BGA SECURITY

Siber Dünyada Modern Arka Kapılar

BİLGİ GÜVENLİĞİ AKADEMİSİ

Netsec Etkinliği
2016 İstanbul

NETSEC 2016

Ozan UÇAR

BGA Security Kurucu Ortak
@ucarozan

BGA SECURITY

BGA Bilgi Güvenliği A.Ş

BGA Security Hakkında

Siber güvenlik dünyasına yönelik, yenilikçi profesyonel çözümleri ile katkıda bulunmak amacı ile 2008 yılında kurulan BGA Bilgi Güvenliği A.Ş. stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında büyük ölçekli çok sayıda kuruma hizmet vermektedir.

Gerçekleştirdiği vizyoner danışmanlık projeleri ve nitelikli eğitimleri ile sektörde saygın bir yer kazanan BGA Bilgi Güvenliği, kurulduğu günden bugüne kadar alanında lider finans, enerji, telekom ve kamu kuruluşları ile 1.000'den fazla eğitim ve danışmanlık projelerine imza atmıştır.

“Ürün Bağımsız Güvenlik Yaklaşımı”

BGA SECURITY

future

BGA Security, deneyimli ve uzman kadrosu ile siber saldırılara karşı kurumların ihtiyaç duyacağı desteği, **“ürün bağımsız güvenlik yaklaşımı”** vizyonu ile sağlama adına her zaman yanınızda…

Sunum

Sunum Hakkında

Digital varlıklarda, bilgisayar ağlarında ve iletişim teknolojilerinde yer alan yada olması muhtemel arka kapı risklerini yaşanmış örnekleri ile ele almaktadır.

Arka kapıların sahip olduğu tehlikeleri ve beraberinde yaşatacakları riskleri görüp bakış açımızı genişletmek, bu risklere karşı korunma yöntemlerini tartışmak ve yeni ürün/çözüm önerileri oluşturmaktır.

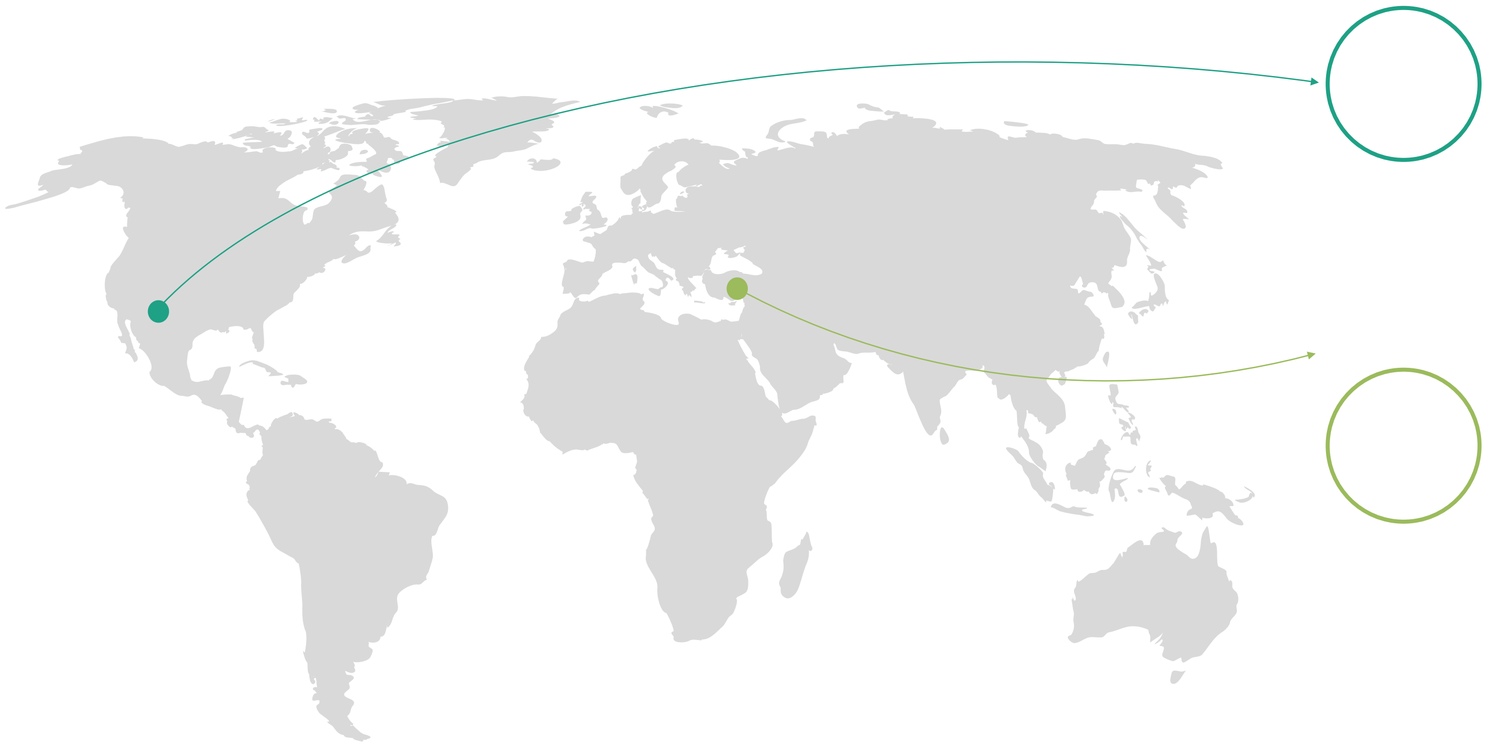
Sunumda yer alan detaylar her ne kadar paronoya riski taşısada asıl amaç hem bireysel hem kurumsal önlemlerinizi arttırmanızı sağlamak hemde olası tehlikelerin varlığını bilerek adım atmak.

Arka Kapı Türleri

BGA SECURITY

Ark Kapı Türleri

Geleneksel & Alışılmadık Arka Kapılar



Geleneksel

Süre gelen yaşantımızda sık karşılaştığımız klasik yöntemler

- Gizli parametreler
- İhtiyaç olmayan arabirimler ve kullanıcı hesapları
- Gizli hesaplar vb.

Alışılmadık

İşte en tehlikeli olanlar, alışılmışlığın dışında ve dökümante edilmemiş yöntemlerle hayatımızda olan arka kapılar.

- Uygulama geliştiricileri tarafından dizayn edilenler.
- Devlet/İstihbarat örgütleri tarafından donanım yada firmware seviyesinde yerleştirilenler
- Protokol hataları

Kimler İhtiyaç Duyar (?)

Siber saldırılar gerçekleştiren saldırganlar

Arka kapı dizayn eden saldırganlar, zaman zaman farklı yazılım yada servislere bu arka kapıları yerleştirerek yeni sistemleri ele geçirmeyi hedeflemektedirler. Aynı zamanda ele geçirdikleri sistemlerde erişimi devam ettirmek, uzaktan kod komut çalıştırmak içinde bu kötücül yazılımlardan faydalanırlar.

Securi Firmasının 2016 yılının ilk çeyreği için yayınlamış olduğu raporda ele geçirilen web sitelerin %70'nde arkakapı tespit edilmiş.

Köle bilgisayarlar ile robot ağlar kurmak isteyenler

Ele geçirilen bilgisayarlar, gerektiğinde bir hedefe yönelik saldırının bir parçası yapılmak istediğinde (örneğin servis dışı bırakma) bu arka kapılar sıklıkla kullanılır. Bilgisayarlarda çalışan bu zararlılar, saldırganın komuta kontrol merkezinden aldığı emir ile siber saldırılar gerçekleştirmek için harekete geçer.

Kimler İhtiyaç Duyar (?)

İstihbarat örgütleri

Digital casusluğun en etkili silahlarından biridir arka kapılar ve devletlere bağlı çalışan istihbarat örgütleri, hedefleri hakkında bilgi toplamak, sızmak ve hedefleri yok etmek için bu arka kapıları sıklıkla kullanır. Bu konuda yenilikler için araştır ve geliştirme faliyetleri, satın almalar sıklıkla yaşanmaktadır.

Bknz. NSA, GCHQ, Mossad ...

Üreticiler

Müşterilerine kolay destek vermek isteyip, yeri geldiğinde sorun çözmek için bu yöntemleri kullanmaktadırlar. Bu durum açığa çıktığında üreticinin kontrolünden çıkıp saldırganların suistimaline dönüşebilmektedir. Dökümanın ilerleyen sayfalarında örnekler bulabilirsiniz.

Hangi Amaçlar ile Kullanılır (?)

Sistemlere uzaktan erişimi sürdürmek

Gerektiğinde ele geçirilmiş sistemlere kimlik doğrulamasız ve gizlice bağlanmak için kullanılır.

Veri sızıntısı

Hedef sistemden hassas verileri almak, veri aktarmak için kullanılır. Örneğin, kredi kartı vb. finansal veriler, skype, what'sapp vb. anlık iletişim araçlarının verileri, sözleşmeler vb. hassas dökümanlar ve fotoğraf, video gibi özel veriler …

Sistemleri çalışmaz hale getirmek

Arka kapılar bulaştıkları sistemlere zarar verme, verileri geri dönülemez şekilde (pratik olarak) bozma gibi hayati risklerde taşımaktadır.

Hangi Amaçlar ile Kullanılır (?)

Para kazanmak (?)

Sanal para birimlerinin hayatımıza girmesi ile ele geçirilen sistemlerde yaşayan arka kapılar, saldırganların bu sistemlerin kaynaklarını (cpu,ram,disk vb.) kullanarak işlem yapmasınında önünü açmıştır.

Bir diğer kazanç kapısı internet reklamcılığı (bknz. adwords) ile köle sistemlerin bu kaynaklarda aktivite gösterip saldırgana para kazandırması.

Offline parola özeti kırma saldırılarında da arka kapılar hedef sistemde işlem yapması üzere saldırganlara erişim imkanı sunar.

Dijital Dünyamızı Etkilediği Alanlar

Sosyal & Kurumsal Yaşantımızda

NETSEC 2016

BGA SECURITY

Arka Kapıların Digital Dünyamızı Etkilediği Alanlar

Sosyal Yaşantımızda

Taşınabilir Aygıtlar
Akıllı ev teknolojileri
Modemler ve Kablosuz ağ cihazları
Kameralar
IoT - Internet of Things
Arabalar ve kendilerine özel iletişim protokolleri

Kurumsal Yaşantımızda

Sınır güvenliğini sağlayan cihazlar
İşletim Sistemleri
Taşınabilir Aygıtlar
Donanımlar
Ekipmanlar
İletişim Kanallarında
3. Party yazılımlarda

BGA SECURITY

Gerçek Dünyadan Örnekler ile Yeni Nesil Arka Kapılar

NSA’in küresel çaplı siber casusluk projesi: ANT

Kaynak: https://nsa.gov1.info/dni/nsa-ant-catalog/usb/index.html

BGA SECURITY

Sosyal Yaşantımızda

Taşınabilir Aygıtlar

- Mobil aygıtlar için geliştirilen siber istihbarat projesi, https://nsa.gov1.info/dni/nsa-ant-catalog/mobile-phones/index.html
- Yeniden programlanabilir ve zararlı yazılım taşıyan USB aygıtlar, https://nsa.gov1.info/dni/nsa-ant-catalog/usb/index.html

Akıllı Cihazlar

- Android Backdoor, http://thehackernews.com/2015/11/android-malware-backdoor.html
- http://thehackernews.com/2014/03/backdoor-found-in-samsung-galaxy.html
- http://thehackernews.com/2014/08/xiaomi-phones-secretly-sending-users.html

Modemler ve Kablosuz ağ cihazları

- Airties Backdoor, https://twitter.com/hackerfantastic/status/533400063348072448
- D-Link Backdoor, http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/

Kameralar

- https://nsa.gov1.info/dni/nsa-ant-catalog/room-surveillance/index.html

BGA SECURITY

Kurumsal Yaşantımızdan

Sınır güvenliğini sağlayan cihazlar

Firewall, switch, router ve trafiği denetleyen diğer sistemler internet ile kurum ağının sınırlarını belirleyen kritik sistemler oldukları için olası arka kapı tehlikesi suistimal için saldırganlara kolaylık sağlamaktadır.

Yakın zamanda şahit olduğumuz bazı arka kapılar;

- Juniper Screenos, https://community.rapid7.com/community/infosec/blog/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor
- Barracuda Networks, https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20130124-0_Barracuda_Appliances_Backdoor_wo_poc_v10.txt
- Fortinet Hardwares, http://arstechnica.com/security/2016/01/secret-ssh-backdoor-in-fortinet-hardware-found-in-more-products/
- Cisco Routers, https://www2.fireeye.com/rs/848-DID-242/images/rpt-synful-knock.pdf
- NSA'in ANT projesinden Firewall için geliştirdiği methodlar, https://nsa.gov1.info/dni/nsa-ant-catalog/firewalls/index.html

BGA SECURITY

Kurumsal Yaşantımızdan

Taşınabilir Aygıtlar

- Lenovo Backdoor, http://thehackernews.com/search/label/Lenovo%20Backdoor%20Malware

Donanımlar

- Seagate Nas Driver, http://betanews.com/2015/09/07/time-to-patch-your-firmware-backdoor-discovered-into-seagate-nas-drives/
- Seagate and LaCie wireless, http://www.kb.cert.org/vuls/id/903500
- UEFI Backdoor, http://techrights.org/2013/12/16/boot-process-threat/
- Reprogram hard drive, http://bofh.nikhef.nl/events/OHM/video/d2-t1-13-20130801-2300-hard_disks_more_than_just_block_devices-sprite_tm.m4v
- https://media.blackhat.com/bh-us-12/Briefings/Brossard/BH_US_12_Brossard_Backdoor_Hacking_Slides.pdf
- Maldrone [MALware DRONE], http://garage4hackers.com/entry.php?b=3105

Ekipmanlar

- USB aygıtlar
- Klavyeler

İletişim Kanallarında

- SSL

3. Party yazılımlarda

- VS FTPD, https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor

Korunmamız Mümkün Mü

BGA SECURITY

Geleneksel Korunma Yöntemleri

NETSEC 2016

Erişim Kısıtlamaları

Arka kapıların uzaktan tetiklenmesini engellemek için erişim kurallarını sıkılaştırmak, yönetim servislerine sadece size ait adreslerden erişim tanımlamak etkili korunma yöntemlerinden biri.

Tehtit istihbaratı

Arka kapı barındıran yada yüklenmesine olanak sağlayan durumlar zaman zaman saldırganlar tarafından keşfedilmekte zaman zamanda istihbari bilgi olarak sızmaktadır

Gerektiği Kadar Yetki

Uygulamaları kısıtlı kullanıcı hakları ile yada minimum yetkiler ile çalıştırmak.

Düzenli Zafiyet Analizi

Arka kapı yüklenmesine olanak sağlayacak sıfırıncı gün zafiyetlerini ve bilinen zafiyetleri keşfedip bildirecek bir sistem.

Anormallik Tespiti

Tüm ağı gözlemleyebildiğiniz bir sistem ile; ağınızın normal değerlerini bilip, anormal durumlar için alarm üretmek. Davranış tabanlı kolerasyon kuralları geliştirmek. Tatbik ederek öğrenmek ?

BGA SECURITY

-Teşekkürler-

ozan.ucar@bga.com.tr| @ucarozan