farmafarm

YILAN YAĞI KRİPTO

Ruşen Eşref YAZGAN

farmafarm

YILAN YAĞI KRİPTO

NE DEMEK?

- **“Yılan Yağı” (İng. Snake Oil),
işe yaradığı bilimsel olarak kanıtlanmamış kripto sistemleri, genellikle algoritmalar için kripto jargonunda kullanılan tabirdir.**
- **Dilimizde karşılığı, “şarlatanlık”, “palavra” veya en hafifinden “kerameti kendinden menkul” olabilir.**

farmafarm

YILAN YAĞI KRİPTO

NEREDEN GELİYOR?

Bu tabir, önceleri ilaç ve eczacılık sektöründe kullanılırdı.

- **Tıbbi değeri olmadığı halde her derde deva olduğu iddia edilen;**
- **Belirli bir hastalığı iyileştirmede faydalı olduğu kanıtlanmamış;**
- **İnsan sağlığı üzerindeki etkileri araştırılmamış;**
- **Bilimsel yöntemlerle geliştirilmemiş**

ilaçlar genel olarak "yılan yağı" diye adlandırılırdı.

Bilahare, faydası kanıtlanmamış, işe yarayıp yaramadığı dahi bilinmeyen her türlü ürün, mal ve hatta görüş, politika, çözüm önerisi, vs. için kullanılır oldu.

Kolayca oya tahvil edilebilen ama halkın yararına olmayan, işe yaramayan politikalar için de kullanılır "yılan yağı" tabiri.

farmafarm

YILAN YAĞI KRİPTO

NEREDEN GELİYOR?

Kullanıcının menfaatini ve ürünün prestijini düşünmeden, sadece kâr odaklı hareket eden satıcılar için bugünlerde bile "yılan yağı taciri" tabiri kullanılır.

Tabir nereden geliyor?

1800'lerde demiryollarının yapımında çalışmak için Amerika'ya göç eden çok sayıda Çinli işçi beraberlerinde getirmiş oldukları geleneksel, ev yapımı ilaçları kullanıyorlardı.
Çin'deki bir su yılanının yağından elde edilmiş olan, fazla miktarda Omega-3 içeren Yılan Yağı, yorucu bir günün sonunda eklemlerde oluşan şişi, ağrıyı ve yanmayı gidermede çok etkiliydi.

Peki, böylesi etkin bir geleneksel ilaç nasıl oldu da işe yaramayan ürünler için isim kaynağı haline geldi?

farmafarm

YILAN YAĞI KRİPTO

NEREDEN GELİYOR?

1800'lerin sonuna doğru, geleneksel bir Çin ilacı olan yılan yağının ünü tüm ülkeyi sarmış ve tabii sahteleri de piyasaya sürülmüştü. Hatta, eklem ağrılarının yanı sıra baş ağrısına, böbrek ağrısına, adet ağrısına ve daha bir dolu derde iyi geldiği iddia edilir olmuştu. Yalnız mesele şu ki geleneksel yılan yağının elde edildiği Çin su yılanı Amerika'da bulunmuyordu. O zaman, Amerikan çıngıraklı yılanları ne güne duruyordu?..

Çıngıraklı Yılan Kıralı diye tanınan eski kovboy Clark Stanley, 1893 Şikago Dünya Fuarı'ndaki reyonunda canlı canlı karnını yardığı çıngıraklı yılanları kaynar suya atıyor ve suyun üzerinde biriken yağı alıp şişeleyerek satıyordu.

Stanley'in veya başkalarının şişeleyip piyasaya sürdüğü yılan yağı neredeyse yok satıyor, üreticisine ve satıcısına büyük kâr sağlıyordu.

farmafarm

YILAN YAĞI KRİPTO

NEREDEN GELİYOR?

Ancak, yılan yağı sayesinde ün ve para kazananların piyasaya sürdüğü ürünlerde oldukça ciddi iki sorun vardı:

1. **Amerikan çıngıraklı yılanının yağındaki iyileştirici etken madde Çin su yılanınınkine nazaran çok daha azdı.**
2. **Bazı ürünlerde, bırakın çıngıraklısını, hiçbir yılanın yağı bulunmuyordu.**

İşte o zamandan bu yana yılan yağı, özellikle ilaç ve eczacılık sektöründe şarlatanlığın adı oldu.

Bilgisayar sektörü (ki kriptologların çoğu bu sektördendir) kelime dağarcığına kattığı "menu", "folder", "firewall", "backbone", "firmware", "hibernate", "kernel", "interface", "virtual", "web", "net" gibi bir dolu egzotik terimin yanına "yılan yağı"nı da eklemeyi ihmal etmedi.

farmafarm

YILAN YAĞI KRİPTO

NASIL GELİŞİYOR?

Peki, yılan yağı gibi bir şarlatanlık kripto sektörü gibi oldukça "akıllı" kişilerin çalıştığı bir sektörde nasıl oldu da kendine yer buldu?

Birçok sebep sayılabilir:

- **"akıllı" kişiler genellikle kendi "akıl"larını beğenir, başkalarınınkini küçümserler; bu yüzden, kendi "akıl"larıyla geliştirdikleri sistemin diğerlerininkinden daha üstün olduğuna inanırlar.**
- **Daha kötüsü, birçoğu buna kalben inanırlar.**
- **Tabiidir ki iyi niyetlilerin yanı sıra yaptıklarının şarlatanlık olduğunu bilip de umursamayan, kısa yoldan kâr elde etmeye çalışan kötü niyetliler de piyasadadır.**

farmafarm

YILAN YAĞI KRİPTO

NASIL GELİŞİYOR?

- Yılan yağı kripto sistemini başkalarının (mesela müttefiklerinin, iş ortaklarının) kullanımına verip ondan fayda sağlamaya yeltenen profesyonelleri göz ardı etmemek gerekir.
- Eğer sebep hamaset ve hamiyetse?.. Konuyu çok iyi bilmeyen ve bilmek zorunda olmayan yöneticilerin veya halkın hamaset ve hamiyet hislerini okşayanlara ne demeli?
- Üstüne üstlük sektör kalın bir gizlilik ve güvenlik perdesi ardındaysa; yapılanlar bu perdenin ardına saklanıp kimseyle paylaşılmıyorsa ve sektördekiler bundan paye çıkarıp haz alıyorsa?..

Görünen o ki kriptoloji sahası yılan yağı için hayli elverişli bir ortam oluşturmaktadır.

farmafarm

YILAN YAĞI KRİPTO

NİÇİN YAYGIN?

Yılan yağı, kötü kriptonun en yaygın örneğidir;

çünkü:

- **Kötü kriptoyu iyisinden ayırt etmek çok zordur; hatta kötü kripto çoğu zaman iyi kripto gibi görünür.**
  - ✧ **Aslında tüm güvenlik uygulamaları için geçerlidir bu. Maalesef, kötü güvenlik genellikle iyi güvenlik gibi görünür. (hatta -bilmeyen göze- daha iyi görünür.)**
  - ✓ **Her ikisinde de son ürüne bakıldığında farkı anlamak zordur. (karmaşık sayılar, harfler, karakterler üretirler.)**
  - ✓ **Her ikisi de kabul görmüş ara yöntemleri uyguluyor olabilir ama tüm sistem olarak ele alındığında biri iyi, diğeri kötüdür.**
  - ✓ **Kötü kriptoyu geliştiren, kendisi veya güvendiği tanıdıkları çözemediğinde, yaptığını iyi zanneder. (kuzguna yavrusu misali...)**

farmafarm

YILAN YAĞI KRİPTO

NİÇİN YAYGIN?

- Yöntem (algoritma), kullanıcıya izah edilmez veya kullanıcı tarafından anlaşılması mümkün olmayan ifadelerle izah(!) edilir.

İlaveten:

- Kripto sistemini geliştirenin sorumluluğu tanımlanmamış veya hiç yoksa (?..)
- Sektör kalın bir gizlilik ve güvenlik perdesi ardındaysa; yapılanlar bu perdenin ardına saklanıp kimseyle paylaşılmadığı için sadece yılan yağı tacirleri ve inananları bundan paye çıkarıyorsa (?..)

Dahası:

- Yılan yağı kripto sisteminin zaafını fark eden karşı taraf (düşman, rakip, vs.) fayda sağlamak için bu zaafı açıklamıyor ve bu zayıf sistem kullanılmaya devam ediyorsa (!..)

farmafarm

YILAN YAĞI KRİPTO

İLAÇ SEKTÖRÜNÜN BASİRETİ

İlaç ve eczacılık sektöründe de yapılan iddiaların geçerliliği kullanıcı tarafından doğrulanamaz veya sorgulanamazdı ve sektörün sorumluluğu belirsiz, hatta yoktu.

İlaç ve eczacılık sektörü, 1800'lerin ikinci yarısı ve 1900'lerde ilaç geliştirme ve üretme kurallarının iyileştirildiği bir süreçten geçti ve iyi yöntemlerin (Good Practices) bağlayıcı şekilde uygulandığı bir seviyeye ulaştı.

Sonunda gelinen noktada gerek ilaç öneren doktorlar, gerekse ilaç kullanan hastalar hayli yüksek güvenilirlik seviyesinde yararlanmaktadır ilaçlardan.

Peki, ilaç ve eczacılık sektörünün göstermiş olduğu basireti kripto (güvenlik) sektörü niçin gösterememiştir?

farmafarm

YILAN YAĞI KRİPTO

DÜSTUR

Soruyu tekrarlayalım:
İlaç sektörünün göstermiş olduğu basireti kripto (güvenlik) sektörü niçin gösterememiştir?

Bu sorunun cevabı, sektörün ardına sığındığı gizlilik ve güvenlik perdesinin altında yatmaktadır.

Düstur:

Herhangi bir güvenlik sistemi ne denli gizliyse
güvenliğinin zayıf olma ihtimali o denli yüksektir.

Kripto sistemleri de ne yazık ki bu düsturdan vareste değildirler.

Felakete giden yol:

gizlilik -> denetimsizlik -> tehlikeyi fark edememe -> felaket

farmafarm

YILAN YAĞI KRİPTO

TEHLİKE

- **Gizlilik**
- **Hamaset, hamiyet (milli...)**
- **Açık incelemeden uzak (bilimsel, mesleki, profesyonel, amatör...) (peer review)**
- **Yılan yağını yapan yaptığının yılan yağı olduğunu bilmeyebilir (bilebilir de...)**
- **Yılan yağının yılan yağı olduğunu anlamak zordur**
- **Yılan yağında hiç yılan dahi olmayabilir.**
- **Yılan yağı aslında yılan zehri olabilir.**
- **Yılan yağını fark eden açıklamak zorunda değildir**

Tehlikenin giderilmesi için öncelikle sağduyulu davranmak ve olası ipuçlarına, uyarı işaretlerine dikkat etmek gerekir

farmafarm

YILAN YAĞI KRİPTO

SAĞDUYU

SORMAK GEREK

- **Kendiniz veya bir yakınınız hastalandığında modern tıp ve eczacılık sektörünün uluslararası normlar çerçevesinde düzenlenmiş kuralları, teşhis ve tedavi protokolleri içerisinde çare ararken kişisel güvenlik, kurumsal güvenlik ya da ülke güvenliği söz konusu olduğunda niçin başka yollara sapıyoruz?**
- **İçeriğinin ne olduğunu, nasıl üretildiğini ve hangi endikasyonları ve kontrendikasyonları olduğunu tam olarak bilmediğimiz bir ilacı kullanmak ister miyiz?**
  - Tabii ki tıp veya eczacılık uzmanı olmadığımız için bu ayrıntıları bilemeyiz; bu yüzden yetkin ve yetkili devlet kurumları ve uluslararası kuruluşlar tarafından denetlenmiş ve onanmış ilaçları kullanmaktayız.

farmafarm

YILAN YAĞI KRİPTO

SAĞDUYU

SORMAK GEREK

- **“Ben bir ilaç buldum; ancak, içeriğini ve nasıl üretildiğini söyleyemem, çok gizli; etkili olup olmadığı hususunda ve yan etkileri hakkında henüz bir şey bilmiyorum, yeterince denenmedi; ama bana güvenin, yemin ederim ki bu ilaç çok iyi gelecek size,” diyen bir doktora veya eczacıya güvenir miydiniz?**
  - Siz güvenseniz dahi devletin yetkili kurumları ve ilgili meslek kuruluşları güvenmez; güvenmemekle kalmaz, suç duyurusunda bulunur.
- **Yukarıdaki iddialara ilaveten, “Bu ilaç milli; tamamen milli kaynaklarla milli emekle ve milli beyin gücüyle üretildi,” deseler bu sizi etkiler miydi? Alacağınız kanser ilacı “milli” olunca kanser hücreleri üzerinde daha etkili olur zannına kapılır mıydınız?**
  - Bunu söyleyen eczacının diplomasını alırlar elinden.
- **“Milli açık kalp ameliyatı” veya “Prostat kanserinde özgün, milli tedavi protokolü” duydunuz mu hiç? Duysanız ciddiye alır mıydınız?**
  - Kaygılanmayın, bunları duymayacak kadar emin ellerdedir sağlık sektörü.

farmafarm

YILAN YAĞI KRİPTO

SAĞDUYU

SORMAK GEREK

- **“Ben bir ameliyat -veya tedavi- yöntemi uyguluyorum; ancak, nasıl yaptığımı kimseye göstermiyor, Sağlık Bakanlığı ve üniversitelerin yetkilileriyle paylaşmıyorum. Henüz kabul görmüş bir protokol değil ama ben uyguluyorum, hastalarım da çok memnun kalıyorlar,” diyen bir doktorun ameliyat masasına yatar mıydınız?**
  - Zaten hiçbir doktor bunu söylemez, söyleyemez.

<u>Soru</u>: Konu sağlık olduğunda oldukça sağduyulu davranan biz, konu güvenlik olduğunda niye yitiriyoruz bu sağduyumuzu?

<u>Cevap</u>: Çünkü, sağlık hayli somut bir konudur, bire bir etkiler bizi; güvenlikse soyut bir kavramdır; etkisini dolaylı yoldan gösterir. (ta ki bir gün gelip bire bir etkileyene dek...)

İşte, tehlike algısındaki bu farklılık yılan yağı için müsait ortamı hazırlamaktadır.

farmafarm

YILAN YAĞI KRİPTO

MİLLİ OLMALI MI?

NEREYE KADAR?

- Milli kripto hevesi ve çabası bir yere kadar iyidir ve desteklenmelidir.
- Burada amaç yerel iş gücünün (beyin gücünün) yaratılması ve geliştirilmesi olmalıdır.
  (O beyin gücüdür ki yılan yağını fark edebilir ve engeller.)
- "Milli"den kasıt, milli menfaatin korunması ise bu ancak milli menfaati önde tutan ve bu doğrultuda çalışan akıl ve vicdan sayesinde mümkün olabilir.
  Bu doğrultuda çalışırken bilimsel doğrular ve pratik gerçekleri göz ardı etmek en hafifinden kendini kandırmak olur ama konu güvenlik olduğunda çok daha vahim sonuçlar söz konusu olabilir.
- Hamaset ve hamiyet saikıyla yılan yağından medet umman akıl ve vicdan, yarardan ziyade zarar verir milli menfaate.

farmafarm

YILAN YAĞI KRİPTO

MİLLİ OLMALI MI?

MİLLİ MATEMATİK

Soru: Milli matematik olur mu?
Cevap: Hayır.

Kriptoloji, nihayetinde matematik bilimidir.
Kriptografi algoritması matematiksel bir uygulamadır.

İnsan hakları, hukuk, tıp, kimya, fizik ve daha birçok konuda evrensel ölçütler geçerlidir; milli - gayri milli ayrımı olmaz.

Peki, fizikte olmuyor, tıpta olmuyor, hukukta olmuyor da matematikte nasıl oluyor?

"Milli kanser tedavisi" diyen tıp doktoruna ne gözle bakıyorsak, "milli kripto algoritması" diyen matematikçi veya mühendise de aynı gözle bakmak gerekir.

farmafarm

YILAN YAĞI KRİPTO

KUŞKU VE KORKU

- Yılan yağı için ortamı müsait hale getiren “kuşku” ve “korku”dur.
  - Yöntem açık ve bilinirse güvenli olmaz kuşkusu ve korkusu
  - Yabancı el değmişse güvenilmez kuşkusu ve korkusu
- Yılan yağı tacirleri hemen her fırsatta bu kuşkuyu dile getirirler ve kullanıcının zaten duymakta olduğu kuşkuyu daha da artırarak korkuya, hatta paranoyaya çevirirler.
- Korku hayli yaygın ve etkin bir reflekstir; çokça ve kolayca manipüle edilebilir.
- Kullanıcı bir kere korkunun pençesine düştü mü artık yılan yağı tacirinin oyuncağı olmuştur; onun istediği her şeyi yapar.

farmafarm

YILAN YAĞI KRİPTO

KUŞKU VE KORKU

- Yılan yağı tacirleri, yılan yağına karşı duran görüşün düşman tarafından ortaya atıldığını iddia edebilirler. İddialarını desteklemek için NSA ve Snowden gibi bilinen örnekleri öne sürebilirler.
- Peki ya düşmanı (hasmı, rakibi, herkesi) bilhassa yılan yağı kriptoya yönlendirmek amacıyla yaygın algı yaratmak için Snowden mizanseni kurulduysa?
- Kuşku duymanın sonu yok; aslında kuşku bir yere kadar iyidir de. Olmaması gereken korkudur.
  Korku güdülü refleksif tepkiler çoğunlukla zarar verici sonuçlara yol açar. Özellikle güvenlik söz konusu olduğunda bu tür tepkiler güvenliği kuvvetlendirmekten ziyade zayıflatır.
  Bu yüzdendir ki güvenliği zayıflatmak isteyen düşman (hasım, rakip) öncelikle korku yaratarak hata yapmaya sevk eder karşı tarafı.

farmafarm

YILAN YAĞI KRİPTO

YILANA SARILMALI MI?

- **“Denize düşen yılana sarılır” misali, bilgisizlik denizine düşen de yılan yağından medet umar .**
  - Hangisi daha korkutucu?

  Yüzme bilmediği için denizde boğulacağı kesin olan biri eğer yılanı idare edebiliyorsa yılana sarılmayı tercih edebilir. O an için doğru bir çözüm olarak görülebilir. Ama ya bilinçli bir sarılma değil de panik halinde tutunuyorsa yılana; o zaman vay haline...

- **Halbuki, olması gereken, iyi yüzme bilmektir.**

farmafarm

YILAN YAĞI KRİPTO

NASIL SAKINMALI?

Kuşku bir yere kadar yararlı olabilir, ancak korku ve reflekslerin bizi yönetmesine izin vermemeliyiz.

- **Korku ve korkunun sonucu panik ve refleks güdülü hareketler tehlikeli sonuçlara yol açabilir.**
- **Ciddi güvenlik zaafına yol açan yılan yağından sakınmada da aynı esas geçerlidir.**
- **Kuşkuyu anlamlandırmada ve yönetmede ipuçları çok önemlidir.**
- **İpuçlarını gözden kaçırmamalı, aramalı, bulmalı;**
  ancak her ipucundan yola çıkarak genelleme yapmamalı;
  her bir ipucunu sağlıklı değerlendirmeliyiz.
  Aksi takdirde, her şeyden kuşkulanma, her şeyi reddetme ve yılan yağı olmayanı da yılan yağı sanma hatasına düşeriz ki bu da arzu edilmez.

farmafarm

YILAN YAĞI KRİPTO

NASIL SAKINMALI?

İPUÇLARI

 # 1 Anlamsız, yarı matematiksel saçmalık

Kripto algoritmasını tarif eden tanıtım dokümanda, "Özel olarak geliştirilmiş sanal matris yardımıyla ikili tabanda yarı-rastgele sayısal modüler kaydırma yöntemi..." gibi bir ifade okuduğunuzda veya "Herhangi bir matematiksel algoritma kullanılmadığı için tersine mühendislik yoluyla kırılması imkânsız..." gibi bir iddia duyduğunuzda hemen uzaklaşın oradan.
Zekânıza hakaret eden biriyle çalışmak istemezsiniz, herhalde.

 # 2 Cehalet

Konuyu tam anlamadığını belli eden ifadeler çoğu zaman cehaletin göstergesidir; hele bir de alakasız bir takım genel doğrular içeriyorsa...

 # 3 Yeni, özgün matematik

Mümkün, ancak kolay değil. Çok ciddi bilimsel altyapı ve çalışma gerektirir.

farmafarm

YILAN YAĞI KRİPTO

NASIL SAKINMALI?

İPUÇLARI

 # 4 Anlamsız kanıtlama

Güvenlikle alakalı olmayan, yanıltıcı kanıtlama yöntemleri...

Kuşku ile bakmakta yarar var. (Bu iddiada bulunana nasıl yaptığını, özellikle anahtar yönetimini nasıl hallettiğini izah ettirmek gerekir.)

 # 5 Asılsız iddia

İçi boş, altı doldurulmamış iddialar...
"Dünyanın en kuvvetli, kırılması imkânsız algoritması" şeklinde bir iddia ne gibi bir kanıta dayanıyor diye sormak gerekir.

 # 6 Aşırı uzun anahtar

Çok uzun anahtar kullandığını belirten bir kripto sistemi pratikten uzaktır.
Gereksiz uzunlukta anahtar kullanan bir sisteme niye güvenilsin ki?
Ayrıca, pratik olmadığı için düzgün yönetilemeyen her sistem gibi zaaf içerisindedir ve tehlikeye açıktır.

farmafarm

YILAN YAĞI KRİPTO

NASIL SAKINMALI?

İPUÇLARI

 # 7 Gizli kripto algoritması

Nasıl işlediği açıklanmayan, gizli tutulan bir algoritma söz konusuysa, amatörlük ya da açığa çıkması istenmeyen bir şeyin varlığı söz konusudur genellikle.

 # 8 Tek kullanımlık defter (one-time-pad)

**Doğru tasarlandığında ve doğru kullanıldığında en güvenli sistemdir;
ancak, günümüz pratiğinde kullanılması hayli zordur;
dolayısıyla, kullandığını söyleyenlere şüphe ile yaklaşmak gerekir.**

 # 9 Yarışma veya saldırı

Sistemin güvenliğini yarışma yoluyla kanıtlamaya kalkışmak güvenlik konusunu anlamamış olmanın göstergelerinden biridir. Öte yandan, herkes yarışmaya katılmak zorunda mı veya her katılan iyi niyetli olmak durumunda mı? Yarışma veya penetrasyon testi düzenleyen en az katılanlar kadar bu işi iyi biliyor olmalı. Kripto sistemini, birilerine kurcalatmak iyi sonuç vermeyebilir.

farmafarm

YILAN YAĞI KRİPTO

SONUÇ?..

Diyeceksiniz ki,
“Onu yapma, bunu yapma, ondan kuşku duy, bundan şüphelen...
Peki, ne yapacağız?”

Tek cevabım: Haklısınız sormakta.

- **Kuşku duymaya devam edin ama kesinlikle korku duymayın, paniğe kapılmayın.**
- **Akıllı, sağduyulu davranın.**
- **Saçmalığa prim vermeyin.**
- **Kanıtlanmamış, yöntemlerden medet ummayın.**
- **Bilime, bilim dışı unsurlar katmayın.**
- **Kendini kanıtlamış, “dürüst bilim” yapan uzmanlardan yardım alın.**
- **Denetleyin, denetleyin, denetleyin...**

farmafarm

YILAN YAĞI KRİPTO

KAYNAKÇA

http://www.merriam-webster.com/dictionary/snake%20oil

http://www.oxforddictionaries.com/definition/english/snake-oil?q=snake+oil

http://www.urbandictionary.com/define.php?term=snake%20oil

http://en.wikipedia.org/wiki/Snake_oil

http://www.npr.org/blogs/codeswitch/2013/08/26/215761377/a-history-of-snake-oil-salesmen

https://www.schneier.com/crypto-gram-9902.html

farmafarm

YILAN YAĞI KRİPTO

TEŞEKKÜR EDERİM

Ruşen Eşref YAZGAN