Source Code AKP

İrtica ile mücadele eylem planı

www.gurbuz.net

Bizleri süzme salak yerine koyan, eskimiş ve köhne alışkanlıklarını çağdaş yaşam tarzının tehdidi altında his edenler, olmadık yöntemlere başvurmayı sürdürüyorlar. Gazetecileri, bilim adamlarımızı tutuklamakla Atatürkçüleri yendiklerini sananların önündeki en büyük engeli, hala Türk Silahlı Kuvvetleri teşkil etmektedir. TSK'ne karşı yürütülen bu amansız yıpratma kampanyasında benim ve benim gibi düşünenlerin saffı belidir. Bizler yerine göre, zaman zaman Türk Silahlı Kuvvetlerinin önünde ama her zaman ve kesin olarak bu kurumun arkasında olmayı sürdüreceğiz. Bu yazıyı kaleme almamdaki amaç, sizlere birtakım önerilerde bulunmayı, bu zihniyetin dijital ortamda "kolay zaferlere" ulaşmasını engellemektir. Yazılarımı takip edenler benim bilgisayarcı olduğumu bilirler. Dünya üzerinde kullanılan mevcut kişisel bilgisayar sistemlerinin çoğunluğunu hala Microsoft şirketinin Windows işletim sistemi oluşturmaktadır. Bu yüzden önerilerimi Windows sistemleri üzerinde yoğunlaştıracağım.

Meslek hayatımın önemli bir bölümünü banka ve sigorta şirketlerinde dijital güvenliği sağlamakla geçti. Ancak Bundeskriminalamt (BKA) gibi kurumlarda müşterilerim arasındaydı ve orada gördüklerim dolayısıyla öğrendiklerim yabana atılacak gibi değil. BKA, Almanya ve Avrupa'da önde gelen kriminoloji merkezlerinden birdir. Önerilerimi ikiye ayırmak zorundayım; kişilere karşı alınacak önlemler ve devlete karşı alınacak önlemler. Genel anlamda bilgisayar sistemlerine karşı oluşabilecek tehditler ikiye ayrılır.

1. İç tehdit
2. Diş tehdit

Baştan hata yapmaya başlarsanız, oluşacak olan hatalar zinciri malum sonuçları hazırlayabilir. Bu yüzden bilgisayar alınacaksa dikkat edilmesi gereken hususların başında bilgisayarınızda en az fiziki iki sabit diskin bulunması gelir (NTFS formatlı). Orijinal yazılım kullanmaya özen gösterin. Bunun iki nedeni vardır ama bu nedenlerin ayrıntılarına değinmeyeceğim. Bu iki sabit diskten (Hard disk) biri yalnız işleştim sistemi için ayrılırken diğer sabit diski yalnızca bilgilerinizi kayıt etmek için kullanmanız gerekir. Yani C sürücüsü Windows için, D sürücüsü de bilgileriniz için. Çok fazla teknik ayrıntıya girmem bu makalenin sınırlarını zorlayacağı için mutlaka ve gerçekten bilgisayardan anlayan birisini danışman olarak yanınıza almanız gerekir. Gelelim biz yine konumuza; yanlışlıkla bilgileri işleştim sistemindeki sabit diske kaydetmenizi önlemek için gereken tüm önlemleri aldıktan sonra ki bu önlemler son derece basit ve etkilidir, önünüzdeki bilgisayara sizin ihtiyaçlarınızı karşılayacak yazılımlar eklenir. Sistem çalışırlığı ve güvenliği denendikten sonra yapılacak işlemlere değinmeden önce bir hatırlatmada bulunmak istiyorum:

Son olarak avukatın bilgisayarından çıkarılan kâğıt çöp kutusundan geri dönüştürülmüştü. Bu gibi gerçekten aptalca ihmalleri önlemek için sistem ve bilgilerin bulunduğu dosyalar fiziki ve lojik olarak birbirinden ayrılması zorunludur.

Sistem istediğiniz gibi aksaksız çalışıyor ise otomatik sistem güncelleştirmesini mutlaka ayarlayın. Sisteminizi teferruatlı olarak güncelleştirin. Bu teferruatlı güncelleştirme çok önemli! Güncelleştirme yalnız işletim sistemine yönelik değildir! Kullandığınız tüm yazılımları güncelleştirmenizi önemle rica ediyorum. Bu önlem sizi ilk etapta hem iç hem de diş tehditlere yönelik korumaya yöneliktir. Eğer sistem sizce kullanıma hazır hale geldiyse bundan sonraki adım bilgisayardaki kullanıcıları sınırlandırmak ve şifrelemekten geçer. Administratör kullanıcısına başka bir isim ve şifre verin. Şifre en az 12 sembolden oluşmalı.

Örnek: aQÖü15@'eZ°~

Buraya kadar anlatmış olduklarım sıradan ve basit hazırlıklardır. Hazırlık safhasından uygulama safhasına geçmeden önce, ilke olarak şu cümleler üzerinde düşünmenizi isteyeceğim:

1. Kişilere karşı korunma ile devlet kurumlarına karşı korunma farklı şeylerdir ve farklı tedbirler gerektir.
2. Her tezin bir antitezi vardır. Anlayacağınız, her önlemin bir karşı önlemi vardır.
3. İnsan beyni en iyi ve en gelişmiş bilgisayardır! Bu cümle en azından günümüz koşullarında hala geçerliliğini kısmen korumaktadır.
4. İki kişinin bildiği bir şey sır olmaktan çıkar.
5. Dijital ortamda, harcamaya hazır olduğunuz vakit ve nakit oranında her şey geri dönüştürülebilir veya değiştirilebilir.
6. Dijital ortamda en önemli aracınız beyniniz, hafızanız, dikkatli, sistematik ve özenli çalışma şeklinizdir.

Uygulama aşamasında Microsoft şirketinin Windows SteadyState (ücretsizdir) yazılımına ihtiyacınız var. Bu yazılım bilgisayarınızın mevcut durumunu koruyan bir programdır. Yani C sürücüsünün üzerinde sizin izin verdiğiniz güncelleştirmelerin dışındaki tüm değişiklikleri sıfırlamaya yarayan bir yazılımdır. Konu, işin uzmanı olmayanlar için anlaşılması gerçekten zor bir mevzu olduğu için izin verirseniz birde bu şekilde anlatmaya çalışayım:

Diyelim ki 02.02.2009 tarihinde bir bilgisayar aldınız ve aynı gün yukarıda belirtilen işlemleri bilgisayar üzerinde uyguladınız. Bilgisayar ile süreç içersinde çalıştınız ve bugün itibarıyla bilgisayarınız denetleniyor!?

Mevcut işletim sistemi ve anti virüs güncelleştirmelerinin dışında ki tüm sistemde oluşan değişiklikler 02.02.2009 tarihinde bilgisayarınızı aldığınız durumdadır. Dolayısıyla bizim gibilerinin sürebileceği her hangi bir iz yok!

Bilgisayar yeni, gıcır gıcır…
İz yok, delil yok…

Konuyu burada biraz amcam gerekiyor. Mesela her Word, Excel veya herhangi bir yazılımı açtığınız ve bu programlar ile bilgiişlem yaptığınız zaman bu yazılımlar, fragman şeklinde de olsa işletim sistemi sürücüsü üzerinde iz bırakır. Bilgiyi kayıt etmemiş olsanız bile bazen bilginize olduğu gibi erişilebilir. Timestamp, Hash gibi konulara hiç değinmeyeceğim ki sizi umutsuzluğa sürüklemeyeyim. Bakın makalenin başlarında iki sürücüden söz etmiştim. Konuyu yavaş yavaş toparlamaya çalışacağım. Duruma göre ampulün saçtığı ışığı ayarlayan bir zihniyete karşı dikkatli olmakta fayda var diye düşünüyorum.

Hani derler ya:

"*karda yürü izini belli etme*"

İşte bu yöntem onun gibi bir şey ki bu en basit gerçekleştirebileceğiniz yöntemlerden sadece biridir. Arkanızda en azından işletim sistemi sürücüsü üzerinde mümkün mertebe en az iz bıraktığınız yöntemdir. Eğer bilgilerinizi muhafaza etmek istiyorsanız ki, bu durumda bilgiler her bilgisayar kapatılışında sıfırlanıyor, ikinci sabit disk devreye giriyor. Zaten asıl sizlere izah etmeye çalışacağım yöntemler bundan sonra başlıyor. Söze yine bir hatırlatma ile başlamak istiyorum:

"*Her zaman karşına senden daha akılı ve bilgili birisi çıkabilir…*"

İkinci sabit diskiniz sizin bilgilerinizi kayıt edeceğiniz sürücü konumunda olduğundan bu sürücü üzerinde daha itinalı bir çalışma gerçekleştirmemiz gerekiyor. Bu durumda karşımıza iki önemli sorun çıkıyor:

1. Bilgileri şifreleme
2. Bilgileri güvenli bir şekilde silme

İki konuda başlı başına bir bilim ve anlaşılması zor konular olduğundan, işin matematiksel yönlerini bitaraf edip konuyu mümkün olduğu kadar basit bir şekilde anlatmaya gayret edeceğim. İşe bilgilerinizi silmekle başlayalım. Bilgisayarınızda bir doküman hazırladınız. Bu dokümanı bilgisayarınızdan sildiniz ve çöp kutusunu boşalttınız diyelim; siz dokümanı görmeseniz dahi belge olduğu gibi sabit diskinizde kayıtlı. Her sabit diskin beli bir kapasitesi vardır ve bu durumda Windows'un bir özelliği devreye girmektedir. Windows sabit diskte yer olduğu sürece boş bir alana bilgileri kayıt eder. Dolayısıyla sizin önceden silmiş olduğunuz belgenin bulunduğu bölgeye, büyük bir ihtimale herhangi bir kayıt yapılmayacaktır. Sabit disk üzerindeki kapasite azaldıkça önceden silmiş olduğunuz bölge üzerine kayıt yapılmaya başlanacaktır. Umarım buraya kadar yazdıklarımı anlayabildiniz.

Aslında eğer gerçekten yazıklarımdan bir şey anladıysanız durum gayet açık bir şekilde ortada. Windows sistemlerinde bir bilgiyi güvenli bir şekilde silmek istiyorsanız, sildiğiniz bölgeye tekrar bilgi yazmanız gerekiyor ama bu sizin elinizde değil! Yani siz isteseniz de beli bir sektör içersine bilgi kaydetme şansınız yok. Kaldı ki diyelim siz aynı sektöre bilgi kayıt etmeyi başardınız matematiksel yöntemler ile bu silinmiş ve üzerine kayıt yapılmış sektör geri dönüştürülebiliyor.

Hayda demeyin!
Bilgisayar bu, ne yapacağı beli mi olur. Şaka bir yana…

Benim tavsiyem sabit diskinizin çok önemli bilgilerde en az yedi defa tesadüfî içerikle silinmesidir. Bu *Department of Defense* (DoD 5220.22-M ECE) yönetmeliğine göre gerçekleştirilmelidir. Yani sizin silmiş olduğunuz belgenin sabit disk üzerinde kayıt edildiği bölge tesadüfî içeriklerle 7 defa yeniden yazılarak önceki bilgiler siliniyor. Şayet çok gizli, sakıncalı bilgiler imha edilmesi gerekiyorsa *Gutmann* yöntemini öneriyorum. Bu yöntem bilgileri 35 defa silme ve yeniden yazma, yeni kodlama (27 ayrı kod) ve sekiz ayrı tesadüfî içerik kullanmaktadır. Yada *Pfitzner* yöntemini kullanacaksınız. Bu yöntem bilgileri 33 defa silme ve yeniden yazma ve otuz üç ayrı tesadüfî içerik kullanmaktadır. Her iki yöntemde laboratuar ortamlarına karşı "bağışıklık" kazanmış ve denenmiş yöntemlerdir. Anlayacağınız üzere bilgisayarınızdan herhangi bir doküman güvenli bir şekilde silinmesi gerekiyorsa yukarıda belirmiş olduğum yöntemleri kullanmak zorundasınız. Bunun başka yöntemleri yok mu?

Var tabii, ama bu gibi konular ulu orta anlatılmaz!

Yinede ben size ileride bir kaç yöntem daha önermeyi düşünüyorum. Gelelim bilgileri şifreleme yöntemlerine…

Gören göz kılavuz istemezmiş, aşikâr olanı gizlemeye çalışma… Gören gözü eğitilmiş göz olarak kabul edersek ve bu göz ne arayacağını, nerde arayacağını bilirse gerçekten kılavuz istemez! Bir ihtimal bundan bir kaç ay önce İngiltere hükümetinin, Microsoft şirketinden sürücü şifreleme yazılımı Bitlocker hakkında teknik bilgi istediğini duymuşsunuzdur. Bir devlet, bir kıta, bir şirketten yardım isterde bu şirket hayır diyebilir mi?

Belki Microsoft gibi birçok devletin bütçesinden daha fazla maddi imkâna sahip olan bir şirket diyebilir. Ama bu gibi uluslararası bir güce sahip şirket gerçekten çok az. Neyse, biz yine konumuza dönelim. Şifreleme, iz bırakmama, güvenlik yazılımları gibi konular dijital ortamda aslında vakit kazanmaktan başka bir şey değildir. Kime karşı vakit kazanıyorsunuz? Sizin bilgilerinize ulaşmaya çalışana karşı! Vakit kazanmak size ne getiriyor? Karşı tedbirler almak için gereken zamanı sağlıyor. Bilgilerinize ulaşmaya çalışan için vakit çok önemli bir faktördür! Bunun değişik nedenleri

olabilir ama zaman "onun" için gerçekten çok değerlidir. İşte bu ortamda iki taraf içinde "gören göz" önem kazanıyor!

İşte bu yüzden size insanoğlunun zaaflarından yararlanmayı öneriyorum. Ayrıntılara değinmeden önce bir kaç teknik bilgiyi vermem gerekiyor.

Ama önce dün bir okurdan aldığım bir tenkite yanıt vermek zorundayım:

Ercüment Rakap demiş ki:

"Sayın Önder Gürbüz güzel ve faydalı açıklamalarda bulunmuş. Önerilerini uygulayacak olanlar sahte bir güvenlik duygusuna kapılabilirler. Yazıdan görüldüğü gibi güvenlik gerçekten önemliyse, şu öneriyi beklerdik kendisinden: Bütün Microsoft yazılımlarından kurtarın kendinizi! Windows dahil! Bilgisayarınızda Windows işletim sistemi olduğu sürece güvenlikten bahsetmek abesle iştigaldir!

Genelkurmayın hassas verilerinin hala Windows / Microsoft sistemlerinde işleniyor olmasının bir tek açıklaması olabilir: Genelkurmay TSK'yı Türkiyenin değil, NATO'nun ordusu olarak görüyor olmalı hala…"

Kendisine cevabım:

Sayın Ercüment Rakap,

Makalenin tümünü okuduktan sonra fikrinizi değiştireceğinizden eminim. Ancak vaktim müsaade ettiğince yazabiliyorum. Konu çok hassas bir mevzu ve dediğim gibi bilgisayarların büyük çoğunluğu Microsoft işletim sistemi kullanmaktadır. Kaldı ki Linux gibi tüm yazılım ve işletim sistemlerinin de kendilerine göre zayıf yanları vardır, önemli olan bu zafiyetlerin bilincinde olup gerekli önlemleri almaktır. Bilmem Sans Institute size bir şey ifade ediyor mu? Dünyanın önde gelen güvenlik ve araştırma şirketlerinden biridir. Bu şirkete göre Windows, ister kişisel - ister Server işletim sistemi olarak kurulmuş olsun, "hakkı verilerek kurulursa" Unix'e eşdeğer anlamda güvenilir bir sistem olduğudur. Neyse, sizinle tartışma niyetinde değilim. Elbet benimde 25 senelik ekmeğimde bildiğim ve öğreneceğim yeni şeyler vardır ama inanın makalenin sonunda fikrinizi değiştireceksiniz.

Saygılarımla

Şifreleme yöntemleri genel anlamda üç gruba ayrılır. Simetrik, Asimetrik ve Hybrid. Bunların ne anlama geldiğini kısaca izah etmeye çalışacağım. Simetrik (***Secret-Key)*** geleneksel şifreleme yöntemidir. Yani şifre tek bir "anahtardan" oluşur. Genel anlamda çok hızlı bir yöntemdir. Bilgiyi şifreleme ve şifrenin içeriğini görme tek bir parola ile gerçekleştirilebilir. Şifreleme kalitesi seçeceğiniz parolanın uzunluğu oranındadır. Yukarıda bilgisayarınızın giriş şifresini en az 12 karakter olarak seçin demiştim. İnanın işin uzamın en geç on dakika içersinde bilgisayarınıza giriş yapacaktır. Ama bunun hiç bir ehemmiyeti yoktur! Bilgisayarınıza giriş yapması demek bilgilerinize ulaşması anlamına gelmez. Kaldı ki tavsiyelerime uyacak olursanız kolay kolay sürebileceği her hangi bir ize de rastlayamaz.

Daha öncede değinmiş olduğum gibi şifrelemede esas olan gizliliktir. Gizlilik ve parolanızın kalitesi sizi koruyan yegâne unsurlardır. Şahsen şifreleyeceğim içeriğin ehemmiyetine göre kullandığım parolanın uzunlukları 32 karakter (192 Bit) ile 342 karakter (2048 Bit) arasında değişir.

1024 Bitlik (171 karakter) parolaya bir örnek vermek istiyorum:

Jx4PuGdaDHEs643jr2C/a2gJqdvJk5b8IPDR6meh2bi2JJfVGpY7zq0A0DkxDU5LLEn7iSVVrLnATQ7pwMZjHkJITQV1K1/dvg0q1druBxdpsx0oy130h8nZ()mgvpYPp5Q§c3iuv725P1/zy6AGGoWKhr3JIc1VK1q6n08sV#s

Kullandığınız parolanın kalitesine bakın

Simetrik şifreleme yöntemlerinden bazıları:

DES
3DES
IDEA
CAST
RC4'den RC6'ya kadar
A5
Blowfish
Twofish
AES

Asimetrik şifreleme konusuna girmeden, Biometrik şifrelemeyi şu an için önermediğimi belirtmeliyim. İlerde mutlaka bir nevi standart olacağına inancımı korumakla beraber, teknoloji kanımca daha yeterince gelişmedi. Gelelim asimetrik şifrelemeye. Simetrik şifrelemenin aksine asimetrik şifreleme iki anahtar ile çalışır. Aleni (*Public–Key*) ve özel anahtar (*Private-Key*) arasında öyle bir matematiksel bağ var ki, oluşturulmuş olan anahtar çiftinden birine sahip olursanız hiç bir işe yaramaz ve matematiksel olarak da diğer anahtar yaratılamaz. Yani bir nevi tek yön istikametidir. Ancak dikkat edilmesi gereken bir husus olarak simetrik şifreleme siteminde, 128 Bitlik bir parola "yeterince güvenli" olarak algılanırken, asimetrik şifreleme yönteminde 128 Bitlik simetrik parolanın karşılığı yaklaşık 3000 Bitlik bir paroladır.

Asimetrik şifreleme yöntemlerinden bazıları:

Diffi – Hellman
RSA
ElGamal

Asimetrik şifreleme yöntemi, simetrik yönteme kıyasla çok daha yavaştır ve bu durum büyük içeriklerde sorun olarak karşınıza çıkar. Gelelim Hybrid şifrelemeye, adın da anlaşılacağı gibi simetrik ve asimetrik yöntemlerin bir bileşimini oluşturmaktadır. Simetriğin hızı, asimetrik sistemin iki anahtarından oluşan bir bileşimdir.

Tüm şifreleme yöntemlerinin ortak özelliği ve "zayıf" yanı kullanacağınız parolanın kalitesidir. Eğer parolanızı bir program vasıtasıyla oluşturuyorsanız, bu programın herhangi bir anlaşılabilir sistematiğe göre çalışmamasına özen gösterin.

Sizlere buraya kadar prensip olarak anlatmaya çalıştıklarım, sizi koruyacak ve size zaman kazandıracaktır. **A**ldatma, **K**azıklama ve **P**alazlanmayı ilke olarak kabul etmiş badembıyıklılar, onların intikam hırsı, yalakaları ve yalan makinelerine karşı sizi ne korur bilemeyeceğim. Bu gibi zararlı organizmalara karşı geliştirilmiş herhangi bir sprey var mı onu da bilmiyorum ama bildiğim bir şey varsa, o da kendinizi korumak istiyorsanız insanların zaaflarından yararlanmanız gerektiğidir. Gelelim en önemli faktöre, I N S A N …

Güneydoğudaki vatandaşların dikkatine

Yazımda "gören göze" değinmiştim. Gören gözün karşılığı bakar kördür…

Bir yetişkin ile bir çocuk arasında ne fark vardır?

Biliyorum şimdi bana birçok fark sıralayacaksınız ama sanırım duymak istediğimi ancak bir kaçınız söyleyecektir. Yetişkin insan gözü, geneli görmeye alışmış olup beyni "durum değerlendirmelerini" çoğu zaman olduğundan daha karışık işleme koyar. Dikkat ettiyseniz eğer, alışmış olduğundan bahis ettim. Çünkü insan beyni aslında genele "programlanmamış" olup sonradan bu "program" değişikliğe uğramıştır. Şimdi size bakar kör desem bana kızar mısınız?

Aslında kızmamanız lazım çünkü gerçek bu!
Eminim 100 kişiden ya biri gördü ya da görmedi…

Yukarıdaki resmi çok amatörce değiştirdim, profesyonel işlem yapsaydım ancak işin uzmanı görürdü. Uncle Sam'ın şapkasına dikkat ettiniz mi?

Kaçınız orada adımı gördü, ya da orada bir şey olduğundan şüphelendi? Sorumu elinizi vicdanınıza koyarak cevaplandırın lütfen… Resmi büyüterek incelerseniz adımı göreceksiniz.

Steganografi terimi yunanca kökenli olup "gizli yazı" veya "gizleme sanattı" olarak günümüze kadar gelebilmiştir. İster Microsoft, Linux veya Macintosh olsun her sistemin kendine göre backdoor prosedürleri vardır. Bu güvenlik riskleri forensik bilimcileri tarafından genelde bilinir ve söz konusu suç unsurları açığa çıkarılarak suçlu adalete teslim edilir. Forensik bir bilim dalıdır ve dijital ortamda işinin ehli forensikeler gerçekten azdır. Türkiye neredeyse her alanda olduğu gibi bu konuda da medeni toplumların arkasından düşe kalka gitmektedir. Gerçi batı devletlerinin hepsinde olmamakla birlikte bir kaçında çok gelişmiş ve özel bilgisayarlar bulunmaktadır. Bu bilgisayarlardan Türkiye'de var mı bilemeyeceğim. Çünkü bu konuda ne bir makale okudum ne de herhangi bir yerde bir ibareye rastladım. Gerçi benim okumamam bir şey ifade etmez ama…

Birkaç örnek vermek gerekirse:

Bir IBM Blue Gene'in kapasitesi yaklaşık 150.000 güncel bilgisayara eşdeğerdedir.
Bir Jugene'nin kapasitesi yaklaşık 50.000 güncel bilgisayara eşdeğerdedir gibi…

Bilimin engin derinliklerine dalarak boğulmadan, ben size "gizleme sanatından" bir kaç örnek vererek devam edeyim.

Alternate Data Stream birçok zararlı yazılımın bilgisayarınıza giriş yaptığı yöntemdir. Siz bu yöntemi bilgisayarınızdaki bilgileri meraklı gözlerden saklamak için kullanabilirsiniz. Yeni kurulmuş bir Windows sisteminde en az, her hangi bir program yüklenmeden, yaklaşık 20.000 komut, dosya, vs. (hangi Windows sürümü ve hangi güncelleştirme durumunda olduğuna bağlı olarak) olduğunu düşünürsek, aslında bir şeyi saklamak için uygun bir zemin olduğunu düşünebiliriz. Bir kaç ilave güvenlik önlemi ile bilginizi nispeten iyi korumuş sayılırsınız. Bilgilerinizi gizlemek için ADS veya daha tanıtacağım yöntemleri kullansanız bile, zekânız sizin bu arz-ı endam eden zihniyete karşı en önemli silahınız. Nostradamus kehanetlerini açık seçik olmayan, sembolik ifadelerle dile getirmiştir. Bakın aradan yüzyıllar geçmesine rağmen kehanetleri hala sırlarını korumaktadır. Sizde saklama yöntemlerinizi seçerken öyle bir seçmelisiniz ki "yalnızca anlayabilen anlasın" . Bunlar harf oyunları, yalnız sizin ve yetkililerin bildiği şifreleme yöntemleri olabilir. Hepine daha sonra örnekler vereceğim. Önce Alternate Data Stream'li gizli bir içerik nasıl oluşturulur ona bakalım. İstisnasız tüm Windows sürümlerinde calc.exe diye bir program vardır. Vereceğim örnek yerine herhangi bir komut, dosya veya benzeri şey olabilir. Ben özellikle calc.exe'yi seçtim çünkü bu komut hesap makinesidir ve biz hesap makinesinin içine örneğin bir şifre gizleyeceğiz. Hadi sizinle beraber gizli âlemlerin derinliklerine bir dalış yapalım.

Diyelim ki notepad.exe ile gizli.txt diye bir dosyayı c:\ kayıt ettiniz. Bu gizli.txt'nin içeriği "*Ne mutlu Türküm diye*" olsun, şimdi biz bu gizli.txt'yi, calc.exe programına ekleyerek - ki programın ne işlevini nede dosya ebadını değiştirmiş olacağız- saklama işlevini gerçekleştirelim. Gizli.txt'yi güvenli bir şekilde bilgisayarınızdan sildikten sonra saklama işlevi bitmiş olacaktır.

Windows XP ve Vista için örnek:

Komut istemi penceresinden (cmd.exe) bu satırı yazın:

type c:\gizli.txt > c:\windows\system32\calc.exe:gizli.txt

Not: echo komutu ile içerik uzunluğu oldukça kısıtlanacağı için type komutunu öneriyorum.

Bundan sonra örneğin bir CD üzerinde calc.exe programını başkasına verebilirsiniz. CD ö z l ü çocukların eline geçse bile ilk bakışta CD üzerindeki başka programlar arasında göze batmayacaktır. Programın kendisi işlevini kaybetmediği için her zamanki gibi hesap makinesi olarak çalıştırabilecektir. ADS'in bilincinde olan birisi için bu devede kulak gibi kalır ama… Diyelim ki CD ö z l ü çocukların değil de gizli içeriği vermek istediğiniz kişiye ulaştı. O da sizin gibi komut istemi penceresinden şu satırları yazarsa:

Notepad calc.exe:gizli.txt

Gizli içeriğe ulaşmış olacaktır. Biliyorsunuz bu zihniyetin temsilcileri genelde Ö Z ile başlayarak milletin anasını kovalıyor. Prof. Özbudun adına yakışır özlü bir şekilde anayasayı budayacak ama şükür engelleri aşamıyorlar. Diğer Öz ise Ergenekon safsatası ile milletin dikkatini asıl gündemden hayal âlemlerine doğru çekmede çok başarılı…

Gizleme, şifreleme, saklama ve güvenliği sağlama gibi konular çocuk oyuncağı değildir! Her bilgisayarı açıp – kapamasını bilenin kendini uzman saydığı günümüzde, gerçekten çok dikkatli olmakta fayda var. Şahsen müzik, video ve özellikle programlara saklamayı severim. Program ve resim kütüphanem tahmin edemeyeceğinizden büyük olduğu için özü, sözü ve Müslümanlığı tartışılır zihniyetin işi, benim bibliyoteğimde çok zor olacaktır. Müslümanlığı tartışılır dedim çünkü benim bildiğim Müslüman yalan söylemez, çalmaz, aldatmaz ve iftira atmaz. Ama bir takım şeylerin teğet geçmediği, ortalığın gülük gülistanlık olmadığı da ortada, Aslında olayların gelişmesine bakacak olursanız; birtakım köşelerden çıkarılırken bir kaç bomba, üç – beş kurşun oradan, bir – iki kâğıt parçası buradan derken…

Kâğıt dedik aklıma geldi, Almanya'da resmi olarak iki tip imza hukuki geçerliliğini korumaktadır:

- Unterschrift dediğimiz imza.
- Kurzzeichen dediğimiz imza yerine geçen bir tür sembol

Ben her iki imzayı da kullanırım. Tabii iki imza şeklinin de fotokopi üzerinde hukuki anlamda herhangi bir değeri yoktur.

Gelelim resmi gizli bilgilerin taşıyıcısı olarak tanımlamaya. Buda sevdiğim bir usuldür. ADS konusunu kapatarak şimdi size başka bir yöntem tanıtacağım.

Yukarıda görmüş olduğunuz resim bir resim olmakla birlikte aslında gizli bir bilgiyi içermektedir. Bu yönteme Embedded files denir ve çok kullanılan bir yöntemdir. Nasıl yapıldığına gelmeden önce eğer siteminizde mevcut değilse şu programı bilgisayarınıza yüklemenizi isteyeceğim. Winrar bir arşiv oluşturma programıdır.

Konuya girmeden Winrar programının temel çalışma şeklini öğrenmeniz lazım. Ben sizin bilginizi farz ederek devam ediyorum. Gizlemek istediğiniz bilginin Winrar ile bir arşivini çıkartın. Diyelim ki çıkardığınız arşiv d:\ üzerinde, şimdi birde resim lazım size. Gizli belgemizin arşiv adı: gizlibilgi.rar gizleyeceğimiz resim adı da ÖrnekResim.jpg olsun. İkisinin de d:\ üzeride olduğunu farz ederek;

Komut istemi penceresinden (cmd.exe) bu satırı yazın:

Copy /b ÖrnekResim.jpg + gizlibilgi.rar AilemVeBen.jpg

Bu komut ile oluşturduğunuz AilemVeBen.jpg resmi bundan sonra gizli içeriği taşıyan resim olmuştur.

Elbet sakladığınız bir nesneyi yine bir şekilde ortaya çıkarmanız lazım. Çok kolay:

Winrar programını açıp program üzerinden AilemVeBen.jpg tıklayın. İsterseniz yukarıdaki hacker resmini bilgisayarınıza indirerek bir deneyin.

Bakın bunlar çok çocukça yöntemler ama bilmeyen bilmiyor işte. Profesyonellerin kullandığı araçlar farklı. Farklı olmasına farklı ama prensip olarak aynı. Size buradan program isimleri vermemi beklemiyorsunuzdur inşallah!?

Sizin okuduğunuzu başkası da okuyor, bilmem anlatabiliyor muyum. Sabırsızlanmayın daha ilginç yöntemler bölümünü aralamadık…

Özellikle yazmadım bakalım kaçınız farkına varacaksınız diye. Dün hazırlamış olduğumuz gizlibilgi.rar belgesini kaçınız güvenli bir şekilde sürücüsünden sildi?

Şayet unuttuysanız **A**tatürkçülüğü **K**atletme **P**artisi ve yandaşları avuçlarını ovuşturacaktır. Gerçi aradan yıllar geçti ve ben bu arada bu gibi konulara uzak kaldım ama zamanında öğrendiğim iki şey vardı:

1. Eğer silahını çekersen öldüreceksin! Öldürmek için, ya kişinin alnının ortasına nişan alarak ateş edecesin ya da teflon kaplama kurşun kullanacaksın.
2. "Bildiklerini" hemen unutacaksın!?

Teflon kaplama kurşun artık piyasada kolay kolay bulunmuyor, gerçi para her kapıyı açar ama…

Ne alaka, konuyla ne ilgisi var diye sorabilirsiniz. Anlatayım;

Genel olarak çelik yelek kurşungeçirmez olarak bilinir. Siz öyle sanarak hayatınızı riske atın, bu sizin bileceğiniz iş! Ben olsam gereken tüm önlemleri alırdım… Teflon kaplama kurşun, çelik yeleği deler geçer.

Bilmiyor muydunuz, öğrenmiş oldunuz!

Siz birisine öldürmek için ateş edeceksiniz, ya o kişi çelik yelek taşıyorsa!?
İyi nişancı olsanız da adamı alnının ortasından vurmak kolay iş değildir!

Bir nevi sizin bilgisayarınıza girerek bilgilerinizi, özelinizi ortaya dökmeye çalışanlarda sizin canınıza kast ediyorlar. Konuya hiç bu yönden yaklaştınız mı?

Siz şimdi çelik yeleğinizi sırtınıza geçirin ve göğüs kafesindeki hayati önem arz eden organlarınızı emniyete aldığınızı sanmaya devam edin. Aranızda Uzakdoğu sporuna meraklı olanlar bilirler, savunmanın en iyi yöntemi saldırana mümkün olduğu kadar küçük bir hedef göstermektir. Bu arada eskiden deniz savaşlarında da bu konu çok önemliydi… Embedded files'e bir örnek daha vererek başka bir konuya geçelim. Hedef küçültmek, hedef yanıltmak! Hedef yanıltmak en sevdiğim yöntemlerden biridir. Bayılırım rakibimi yanlış yönlendirmeye. Bizler Honeypot dediğimiz yöntem ile hackerleri izleriz. Bu yöntem bir nevi hedef yanıltmadır ve çok etkilidir.

Genel anlamda hayata hiç bir şey göründüğü gibi değildir! İçine girerek, perde arkasına baktığınızda gerçekler ile yüzleşirsiniz.

HerHangiBirDoküman.doc

Yukarıdaki dokümanı bilgisayarınıza indirin, üzerine tıklayın. Bir Microsoft Word dokümanı… Aynı dokümanı Microsoft Excel ile açın. Şaşırmanıza gerek yok. Sağ gösterip sol vurmaktır bu… Gelelim hedef küçültme ve yanlış yönlendirme konusuna.

Hani bu makalenin başlarında sistem güncelleştirmelerinden söz etmiştim ya, işte bu güncelleştirmeler sisteminize karşı oluşabilecek saldırılarda hedefi küçülten öğelerden sadece biridir.

Hedef küçültme ve gizleme önlemlerinin kalitesi, birçok yöntemin bileşiminden elde edilenin toplamıdır.

Bıkmamdan ve usanmadan tekrarlarım; güvenliğinizin teminatı zekânızdır. Bulmaca çözmesini sever misiniz?

Sevsenize sevmemenizde şimdi birlikte bir bulmaca çözmeye çalışacağız. Diyelim ki ben yasadışı bir oluşumun içindeyim ve örgütten güvendiğim birine şu bilgiyi verdim:

"*Gerekli şifreyi sabit diskimin üzerinde bulacaksın...*"

Desem ve siz **A**a **K**ee **P**ee'nin has evlatlarından biri olarak bu bilgiye ulaşsanız ne yaparsınız? Hadi bakalım, biraz düşünün!

Büyük bir ihtimale sabit disk üzerinde bulunan tüm bilgileri didik didik arayacaksınızdır. İnanın her hangi bir şifre ibaresine bile rastlayamayacaksınız!

Neden mi?

Dedim ya, şifre sabit diskin üzerinde! Her elektronik eşyanın üzerinde üreticisinin bir etiketi bulunur. Bu etiketi profesyonelce yerinden çıkarır, altına şifreyi yine şifreli bir şekilde yazarak aynı yere geri yapıştırırsanız dikkat çekmeyecektir.

Gerçi itiraf etmeliyim ki bu örnek son derece basit bir kelime oyunundan ibaretti. Siz güvenlik mimarinizi dokuz şiddetinde bir depreme karşı tasarlamaya özen gösterin.

Şimdiye kadar değinmiş olduğumuz yöntemler sizi bir yere kadar kişilerin saldırısına karşı koruyacaktır. İyide saldırgan devletse ne yapmak gerek?

Defalarca üstüne basarak belirtmiş olduğum gibi kafayı çalıştıracaksınız. Başka çaresi yok!

Bilinen Matematiksel yöntemler ile şifrelenen bir nesne eninde sonunda deşifre edilecektir. Bunun sayısız örnekleri var. Enigma ikinci dünya savaşında almanlar tarafından kullanılan bir makineydi ve sonunda deşifre edildi! Ama Nostradamus örneğinde olduğu gibi bir Amerikan başbakanına arkadaşı tarafından yazılan bir şifre ancak iki yüz sene sonra deşifre edilmiştir. Nostradamus'un kehanetleri henüz deşifre edilemedi, eninde sonunda bu kehanetlerinde deşifre edileceğinden eminim ama zamanı henüz gelmedi…

Anlayacağınız üzere yanlış adama, yanlış zamanda rastlarsanız işiniz çok zor!

Türkçe adını bilmiyorum ama bir ihtimal görmüşsünüzdür. Genelde ahşaptan yapılma bir bebek. Bebeğin içinden dört – beş bir önceki bebekten küçük bebekler çıkıyor. İşte bu sizin şifreleme yönteminiz olmalı!!!

Gören göz, nerede neyi arayacağını bilmezse bir anlamda kördür!
Hani atalarımız "*nerde çokluk, orada bokluk*" der ya, bakın bu cümle bu bağlamda yanlış!
Büyük bir ormanın içinde belirli bir ağıcı aramak, samanlıkta iğne aramak gibi bir şey…

Hesaplarınıza şans ve tesadüf gibi etkenleri de katmayı unutursanız güvenlik mimariniz çökebilir. Birçok insanlık tarihini etkileyen buluşun tesadüfen yapıldığını unutmayın…

Konu çok kapsamlı, çok yönlü ve karmaşık ama unutmayınız ki aptallığın da sınırı yok!

Bu gibi konulara değinmemin yegâne amacı, AKP'nin uyguladığı siyasi teröre karşı savunmasız olmadığınızı sizlere hatırlatmaktı. Hani AKP'nin (yalan söyleyen, aldatan Müslüman!?) baş yalanlarından biri olan Avrupa Birliği namına uygulamalar, özgürlük (ne demekse) ve sınırsız sözüm ona demokrasi var ya… Gelin AB'deki son duruma birlikte bir bakalım; Avrupa Birliğinde, şifrelemeyi değişik nedenlerden dolayı yasaklanma en azından kısıtlanma yolunda! Neticede bunu gerçekleştirip gerçekleştiremeyecekleri Avrupalıların yani halkın tutumuna bağlı olacaktır. ABD ve AB yazılım şirketlerine karşı uzun zamandan beri "devlete" ödün vermelerine yönelik baskı uygulamaktadır. Yani devlet güçleri gerek gördükleri takdirde, şifrelenen içeriği standart bir şifre veya açık bırakılan "gizli" bir kapıdan (backdoor) görebilmelidirler. Bazen ise belirli teknolojilerin yurtdışına çıkısını toptan yasaklamaktadırlar. Şimdi diyeceksiniz ki Microsoft kullanmam olur biter.

Peki…

Çoğu zaman kaynağı açık yazılımların (Open Source) arkasında SUN veya Novell gibi devlerin "saklandıklarını" biliyor muydunuz?

Bu milyarlarca Dolarlık piyasada etken olan şirketlerin merkezleri nerede?

Evet, SUN veya Novell ölmedi! Sadece "başka" bir isim altında piyasada etkililer, o kadar.

Arkadaşlar, bunlar beyhude gayretler…

Siz hangi işletim sistemini, hangi yazılımı kullanırsanız kullanın, Avrupa Birliğinin bu "sınırlandırma" gayretleri açıkça gösteriyor ki şifreleme her ne şekilde olursa olsun devlete karşı da belirli bir yere kadar etkili. Unutmayın zaman faktörü sizin lehinize çalışıyor!

Sizlere şifreleme, gizleme ve yanlış yönlendirmeye yönelik son bir örnek vererek bu konuları kapatmak istiyorum.

Aranızda yazdıklarımı dikkatli okuyanlar benim bir çelişkiye düştüğümü sanabilirler. Biraz daha sabır edin…

Süper Bilgisayarları, özel şifre kırıcı işlemcileri bir kenara bırakarak (aslında sürekli aklınızda olmalılar) konuya girelim. *Security by Obscurity* prensibi ile Eric Raymond'un* bu unutulamaz sözünden yola çıkarak sizlere bir bileşimi önermek istiyorum.

"*Given enough eyeballs all bugs are shallow*"

Diyelim ki sizin çok önemli bir bilgiyi gizlemeniz gerekiyor. Bu bilgi ticari, siyasi veya herhangi başka bir önem arz ediyor olabilir. İlk ve kesin olarak yapmanız gereken bilginin arşivini çıkarmak olacaktır. Konuyu dağıtmamaya dikkat ederek neden diye soranlara şu cevabı vermek istiyorum:

Hiç bir zaman rakibini hafife alma

Arşiv çıkartmanın (arşiv çıkardıktan sonra güvenli silmeyi unutmamak şartı ile) iki nedeni vardır:

1. İstatistik analitik, analize maruz kalacak alanı küçültmek**.
2. Şifrelemek istediğiniz bilgi boyutlarını küçültmek.

Bu örnekte çıkaracağınız arşivi ikiye bölerek parola ile korumanızı öneriyorum (Winrar, Winzip gibi tüm arşivleme sistemlerinde, arşive parola ekleyebilirsiniz). Şimdi elinizde olan ikiye bölünmüş bilgiyi şifreleme işlemine geçmeden önce iki ayrı gerçek anlamda 128 mümkünse 256 Bitlik parola oluşturun. Diyelim ki arşivin 1. bölümünü Blowfish, 2. bölümünü AES 256 ile şifrelediniz. Bu bilgi ve oluşturmuş olduğunuz şifreleri birbirinden bağımsız ve dışarıdan bakıldığında birbiriyle alakasız dört ayrı kişiye emanet edin veya saklayın. Bu kişilerin veya yerlerin kesinlikle birbiriyle alakasız

olduklarına özen göstermenizde fayda var. Yanlış anlaşılmaya sebebiyet vermemek için tekrar ediyorum:

İki kişide (yerde) tüm bilginin birer parçası, iki kişide (yerde) iki ayrı şifreden yalnız birini vermek suretiyle bilginin tümünü saklamış olun. Bilgileri şifreleme yönteminin tersini uygulayarak tekrar bilgilerinize erişebilirsiniz.

Ya parolamı unutursam paranoyası

Bilinen bir yöntem olmakla birlikte oldukça sübjektif temellere dayanan bir uygulamayı önermek istiyorum. Sübjektif olması gizlilik ilkesiyle birlikte sizi koruyan unsur olacaktır. Kendimi örnek göstermek istiyorum:

Kütüphanemde yaklaşık 5000 civarında elektronik kitap, yarısı kadar da gerçek kitabım var. Tercih ettiğim, sevdiğim – sürekli elimin altında bulunan kitaplar 100 civarında. Bunların hangileri olduğunu ben ve bir ihtimal bana çok yakın olanlar biliyor. Diyelim ki bu kitaplardan birini gözüme kestirdim ve hiç bir gizleme, saklama ihtiyacı duymadan bir yere şu notu karaladım:

02055x2x3.-29x1x2

Siz şimdi bu yazılandan ne sonuç çıkarırsınız?
Bir şeyler yazıyor orada ama ne yazıyor, anlayabildiniz mi?

Anlamı şu:

Bilginize sunarım Rauf Bey

Açın Atatürk'ün 125. doğum yılı anısına ADD tarafından dağıtılan Nutuk kitabını ve kendiniz kontrol edin!

Deşifre şekli:

İlk 4 sayı safa
5. karakter sayfadaki satır
X'den sonra gelen kelime
Nokta işlemin bittiğini gösteriyor.
Eksi işareti aynı sayfada devam ettiğini gösteriyor. Ondan sonra gelen sayı yine satırı, X'den sonra gelen kelime(leri) gösteriyor.
Artı işareti başka bir sayfayı göstermekle birlikte artı işaretinden sonra gelen ilk dört sayı sayfayı göstermektedir vs.

Not: boşluklarda sayılıyor.

Gördüğüne inanma, bu konularda bildiğini kendine sakla!

Pardon siz beni bu kadar aptal mı sandınız?
Bu yöntemi kullanın, kullanın ama ek bir güvenlik önlemi almadan sakın kullanmayın!

Hiç kimsenin bilmediği, hiç bir yere yazmadığınız bir sayfa adaletini ± işleyin. Gözle görülen 0205'ci sayfa. Sizin belirtmediğiniz yalnız sizin aklınızda olan; görünen sayfa artı 3 veya eksi 15 işlemi sizi gerçek parolaya götürecektir. Yani bu 0208'ci veya 190'inci safa olabilir.

*Open Source düşüncesinin fikir babalarından biri.
** Misal olarak, *Hiç bir zaman rakibini hafife alma* cümlesini parola olarak kullandığınızı düşünelim. Bu cümle 34 karakterden oluşmaktadır. Yani siz simdi 34 x 8 = 272 Bitlik bir parola ile bilgilerinizi koruduğunuzu sanabilirsiniz. Ama bu yanılgı gerçekleri yansıtmıyor!!!
Her dilin kendine göre yoğun olarak kullandığı harfler vardır. Türkçemizde en çok kullandığımız harf A harfidir. Almanca, İngilizce ve Fransızca gibi dillerde E harfi çok kullanılır. Bu bilgiden yola çıkarak yukarıdaki formülü istatistik açıdan şu şekle çevirmek zorundayız: 34 x 1,5 = 51 Bit

Anlayacağınız üzere bir bilginin arşivini çıkarırken yukarıda belirtmiş olduğum nedenden dolayı, hem bilgi boyutunuz küçülecek hem de bu gibi analizleri yapabilecek kapasitede olanlara karşı, saldırı alanını daraltmış olacaksınız.

Âlice ve Bob

Simetrik şifreleme yöntemlerinde şifreyi gönderen Âlice, şifreyi alanda Bob olarak adlandırılırlar. Güvenlik açısından Âlice ve Bob güvenli bir yerde şifre alışverişinde bulunmaları zorunludur. Bu gibi konular elektronik ortamda, Telefon vasıtasıyla gerçekleşmemeli. Pratik yönden şifreleme yönteminde kullanacağınız algoritmanın ve parolanın kalitesine oranla deşifre işlemi ve deşifrelenecek içeriğin değeri birbirine orantısızsa güvende sayılabilirsiniz. Ama cümle kurdum ama…

Ben size söyle izah edeyim; bir apartman ve bir hırsız düşünün. Hırsızın genel anlamda önce söyle bir kapılara bakacağını farz edelim. Bu hırsız bir çelik kapının ardında, bildik bir kapıya oranla daha değerli bir şeylerin olabileceğini düşünecektir. Şimdi bu çelik kapıyı açmak için harcayacağı zaman ve yakalanma riskine oranla diğer evden çalacağı maddi değer daha fazla olabilir. Çünkü oradaki risk ve çıkar, çelik kapılı eve nazaran daha az olabilir. Risk (ortaya koymam gereken teknik ve maddi donanım) ve elde edeceğim çıkar orantılı olmalı.

Telefon dedikte aklıma geldi

Günümüzde Türkiye'de herkes telefonlarının dinlendiğinden şikâyetçi, hâlbuki telefon konuşmaları da eşzamanlı şifrelenebiliyor. Bizim On-Demand dediğimiz şifreleme yönteminde en azından şu an için eşzamanlı deşifre imkânları çok ama çok kısıtlı.

Birkaç pratik (Avrupa Birliği) veriyle konuyu kapatalım:

Şifrelenecek içerik	Zamanaşımı	En az Simetrik parola uzunluğu
Askeri bilgi*	Bir kaç dakika / saat	64 Bit
Kısa vadeli ticari bilgiler	Gün / Hafta	64 Bit
Uzun vadeli ticari bilgiler	Sene	64 bit
Ticari sırlar	Onlarca yıl	112 Bit
Kişisel bilgiler	50 sene	128 Bit
Diplomatik bilgi / sır	65 senenin üzerinde	256 Bit

*En az gerçek 64 Bit ile şifrelenen askeri bir bilgiyi bir kaç dakika veya saat içinde deşifresi şimdilik mümkün değil. Diğerleri için zaten genelde başka ek önlemlerde alınıyor.

Simetrik şifre uzunluğu	Asimetrik şifre uzunluğu
56 Bit	384 Bit
65 Bit	512 Bit
80 Bit	768 Bit
112 Bit	1792 Bit
128 Bit	2304 Bit

Mea Culpa*

Zaman zaman muhtelif boy ve ebatlarda karşımıza çıkan irtica sorununu, bir müddet daha göğüslememiz gerekecek. Dilleri farklı olsa da, aslında din ve bilim aynı şeyi anlatmaya çalışıyorlar. İkisi de gerçeklerin peşinde, bilim ve din birbirini tamamlayan iki unsurdur.

Mamafih, Allah insanın imanını başkalarının müdahalesiyle sınamasın…

Vatana hizmet, her zaman meşakkatli olmayabilir ama vatan sevgisi özelde, sevgi ise genelde zaman zaman ispat ister. Atatürk ilke ve inkılâpları için liyakatimizi terazilemedeki sorunlarımızı, son kullanma tarihi geçmiş bir zihniyet ile çözemeyeceğimiz ortada. Ancak bende Atam gibi milletime güveniyor, onlara inanıyorum. Biz başaramasak ta, evlatlarımız bu sorunun üstesinden gelecektir!

AKP zihniyeti uzatmaları oynuyor, bir ayağı çukurda. Elbet fırtınalı günlerin ardından sükût gelecektir…

Söz verdiğim halde sözümü tutmamanın utancını yaşıyorum. Ama bu gibi hatalar telafi edilebilir hatalardır. Sanal ortamlarda, sanal bir "hükümet" tarafından yönetiliyoruz. Sanal sorunların, sanal çözümleri - sanal zihniyeti, somut "devrimler" yapmakta cesaretlendiriyor. Bu cürete karşı bizde kendimizi sanal bilgisayar ve sanal klavye** ile koruyalım!

Tüm sabit diski bir çırpıda şifrelemeyi önermiyorum çünkü bir kere deşifre edildiğinde, tüm bilgileriniz kabak gibi ortada çıkacaktır. Onun yerine bilgileri ayrı ayrı değişik yöntemler uygulayarak gizlemeniz daha sağlıklı olacaktır. Saldırgan bu yöntemde her defasında sıfırdan başlamak zorunda. Client – Server çerçevesinde çalışmadığınızı varsayarak bu konuda hiçbir öneride bulunmadım (güvenlik açısından daha sağlıklı bir çalışma şeklidir).

Gerçek bilgisayarınızın sanal bir kopyasını çıkararak D sürücüsüne kopyalayın (orijinal halini DVD'e kopyalayarak muhafaza edin. Böylelikle her zaman orijinali D sürücüsüne tekrar kayıt edebilirsiniz). Bir önceki makaleme atfen D sürücüsünde olan sanal bilgisayarınızı çalıştırarak gereken tüm işlemleri yapabilirsiniz. D sürücüsünü güvenli bir şekilde sildiğiniz takdirde ardınızda iz bırakmayacaksınız.

VirtualBox 2.2.2*** (işletim sistemi emülatörüdür bilinen çoğu işletim sistemini emüle edip çalıştırabilir)

*Latince benim suçum / hatam
**Sanal klavyeyi şiddetle kullanmanızı öneriyorum, keylogger`lere karşı önlem.
*** VirtualBox ücretsizdir. Şahsen VMWare'i öneririm ama "pahalı" bir yazılımdır.

Saygılarımla

Önder Gürbüz

Almanya

İrtica ile mücadelemiz sonuna kadar sürecek