pupy tarafından sunulan diğer birçok aktarım seçeneğinden biri üzerinden gönderilir. Sonuç olarak, Pupy DNS istemcisi denetleyiciyi kontrol etmek, komutları onaylamak, sistem bilgisi sağlamak ve diğer birkaç görevle sınırlıdır. Sunucudan gelen komutları işleme arasında istemci uyur.

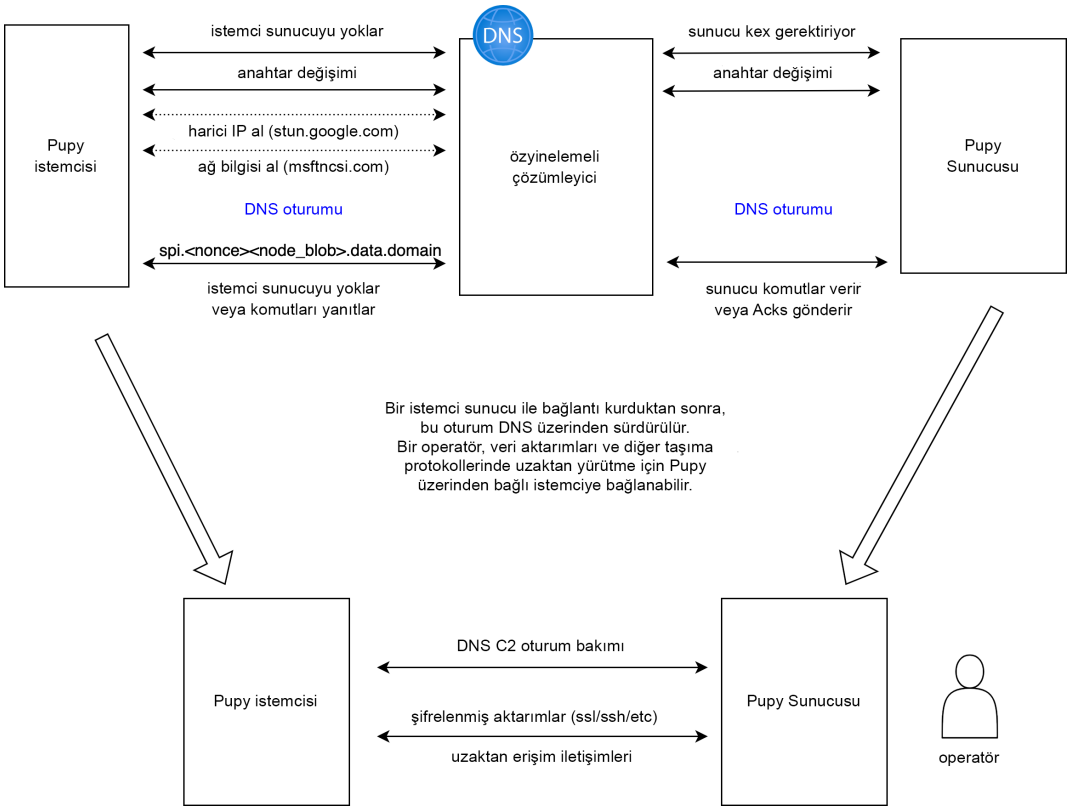
DNS iletişimleri istemci tarafından başlatılır ve sürdürülür. İstemci, etkinleştirildiğinde ve kullanılabilir olduğunda sorguları normal DNS çözümleme yolu veya HTTPS üzerinden DNS (DoH) aracılığıyla gönderir.[10] Denetleyici, istemci isteklerine yanıt olarak şifreli IP adresleri biçiminde komutlar gönderir. Her sorgu yanıtı tam bir iletişimdir, yani ne istemci ne de sunucu tek bir komut için verileri iki DNS sorgusuna bölemez. Bu protokol, istemcinin iletişimi işlemek için her iki uçta da birkaç paketin yeniden yapılandırılmasını içerebilecek DNS üzerinden bir oturum oluşturduğu Iyotine[11] gibi yaygın DNS tünel sistemlerinden farklıdır. İstemci çoğu komutu onaylamakla yükümlüdür ve sunucu her geçerli istemci sorgusuna komutlar veya onay ile yanıt verir. İstemci kelime dağarcığı son derece sınırlıdır. Oturumları yönettiği, komutları onayladığı, sistem bilgilerini gönderdiği ve anahtarları oluşturduğu dokuz tür sorguya sahiptir. Ek işlevler yazılarak özel komutlar eklenebilir, ancak yazılımın tam olarak anlaşılmasını gerektirir.

Uyandıktan sonra istemci, paylaşılan bir anahtarın oluşturulup oluşturulmadığına bağlı olarak sunucuyu iki farklı yoldan biriyle sorgular. Bu sorgu sunucuya Pupy istemcisinin sistemi ve durumu hakkında güncel bilgiler sağlar veya yeni bir şifreli oturum başlatmaya yarayan basit bir sorgu yapar. Şifrelenmiş oturumları devre dışı bırakmak mümkün olsa da, bu varsayılan değildir ve Decoy Dog'da gözlemlenmemiştir. Yanıt olarak denetleyici isteği onaylar, istemcinin bir anahtar değişimi gerçekleştirmesini ister veya yeni komutlar gönderir. Tüm komut seti tamamlandığında, istemci varsayılan olarak 60 saniye olan belirlenen aralık boyunca uyuyacaktır. Bu süreç istemci çalışırken tekrarlanır. Pupy istemci-sunucu iletişimine üst düzey bir genel bakış Şekil 1'de gösterilmektedir ve istemci sürecinin daha ayrıntılı bir görünümü Ek A'da bulunabilir.

9 https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/dog-hunt-finding-decoy-dog-toolkit-via-anomalous-dns-traffic/

10 Pupy, DoH için varsayılan olarak Quad9 sunucularını kullanır.

11 https://github.com/yarrick/iodine



Şekil 1. Pupy iletişimlerine üst düzey bir genel bakış.

Pupy aktörü, denetleyici komut satırı yardımcı programından istemcilerle etkileşime girer. İstemci denetleyiciyle iletişim kurduğunda, kuyruğa alınan tüm komutlar DNS yanıtında kodlanır. Operatör, bir istemci açık portunda bağlantı kurar ve sızma için kullanılacak taşıma katmanını belirtir. Sunucu DNS iletişimleri, istemciden daha kapsamlı olmasına rağmen hala oldukça kısıtlıdır. Çok çeşitli komutlar vardır ve bunlar istemciye verilen tek bir yanıtta birleştirilebilir. İstemci iletişim alışverişini başlatırken, sunucu iletişimin güvenliğinin sağlanmasından sorumludur. Bunu, her istemciyle şifreleme anahtarlarını döndürmeye yarayan oturumlar adı verilen oturumları zorlayarak yapar. Bu bir sonraki bölümde açıklanmaktadır.

OTURUM BAŞLATMA

Pupy, aktörün komutlarını iletmeden önce istemci ve denetleyici arasında şifreli bir oturum kurulmasını gerektirir. Bu oturum, istemci iletişimleri zaman aşımına uğradığında sona erer ve DNS sorgu çözümlemesindeki hatalar veya istemcinin yeniden başlatılması gibi diğer nedenlerle yenilenmeye zorlanabilir. Oturumlar, sorguda bir güvenlik parametresi dizini (SPI) etiketinin varlığıyla tanımlanır ve geçici bir paylaşılan anahtar kullanılarak şifrelenir. İletişim ayrıntıları, istemcinin daha önce sunucuya bağlanıp bağlanmadığı da dahil olmak üzere çeşitli faktörlere bağlı olduğundan, oturum başlatmaya yönelik tam protokol farklılık gösterebilir ve gözlemlenen DNS değişimlerinde farklılık yaratabilir. Bununla birlikte, tipik değişim aşağıdaki gibidir:

- İstemci sunucuya ya kurulmuş bir oturum olmadan ya da süresi dolmuş bir oturumla giriş yapar (sorgu 1).
- Sunucu, anahtar değişimi ve istemci sistem bilgisi gerektiren bir komutla yanıt verir.[12]

12 Bu genellikle sunucu tarafında Politika ve Yoklama olarak adlandırılan iki komut şeklindedir.

- Müşteri, sistem bilgisi gereksinimini kabul eder (sorgu 2).
- İstemci eliptik eğri algoritması kullanarak rastgele bir özel-genel anahtar çifti oluşturur ve bunu sunucuya gönderir; sunucu da aynısını yapar ve yeni anahtarlarıyla yanıt verir (sorgu 3).
- İstemci ve sunucu, paketleri AES şifrelemeyle şifrelemek için kullanılan yeni bir paylaşılan oturum anahtarı oluşturmak ve ayrıca oturumu tanımlamak için SPI'yi oluşturmak için bu alışverişi kullanır.
- İstemci, diğer hizmetlere ek DNS sorguları kullanarak harici IP adresi de dahil olmak üzere ağı hakkında bilgi toplar.
- İstemci bu bilgiyi paylaşılan şifreleme anahtarını kullanarak ve SPI'nın sorguya dahil edilmesiyle aktif bir oturumun varlığına işaret ederek iletir (sorgu 4).
- İstemci ek sistem durumu bilgileri gönderir (sorgu 5).

Anahtar değişimi teknik olarak tek bir sorgu ve yanıt olmasına rağmen, paylaşılan anahtar ve SPI genellikle üç sorgudan sonra oluşturulur. Bir oturum sırasında, her sorgu ve yanıt bu paylaşılan anahtar kullanılarak şifrelenecektir. Şifreleme ayrıca istemci tarafından oluşturulan ve her sorgu için değişen 32 bit nonce kullanır. Yeni bir oturum oluşturulduğunda, anahtarlar yeniden oluşturulur, ancak istemci nonce değeri istemci çalışırken devam eder. Bu konu aşağıdaki bölümde daha ayrıntılı olarak ele alınmıştır.

SORGU KODLAMA

İstemci, sunucuyla şifrelenmiş iletişimler içeren sorgular oluşturur. Bunlar anahtar değişim bilgilerini veya sunucudan gelen komutlara verilen yanıtları içerebilir. Her sorguda iletilebilecek maksimum 52 bayt aktarılan veri vardır. Aktarılan verilere ek olarak, her sorgu şunları içerir:

- nonce, istemci tarafından oluşturulan 4 baytlık bir artış değeri
- sürüm, Pupy DNS C2 sürümünü belirten 1 baytlık bir değer
- cid, istemcinin yapılandırmasından 4 baytlık bir değerdir ve istemci oluşturulurken rastgele oluşturulur
- iid, Pupy istemci sürecinin alt 16 bitini içeren 2 baytlık bir değer
- node id, istemciden gelen 6 baytlık bir değer, tipik olarak cihazın MAC adresi
- isteğe bağlı olarak, SPI, anahtar değişimi sırasında oluşturulan ve belirli bir istemci için sunucudaki bir oturumu temsil eden sorgularda bulunan 4 baytlık bir değer.

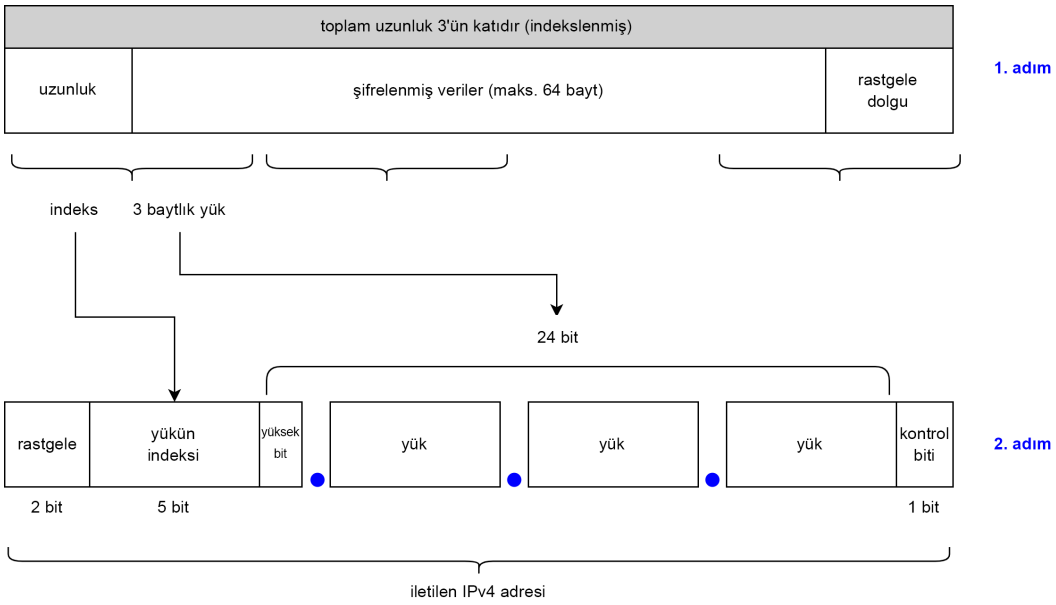
Her istemci sorgusu bu 13 baytlık istemci bilgisinin yanı sıra temel yük üzerinde 4 baytlık bir sağlama toplamı içerir. Temel yük şifrelenmiştir ve bir dizi komut ve ilgili verilerden oluşur.

İstemci, sunucuya iletilecek verileri DNS protokolünde sorgu adı (qname) olarak adlandırılan tam nitelikli bir alan adı (FQDN) olarak şifreler ve kodlar. Aşağıdaki Şekil 2'de gösterilen tüm süreç, hem iletilen verilerin hem de sunucu tarafından ihtiyaç duyulan ek bilgilerin şifrelenmesini, düzenlenmesini ve kodlanmasını içerir. Aşağıdaki gibi çalışır:

- İletilecek veriler, ana bilgisayara özgü bilgilerle eklenir.
- Bu bileşik bayt dizesi, paylaşılan bir simetrik anahtar ve geçerli nonce kullanılarak şifrelenir.
- İletilen verinin ilk şifrelenmiş baytı, 35 bayta kadar, kodlanır ve qname'in ilk veya en sağdaki etiketi için kullanılır.
- İletilen verinin en fazla 17 baytını içerebilen şifrelenmiş baytların geri kalanının başına geçerli nonce değeri eklenir ve qname'in ikinci etiketini oluşturmak için kodlanır.

- Güvenlik parametresi indeksi (SPI) istemcide mevcutsa, kodlanır ve qname'in üçüncü veya en soldaki etiketinde kullanılır; bu değer sunucuyla yapılan bir anahtar değişiminin ardından ayarlanır.
- Nonce, bir sonraki sorgu için kullanılmak üzere istemci içindeki şifrelenmiş verilerin uzunluğu kadar artırılır.

Şifrelenmiş baytlardan bir alan adı etiketine kodlama önceki makalemizde açıklanmıştır. Nihai sonucun geçerli bir alan adı olmasını sağlamak için 32 bit kodlama ile birlikte özel bir eşleme kullanır. Temel veri yükü yapısı Ek B'de açıklanmıştır.



Şekil 2. Bir DNS sorgusu için istemciden gelen verileri bir qname'e dönüştürme işlemi. Temel alan adı Pupy sunucusunun alan adıdır.

Pupy, DNS sorgularını şifrelerken varsayılan olarak AES'i kullanır. İstemci ile paylaşılan bir anahtar oluşturulmuşsa, tam bayt dizesini simetrik olarak şifrelemek için bunu kullanır, aksi takdirde oluşturulan ortak anahtarı kullanır. Her iki durumda da, temelde iletilen veriler birden fazla sorguda aynı kalsa bile, kodlanmış sorgunun benzersiz olmasını sağlamak için şifrelemede geçerli nonce da kullanılır. Bu, kriptografik saldırılara karşı koruma sağlayan standart bir mekanizmadır. Sonuç olarak, sorgulanan alan adı şifrelenmiş veriyi ortaya çıkarmak için çözülebilir, ancak şifrelenmiş verinin şifresi anahtar olmadan çözülemez. Nonce değeri rastgele 32 bitlik bir değerle başlatılır ve her sorguda yükün uzunluğu kadar artırılır.

Pupy ad sunucusu bir sorgu aldığında, SPI değerini, nonce'u ve şifrelenmiş yükü ortaya çıkarmak için alan adının kodunu çözer. Geçerli istemci iletişimi aldığından emin olmak için sunucu, SPI'ın mevcut olduğunda geçerli olup olmadığını ve nonce'un istemci için kaydedilen bir önceki değerden daha büyük olup olmadığını kontrol eder. Veri üzerinde, yükte şifrelenmiş olan sürüm numarasının kontrolü de dahil olmak üzere başka kontroller de yapar. Bu kontrollerden herhangi biri başarısız olursa istemciye bir hata döndürülür.

Özellikle, Pupy aynı sorguya iki kez cevap vermez ve değiştirilmemiş herhangi bir Pupy sunucusu, geçmişte zaten aldığı bir sorguya bir NXDOMAIN (böyle bir alan adı yok) ile yanıt verecektir. Bu davranışı, daha önce sorgulanmış bir alan adını sorgulamaya çalışarak kendi Pupy sunucumuzla doğruladık. Decoy Dog'un bir özelliği, yeniden oynatılan DNS sorgularına Pupy C2 protokolüyle tutarlı cevaplarla yanıt vermesi olduğundan bu önemli bir noktadır.

DNS sorgusu nonce'un tersine çevrilebilir bir kodlamasını içerdiğinden ve nonce her sorguda yük uzunluğu kadar arttığından, tek bir istemciyle ilişkili sorgu dizilerini yeniden yapılandırabiliriz. Bu makalede daha sonra göreceğimiz gibi, bir Pupy veya Decoy Dog alanı için pasif DNS koleksiyonu verildiğinde, bu yeniden yapılandırmayı istemci sayısını ve belirli durumlarda iletişimin doğasını tahmin etmek için kullanabiliriz.

ÖZEL ALAN ADI İŞLEME

Bir sorgu alındığında, sunucu sorgu adını inceler ve bir istemciden gelen şifrelenmiş bir paket için uygun yapıyla eşleşip eşleşmediğini belirler. Benzersiz işlemeye sahip birkaç özel durum vardır. Bu özel durumlar dışında, beklenen formatı karşılamayan herhangi bir talebi reddedecektir. Bu özel durumlardan biri, önceki makalemizde açıkladığımız ping istekleridir. Bir alt alan adı pingN'si için bir sorgu; N bir tamsayıdır, N uzunluğunda bir dizi localhost yanıtı döndürür. Ping için yapılan bir sorgu 15 yanıt döndürür ve temel alan için yapılan bir sorgu tek bir localhost yanıtı döndürür, yani 127.0.0.1.

Ping istekleri dışında, sunucu tek bir IP adresi ile tek etiket sorgularına yanıt verecek şekilde yapılandırılabilir. Bu işlevin amacı bilinmemekte ve istemcide kullanılıyor gibi görünmemektedir; kaynak kodda DNS etkinleştirme isteği olarak adlandırılmaktadır. Bu yetenek belgelenmemiştir ve bunu kullanmak için bir aktörün sunucu yazılımının nasıl çalıştığını anlaması gerekir.

Tek etiketli alt alanlar için özel işlem, anahtar-değer dize çiftleri olan 'aktivasyon' girişlerini yapılandırarak gerçekleştirilir. Bu değer daha sonra sunucunun özel anahtarı ile birlikte kullanılarak bir yanıt IP adresi oluşturulur. Bu yanıt tek yönlü bir hash fonksiyonu kullanılarak oluşturulur ve tersine çevrilemez. Hash büyük/küçük harfe duyarlıdır ve şu şekilde tanımlanır

MD5(subdomain_label + activation_value + private_key)

YANIT KODLAMASI

Sunucu bir istemciden bir sorgu aldığında, istemci verilerinin kodu ile şifresini çözecek, sonuçları kontrol edecek ve işleyecektir. Özellikle, uygun şekilde biçimlendirilmiş bir istemci iletişiminin, sorgu kodlama bölümünde daha önce açıklandığı gibi iki veya üç etiket içermesi gerekir. Sunucu daha sonra istemciye bir veya daha fazla komut içeren bir yanıt gönderir. IPv4 (A) veya IPv6 (AAAA) sorgularını döndürebilmesine rağmen, basitlik için açıklamamızı IPv4 (A) sorgularıyla sınırlayacağız.

Sunucu yanıtı şifrelenmiş bir ikili dizedir ve daha sonra bir veya daha fazla A kaydına kodlanır.[13] Bu kodlama işlemi aşağıdaki Şekil 3'te gösterilmektedir. Yanıttaki maksimum bayt sayısı 64'tür ve bu baytlar 3 baytlık segmentler halinde kodlanarak yanıtta maksimum 22 IPv4 adresi elde edilir.

- İlk adımda, sunucu yanıtın uzunluğunu hesaplar ve bunu yanıt verilerine ekler. Daha sonra rastgele baytlar ekleyerek uzunluğu 3 baytın katı olan bir bileşik dize oluşturur.[14] Bu bileşik dizeye yük diyoruz.
- İkinci adımda, IPv4 adresleri, yükün 3 baytlık bölümlerinden yinelemeli olarak oluşturulur. Her IPv4 adresi 32 bit değerle temsil edilir (burada bit 0 yüksek bittir).
- Her adresin ilk 3 biti rastgeledir.

13 Bir dizi komut bir araya getirilir ve ardından bir anahtar değişimi tamamlanmışsa, kodlamadan önce paylaşılan bir anahtar ve geçerli nonce kullanılarak şifrelenir. Aksi takdirde sunucunun özel anahtarı, nonce ile birlikte verileri açık anahtarlı eliptik eğri algoritması ile şifrelemek için kullanılır.

14 Kodda bu işlem daha karmaşıktır ancak aynı sonucu verir.

- Her segmentin, verilerin alındıktan sonra istemci tarafından sıralanmasını sağlayan bir indeksi vardır; bu 5 bit ile temsil edilir. Bu indeks, sonucun 3-7. bitlerindedir.
- Yük segmenti 8-30 bitlerindedir, bu da yük segmentinin yüksek bitini IPv4 adresindeki ilk sekizlinin alt biti olmaya zorlar.
- Son olarak, en az önemli bit olan bit 31, yük segmentinde oluşturulan bir kontrol bitidir. Bu kontrol toplamının doğası gereği, bu bit IPv4 adreslerin %75'inde 1'idir.
- Elde edilen 32 bit dize bir IPv4 adresi olarak yorumlanır ve yanıta eklenir.

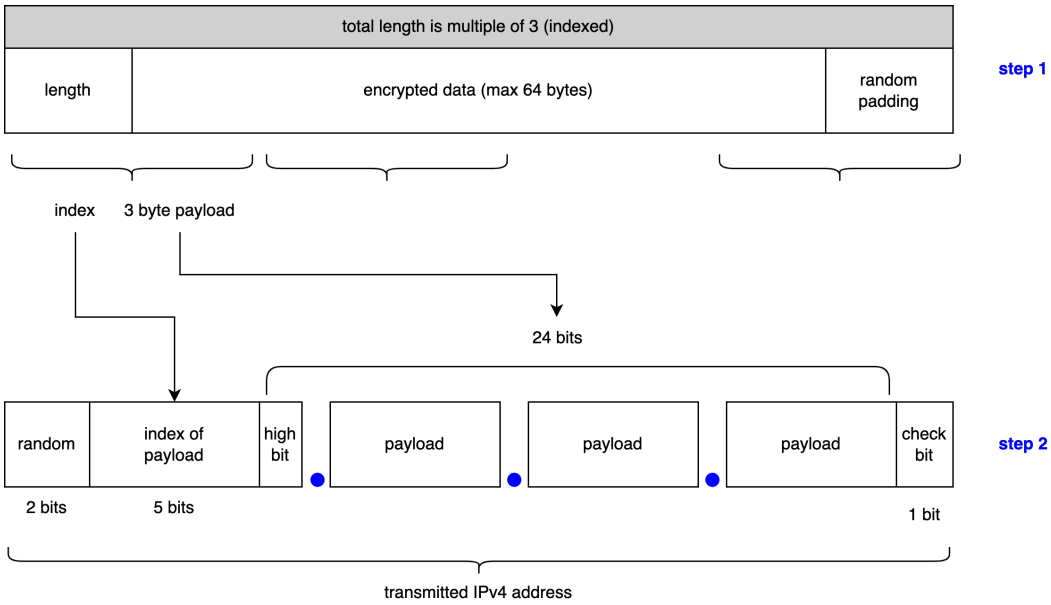


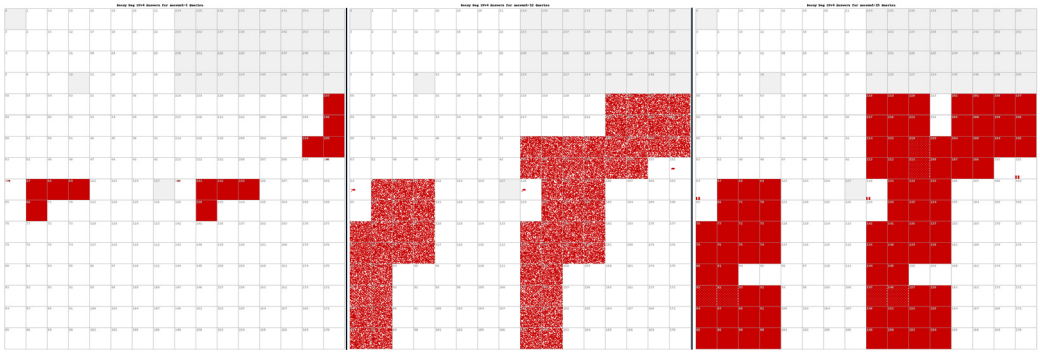
Figure 3. Pupy server encoding of an IPv4 response to a client query. The data is encoded into a series of IPv4 addresses using 3 bytes of the payload in each address.

Önceki makalemizde, Decoy Dog'un şaşırtıcı bir IPv4 yanıtı dağılımına sahip olduğunu belirttik. Artık bunun Pupy yanıt kodlamasının bir eseri olduğunu biliyoruz. Her yanıtta ilk sekizlinin ilk 7 biti olarak üç rastgele bitin ve artan bir indeksin kullanılması, elde edilen IPv4 adreslerinin belirli aralıklarda olacağını ve bu aralıkların yanıttaki yanıt sayısıyla doğrudan ilişkili olduğunu garanti eder. Bu da müşteriye iletilen verinin boyutuna göre belirlenir. Özellikle, ilk IP adresi her zaman 64.0.0.0/8, 128.0.0.0/8 veya 192.0.0.0/8 aralığında olacaktır.

İndeks her artırıldığında, IP adresinin ilk sekizlisine ilişkin seçenekler ikiye kaydırılır. Özellikle:

- İlk IP adresi 64, 128 veya 192 ile başlayacaktır çünkü indeks 0'dır ve uzunluk en fazla 64'tür. Sonuç olarak, yanıtın ilk IP adresinde yalnızca en üstteki 3 bit ayarlanır.
- İkinci IP adresi 66, 67, 130, 131, 194 veya 195 ile başlayacaktır çünkü indeks 1'dir, bu da rastgele oluşturulan 3 üst bite 2 ekler ve veri yükünün en üst biti 0 veya 1 olabilir.
- Üçüncü IP adresi 68, 69, 132, 133, 196 veya 197 vb. ile başlayacaktır.

Bu algoritmanın artan sayıda yanıt için sonucunu aşağıdaki Şekil 4'te görebiliriz. Özellikle, IP adreslerinin ilk oktetinin 3, 12 ve 15 yanıt için toplam yanıt sayısıyla nasıl ilişkili olduğunu göstermek için bir Hilbert haritası kullanıyoruz.



Şekil 4. Sırasıyla 3, 12 ve 15 yanıt içeren Pupy yanıtlarındaki IPv4 adreslerinin dağılımını gösteren Hilbert haritaları.

IPv4 adreslerinin yapısı, tam yanıtı gözlemleyen herkesin iletilen verileri yeniden yapılandırmasına olanak tanır. Bu veriler şifrelenirken, yanıtlar uzunluk ve zaman serisi analizi kullanılarak profillenebilir. Bu tür bir analiz, bu makalenin ilerleyen kısımlarında göreceğimiz gibi iletişimlerle ilgili bilgileri ortaya çıkarabilir.

PASİF VERİ ANALİZİ

Pupy iletişimleri güçlü bir şekilde şifrelenirken, paketlerin şifresini çözmek ve izlemek için gerekli bilgiler tersine çevrilebilir bir şekilde kodlanır. DNS sorguları ve yanıtları toplanırsa, Pupy dağıtımı ve istemcileri hakkında bilgi elde etmek için toplu olarak analiz edilebilirler. Genellikle pasif DNS (pDNS olarak da bilinir) olarak adlandırılan DNS verilerinin pasif olarak toplanması, kurumsal çözümleyiciler, genel özyinelemeli çözümleyiciler, kök ve TLD sunucuları da dahil olmak üzere internetin birçok yerinde gerçekleşir. Takip eden bölümlerde, Pupy sorgularının pasif DNS koleksiyonunun iletişim hakkında bilgi edinmek için nasıl kullanılabileceğini gösteriyoruz.

Bir Pupy denetleyicisi ve istemcileri hakkında pasif DNS'den çok sayıda bilgi elde edebiliriz. Özellikle,

- herhangi bir zamanda yaklaşık aktif istemci sayısını,
- sunucu ile istemciler arasında meydana gelen değişim türlerini,
- istemci uyku aralığı gibi dağıtım imzalarını ve istemci anahtar değişimlerinin ve
- genel etkinliğin zaman çizelgesini öğrenebiliriz.

Bu teknikleri hem kendi sunucumuzdan hem de Decoy Dog sunucularından gelen trafiği analiz etmek için kullandık. Bu, Decoy Dog'un Pupy'ye ve sunucuların birbirine ne kadar benzer olduğunu anlamamızı sağladı. Nihayetinde bu teknikler her Decoy Dog dağıtımının profilini çıkarmamızı sağladı. Kullanılan yöntemlerin teknik detayları Ek C'de ayrıca ele alınmıştır.

PUPY YÜK İMZALARI

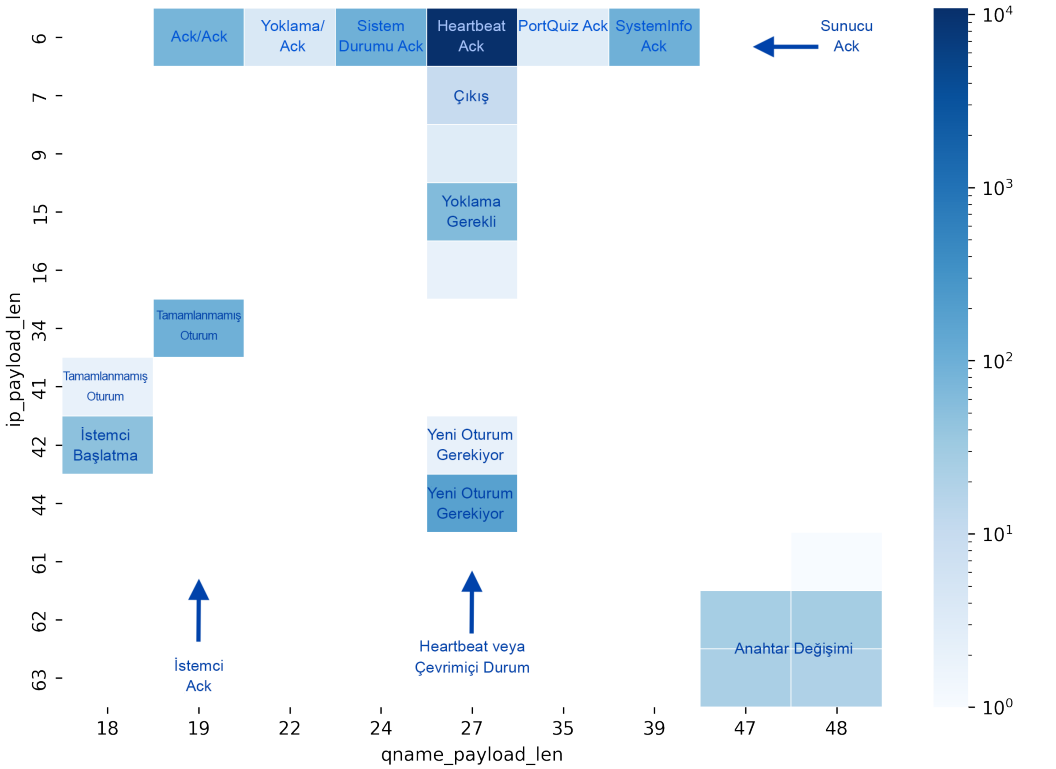
Bir istemci ve sunucu arasındaki iletişimin doğası, pasif veri analizi kullanılarak belirli bir dereceye kadar çıkarılabilir. İstemci kelime dağarcığı, yani yapabileceği farklı yükler oldukça kısıtlıdır: yalnızca dokuz tür istemci iletişimi vardır. İki tür aynı yük uzunluğunu paylaşırken, başka bir tür birden fazla uzunluğa sahip olabilir. Bir aktör Pupy'de özel olaylar oluşturarak potansiyel olarak ek yük uzunluğu çeşitliliği yaratabilir.

Sunucu daha esnek bir kelime dağarcığına sahiptir ve tek bir DNS yanıtında birden fazla komut iletebilir, bu da profil oluşturmayı daha zor hale getirir. Ancak bir Pupy sistemindeki iletişimin büyük çoğunluğu oturum başlatma, anahtar değişimi ve sunucuya istemci kalp

atışları ile ilgilidir. Sunucu iletişimlerine, istemci isteklerinin onaylanması, yeni bir oturum kurma ihtiyacı da dahil olmak üzere hata mesajları ve anahtar değişimleri hakimdir.

Sonuç olarak, DNS sorgularının ve yanıtlarının temel yüklerinin uzunlukları kullanılarak farklı iletişim türleri için imzalar oluşturulabilir. Bu imzalar, yaygın bakım faaliyetlerini sunucudan gelen anlamlı komutlardan ayırmamıza ve özel olay türlerinin kullanımını izole etmemize olanak tanır. Bunlar, Decoy Dog da dahil olmak üzere pasif olarak gözlemlenen bir Pupy istemcisinin ve sunucusunun genel davranışının profilini çıkarmak için kullanılabilir.

Aşağıdaki Şekil 5'te, kendi Pupy verilerimizdeki istemci sorgularında ve sunucu yanıtlarında gözlemlenen yük uzunluklarının bir ısı haritası gösterilmiştir. Sunucu uzunlukları komut argümanları ve birleştirilmiş komutlar nedeniyle daha fazla değişkenlik gösterirken, istemci iletişimleri iyi tanımlanmıştır. İletişimlerin profilini çıkarmak için, sağlama toplamları ve düğüm bilgileri de dahil olmak üzere temel yükün uzunluğunu kullanırız. Sonuç olarak, örneğin, istemci onayı (Ack) 19 bayt uzunluğunda ve sunucu Ack'ı 6 bayt uzunluğundadır. Ek D, yaygın istemci ve sunucu yük uzunlukları ve bunların komutlarla ilişkileri için tablolar içerir.



Şekil 5. Pupy trafiğinde gözlemlenen ortak yük uzunluğu çiftlerinin açıklamalı dağılımı. Yük, sorguda veya yanıtta iletilen şifrelenmiş verilerdir. Bu grafik sunucudan gelen karmaşık DNS C2 komutlarını içermez ve açıklama içermeyen hücreler tam olarak tanımlanmamıştır. Uzunluk bayt cinsindendir.

Decoy Dog

Decoy Dog iletişimi sadece Infoblox çözümleyicilerde değil, birçok genel ve ticari çözümleyicide gözlemlendi. Decoy Dog operasyonlarını ve araç setinin Pupy'den farkını daha iyi anlamak için, kendi koleksiyonumuzu güçlendirmek amacıyla diğer pasif DNS koleksiyonlarını kullandık. Toplamda, analizimiz 29 Mart 2022 - 16 Haziran 2023 döneminde 15 milyondan fazla DNS olayını kapsamaktadır. Ayrıca, ad sunucularını aktif olarak araştırdık ve pasif olarak toplanan DNS trafiğini kendi Pupy istemcimiz ve sunucumuz tarafından oluşturulan trafikle karşılaştırdık.

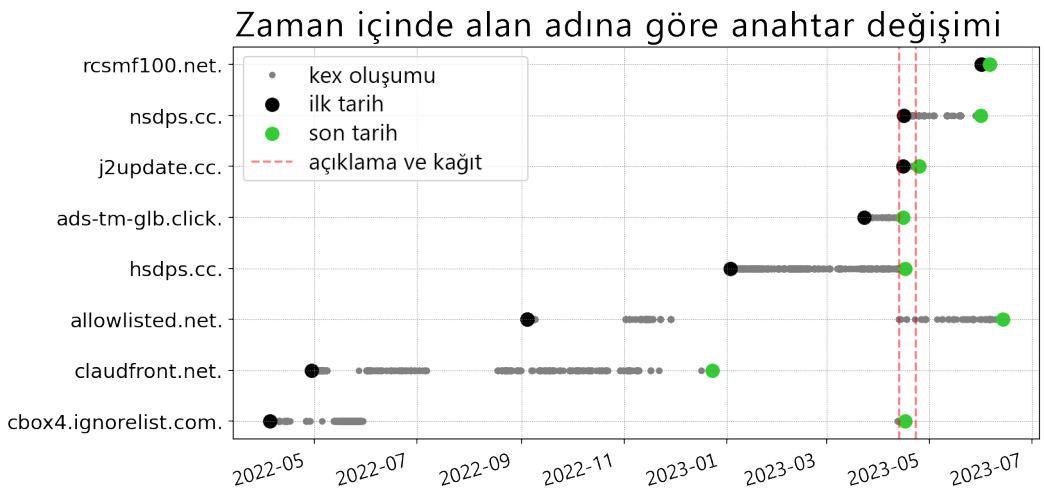
Decoy Dog'u ve faaliyetlerini daha iyi anlamak için bir dizi teknik kullandık. Ayrıca halka açık VirusTotal havuzunda bulunan örneklere tersine mühendislik uygulayarak DNS bulgularımızı doğruladık ve diğer yetenekleri ortaya çıkardık. Takip eden bölümlerde analizimizi ayrıntılı olarak açıklayacak ve sonuçları göstereceğiz. Bu çalışmada öne çıkan hususlar şunlardır:

- Decoy Dog, Pupy olmasa da kötü amaçlı yazılımın yeteneklerini önemli ölçüde artıran ve ele geçirilmiş bir cihazda kalıcılığı sağlamaya yardımcı olan büyük bir yeniden düzenlemedir.
- Farklı TTP'ler kullanan ve Nisan 2023'te araç setini ifşa etmemize farklı tepkiler veren bir avuç aktör tarafından işletilmektedir.
- Genel olarak etkilenen cihaz sayısı azdır ve tek bir denetleyicide dört kadar az sayıda cihaz bulunmaktadır.
- Nisan 2023'ten bu yana kaydedilen yeni denetleyiciler, orijinal makalemizde belirtilen özellikleri hafifletmek için uyarlanmıştır. Bu, istemci IP adreslerine verilen yanıtları belirli konumlarla sınırlandırmak için coğrafi sınırlama mekanizmalarını içerir.
- DNS analizi, yalnızca Decoy Dog'u algılamak için değil, kullanımını anlamak ve onu Pupy'den ayırmak için güçlü bir araç olduğunu kanıtladı. Bu, seçici ters mühendislikle birleştiğinde, Decoy Dog'un ve oluşturduğu tehdidin net bir resmini ortaya çıkardı.

ANAHTAR DEĞİŞİMLERİ

Daha önce açıklandığı gibi, anahtar değişimi tamamlandığında ve SPI değeri ayarlandığında bir oturum başlar. Teorik olarak, tek bir şifreli oturum süresiz olarak devam edebilir, ancak pratikte, denetleyicinin yeni bir oturumun oluşturulmasını gerektireceği bir dizi koşul vardır. Bu nedenle, çalışan tek bir istemci örneği tipik olarak birçok oturuma sahip olabilir. Pupy yük imzalarını kullanarak, bir istemci ve sunucu arasında paylaşılan anahtarların ne zaman oluşturulduğunu belirleyebilir ve zaman içinde her denetleyici için yeni bir uzlaşmadan veya istemcinin yeniden başlatılmasından kaynaklanan istemci başlatma sayısına ilişkin kaba tahminler yapabiliriz.

Aşağıdaki Şekil 6, birkaç Decoy Dog denetleyicisi için anahtar değişimlerinin zaman çizelgesini göstermektedir. Bazı denetleyiciler için gözlemlenen anahtar değişimlerinde boşluklar vardır. Claudfront[.]net için son anahtar değişimi Aralık 2022'de gözlemlendi, ancak istemci aktivitesi sadece devam etmekle kalmadı, aynı zamanda 2023'te arttı; tüm benzersiz SPI değerlerinin %70'inden fazlası ilk olarak 2023'te gözlemlendi. Benzer şekilde, allowlisted[.]net denetleyicisi Aralık 2022'den Nisan 2023'deki açıklamamızdan sonrasına kadar hiçbir anahtar değişimi yoktu. Son olarak, cbox4[.]ignorelist[.]com da anahtar değişimlerinin olmadığı uzun bir süre göstermekte olup, alan adı çalışmayı durdurmadan hemen önce az sayıda anahtar değişimi gerçekleşmiştir. Aktörlerin anahtar değişimini DNS'den farklı bir aktarım üzerinden gerçekleştirmek için istemcileri yeniden yapılandırdığından şüpheleniyoruz.



Şekil 6. Belirli Decoy Dog alanları için gözlemlenen anahtar değişimlerin zaman çizelgesi.

MÜŞTERİ ZAMAN ÇİZELGELERİ

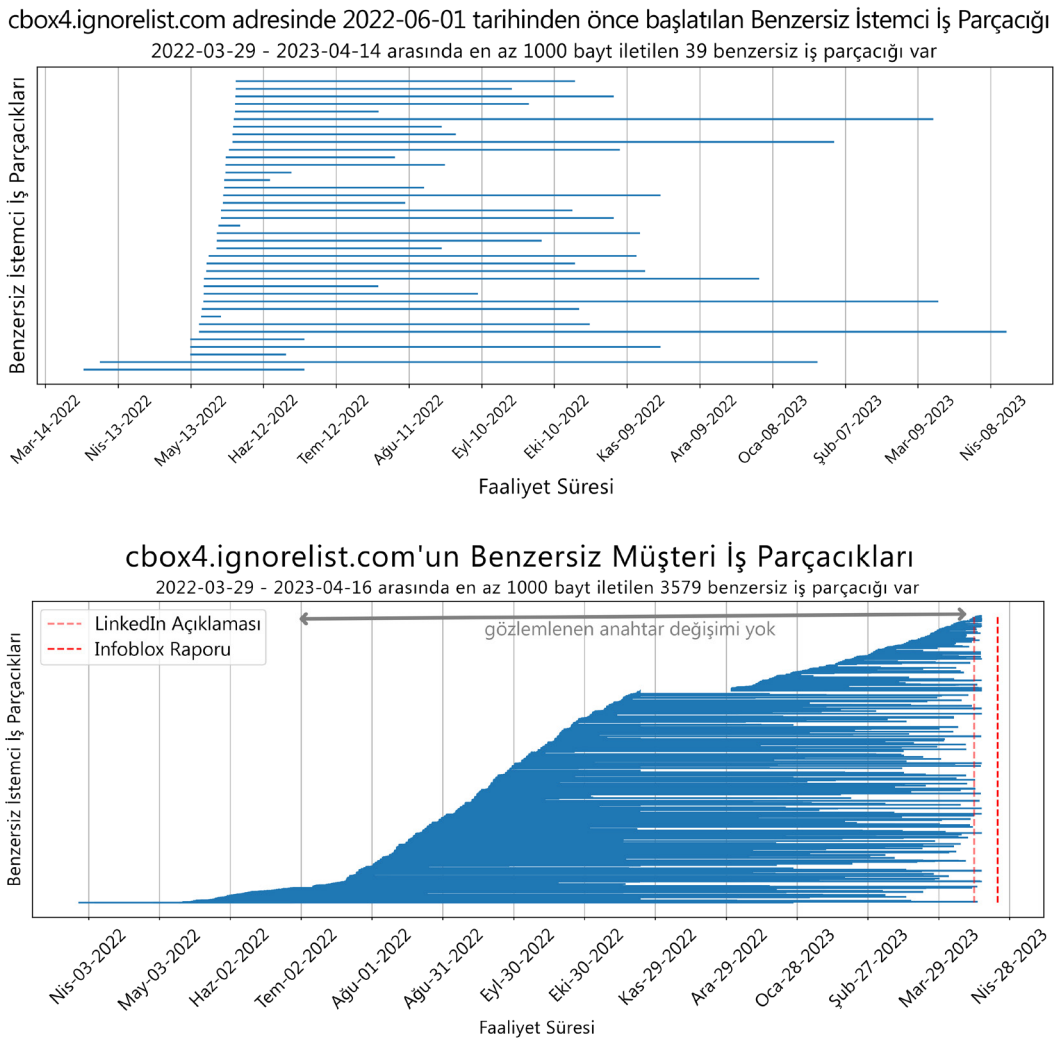
Toplam istemci sayısına ek olarak, her bir denetleyicinin aynı anda kaç aktif istemci bulundurduğunu ve istemcilerin sunucuyla ne kadar süreyle aktif olarak iletişim kurduğunu belirlemek istedik. Ek C'de açıklanan nonce değerlerini gruplama yöntemini kullandık. Bu analiz, aşağıdaki grafiklerde gösterildiği gibi, uzun bir süre boyunca Decoy Dog operasyonlarına ilişkin önemli bilgilerle sonuçlanmıştır. Özellikle de:

- Tüm denetleyiciler, herhangi bir anda az sayıda istemciyi yönetiyor. Bazıları dört kadar az ve hepsi ellinin altında istemciyi kontrol ediyor.
- Orijinal alan cbox4[.]ignorelist[.]com, daha büyük denetleyicilerden biri ve zaman içinde birden fazla noktada istemcilerde bir sıçrama sergiliyor. Ayrıca az sayıda çok uzun süredir çalışan istemciyi koruyor.
- Gözlemlenecek ikinci denetleyici claufront[.]net için Şubat 2023'te aktivitede dramatik bir artış var.
- Gözlemlenecek üçüncü denetleyici olan allowlisted[.]net, sürekli olarak az sayıda eşzamanlı istemciyi korumuştur.
- Denetleyiciler ads-tm-glb[.]click ve hsdps[.]cc açıklamamızı takiben istemcileri yeni denetleyicilere devretti.
- Claudfront[.]net ve izin verilenler listesine eklenen[.]net ifşaatımıza yanıt olarak işlemlerini değiştirmedi, cbox4[.]ignorelist[.]com operasyonları durdurdu ve hem hsdps[.]cc ve ads-tm- glb[.]click istemcileri yeni alan adlarına aktardı.

Tüm zamanlardaki toplam istemci sayısını tahmin etmek zor olsa da, aynı anda aktif olan istemci sayısının az olması bu operasyonların yüksek oranda hedefli olduğunu göstermektedir. Ayrıca güvenlik sağlayıcılarının neden bu etkinliği algılamadığını ve virüslü cihazları henüz bulamadığını da açıklıyor. Virüs bulaşmış istemciler çok az sayıda ağda bulunmaktadır. Görünüşe göre bu ağlar DNS'deki C2 iletişimlerini tanımlayamamakta ve engelleyememektedir.

Aşağıdaki çizgi grafik diyagramlarında, tek bir istemcinin etkinliğini bir çizgi olarak temsil ediyor ve buna istemci iş parçacığı diyoruz. Y ekseni, bir nonce zinciri tarafından tanımlanan farklı istemci iş parçacıklarını gösterir. Bir Pupy istemcisi yeniden başlatıldığında, yeniden başlatma veya başka bir yolla, yeni bir nonce üretilecek ve yeni bir iş parçacığı gözlemlenecektir. Bazı diyagramlarda, faaliyette muhtemelen istemcinin yeniden başlatıldığını gösteren net kesintiler vardır. X ekseni zamanı gösterir.

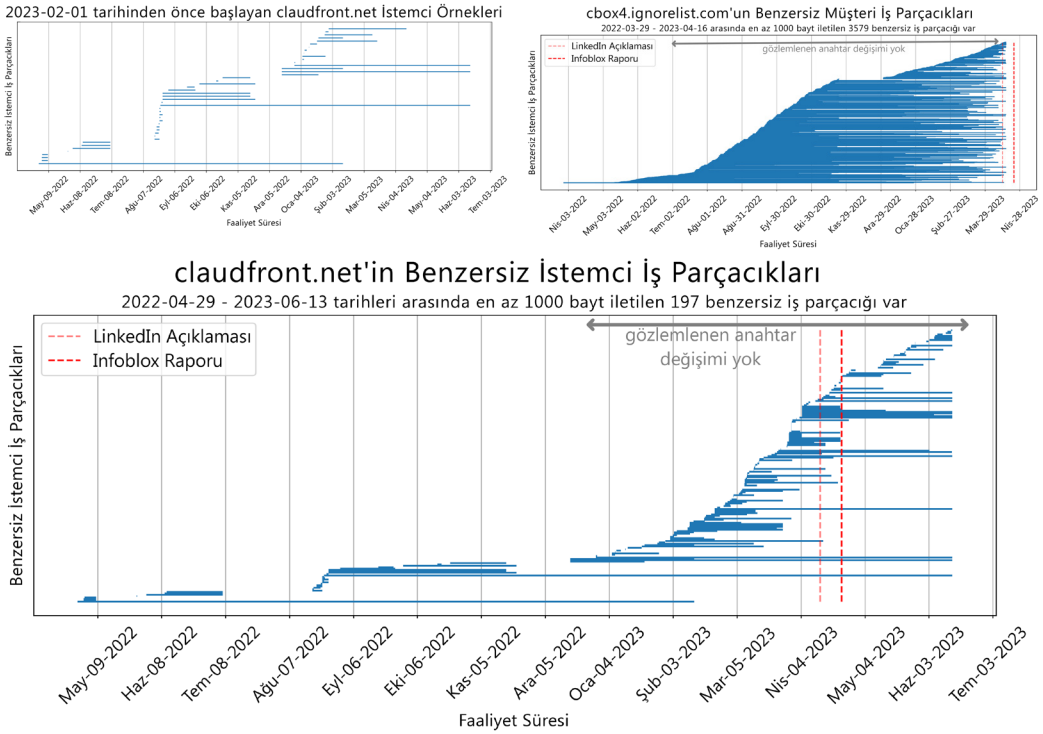
Şekil 7'de ilk Decoy Dog alanı cbox4[.]ignorelist[.]com için istemci etkinliği gösterilmektedir. İlk istemci dizisi Mart 2022'nin sonlarında başladı ve en uzun iş parçacığı yaklaşık bir yıl sürdü. Bu denetleyicinin başlangıçta yalnızca birkaç istemciye, ancak Mayıs 2022'nin ortalarında meydana gelen bir değişiklikle yaklaşık 40 eşzamanlı aktif istemciye sahip olduğunu görebiliyoruz. En büyük aylık artış Ağustos 2022'de olmak üzere, istemci iş parçacıklarında benzer artışlar periyodik olarak gerçekleşmiştir; ancak yeni istemci iş parçacıkları başlarken diğerleri sona ermiştir. Tüm faaliyet yılı boyunca, eşzamanlı istemci sayısının her zaman 50'nin altında olduğu görülmektedir. Ayrıca Şekil 7'den, istemci iş parçacıklarının dörtte birinin altı ay veya daha uzun süre devam ettiğini görebiliyoruz. Bu da sürekli bir operasyonla tutarlıdır. LinkedIn paylaşımının ardından tüm iletişimler kesilmiş ve bir daha gözlemlenmemiştir.



Şekil 7. Üstteki şekil, 1 Haziran 2022'den önce mevcut olan istemcileri ve alttaki şekil zaman içindeki istemci iş parçacıklarını gösterir.

Kronolojik olarak ikinci Decoy Dog alanı olan claudfront[.]net'in DNS etkinliği cbox4'ten oldukça farklıdır. Aşağıdaki Şekil 8'de gösterildiği gibi, Şubat 2023'ün başlarına kadar bu denetleyicide eşzamanlı olarak ondan az aktif istemci vardı. O zamandan sonra, yaygın bir enfeksiyondan beklenecek ölçüde olmasa da, istemci sayısı önemli ölçüde artmıştır. Bu artışın zamanlaması, denetleyici etki alanını içeren ikili bir örneğin 13 Şubat'ta VirusTotal'a

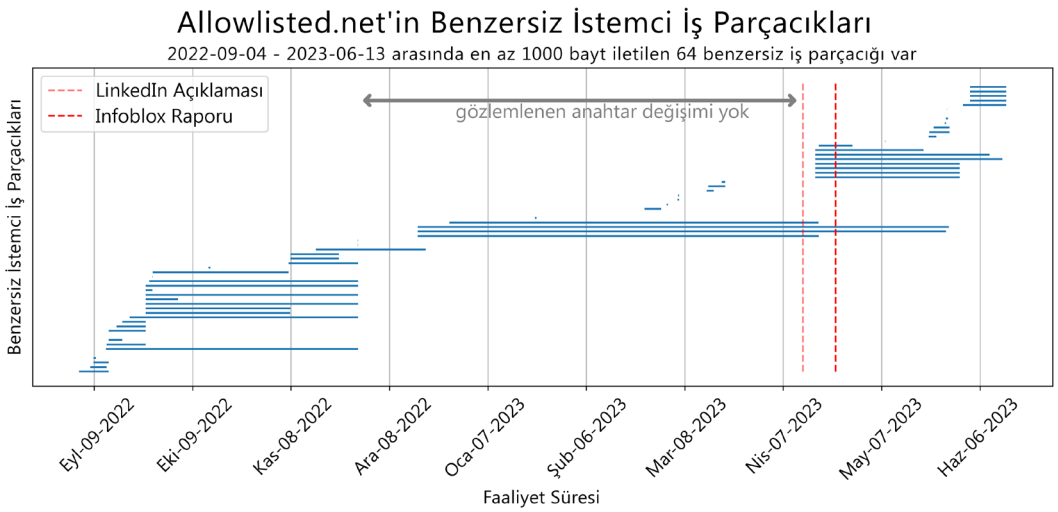
gönderilmesinden kısa bir süre öncesine denk gelmektedir.[15] cbox4[.]ignorelist[.]com'un aksine, claufront[.]net sorgularında açıklamamızın ardından dikkate değer bir değişiklik olmadı.



Şekil 8. Zaman içinde nonce iş parçacıklarına dayalı olarak Claudfront[.]net için istemci iş parçacıkları. Şubat 2023'ün başlarında, farklı zaman dilimlerini gösteren ayrı görüntülerle yakınlaştırılan önemli bir değişiklik var.

Üçüncü alan adı olan allowlisted[.]net, davranışın başka bir varyasyonunu gösteriyor. Bu durumda, istemci sayısı sürekli olarak azdır: herhangi bir zamanda onun altındadır. claudfront[.]net'in aksine Şubat 2023'te herhangi bir değişiklik yok ve allowlisted[.]net içeren bilinen bir ikili örnek yok. Şekil 9'da gösterildiği gibi, Kasım 2022'nin ortasından açıklamamızdan kısa bir süre sonrasına kadar, istemci faaliyetlerinin keskin bir şekilde sona ermesi ve Nisan 2023'te birkaç iş parçacığının yeniden başlatılmasıyla aynı zamana denk gelen hiçbir anahtar değişimi görülmemektedir.

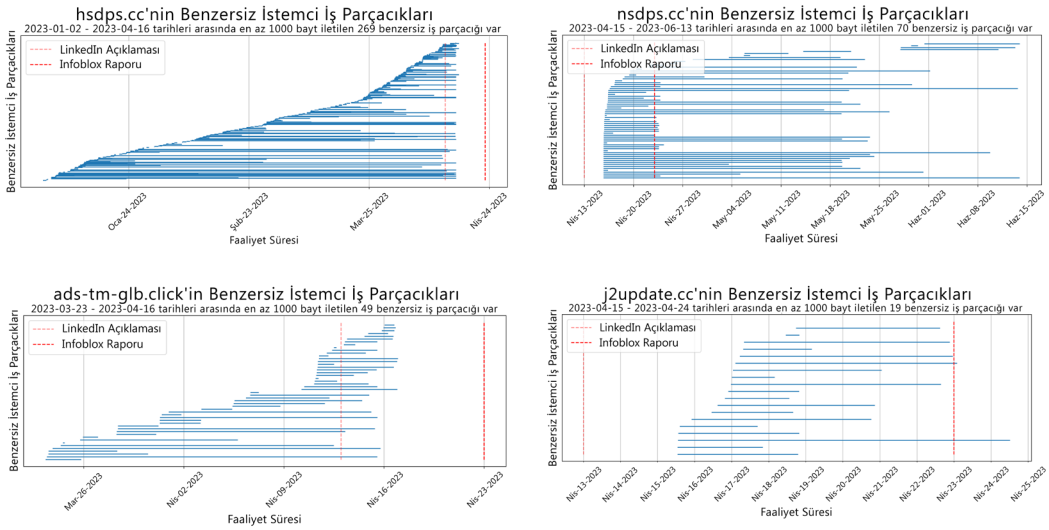
15 0375f4b3fe011b35e6575133539441009d015ebecbee78b578c3ed04e0f22568, ilk gönderim 2023-02-13 07:39:55 UTC



Şekil 9. allowlisted[.]net için istemci iş parçacıkları. allowlisted[.]net'te tarihsel olarak çok az sayıda istemci var ve bu durum açıklamadan bu yana değişmedi.

Son olarak, hsdps[.]cc, nsdps[.]cc, ads-tm-glb[.]click ve j2update[.]cc tarafından ilgili faaliyetler gözlemledik. hsdps[.]cc ve ads-tm-glb[.]click alan adları sosyal medyada ifşa etmemizin ardından faaliyetlerini durdurdu, ancak istemcilerinin birçoğu sırasıyla nsdps[.]cc ve j2update[.]cc'ye aktarıldı. Bunu, zaman içinde tüm alanlarında nonce zincirleri oluşturarak ve bir denetleyiciyle iletişim kurmaya başlayıp diğeriyle sonlanan iş parçacıklarını belirleyerek keşfettik.[16]

Yeni alan adları, nsdps[.]cc ve j2update[.]cc, sosyal medya duyurularımızdan 48 saatten kısa bir süre sonra kaydedildi. İstemci iş parçacığı diyagramlarından, bir alan kümesi faaliyeti dururken diğerlerinin başladığını görebiliriz. Denetleyiciler hemen sonrasında istemcilerle aktif olarak iletişim kurmaya başladı. DNS analizi yoluyla istemci aktarımının keşfedilmesinin ardından, daha sonra açıklayacağımız gibi, bu değişikliği yapmak için bir komutun ikili örneklerinde kanıt bulduk.



Şekil 10. Dört Decoy Dog denetleyici alanının zaman çizelgesi karşılaştırması. Denetleyiciler hspds[.]cc ve ads-tm-glb[.] click Infoblox açıklamasını takiben iletişimi durdurdu ve nsdps[.]cc ve j2update[.]cc alanları iletişime başladı. Ayrıca bu alanlar arasında istemci transferlerini de gözlemledik.

16 Bunun 32 bitlik rastgele bir nonce ile rastgele gerçekleşme olasılığı son derece düşüktür ve bu alanlar için bir denetleyiciden diğerine nonce 'aktarımlarının' sayısı yüksek.

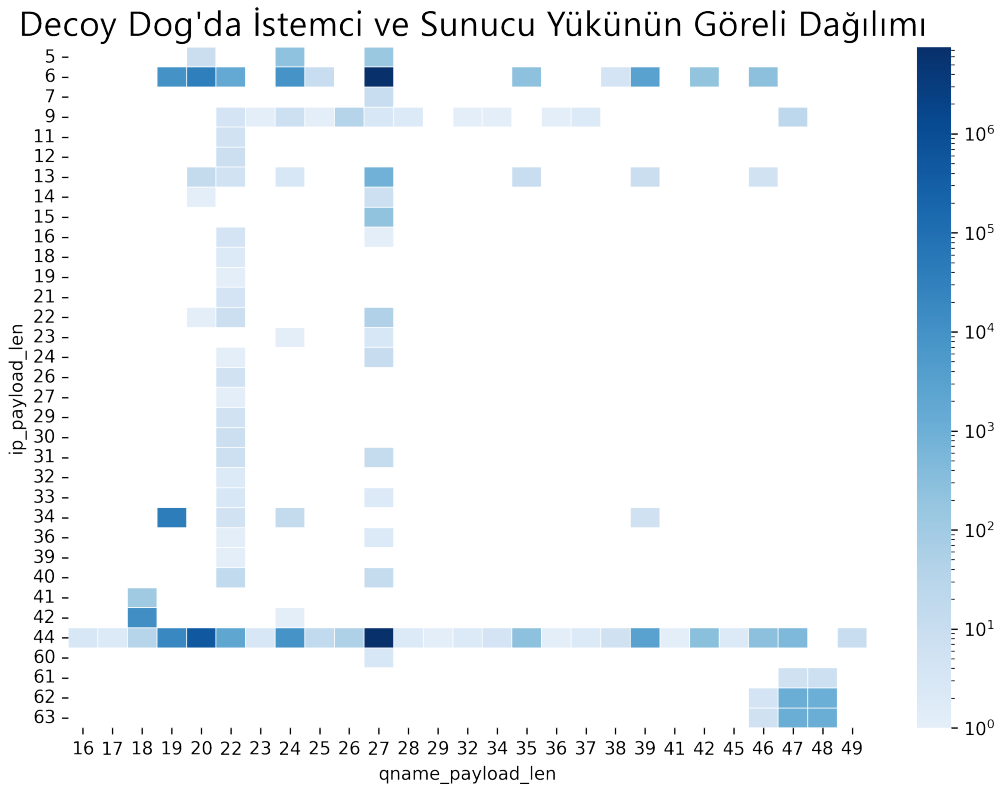
Orijinal makalemizden bu yana, her biri çok az sayıda istemciye sahip başka denetleyicilerin aktif hale geldiğini gördük. Burada gösterilen istemci davranışı, duyurumuza verilen yanıtla birlikte, Decoy Dog araç setinin birden fazla aktör tarafından kullanıldığını gösteriyor.

DECOY DOG YÜK IMZALARI

Küresel pDNS'de 13 aylık bir süre boyunca gözlemlenen 15,5 milyon sorgu yanıtının istemci ve sunucu yük uzunluklarını çözdük. Daha sonra sunucuların davranışını anlamak için istemci-sunucu yükleri için Pupy imzalarını Decoy Dog'da gözlemlenen verilerle karşılaştırdık. Genel trafik dağılımlarının Pupy ile uyumlu olduğunu tespit etsek de, kesin farklılıklar vardı. Decoy Dog istemcileri, varsayılan Pupy'de bulunandan daha büyük bir istek kümesi veya kelime dağarcığı kullanır.

Şekil 11, tüm Decoy Dog sistemlerindeki faydalı yük uzunluk çiftlerinin göreceli dağılımlarını göstermektedir. Ek D'de ayrıntılı olarak açıklandığı gibi Pupy imzalarımızı kullanarak birkaç hemen sonuç çıkarabiliriz:

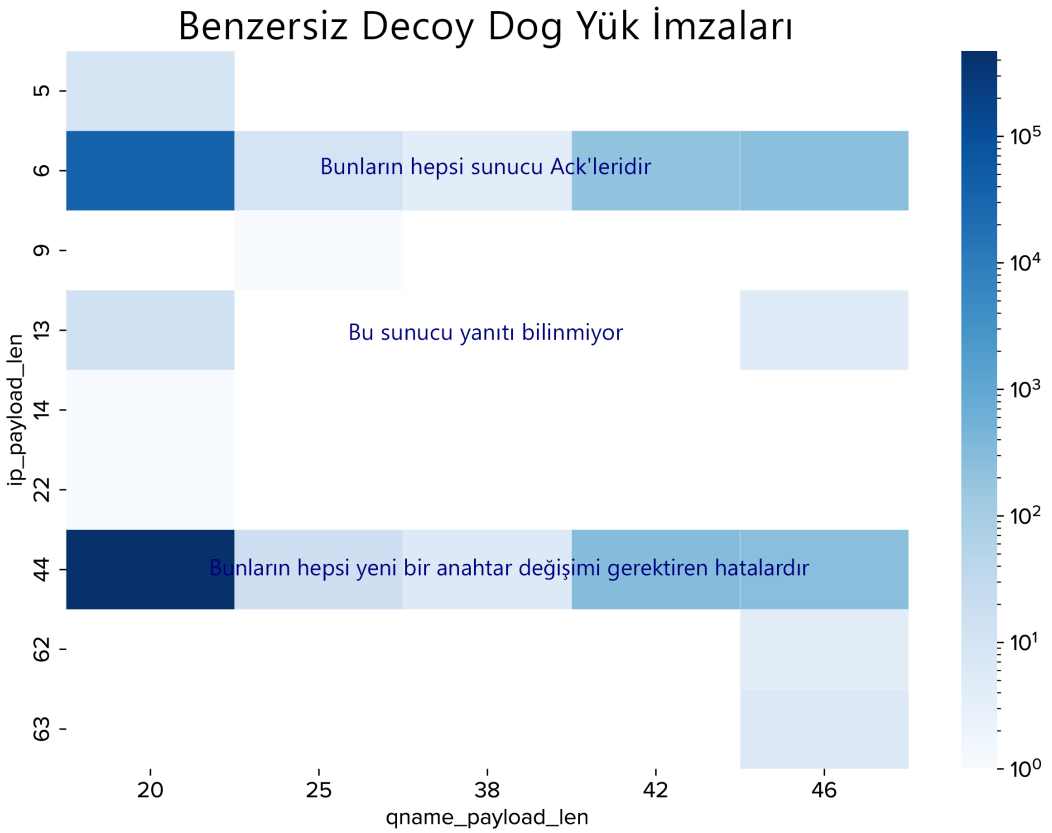
- Beklenen dokuz müşteri yükünden daha fazlası mevcuttu.
- Laboratuvarımızda gözlemlemediğimiz sunucu yük uzunlukları vardı.
- İletişimlerin çoğunluğu oturum bakımı ve anahtar değişimleri ile ilgilydi.
- Decoy Dog sunucularına yapılan sorguların büyük bir yüzdesi hata yanıtı almış ve gerçek bir istemciden ziyade üçüncü bir tarafın taramasıyla tutarlı varyasyonlar göstermiştir. Bunların çoğu duyurularımızdan sonra gerçekleşti.



Şekil 11. Decoy Dog iletişimlerinde gözlemlenen istemci ve sunucu yük uzunluklarının göreceli dağılımı.

Benzersiz müşteri yükleri 20, 25, 38, 42 ve 46 uzunluklarını içeriyordu. Bunlardan bazıları farklı bir anahtar yapılandırması veya yoklama parametrelerindeki bir değişiklikle ilişkili olabilir; iletişimin ne olduğunu belirleyemiyoruz, ancak varyasyon mevcut. Ayrıca, Pupy'de gözlemlenenlerin ötesinde ek yanıt yükü uzunlukları vardı. En önemlisi, Decoy Dog'un

13 baytlık bir sunucu yükü var ve bu yük zaman içinde aktivite ataklarında görülüyor. Bu yükün ne olduğunu belirleyemiyoruz, ancak istemciye iletilmek üzere 8 bayt veri gerektiren tek bir komutla tutarlı. Ayrıca 5 baytlık bir yük, Pupy verilerimizde gözlenmeyen başka bir uzunluk ve istemciye veri aktarımı gerektirmeyen tek bir komutun göstergesi içeren bir dizi sunucu yanıtı gördük. Aşağıdaki Şekil 12, Decoy Dog'da bulunan ve Pupy deneylerimizde görülmeyen benzersiz yük çiftlerini özetlemektedir.



Şekil 12. Decoy Dog'da gözlemlenen ve varsayılan Pupy iletişimlerinde bulunmayan istemci-sunucu yük uzunluğu çiftlerinin bir özeti.

Ayrıca varsayılan konfigürasyonlardaki değişiklikleri belirlemek için zaman serileri kullandık. Yerleşik bir Pupy oturumu altında, istemci her 30 saniyede bir kontrol edecektir. İstemci kalp atışı sorgularının değişimi üzerine istatistiksel analiz kullanarak, varsayılan 30 saniyeye ek olarak 2 dakika 30 dakikalık kalp atışı aralıkları bulduk.

Bu analiz sonucunda, rutin bakım ile uzaktan erişim komutlarını birbirinden ayırarak her bir Decoy Dog alanı için iletişimin doğasını anlayabildik. Ayrıca Decoy Dog sunucularının alt kümeleri arasında ve içinde kullanılan Pupy'nin olası özelleştirmelerini de izole edebildik. Decoy Dog trafiğinin büyük çoğunluğunun rutin onaylar ve hatalar olduğunu ve hata iletişimlerinin Pupy gözlemlerine dayanarak görmeyi beklediklerimizle orantısız olduğunu bulduk. Bu hata yanıtları olgusuna ilişkin araştırmamızın sonuçlarını bir sonraki bölümde paylaşıyoruz.

WILDCARD VE GEOFENCING DAVRANIŞI

Orijinal teknik makalemizde Decoy Dog sunucularının tekrarlanan DNS sorgularını yanıtladığını bildirmiştik. Bu durum kafa karıştırıcı olmaya devam ediyor. Decoy Dog'un başlangıçta günler veya haftalar önce yapılan bir sorguya ne zaman ve nasıl yanıt vereceğini anlamaya çalışırken, daha da şaşırtıcı bir davranış ortaya çıkardık. Decoy Dog sunucularından birkaçı yalnızca tekrarlara yanıt vermekle kalmıyor, Pupy kodlamasıyla tutarlı olan tüm sorgulara yanıt veriyor. DNS'de buna wildcard yanıt diyoruz. Normal bir Pupy sunucusu NXDOMAIN veya SERVFAIL yanıtı döndürürken, Decoy Dog sunucusu genellikle 15 IP adresi döndürüyor.

Aşağıdaki Şekil 13'te rastgele sorgulara verilen yanıtlar gösterilmektedir. Bu durumda, sorgu adının içine 'wild' ve 'wildcard' ifadelerini yerleştirdik ve iki farklı Decoy Dog sunucusundan 15 yanıt aldık. Yanıtlar her sorgu için farklı ve Pupy kodlama şemasına uygun. Araştırmamız sayesinde, Decoy Dog'un beklenen NXDOMAIN yanıtlarını döndürmek yerine neredeyse tüm hataları bu şekilde ele aldığını öğrendik. Hata işleme hakkında daha fazla bilgi için Ek E'ye bakın.

```
; <<>> DiG diggui.com <<>> @ns1.rtupdates.net wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22151
;; flags: qr aa rd; QUERY: 1, ANSWER: 15, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. IN A

;; ANSWER SECTION:
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 64.88.80.242
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 131.163.188.250
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 68.221.203.220
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 198.206.187.196
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 200.37.65.250
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 75.195.241.234
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 141.67.92.44
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 142.153.85.81
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 209.92.80.161
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 147.26.100.52
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 213.83.7.105
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 150.143.51.118
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 153.171.88.194
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 219.226.5.44
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.rtupdates.net. 60 IN A 157.111.237.108

;; Query time: 150 msec
;; SERVER: 5.252.179.232#53(5.252.179.232)
;; WHEN: Sat Jun 03 15:29:11 UTC 2023
;; MSG SIZE  rcvd: 321
```

```
; <<>> DiG diggui.com <<>> @ns1.allowlisted.net wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33023
;; flags: qr aa rd; QUERY: 1, ANSWER: 15, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. IN A

;; ANSWER SECTION:
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 64.88.161.73
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 67.179.145.230
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 69.153.193.38
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 71.14.146.226
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 73.22.176.2
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 138.151.231.153
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 141.232.226.212
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 79.241.118.178
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 209.158.29.150
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 147.248.180.89
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 148.158.234.156
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 215.63.12.236
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 153.141.240.250
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 219.18.219.74
wildcard5yt1j46ra2gwossxhw1q9999.2vzxfwild3999999.allowlisted.net. 60 IN A 156.250.150.9

;; Query time: 151 msec
;; SERVER: 83.166.240.52#53(83.166.240.52)
;; WHEN: Sat Jun 03 15:31:15 UTC 2023
;; MSG SIZE  rcvd: 323
```

Şekil 13. İki Decoy Dog yetkili sunucusundan wildcard yanıt davranışı. Her iki durumda da sunucular 'wild' ve 'wildcard' dizelerini içeren aynı rastgele sorguya Pupy kodlamasıyla tutarlı 15 IP adresi ile yanıt verdi.

Daha da şaşırtıcı olan, bazı Decoy Dog sunucuları, istemci adına sorguyu yapan özyinelemeli çözümleyicinin IP adresine bağlı olarak farklı yanıt veriyor. Şekil 14'te Decoy Dog alanı nsdps[.]cc'ye yapılan bir sorgunun tekrarını gösteriyoruz. Bu aslında birkaç hafta önce meydana geldi. Sorguyu Yandex genel çözümleyicileri üzerinden yaptığımızda 15 IP adresi içeren bir yanıt aldık. Ayrıca Rus TimeWeb genel çözümleyicilerinden 15 IP adresi aldık. Ancak, denediğimiz otuzdan fazla herkese açık çözücünün hiçbiri yanıt vermedi. Bu tür bir davranış, bir sunucunun IP adresinin coğrafi konumuna göre DNS sorgularına yanıt verdiği coğrafi sınırlama ile tutarlı. Bu davranışı Haziran 2023'te keşfettik ve bazı sunucuların yalnızca DNS sorgularını Rus IP adresleri üzerinden yönlendirdiğimizde yanıt verdiğini, diğerlerinin ise herhangi bir konumdan gelen iyi biçimlendirilmiş herhangi bir sorguya yanıt verdiğini gördük. Bu tür seçici yanıt, denetleyicinin yalnızca Rusya'da görünen müşterilerle iletişim kurmasını sağlıyor. Denetleyiciler daha önce Infoblox özyinelemeli çözümleyicilerden gelen sorguları çözdüğü için bu işlevselliğin ifşa sonrası eklendiğini biliyoruz.

```
; <<>> DiG diggui.com <<>> @77.88.8.8 qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42579
;; flags: qr rd ra; QUERY: 1, ANSWER: 15, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. IN A

;; ANSWER SECTION:
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 46 IN A 72.11.125.198
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 36 IN A 203.92.202.218
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 45 IN A 76.74.229.130
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 44 IN A 207.26.86.188
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 31 IN A 80.154.112.164
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 43 IN A 146.160.113.9
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 52 IN A 148.235.159.60
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 41 IN A 151.103.182.130
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 54 IN A 89.76.7.130
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 45 IN A 218.111.60.250
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 42 IN A 93.43.159.18
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 49 IN A 128.88.84.164
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 45 IN A 195.161.207.129
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 51 IN A 68.172.178.156
qnomwvxags5u1pawkzmkllkmuoda9999.abp11i4yk5y1fqyd4tpzm1q9.nsdps.cc. 49 IN A 199.24.240.30

;; Query time: 459 msec
;; SERVER: 77.88.8.8#53(77.88.8.8)
;; WHEN: Tue Jun 20 14:31:11 UTC 2023
;; MSG SIZE  rcvd: 335
```

```
; <<>> DiG diggui.com <<>> @74.82.42.42 hoxlgxq9.yopzgoha3rlp4pdcclosfb63yodq9999.enueh2eluu6uqnjtjpid4lq9.nsdps.cc A
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

```
; <<>> DiG diggui.com <<>> @ns2.nsdps.ns2.name hoxlgxq9.yopzgoha3rlp4pdcclosfb63yodq9999.enueh2eluu6uqnjtjpid4lq9.nsdps.c
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Şekil 14. Yandex'in genel çözümleyicilerinden, Hurricane Electric genel çözümleyicilerinden ve yetkili çözümleyiciden yeniden oynatılan bir Decoy Dog sorgusuna verilen yanıtların karşılaştırılması. Bu sorgular bir Tor tarayıcısı aracılığıyla art arda yapıldı. Yalnızca Yandex üzerinden yapılan sorguya yanıt alındı.

Pupy varsayılan kodlaması kullanılarak çözülemeyen bir alan adı için bir sorgu yapıldığında (bu test için ekstra karakterler ekledik), nsdps[.]cc sunucuları esasen bir çukur olan bir IP adresi döndürüyor. Aşağıdaki Şekil 15'te gösterildiği gibi, sorguyu doğru bir şekilde çözülemeyecek şekilde biraz değiştirdik. Bu durumda, 172.0.0.0/8 aralığında rastgele bir IP adresi döndürüldü. Normalde Pupy bir NXDOMAIN yanıtı döndürür.

```
; <<>> DiG diggui.com <<>> @77.88.8.1 hoxlgxq9.yopzgoha3rlp4pdcclosfb63yodq9999.wildenueh2eluu6uqnjtjpid4lq9.nsdps.cc A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2019
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hoxlgxq9.yopzgoha3rlp4pdcclosfb63yodq9999.wildenueh2eluu6uqnjtjpid4lq9.nsdps.cc. IN A

;; ANSWER SECTION:
hoxlgxq9.yopzgoha3rlp4pdcclosfb63yodq9999.wildenueh2eluu6uqnjtjpid4lq9.nsdps.cc. 32 IN A 172.67.132.113

;; Query time: 1695 msec
;; SERVER: 77.88.8.1#53(77.88.8.1)
;; WHEN: Tue Jun 20 23:44:46 UTC 2023
;; MSG SIZE  rcvd: 124
```

Şekil 15. nsdps[.]cc denetleyicisi için geçersiz bir Pupy alan adı sorgusu beklenen NXDOMAIN yanıtı yerine 172.0.0.0/8 aralığında rastgele bir IP adresi döndürecektir.

Bu davranışın bir kısmı, istemciden gelen DNS çözümlemesinin bir eseri olarak açıklanabilir. DNS'de bir ana bilgisayar sorgulandığında, bazı çözümleyiciler gelecekteki olası sorgulara hazırlanmak için potansiyel olarak ilgili alan adlarını çözümlemeye çalışacaktır. Örneğin, www[.]baddomain[.]com için bir sorgu alan özyinelemeli bir çözümleyici, www[.]baddomain[.]com'a ek olarak baddomain[.]com'u da çözümlemeye çalışabilir. Bu davranışı kendi Pupy sunucumuzda, istemci sorgularını bazı genel çözümleyiciler üzerinden yönlendirirken gördük.

TEK ETİKET YANITLARI

Varsayılan olarak Pupy, bir istemci iletişiminin veya kurulu bir ping sorgusunun yapısıyla eşleşmeyen etiketlere gelen istekleri reddeder. Ancak, yukarıdaki "Özel Alan Adı İşleme" bölümünde açıkladığımız gibi, DNS aktivasyon isteği özelliği bir aktörün Pupy sunucusunu özel kaynaklara yönelik sorgulara yanıt verecek şekilde yapılandırmasına olanak tanır. Küresel pDNS günlüklerinde, tek bir etiket alt alanına sahip sorgular belirledik. Bu tür tek alt alan 'm' idi ve aktivasyon fonksiyonu aracılığıyla bu alanların çözümlenmesinin mümkün olduğunu varsaydık. Aktivatör hash fonksiyonunun doğası gereği, bu sorgular için tek bir statik IP adresi döndürülmelidir. Bu davranışı 4 alanda bulduk: hsdps[.]cc, nsdps[.]cc, j2update[.]cc, ve ads-tm-glb[.]click. Bu diğer denetleyicilerde görülmeyen bu alan adları kümesinin başka bir ortak özelliğidir. Bunların her biri tek bir IP adresi döndürdü; ancak beklenen statik IP adresi yerine yanıtlarda 104 benzersiz adres bulduk. Bu, özellikte varsayılan Pupy'den bir farklılığa işaret ediyor gibi görünüyor, ancak amacını bilmiyoruz.

İKİLİ ÖRNEK ANALİZİ

DNS keşiflerimizin ardından, Pupy'den gelen farklılıkların kaynağının kolayca belirgin olup olmadığını belirlemek için VirusTotal'da bulunan ikili örneklere baktık. İki Decoy Dog örneğinin içe aktarımları ve işlev tablolarını analiz ederek, ek Decoy Dog örneklerini keşfetmemizi sağlayan Decoy Dog implantlarına özgü benzersiz bir imza belirledik. Bu örneklerin ters mühendisliği, Decoy Dog'un Pupy'den önemli ölçüde farklı olduğu ve en olgun kodun ikinci bir geliştirici tarafından oluşturulmuş olabileceğini bulgularımızı daha da doğruladı. İstemci Python 3.8'e yükseltildi ve bir dizi yeni aktarım, yükseltilmiş şifreleme, özel komutlar ve yeni DNS işlevselliği içeriyor. Bir denetleyici olan claudfront[.]net ile ilgili örnek, diğerlerinde bulunmayan özellikler içeriyor. Bu bölümde bazı temel bulgular ve süreç açıklanmaktadır; daha fazla teknik ayrıntı Ek F'de verilmiştir. İkili dosyalarla ilgili analitik veriler de GitHub depomuza eklenecektir.

İlk örnek Eylül 2022'de, diğerleri ise 2023'te yüklenmiştir. Bunlardan üçü de bizim açıklamamızı takiben yüklenmiştir. Farklı Decoy Dog örneklerinin yapılandırmalarını çıkardık ve karşılaştırdık. Bu da şifreleme anahtarlarının sunucular arasında farklılık gösterdiğini ortaya koydu. cbox4[.]ignorelist[.]com ile iletişim kuran tüm örnekler aynı RSA ve SSL anahtarlarını içeriyor. Bu da farklı örneklerin varlığının sunucu anahtarı değişiklikleriyle ilgili olmadığını gösteriyor. Şifresi çözülen anahtarların tam listesi Ek I'da ayrıntıları verilen Github deposunda bulunabilir. Örneklerdeki en eski SSL sertifikası 26 Aralık 2021'de oluşturulmuş ve gözlemlenen ilk denetleyici olan cbox4[.]ignorelist[.]com'a ait.

Önemli bir keşif, Decoy Dog'un Pupy istemcisinde, saldırganların Java modüllerini bir JVM (Java Virtual Machine) iş parçacığına enjekte ederek çalışma zamanında göndermesine ve çalıştırmasına imkan veren özel kod içermesiydi. Bu yetenek Pupy'nin standart sürümlerinde mevcut değil. Bu kod tüm Decoy Dog örneklerinde bulunmuştur ve tüm örneklerde aynıdır. Bilinen tüm Decoy Dog istemci örneklerinde kalan ikili işlevler, temel Pupy istemcilerindeki işlevlerle aynıdır.

Java modüllerinin dahil edilmesi, cevaplardan çok soruları gündeme getiriyor. Varsayılan olarak, Pupy zaten oldukça yetenekli ve Python modüllerinin kullanımını kutudan çıkar çıkmaz destekliyor. Bu yetenekleri genişletmek ve Python modülleri yazmak, sunucu tarafında değişiklikler veya istemci ikili dosyasında değişiklikler gerektirmeyen basit bir işlem.

Biri kolayca Java modüllerini yürütmek ve çalıştırmak için bir Python modülü oluşturabilir. Bunun aksine, jni.h (veya standart Java/C API'sinin geri kalanı) kullanmadan Java modüllerini çalışma zamanında enjekte etmek kolay bir iş değil ve özel bilgi gerektirir. Dolayısıyla, bu Java modüllerinin eklenmesi, saldırganların Python çalıştırmayan sistemleri, ayrıcalıklı veya izlenmeyen bir Java sanal makinesi çalıştıran sistemleri veya dosya oluşturmayarak makinede kanıt bırakmaktan kaçınmayı amaçladıkları senaryoları hedeflemelerine olanak tanıyabilir.

Müşteriler ayrıca zamanla olgunlaşan yeni işlevselliğe sahiptir. İstemci yazılımı, bir Python yapılandırma dosyasını belirli bir ikili dosyaya sıralayarak oluşturulur. Yapılandırma dosyası ayarları, iletişim için gerekli tüm anahtarları (RSA, SSL sertifikaları, şifreler vb.) ve istemci Python modüllerini içerir. Güvenliği ihlal edilmiş cihazlar tarafından paketlenip çalıştırılan örneklerde bulunan modüller, halka açık Pupy kodundan çok farklıdır.

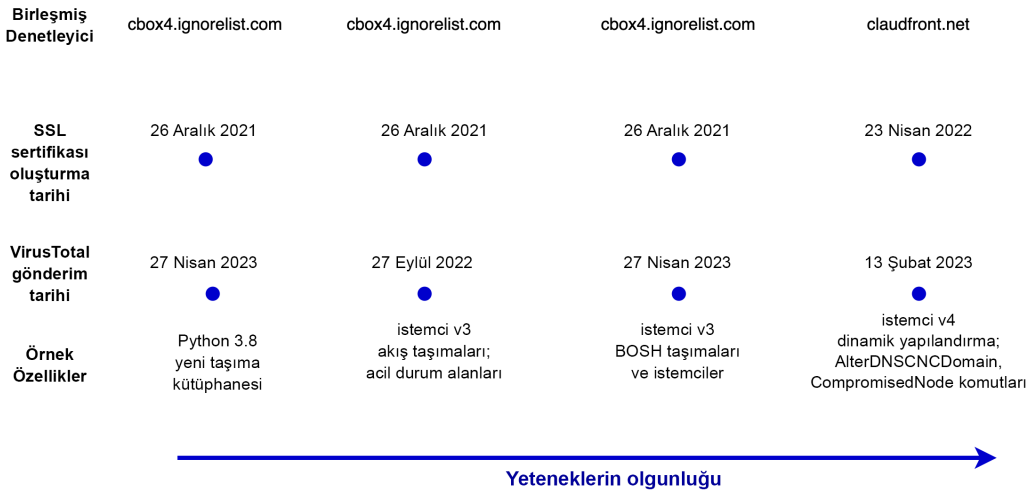
Gömülü modülleri çıkarmak ve analiz etmek, Decoy Dog gelişmelerinin ve özel değişikliklerin büyüleyici bir hikayesini anlatıyor. İlk olarak, önemli sayıda Pupy modülü, muhtemelen saldırganlar tarafından işe yaramaz bulundukları için Decoy Dog'dan kaldırılmıştır. İkinci olarak, benzer örnekler, bazen çok farklı yeteneklere sahip olan modüllerde çok sayıda farklılık sergiler. Üçüncüsü, çok sayıda değişiklik ve yeni işlevlerin eklediği karmaşıklık, Pupy'nin önemli geliştirme süresi ve kaynak ince ayarını göstermektedir. Ayrıca Pupy kod tabanı ve modülleri Python 2.7'den Python 3.8'e taşındı. Bu da kodun kalitesini, bellek işlemlerinin kararlılığını ve Windows ile uyumluluğu geliştirdi. Örnekler, zaman içinde 3'ten 4'e değişen bir istemci sürümü içermektedir. Mevcut en son Pupy istemcisi sürüm 2'dir. Kod olgunluğu ve temel özelliklerle karşılaştırmalı olarak gönderim tarihlerini özetleyen bir zaman çizelgesi aşağıdaki Şekil 16'da yer almaktadır.

Değiştirilen modüllerin yapısını ve sayısını analiz ederek, kod olgunluğu perspektifinden, ad186df91282cf78394ef3bd60f04d859bcacccbcdcbfb620cc73f19ec0cec64 hash değerine sahip örneğin, halka açık en eski Decoy Dog ikili programı olduğunu tespit edebildik. Bu program cbox4[.]ignorelist[.]com ad sunucusu ile iletişim kurar. Pupy ile en çok kodu paylaşmasına rağmen bu örnek, makalemizin yayınlanmasından birkaç gün sonra olan 27 Nisan 2023'e kadar VirusTotal'a yüklenmedi. Ancak dahil edilen SSL sertifikasına göre bu örneğin tarihi Aralık 2021'e kadar geçmişte olabilir. Geliştirici, özel yoklama işlevi, bir XOR işlevi, yeni aktarımlar ve çok iş parçacıklı ağ iletişimi için tam destek ekledi. İlginç bir şekilde, şimdiye kadarki tüm örnekler Linux kütüphaneleri olmasına rağmen, bir dizi yeni modül özellikle Win32'yi hedeflemektedir. Bu çalıştırılabilir dosyada, DNS iletişimlerini işlemekten sorumlu kod varsayılan Pupy ile aynıdır.

Zaman geçtikçe, cbox4[.]ignorelist[.]com ile iletişim kuran örnekler daha karmaşık hale geldi. Üç örnekten oluşan bir seri boyunca, senkron HTTP (BOSH) üzerinden çift yönlü akışlar kullanarak iletişim kurmak için tüm bir modülün yanı sıra SSL, TCP ve UDP modüllerinin tamamen yeniden yazılması da dahil olmak üzere artan sayıda iletişim modülü eklenmiştir. Decoy Dog'un arkasındaki aktörler ayrıca mevcut istismar ve iletişim modüllerini Windows platformlarına taşımak için bir dizi komut dosyası ekledi, DNS iletişiminden sorumlu picocmd istemcisini yeniden yazdı ve eski koda bir dizi yaşam kalitesi ve kararlılık iyileştirmesi uyguladı. Koddaki Windows'a yapılan atıflar, mevcut örneklerin tümü Linux'u hedeflemesine rağmen, yeni Decoy Dog yeteneklerini içeren güncellenmiş bir Windows istemcisinin varlığına dair ipucu veriyor.

Daha sonraki sürümler ayrıca kötü amaçlı yazılımın uzun bir süre boyunca C2 sunucusuyla iletişim kurması engellenirse, güvenliği ihlal edilmiş bir makinenin üçüncü taraf bir DNS sunucusuyla iletişim kurmasını sağlayan bir acil durum modülü içeriyor. Bu modül, istemcinin ücretsiz dinamik DNS hizmetleri içinde sorgulaması için alanları seçmek üzere bir DGA kullanır. Bu sürümler ayrıca C2 denetleyicisini bulmak için önyükleme yapılmasına, işaret alanlarının oluşturulmasına ve CNAME sorgularının acil durum hizmetine dahil edilmesine olanak tanıyor. İstemci sürüm 3'ten itibaren bulunan kapsamlı kalıcılık mekanizmaları, finansal olarak motive olmuş aktörler veya kırmızı ekipler tarafından yürütülenlerden ziyade çoğunlukla istihbarat operasyonlarıyla ilişkilendirilen yeteneklerdir.

claudfront[.]net denetleyicisine bağlanan en olgun kod AlterDnsCncDomain ve CompromisedNode adlı iki yeni komut içeriyor. Daha önce açıklandığı gibi, istemci nonce değerlerinin analizi yoluyla, Decoy Dog aktörlerinden bazılarının, ifşamızın ardından istemcileri yeni denetleyicilere geçirdiğini belirledik. Kamuya açık mevcut Pupy kaynak koduna dayanarak, özel komutlar kullanmadan bunun nasıl mümkün olduğunu göremedik. AlterDnsCnCDomain komutunun bu istemci geçişlerinin kaynağı olması muhtemel görünüyor ve bu nedenle nsdps[.]cc ile ilişkili denetleyiciler en gelişmiş kodu kullanıyor olabilir. Bu kodun diğerlerinden büyük ölçüde ayrılması, yeni bir geliştiricinin dahil olduğunu gösterebilir. Kod, istemcinin 4. sürümünü içeriyor.



Şekil 16. VirusTotal Decoy Dog ile ilgili gönderimlerin zaman çizelgesi ve kodun olgunluğu.

Decoy Dog'un tüm geliştirmelerine rağmen, Pupy'nin daha temel sürümleri için geliştirilen YARA kurallarının hala kötü amaçlı yazılımları tespit etmeyi başardığını belirtmekte fayda var. Ancak, örneklerin bilinen kod ve yeteneklerden önemli ölçüde saptığını algılayamazlar. Bu durum kötü amaçlı yazılım araştırmacılarını Decoy Dog örneklerinin basit Pupy olduğu gibi yanlış bir varsayıma yönlendirebilir çünkü her iki kötü amaçlı yazılım türü de aynı kural tarafından işaretlenmektedir. Bu nedenle, Ek G'de Decoy Dog için yeni bir YARA kuralı ekledik.

DENETLEYİCİLERİN KARŞILAŞTIRILMASI

Infoblox şu anda 21 Decoy Dog alan adını takip ediyor. Bunların bir kısmında gözlemlenebilir C2 faaliyeti ya çok az ya da hiç yok ve şu anda bunları açıklamıyoruz. Bazı denetleyiciler sosyal medyadaki ilk açıklamamızın ardından ve geri kalanı da ilk makalemizi yayınladıktan sonra değişti. Hepsi ya operasyonları durdurarak, ya istemcileri yeni denetleyicilere taşıyarak ya da makalede tanımladığımız "ping" davranışını değiştirerek yanıt verdi. Hatta bazıları coğrafi sınırlama bile ekledi. Bu yanıtlar, kullanılan diğer TTP'lerle birlikte, şu anda araç setini kullanan en az üç aktör olduğu sonucuna varmamızı sağlıyor. Aşağıdaki Tablo 1'de, denetleyici alanlarının bir alt kümesini davranışlarına ve benzer özelliklerine göre gruplandırdık.

Alan Adları Grubu	Özellikler
cbox4.ignorelist[.]com	• İlk aktif alan adı ve muhtemelen Decoy Dog araç setinin kaynağı • ifşa edildikten sonra devre dışı bırakıldı • Afraid dinamik DNS kullanımı • kalp atışı aralığı 30 saniye • coğrafi olarak sınırlandırılmamış • en az üç farklı istemci yazılımı yinelemesi • tarafımızdan ilk olarak Mart 2022'nin sonlarında gözlemlenmiştir, ancak Aralık 2021 gibi erken bir tarihte de mevcut olabilir • istemci v2 ve v3
claudfront[.]net allowlisted[.]net maxpatrol[.]net atlas-upd[.]com	• Mayıs 2022'de başlayan ikinci aktif denetleyici seti • açıklamanın ardından operasyonlara devam edildi • Namecheap ile kayıtlı • uzaktan şifreli iletişim ilk kez görülmeden önceki ping12 sorguları.<domain> • NODATA yanıtına verilen ping yanıtını değiştirdi • Rusya IP barındırma • kalp atışı aralığı 30 saniye • coğrafi olarak sınırlandırılmamış • istemci v3 ve v4 • allowlisted[.]net ve claufront[.]net arasında farklı aktörlere işaret edebilecek bazı farklar var
hsps[.]cc nsdps[.]cc j2update[.]cc ads-tm-glb[.]click	• Aralık 2022'de başlayan üçüncü aktif denetleyici seti • ifşa edildikten sonra istemcileri denetleyiciler arasında taşıdı • park edilmiş orijinal denetleyiciler • 2 dakika 30 dakikalık kalp atışı aralıkları • ifşa edildikten sonra coğrafi sınırlama getirildi • yerel olmayan tek bir geridöngü IP adresine verilen ping yanıtı değiştirildi • tek alan etiketi kullanımı: m • muhtemelen istemci v4
rcmsf100[.]net	• ilk olarak Haziran 2023'te gözlemlendi • barındırmayı allowlisted[.]net ile paylaşıyor • NODATA'nın ping yanıtı • coğrafi sınırlama

Tablo 1. Birkaç Decoy Dog denetleyicisinin karşılaştırması.

INFOBLOX AĞLARINDA DECOY DOG

Infoblox, çözümleyicilerimizin Decoy Dog sorgularını yeniden oynatan bir güvenlik satıcısı tarayıcısı tarafından tetiklendiğini belirledi. Tarayıcının davranışı ve Decoy Dog'un davranışının bir kombinasyonu tespit edilen sinyali oluşturdu. İnternet taraması önemli bir iş haline geldi ve tarama artık internet trafiğinin büyük bir kısmını oluşturuyor. Hem meşru hem de kötü niyetli aktörler tarafından gerçekleştirilmektedir. Yakın zamanda yapılan bir çalışmada bu taramaların etkisini anlamak için bir darknet teleskopu kullanılmıştır.[17] Taramalarınçoğu port taramalarıyla sınırlı olsa da küresel IP alanındaki açık portları belirlemek için, ortamda çok çeşitli başka tarama faaliyetleri de vardır. Örneğin, açık dizinleri ve açık DNS çözümleyicilerini arayan tarayıcılar vardır. Bazı kuruluşlar tarama faaliyetlerini tam olarak belgelemektedir, ancak çoğu bunu yapmaz.

"Agresif tarama", bir ağın performansını düşürme potansiyeli olan yetkisiz veya yüksek hacimli tarama etkinliğidir. Bir ağa hizmet reddi oluşturabilir veya Decoy Dog örneğinde olduğu gibi yanlış güvenlik olayları oluşturabilir.[18] Agresif tarama, sahipleri faaliyeti kabul etmeyen ağlar pahasına operatöre fayda sağlar. Nisan 2023'te, Decoy Dog algılamalarına sahip ağların güvenlik ekipleri, sistemlerinin güvenliğinin ihlal edilmediğinden emin olmak için bu DNS sorgularının temel nedenini bulmaya çalışmak için önemli kaynaklar harcadı. Bu sorgular, ağırlıklı olarak güvenlik duvarlarından kaynaklandığı için özellikle endişe vericiydi ve güvenlik duvarı sektörü, son aylarda güvenlik duvarlarına yönelik saldırılarla ilgili artan endişelerini dile getirdi.[19]

Decoy Dog sorgularının çözümleyicilerimize ulaşma şekli ve neden hedefli bir kötü amaçlı yazılım C2 işaretçisine benzer bir sinyale neden oldukları karmaşıktır. Savunucuların benzer faaliyetleri fark etmelerini desteklemek için kısa bir açıklama ve Şekil 17'de bir örnek sunacağız.

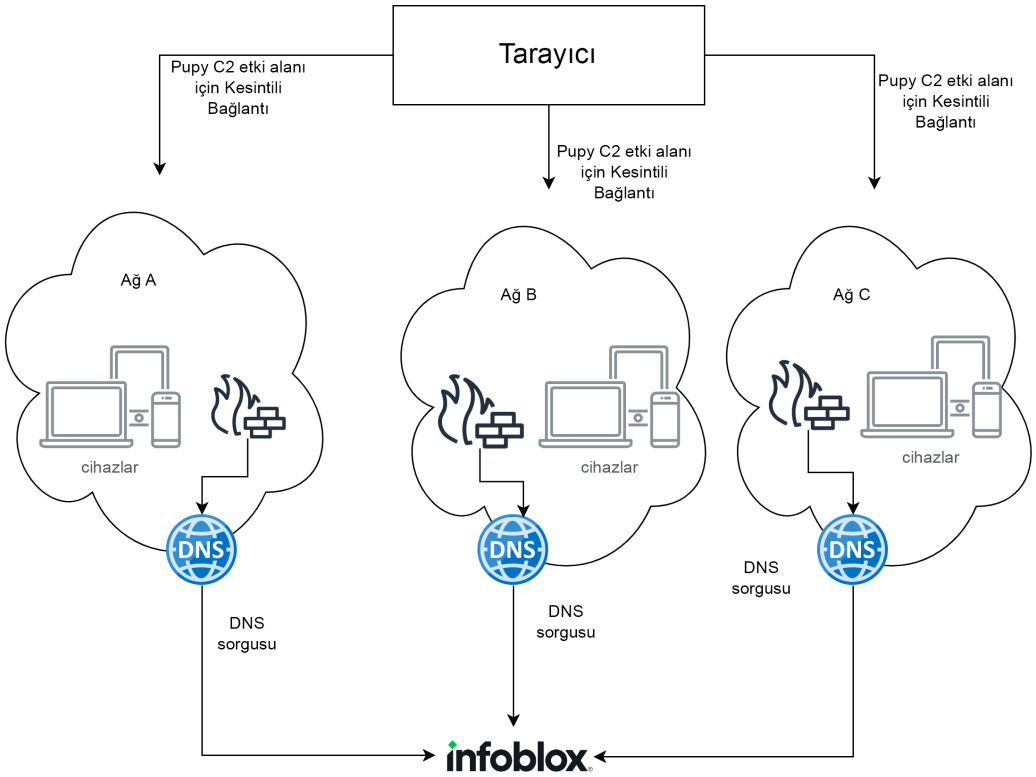
Infoblox'un Decoy Dog DNS sorgularını alabilmesi için, bir müşteri ağının DNS sağlayıcısı olarak Infoblox'a sahip olması gerekir. Ek olarak müşterinin, hem gelen URL filtrelemesi yapılandırılmış hem de bu cihazdan çözümleyicilerimize DNS iletmeyi içeren güvenlik duvarları gibi güvenlik araçlarına sahip olması gerek ir. Bu kriterler tek başına kısıtlayıcıdır. Bunlar karşılandığında aşağıdaki sıra meydana gelir:

- Tarayıcı, C2 adlı kötü amaçlı yazılımın içeriğini doğrudan ağ içindeki bir IP adresinden almaya çalışır. Bu DNS C2 iletişimleri web içeriği olmasa bile bunu yapar.
- Güvenlik cihazı isteği durdurur ve alan adını çözümlemeye çalışır.
- DNS isteği, sorguyu çözen ve yanıtı döndüren Infoblox'a iletilir. Alan adı müşteri tarafından yapılandırılmış bir DNS engelleme listesindeyse, sonuç döndürmez.
- Satıcı tarafından taranan alan adı Decoy Dog veya başka bir kötü amaçlı yazılım değilse, çözülecek ve güvenlik duvarı kurallarına bağlı olarak web sitesinin içeriği tarayıcıya iade edilecektir.

17 Aggressive Internet Wide Scanners: Network Impact and Longitudinal Characterization, May 2023, Anand, Dainotti, Sippe, Kallitsis. https://arxiv.org/pdf/2305.07193.pdf

18 https://live.paloaltonetworks.com/t5/general-topics/spurious-hits-from-the-expanse-webcrawler/td-p/447239, son erişim tarihi: 2023-06-11

19 https://blog.talosintelligence.com/state-sponsored-campaigns-target-global-network-infrastructure/, son erişim tarihi: 2023-06-11



Şekil 17. Decoy Dog DNS C2 alanları için sorgular, farklı ağların içindeki cihazlardan Infoblox çözümleyicilerine yapıldı. Bunlar ticari bir tarayıcıdan kaynaklandı ve aralıklı olarak tetiklendi.

Infoblox, satıcının IP adresinde bilinen açık bağlantı noktaları olmasa bile tarama gerçekleştirdiğini ve ortak bağlantı noktalarına ek olarak nadir bağlantı noktalarını kullanacağını belirledi. Satıcının hangi IP adreslerini ve portları kullanacağına nasıl karar verdiğini bilmiyoruz. Bu tür gelişigüzel agresif taramaların sonucu, çok hassas cihazların tehlikede olmadıkları halde tehlikede görünebilmeleridir. Satıcı geniş ve sürekli içerik tarıyor gibi görünse de, Infoblox yalnızca yukarıdaki kriterler karşılandığında DNS sorgularını gözlemledi. Sonuç olarak, satıcı tarafından yapılan taramaların sayısı çok fazlaydı ve bu da agresif tarama ile tutarlıydı, ancak zaman içinde aralıklı olarak yalnızca az sayıda sorguyu çözdük. Bu tür bir yapılandırma aynı zamanda bir aktörün belirli ağlar üzerinde keşif yapabilmesini de sağlar; bunu Ek H'de açıklıyoruz.

Infoblox Intelligence, tüm DNS etkinliklerinin geçmiş kayıtlarını tutar ve bunları ağlarımızdaki ve küresel DNS'deki alan etkinliğinin toplu istatistiklerini oluşturmak ve sürdürmek için kullanır. Bu toplamaları, kötü amaçlı yazılım C2 işaretçileriyle tutarlı anormal davranışlar da dahil olmak üzere çok çeşitli tehditleri tanımlamak için kullanırız. Özellikle, zaman içinde anormal sayıda müşteri ağında sorguların meydana geldiği, veri sızıntısı ile tutarlı alt alanlara sahip olan ve beklenen davranışlarına göre düşük sayıda sorguya sahip olan etki alanlarını arıyoruz. Bunu başarmak için, birçok yıl boyunca gözlemlediğimiz her alan adının istatistiklerini ve trilyonlarca DNS sorgusunu kullanıyoruz.

Decoy Dog ve diğer kötü amaçlı yazılım C2 işaretçileri keşfedildikten sonra son derece şüpheli görünür, ancak bunları tespit etmek çok zordur. Doğası gereği, DNS trafiği oldukça değişkendir ve büyük bir aykırı değer yüzdesi içerir, yani nadiren görülen ve veri sızıntısı ile tutarlı bir alan adı yapısına sahip olan alanlar anlamına gelir. Bununla birlikte, DNS sızıntısı ve işaretleme, yerleşik kalem testi faaliyetleri dışında çok nadirdir. Ayrıca, kalem testinin DNS imzası, kötü amaçlı yazılım C2 işaretçilerinden oldukça farklıdır. Decoy Dog, yüksek hacimli bir sistem olan Pupy RAT'ın bir varyantından DNS C2 olduğunu kanıtlasa da, trafik güvenlik satıcısı tarafından ağlara enjekte edildiği için düşük profilli bir işaret gibi görünüyordu.

Çözümleyicilerimize yapılan Decoy Dog sorguları tarayıcı tarafından başlatılmış olsa da, Decoy Dog ad sunucularının olağandışı davranışları nedeniyle tespit edildi. Önceki makalemizde açıklandığı gibi Decoy Dog isim sunucuları, bazen aralıklı da olsa tekrarlanan sorgulara yanıt veriyordu. Bu Pupy ve diğer şifreli iletişim protokolleri ile tutarsızdır. Artık denetleyicilerin iyi oluşturulmuş herhangi bir sorguya yanıt verdiğini öğrendik. Birleşik davranış, sistemlerimizin kesintili düşük hacimli bir işaret algılamasına neden oldu. Bir ağ içindeki bu tür tarama ve açık DNS yönlendirme davranışı, bir kuruluş için ek güvenlik riskleri oluşturur. Bir saldırgan, harici bir tarafın bir ağın içinden DNS sorgularını tetiklemesine izin vererek, bir ağa karşı keşif gerçekleştirebilir. Bu güvenlik açığını Ek H'de daha ayrıntılı olarak açıklıyoruz.

Sonuç

Decoy Dog açıkça ciddi bir tehdit. Bir avuç tehdit aktörü, DNS verilerinin izlenmesinden kaynaklanan tek belgelenmiş tespitlerle birlikte bir yıldan uzun bir süredir araç setini kullanıyor. Son derece hedefli operasyonlarda kullanılır ve yalnızca denetleyicilerinin çok sınırlı sayıda aktif istemciyle etkileşime girdiğini gözlemledik. Decoy Dog hakkında çok şey öğrenmiş olsak da, dayanağını oluşturmak için kullanılan güvenlik açıkları tespit edilene ve hafifletilene kadar ciddi bir tehdit olarak kalacaktır.

Decoy Dog'u ilk kez ifşa etmemizin ardından, tehdit aktörleri kurban sistemlerine sürekli erişim sağlamak için çeşitli şekillerde karşılık verdi. Bu yanıtlar, denetleyicilerin DNS yanıt davranışını değiştirmeyi, denetleyicilere coğrafi sınırlama kısıtlamaları eklemeyi ve istemcileri yeni denetleyicilere taşımayı içeriyordu. Bu adaptasyonlara rağmen, Infoblox onları izlemeye ve Decoy Dog hakkında daha fazla bilgi edinmeye ve Pupy RAT'tan nasıl farklı olduğunu öğrenmeye devam etti.

Decoy Dog'u oluşturmak için Pupy'de yapılan değişiklikler dikkate değer ve sofistike bir tehdit aktörünün göstergesi. Bu değişiklikler şunları içeriyor:

- Pupy Python 2.7'de yazılmıştı. Decoy Dog Python 3.8 gerektiriyor ve Windows uyumluluğu ve geliştirilmiş bellek işlemleri dahil olmak üzere çok sayıda iyileştirme içeriyor.
- Pupy'nin çok sınırlı bir iletişim sözlüğü vardır. Decoy Dog, birden fazla yeni iletişim modülünün eklenmesiyle bu kelime dağarcığını önemli ölçüde genişletiyor.
- Decoy Dog, Pupy'nin yapmadığı şekilde önceki DNS sorgularının tekrarlarına yanıt veriyor.
- Pupy wildcard karakter DNS isteklerine yanıt vermese de Decoy Dog yanıt veriyor. Bu, esasen pasif DNS'de görülen çözünürlük sayısını iki katına çıkarıyor. Aslında Decoy Dog, bir istemci ile geçerli iletişim yapısına uymayan DNS isteklerine yanıt veriyor.
- Decoy Dog, bir JVM iş parçacığına enjekte ederek rastgele Java kodunu çalıştırma yeteneğini ve kurbanın cihazında kalıcılığı korumak için bir dizi yeni yöntem ekliyor.

Bu değişikliklerin karmaşıklığı, Decoy Dog'un iyi hazırlanmış herhangi bir sorguya yanıt verme seçimini daha da merak uyandırıcı hale getiriyor. Bu karar ilk bakışta bir hata gibi görünse de, muhtemelen henüz bilinmeyen bir gerekçesi var. Şu anda bu, Decoy Dog'un başka bir gizemi.

Gelecekte Decoy Dog ile ilgili bu gizemler daha fazla araştırıldıkça, savunucular aşağıdakilere dikkat etmelidir:

- Hem Pupy hem de Decoy Dog'daki IP'ler şifrelenmiş verilerdir. İletişim için kullanılan gerçek IP'leri temsil etmezler. Kötü amaçlı yazılımlarla ilişkili gerçek IP'lere yapılan tüm bağlantılar sahtedir.
- DNS yanıtlarında döndürülen IP'ler anlamlı olmasa da, DNS sorguları ve yanıtlarının kendileri izleme için kullanılabilecek anlamlı bilgilere sahiptir. Bununla birlikte, iletişim hacmi düşüktür, yani tespit edilen iletişimleri izlemek için uzun bir günlük geçmişine ihtiyaç vardır.

- Araç setinin wildcard yanıtları, güvenlik sağlayıcısının agresif taramasıyla birleştiğinde, hiçbir tehlike olmadığı halde tehlike varmış gibi görünebilir.
- Kurban makinedeki Decoy Dog istemcisini tespit edebilen bir YARA kuralı mevcuttur. Bu kural, Decoy Dog'u Pupy'nin halka açık versiyonundan ayırt edebilmektedir.

Decoy Dog yalnızca DNS tehdit algılama algoritmaları kullanılarak tespit edildi. Bugüne kadar, kötü amaçlı yazılımın kendisinin tespitlerini açıklayan kamuya açık bir açıklama yapılmadı ve yeteneklerinin tam kapsamı henüz bilinmiyor. Bu kadar uzun süre tespit edilmeden çalışmış olması, sektörün kötü amaçlı yazılım tabanlı tespite aşırı güvenmesi durumunda ortaya çıkan bir zayıflığı vurgulamaktadır. DNS tespiti ve tepkisi şu anda Decoy Dog'a karşı savunmanın tek yolu ve kurbanların zayıf noktaları ve Decoy Dog'un kendisi tam olarak anlaşıldıktan sonra bile en iyi seçenek olabilir.

Göstergeler

Bu raporda açıklanan denetleyiciler ve örneklerle ilgili Decoy Dog göstergeleri aşağıda listelenmiştir ve açık Github depomuzda mevcuttur.[20]

Alan Adları Grubu	Özellikler
ads-tm-glb[.]click	Decoy Dog C2 alan adı
allowlisted[.]net	Decoy Dog C2 alan adı
atlas-upd[.]com	Decoy Dog C2 alan adı
cbox4[.]ignorelist[.]com	Decoy Dog C2 alan adı
claudfront[.]net	Decoy Dog C2 alan adı
hsdps[.]cc	Decoy Dog C2 alan adı
j2update[.]cc	Decoy Dog C2 alan adı
maxpatrol[.]net	Decoy Dog C2 alan adı
nsdps[.]cc	Decoy Dog C2 alan adı
rcmsf100[.]net	Decoy Dog C2 alan adı
13[.]248[.]169[.]48	Decoy Dog C2 ad sunucusu IP'si
156[.]154[.]132[.]200	Decoy Dog C2 ad sunucusu IP'si
194[.]31[.]55[.]85	Decoy Dog C2 ad sunucusu IP'si
5[.]199[.]173[.]4	Decoy Dog C2 ad sunucusu IP'si
5[.]252[.]176[.]63	Decoy Dog C2 ad sunucusu IP'si
5[.]252[.]176[.]22	Decoy Dog C2 ad sunucusu IP'si
5[.]252[.]179[.]18	Decoy Dog C2 ad sunucusu IP'si

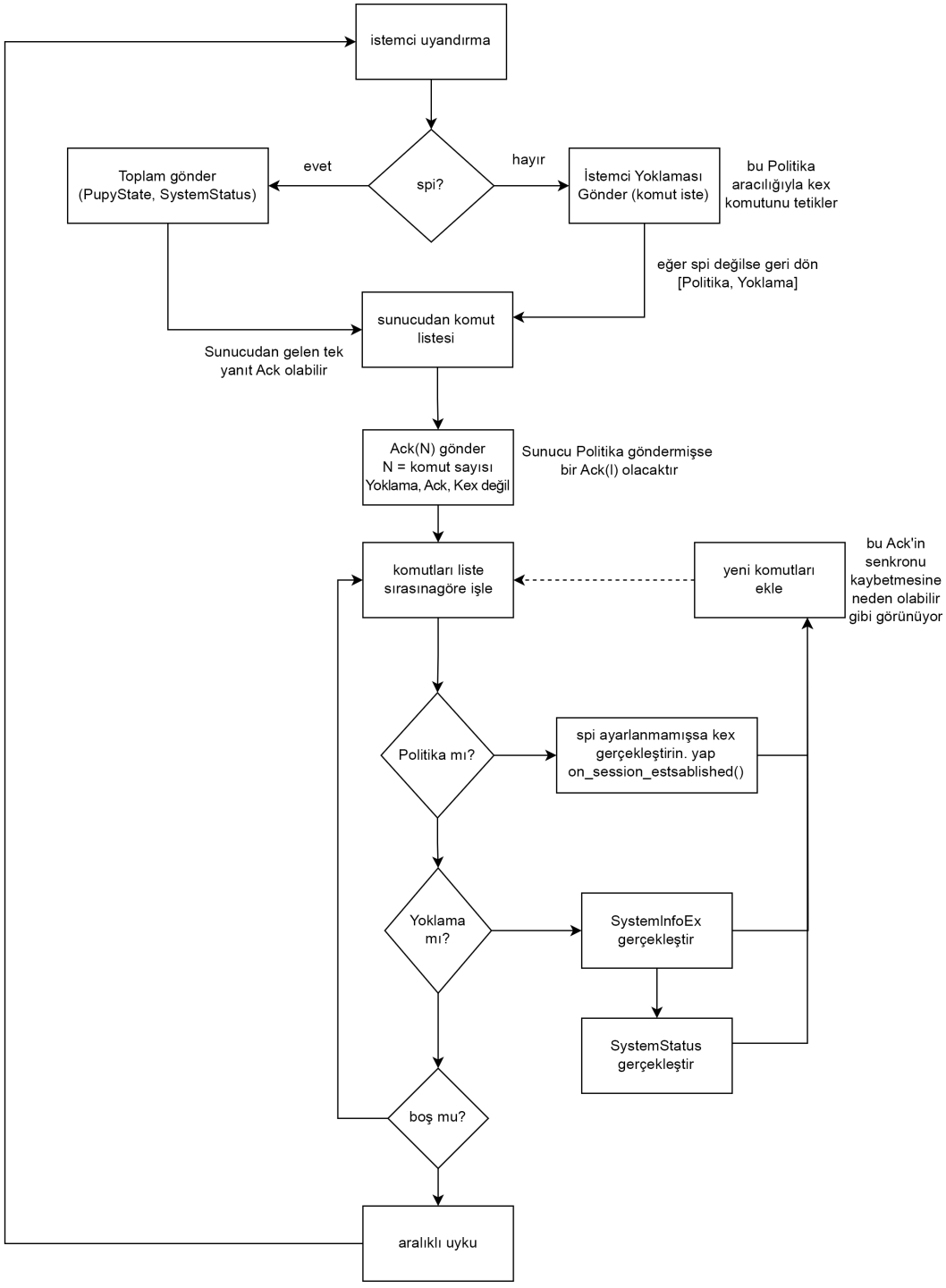
20 https://github.com/infobloxopen/threat-intelligence/tree/main/cta_indicators

67[.]220[.]81[.]190	Decoy Dog C2 ad sunucusu IP'si
69[.]65[.]50[.]194	Decoy Dog C2 ad sunucusu IP'si
69[.]65[.]50[.]223	Decoy Dog C2 ad sunucusu IP'si
70[.]39[.]97[.]253	Decoy Dog C2 ad sunucusu IP'si
83[.]166[.]240[.]52	Decoy Dog C2 ad sunucusu IP'si
4996180b2fa1045aab5d36f46983e91dadeebf d4f765d69fa50eba4edf310acf	Decoy Dog ikili SHA256
ab8e333ef9bc5c5a7d1ed4cab08335861e150 b0639d3d0ca4c30b7def5cdccde	Decoy Dog ikili SHA256
ad186df91282cf78394ef3bd60f04d859bcaccc bcdcbfb620cc73f19ec0cec64	Decoy Dog ikili SHA256
6c8f413111f1abfee788dad4ee7cca37e0c259 7cca66d155af958c535faf55cc	Decoy Dog ikili SHA256
0375f4b3fe011b35e65751335394410 09d015 ebecbee78b578c3ed04e0f22568	Decoy Dog ikili SHA256
6c8f413111f1abfee788dad4ee7cca37e0c259 7cca66d155af958c535faf55cc	Decoy Dog ikili SHA256
t1fde0f101c9395f39ecd16430b41041a59107 c73c904087309fb8d0e8d87e0077129f3f	Decoy Dog Telfhash imzası[21]

21 https://github.com/trendmicro/telfhash

EK A: İSTEMCI KOMUT İŞLEME

Şekil 18, makalede açıklanan istemcinin çalışma döngüsünü göstermektedir. İstemci sürekli olarak uyku, sunucuyu yoklama ve komutlara yanıt verme arasında geçiş yapar.



Şekil 18. İstemci iş akışı.

EK B: İLETİŞİM YÜKÜ YAPISI

İstemci ve sunucu için şifrelenmiş yükün yapısı aynıdır, ancak işlemlerinde farklılıklar vardır. Özellikle, istemci her sorguda daha önce açıklandığı gibi veri yükü ile birlikte 13 bayt istemci bilgisi içerir.

Hem istemci hem de sunucu, alıcıya ilettikleri bilgi türü için komut terimini kullanır. Bu nedenle, istemci uyandıktan sonra sunucuyla iletişim kurduğunda, bu bir istemci komutu olarak kabul edilir. Komutlar, istemci veya sunucunun verilere özel işlem uygulayabilmesi için kaydedilir. Tek bir iletişimde birden fazla komut olabilir, ancak istemciden bu nadirdir.

Kodlama ve iletim için gönderilen yük aşağıdaki forma sahiptir:

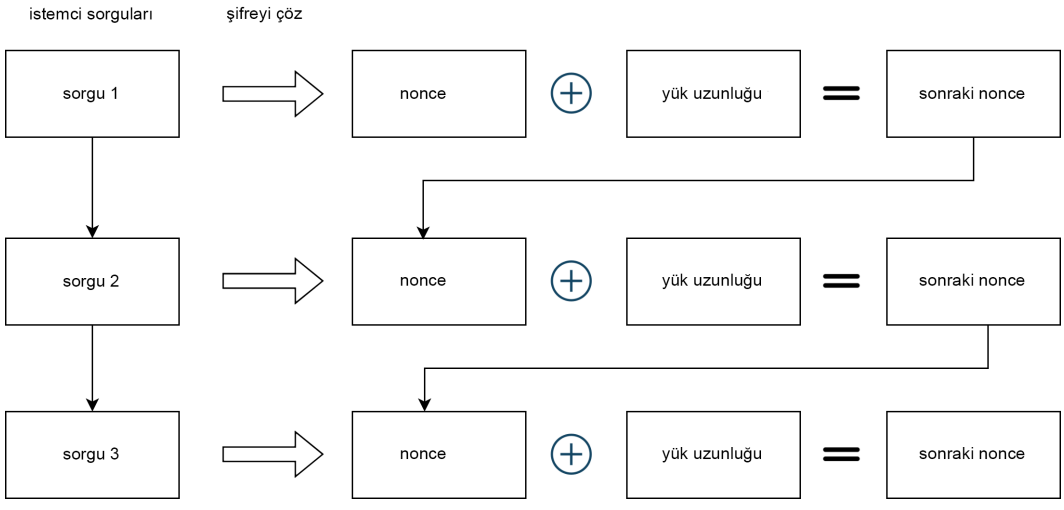
- 4 baytlık bir sağlama toplamı,
- 1 baytlık bir komut tanımlaması ve değişken bir komuta bağımlı veri bölümü içeren birleştirilmiş komut paketleri.

Yükün toplam uzunluğu 52 baytı aşamaz.

EK C: MÜŞTERİLERİN PASİF VERİLERDEN YENİDEN YAPILANDIRILMASI

Daha önce açıklandığı gibi, Pupy sorguları şifrelenmiş veri ve iki kodlanmış değer içerir (nonce ve SPI). Bunlar bir miktar güvenlik sağlar ve sunucunun istemci iletişimlerini sıraya koymasını sağlar. SPI değeri özellikle sunucu içinde devam eden bir oturumu tanımlamak için kullanılır ve başarılı bir anahtar değişiminin ardından sorgularda bulunur. Sonuç olarak, aynı SPI'yı içeren ve yakın zamanlarda gerçekleşen sorguların aynı istemciden geldiği neredeyse garantidir. Öte yandan, tek bir istemcinin zaman içinde birçok oturumu ve birçok SPI değeri olacağı için SPI tek başına istemcileri ayırt edemez. Bunun yerine, istemci iletişimlerini ayırmak için nonce değerlerini kullanırız.

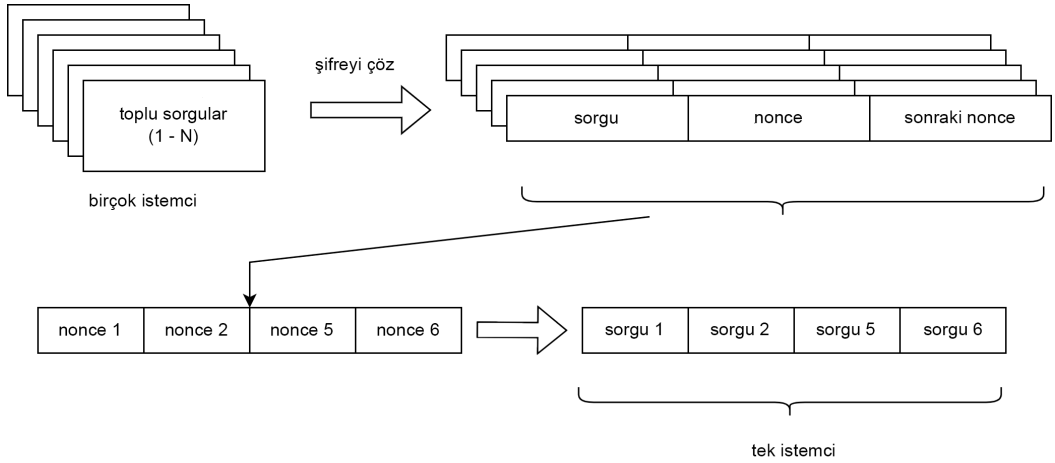
İstemci başlatıldığında, başlangıç noktası olarak kullanılmak üzere rastgele 32 bitlik bir nonce değeri üretir. Her pakette, bu nonce iletilen verinin uzunluğu kadar artırılır. Sunucu, nonce'u küçük bir güvenlik kontrolü olarak kullanır ve alınan her sorguda artmasını sağlar, ancak birincil kullanımı, temel iletişimin doğru şekilde şifresini çözmek ve yorumlamaktır. Gözlemlenen bir dizi Pupy sorgusundan, bu nonce değerlerini çözebilir ve aşağıdaki Şekil 19'da gösterildiği gibi serideki bir sonraki nonce'u hesaplayabiliriz.



Şekil 19. Bir dizi Pupy sorgusu içindeki nonce değerlerinin ilişkisi.

Sonuç olarak, hem tek bir istemciden gelen sorguları sıralayabilir hem de bir dizi sorgunun tek bir istemciye ait olduğunu doğrulayabiliriz. Bir Pupy dağıtımının pasif toplanmasında, sorgular birçok istemciden gelebilir ve zaman içinde çakışabilir. Ancak yine de nonce'un yapısı sayesinde bu gözlemleri yüksek bir güvenle ayrı istemci etkinliklerine ayırabiliriz. Nonce yükü şifrelemek için kullanıldığından, geliştirici bunu oluşturmak için güçlü bir rastgele sayı üreteci kullanmıştır. Bu, her bir istemcinin benzersiz başlangıç nonce değerleri üretmesini sağlar.[22] Nonce, istemcinin her yeniden başlatılmasında yeniden oluşturulur.

Şifreleme için ekstra güvenlik, müşterileri toplu gözlemlerde ayırt etmek için bir mekanizma da sağlar. Bunu yapmak için, her sorgu için hem kodlanmış nonce hem de bir sonraki nonce değerini hesaplarız. Daha sonra aşağıdaki Şekil 20'de gösterildiği gibi sıralı nonce değerlerini kullanarak sorguları birbirine zincirleriz. Temel veriler şifreli kalırken, istemci sayısını tahmin edebilir ve faaliyetlerinin uzunluğu hakkında gözlemler yapabiliriz. Ayrıca, yük uzunluklarını kullanarak ve istemciler arasındaki zaman serilerini karşılaştırarak iletişimin kendisi hakkında bilgi edinebiliriz.



Şekil 20. İstemci sorgu iş parçacığını nonce değerlerini kullanarak toplu gözlem kümesinden ayırma.

Bu tür bir istismarla ilgili iki zorluk vardır: virüslü istemcinin DNS çözümleyicisindeki değişiklikler ve paket bırakmaları. Varsayılan olarak, Pupy istemcinin varsayılan DNS çözümleyicisini kullanır ve çözümleyici seçimi aktörün kontrolü altında olmayabilir. İstemci dolaşıyorsa, yerel ortama bağlı olarak farklı özyinelemeli çözümleyiciler kullanabilir. Kurumsal ağlarda, istemcinin ayarlarından bağımsız olarak DNS sorgularının kurumsal özyinelemeli çözümleyiciler üzerinden zorlanacağı Infoblox gibi satıcıların DNS altyapısını kullanabilirler.[23] yrıca, DNS UDP üzerinden taşındığında paket kaybı kaçınılmazdır. Sonuç olarak, her sorguyu yalnızca pasif DNS'de gözlememiz pek olası değildir. Bu nedenle kurtarılan nonce zincirinde boyut olarak önemli olabilecek boşluklar yaratırız.

Bununla birlikte, nonce'un rastgele oluşturulmuş bir değer olmasından yararlanarak istemci iş parçacıklarını yeniden yapılandırabiliriz. Geliştirici, bağımsız Pupy istemcilerinin bir nonce değerini paylaşma olasılığının son derece düşük olmasını sağlayan güçlü bir sayı üreteci kullandı. Ayrıca, bir seferde yalnızca 52 bayt veri iletilebildiğinden ve nonce değeri yük tarafından arttığından, bağımsız olarak oluşturulan iki nonce zincirinin örtüşmesi olası değildir. Sonuç olarak, istemciler nonce değerleri sıralanarak ve istatistiksel olarak olanları

22 Aynı nonce'un iki farklı istemci tarafından aynı anda üretilmesi nadir bir olasılıktır.

23 Who is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path, Baojun Liu, et al. 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/liu-baojun

gruplandırarak ayrılabilir benzer. Tek bir istemci aynı anda yalnızca bir nonce'a sahiptir, bu da herhangi bir zamanda aktif istemci sayısını tahmin etmemize olanak tanır. Makalenin ana gövdesinde gösterdiğimiz gibi, bu tekniğin Decoy Dog istemci sorgu zincirlerini kurtarmada çok etkili olduğunu gördük.

EK D: YÜK İMZALARI

Bu bölümdeki tablolar, Pupy iletişimlerinde yaygın olarak gözlemlenen belirli komutlar için yük uzunluklarını içerir. Özellikle, her standart istemci komutu için şifrelenmiş yük uzunluğunu sağlarlar. Sunucu yükleri istemcilerinkinden daha esnektir. En yaygın olanları aşağıda gösterilmiştir.

İstemci Komutu	Yük Uzunluğu
İstemci girişi (ilk)	18
Ack	19
Müşteri girişi (nadir değişken)	22
Sistem durumu	24
Çevrimiçi durum	27
İstemci girişi (oturumda)	27
Bağlantı noktası testi	35
Sistem bilgileri genişletildi	39
Anahtar değişimi	47, 48

Tablo 2. İstemci komutları ve yük uzunlukları.

Sunucu Komutu	Yük Uzunluğu
Ack	6
Oturum gerekli: politika, yoklama	42
Oturum tamamlanmadı: onay, politika	34
Hata: mesaj, politika, yoklama	44
Sistem bilgisi gerekiyor: yoklama	15
Anahtar değişimi	62, 63
Çıkış	7

Tablo 3. Ortak sunucu komutları ve yük uzunlukları.

EK E: HATA İŞLEME

Pupy, sunucunun karşılaşabileceği çeşitli hatalar için özel işlemler içerir. Doğru şekilde kodu çözülmeyen veya yeniden oynatılan bir alan adı sunucudan NXDOMAIN yanıtı alınmasına neden olur. Aşağıdaki kod parçacığı sunucu sorgu işlemesini gösterir. Yanıt döndürülmezse bir NXDOMAIN yanıtı döndürülür.

```
answers = self.process(qtype, qname.stripSuffix(self.domain).idna()[:-1])
klass = SUPPORTED_METHODS[qtype]


if answers:
    for answer in answers:
        reply.add_answer(RR(qname, qtype, rdata=klass(answer), ttl=600))


    if self.edns:
        reply.add_ar(EDNS0(udp_len=512))
else:
    reply.header.rcode = RCODE.NXDOMAIN
```

Şekil 21. İstemci sorgularını işleyen Pupy sunucusu kaynak kodu.

Decoy Dog'da, sunucudan bir NXDOMAIN ile sonuçlanması gereken birçok istemci sorgusu, bunun yerine tipik olarak 15 IP adresi gibi bir yanıt döndürür. Bu durum, Decoy Dog'un çok çeşitli olası hatalara aşağıdaki gibi yanıt verdiği koddaki bir değişiklikten kaynaklanıyor gibi görünmektedir DnsCommandServerException dahili olarak. DnsCommandServerException, istemciye karşılaşılan hata türünü ve yeni bir anahtar değişimi gerçekleştirmesini ve ardından sistem bilgilerini iletmesini belirten bir yanıtla sonuçlanacaktır. Bu hata işleme için kod bloku aşağıda gösterilmiştir.

```
except DnsCommandServerException as e:
    nonce = e.nonce
    version = e.version
    responses = [e.error, Policy(self.interval, self.kex), Poll()]
    emsg = 'Server Error: {} (v={})'.format(e, version)
    logger.debug(emsg)
    if node:
        node.warning = emsg
```

Şekil 22. İstemciye hata döndüren Pupy sunucusu kaynak kodu.

Pupy sunucusu ve istemci arasındaki normal iletişimde, bilinen bir istemci için aktif bir oturum olmadığında bu tür bir istisna ortaya çıkacaktır. İstemci yükü geçersiz veya yanlış bir sağlama toplamına sahip olduğunda da kullanılır. Diğer tüm durumlarda sonuç bir NXDOMAIN olur.

EK F: İKİLİ ÖRNEK ANALİZİ

Pupy İstemci İkilileri

Pupy sunucusu ilk kurulduğunda, Pupy kütüphane dosyalarını derler ve her mimari için bir statik şablon dosyası oluşturur. Bu şablon dosyaları sıkıştırılmış, büyük ölçüde gizlenmiş ve tüm sembollerden arındırılmıştır.

İstemci ikili dosyaları daha sonra sunucuda pupygen.py kullanılarak manuel olarak oluşturulabilir. Komut dosyası, belirli yapılandırma baytlarını (uzak ana bilgisayar, taşıma türü, hata ayıklama bayrağı vb.) hedef mimariye ve dosya türüne karşılık gelen statik şablona sıralayarak C2'ye özgü ikili dosyalar oluşturur.

Pupy istemci ikili dosyaları, çeşitli gelişmiş işlevler sunar ve Windows, macOS, Linux, Solaris ve Android dahil olmak üzere hemen hemen her platformu hedefleyebilir. Özellikle, bellekte yerleşik olarak kalabilir, sunucuyla etkileşime girebilir, tam ters kabuk yetenekleri sunabilir, dosyasız kopyalar oluşturabilirler vb. İkili çalıştırıldığında, tespit edilmekten kaçınmak ve kendini işlem öldürme tekniklerine karşı daha dirençli hale getirmek için bellekte kendi kopyalarını oluşturacaktır.

Örnek Java Enjeksiyon Fonksiyonu

Decoy Dog ikili dosyaları Java enjeksiyonu ile ilgili bir dizi yeni işlev içerir. Bu, bu işlevlerden birine bir örnektir.

```
undefined8 FUN_00105903(void)
{
  int iVar1;
  long lVar2;
  long lVar3;
  long lVar4;
  undefined8 uVar5;
  char *pcVar6;
  undefined local_20 [8];
  undefined8 local_18;

  local_18 = 0;
  if (DAT_005fbda0 == 0) {
     pcVar6 = "JVM was not loaded yet";
  }
  else {
       jvm_address = check_jvm_is_running(0);

       if (jvm_address == 0) {
       return 0;
       }
       classloader_address = find_classloader(lVar2);
       if (classloader_address == 0) {
       pcVar6 = "Preferred classloader was not found";
       }
       else {
       thread_class_address = find_jv_thread(lVar2);
       if (thread_class_address == 0) {
       pcVar6 = "Could not find Thread class";
       }
       else {
       iVar1 =
inject_in_thread(jvm_address,thread_class_address,"currentThread","()Ljava/lang/Thread;",&lo
cal_18);
       if (iVar1 == 0) {
       iVar1 = inject_in_class(jvm_address,local_18,"setContextClassLoader","(Ljava/lang/ClassLoader;)V",
                                          local_20,classloader_address);
       if (iVar1 == 0) {
          uVar5 = (*DAT_005fb748)(1);
          return uVar5;
       }
      pcVar6 = "Iteration failed";
      }
      else {
      pcVar6 = "Could not find current JVM Thread";
      }
  return 0;
```

Şekil 23. Kısmen demonte edilmiş Decoy Dog fonksiyonu, enjeksiyon için mevcut çalışan JVM iş parçacığını bulmaya çalışıyor.

EK G: DECOY DOG İÇİN YARA KURALI

Temmuz 2023 itibariyle gözlemlediğimiz Decoy Dog örneklerini tespit etmek için aşağıdaki YARA kuralı kullanılabilir.

```
/*
This rule only detects Decoy Dog. It was adapted from Florian Roth's Pupy Rule
original author : Florian Roth / @neo23x0
original link : https://github.com/Neo23x0/signature-base/blob/master/yara/gen_pupy_rat.yar
*/

/* Rule Set ----------------------------------------------------------------- */
import "elf"
import "pe"

rule DecoyDog_Backdoor {
   meta:
     description = "Detects Decoy Dog backdoor"
     license = "Detection Rule License 1.1 https://github.com/Neo23x0/signature-
base/blob/master/LICENSE"
     author = "Infoblox Inc."
     reference = "https://github.com/n1nj4sec/pupy-binaries"
     date = "2023-07-11"

   strings:
     $x1 = "reflectively inject a dll into a process." fullword ascii
     $x2 = "ld_preload_inject_dll(cmdline, dll_buffer, hook_exit) -> pid" fullword ascii
     $x3 = "LD_PRELOAD=%s HOOK_EXIT=%d CLEANUP=%d exec %s 1>/dev/null 2>/dev/null" fullword ascii
     $x4 = "reflective_inject_dll" fullword ascii
     $x5 = "ld_preload_inject_dll" fullword ascii
     $x6 = "get_pupy_config() -> string" fullword ascii
     $x7 = "[INJECT] inject_dll. OpenProcess failed." fullword ascii
     $x8 = "reflective_inject_dll" fullword ascii
     $x9 = "reflective_inject_dll(pid, dll_buffer, isRemoteProcess64bits)" fullword ascii
     $x10 = "linux_inject_main" fullword ascii
     $x11 = "jvm.PreferredClassLoader" fullword ascii
     $x12 = "jvm.JNIEnv capsule is invalid" fullword ascii

   condition:
     (3 of them and $x11 ) or (3 of them and $x12)
     or (uint16(0) == 0x5a4d and pe.imphash() == "84a69bce2ff6d9f866b7ae63bd70b163" and
$x11) or (elf.telfhash() ==
"t1fde0f101c9395f39ecd16430b41041a59107c73c904087309fb8d0e8d87e0077129f3f")
}
```

Şekil 24. Decoy Dog örneklerini tespit etmek için YARA kuralı.

EK H: AÇIĞA ÇIKAN GÜVENLİK AÇIKLARI

Bir cihaz, gelen bir bağlantıda DNS sorgusu gerçekleştirecek şekilde yapılandırıldığında, harici bir varlığın davranışlarını ve kaynaklarını kısmen kontrol etmesine izin verir.[24] Özellikle bu yapılandırma, tehdit aktörlerine keşif, açık çözümleme ve hizmet reddi saldırısına potansiyel katılım için bir araç sağlayabilir. DNS karmaşık olduğu için hem satıcılar hem de ağ operatörleri bu riskleri anlayamayabilir. Tespit ettiğimiz sorguları ileten güvenlik cihazlarının yeni özelliklere sahip olması amaçlanmış olsa da, bu özelliklerde DNS kullanımı ağı keşif ve potansiyel olarak diğer tehditlere maruz bırakmaktadır.

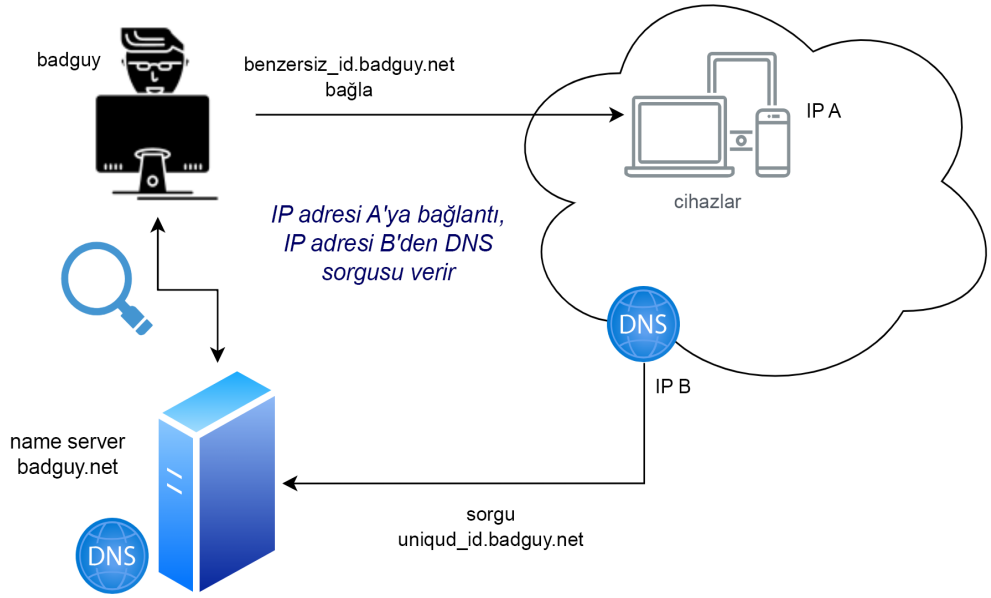
Bir ağ içinde herhangi bir harici varlığa DNS sorguları sunan bir cihaz açık çözümleyici olarak bilinir. Bazı durumlarda, bir cihaz yanıtlar döndürebilir ancak çok çeşitli koşullar nedeniyle harici DNS sorgularını tam olarak çözemeyebilir. Her iki durumda da, bu tür cihazlar ağın

24 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PLRaCAO, son erişim tarihi: 2023-06-11

kendisi ve dağıtılmış hizmet reddi (DDOS) saldırılarını güçlendirmek için ağın kullanımı için bir risk oluşturur. Açık DNS çözümleyicilerinin riskleri iyi belgelenmiştir ve bu riskler nedeniyle Infoblox dahil birçok hizmet sözleşmesi kapsamında açık çözümleyiciler yasaklanmıştır.

Decoy Dog sorguları durumunda, güvenlik araçları açık çözümleyiciler değildi, ancak yine de harici bir tarafın DNS sorgularını tetiklemesine izin verdi. Bu tür bir yapılandırma,

yükseltme saldırısı için kullanılamaz ancak bir tehdit aktörü tarafından başka amaçlarla kullanılabilir. Örneğin, bir tehdit aktörü bir ağa karşı keşif gerçekleştirebilir; aşağıdaki Şekil 25 bunu göstermektedir. Aktör bir alan adı oluşturur ve gelen sorguları günlüğe kaydetmek için ilgili ad sunucusunu yapılandırır. Aktör daha sonra ağa bağlanmak için özel alan adları göndermek üzere bir tarama mekanizması kullanır. Açık çözümleyici araması durumunda, bunlar DNS sorguları olabilir. Decoy Dog için bunlar HTTPS bağlantılarıydı. Her iki durumda da dahili cihaz, aktör tarafından kontrol edilen ad sunucusuna gönderilen bir DNS sorgusu oluşturur. Aktör daha sonra alan adını ve orijinal IP adresini aldığı sorguyla ilişkilendirebilir. Bu tür saldırılar her denemede sınırlı miktarda bilgi elde etse de, daha sonra saldırmak üzere dahili ağların haritasını çıkarmak için iyi kurulmuş mekanizmalardır.



Şekil 25. Bir aktör, kendi ad sunucusuna DNS sorguları oluşturan benzersiz alan adları oluşturarak bir ağ üzerinde keşif gerçekleştirir.

EK I: ARAŞTIRMA VERİLERİ

Araştırmamız için bir Pupy sunucusu kurduk ve sunucu ile istemciler arasındaki iletişimi özyinelemeli çözümleyicilerimiz aracılığıyla yönlendirdik. Analizimiz için bu DNS sorgu günlüklerini topladık ve günlükleri araştırma için kullanılabilir hale getiriyoruz. Veriler birkaç günlük değişen aktiviteyi kapsıyor. Çoğu zaman bir ters proxy kurarak istemcileri kontrol ettik ve komutlar SSL üzerinden gönderildi. Bunun Decoy Dog için de geçerli olduğundan şüpheleniyoruz. Ancak, sunucudan gelen DNS yanıtları aracılığıyla mevcut tüm komutları uyguladık. Ek olarak, birden fazla istemcinin aynı anda aktif olduğu zaman dilimleri ve çok sayıda istemci yeniden başlatılması vardır. Dahil edilen faaliyet kapsamı, burada açıklanan sonuçların yeniden oluşturulmasına izin vermelidir.

Veriler halka açık GitHub depomuzda mevcuttur infobloxopen: threat-intelligence.[25] Sorgu-yanıt günlükleri A kaydı sonuçlarını içerir ve aşağıdaki alanları içeren bir csv dosyasında paketlenir:

- zaman damgası: Unix dönemi saniyelerindeki sorgunun zamanı
- sorgu: istemci sorgusunda iletilen tam nitelikli alan adı
- yanıt: sunucu tarafından döndürülen IP adresleri kümesi
- client_payload_len: ana bilgisayar bilgileri de dahil olmak üzere sorgu içindeki yük baytlarının sayısı
- server_payload_len: yanıttaki yük baytlarının sayısı

Depo, bu belgede yer alan göstergeleri de içermektedir; ek göstergeler talep üzerine TLP:RED bilgisi olarak savunuculara sunulmaktadır. Ayrıca, VirusTotal'da bulunan ikili örneklerin tersine mühendisliğinden elde edilen verileri sağlıyoruz. Buna şunlar dahildir:

- Her örnek için yerleşik yapılandırma parametreleri
- Her örnek için gömülü şifreleme anahtarları ve şifre
  - BIND_PAYLOADS_PASSWORD
  - DCONFIG_PUBLIC_KEY (yalnızca istemci v4 için)
  - DNSCNC_PUB_KEY_V2
  - ECPV_RC4_PRIVATE_KEY
  - ECPV_RC4_PUBLIC_KEY
  - SCRAMBLESUIT_PASSWD
  - SIMPLE_RSA_PUB_KEY
  - SIMPLE_RSA_PRIV_KEY
  - SSL_BIND_CERT
  - SSL_BIND_KEY
  - SSL_CA_CERT
  - SSL_CLIENT_CERT
  - SSL_CLIENT_KEY
- Decoy Dog ikili dosyalarını tespit edebilen bir YARA kuralı ve bir TELF karması

25 https://github.com/infobloxopen/threat-intelligence

Kurumsal Merkez
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

RP-072023 v1