ADIM ADIM GÖMÜLÜ ZARARLI YAZILIMDAN KORUNMA

1. GÖMÜLÜ YAZILIM TANIMI

Donanımlar üzerinde bulunan, işletim sistemi ile donanım arasındaki iletişimi sağlayan yazılımlardır. Firmware olarak da adlandırılırlar. Ana kart, PCI kartları, harddisk, printer, scanner, router, switch, modem ve daha bir çok donanım üzerinde firmware yazılımları bulunmaktadır [1].

2. GÖMÜLÜ YAZILIMLAR ÜZERİNDEKİ TEHDİT

Bilgisayarları kullanmamıza olanak sağlayan ve yöneten yazılımlar işletim sistemleridir. İşletim sistemleri firmwareler aracılığıyla bilgisayarlardaki donanımlara ulaşır ve yazılımların isteklerini yerine getirir. Ana kartlar üzerinde bulunan firmwareler sayesinde işletim sistemleri açılır. Yani işletim sistemleri devrede değilken firmwareler çalışır. İşletim sistemleri üzerinde çalıştırdığımız hertürlü antivirüs, "host based IPS", "integrity checker", vb yazılımları sistemlerin açılışları esnasında yüklü olmadıkları için herhangi bir algılama yapamazlar. Yüklendikten sonra bile işletim seviyesi işlemlere baktıkları ve en düşük seviye olarak işletim sisteminin kernel sevisindeki haberleşmeleri anlayabildiklerinden firmware seviyesinde olan haberleşmelere herhangi bir müdahalede bulunamazlar. Bu sebeplerden dolayı firmware üzerinde yapılan değişiklikle tekrar yüklenen (reflash) zararlı yazılım içeren (malware) firmware tek başına algılanması neredeyse imkansız bir tehdit olarak karşımıza çıkmaktadır. Firmware üzerinde zararlı yazılım oluşturmak konusunda çok tecrübeli uzmanların yapabileceği bir iştir. Bununla birlikle yapılması durumunda ise çok tehlikeli ve etkisi çok büyük olacaktır.

3. GÖMÜLÜ ZARARLI YAZILIM ÇALIŞMALARI

Firmware malware analizleri üzerinde bazı çalışmalar mevcuttur. Bunlardan en çarpıcısı BlackHat 2012 de sunulan BIOS üzerine konumlandırılan ve çalışmaya başladıktan sonra istenildiği zaman uzaktan erişilebilen ve hatta güncellenebilen bir firmware yazılımıdır [2]. Zararlı yazılım firewall ve IPS sistemlerini by-pass edecek şekilde tasarlanmıştır. Wifi üzerinden yada https üzerinden arkakapı (backdoor) açabilmektedir. %100 gizlidir, herhangi bir antivirus tarafından tespit edilemez ve 230 çeşit anakart üzerinde çalışmaktadır. Bu da şunu açıkça göstermektedir ki donanım tedarik sürecinde rol alan herhangi biri donanımı bir arka kapı haline getirebilir. Bununla ilgili olarak Dell firmasının yaşamış olduğu sorun [3] gerçeği açıkça ortaya koymaktadır. Büyük bir üreticinin ürettiği PClerin anakart firmware yazılımda zararlı yazılım olması, üretim zincirindeki güvenliği ön plana çıkarmaktadır. Microsoft tarafından yapılan bir araştırma sonucunda Çin'den satın alınan PC/laptoplarda değiştirilmiş Windows yazılımı kullanıldığı tespit edilmiştir [4].

4. ÖNLEME

Gömülü zararlı yazılımları maliyeti sebebiyle tespit etmek yerine çeşitli önleme teknikleriyle bu gibi yazılımların barındırılması önlenmelidir. Bu teknikler:

- ✓ Satın alınan donanımlar güvenilir kaynaklardan alınmalı, gerekiyorsa tedarik zincirinde yer alan tüm paydaşlar incelenmelidir.
- ✓ Satın alınan hertürlü donanım (anakartlar, network kartları, vb) reflash edilmelidir. Bu maliyetli bir işlem olarak karşımıza çıkmaktadır.
- ✓ Kurumun güvenlik politikaları gömülü zararlı yazılımlarına karşı tekrar güncellenmelidir.

5. TESPİT ETME

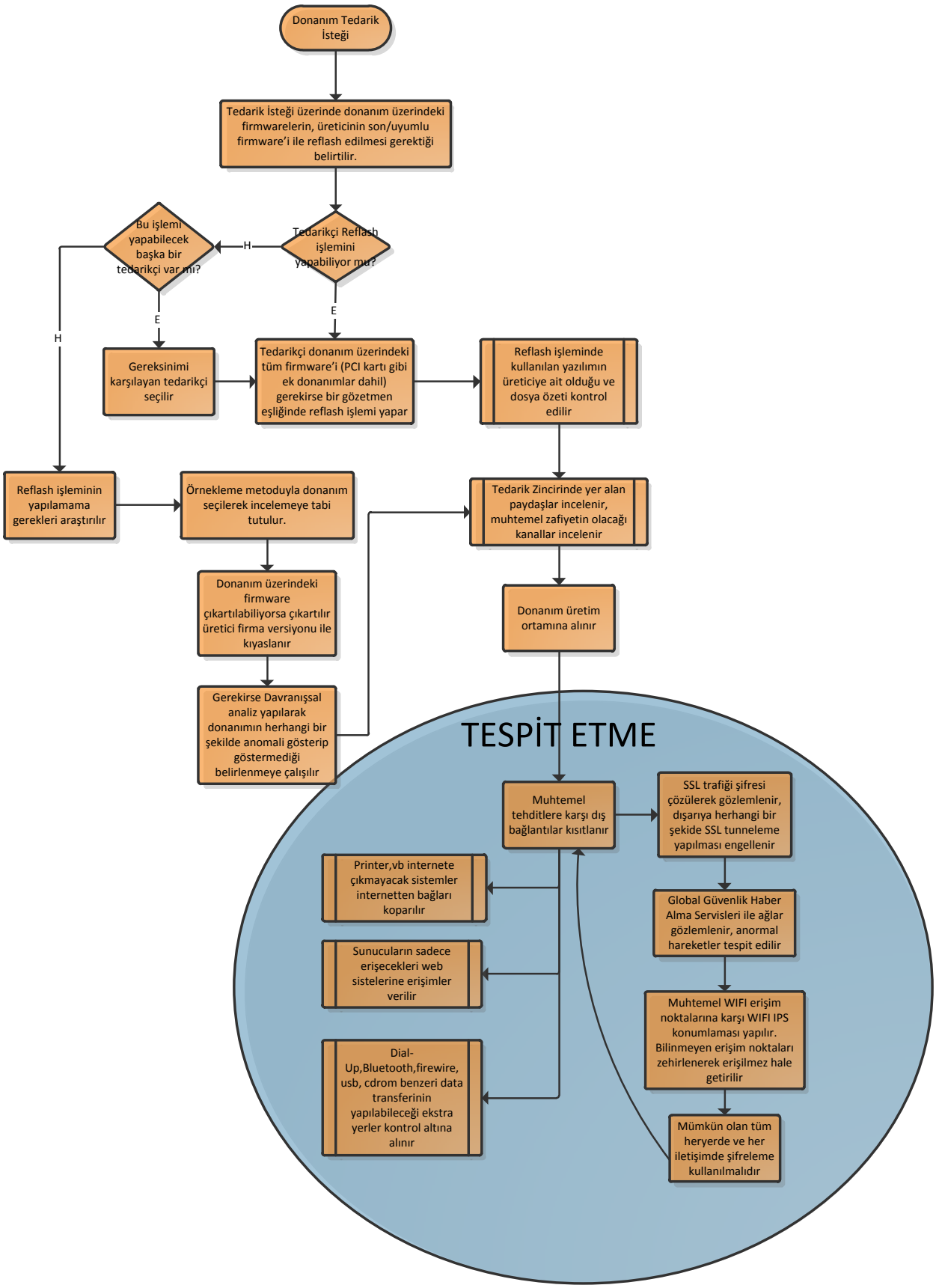
Firmware üzerindeki zararlı yazılımların bulunduğu donanım üzerinde tespit edilmesi çok zordur. Tespit edilmesi davranışsal analiz yapılarak kolaylaştırılabilir. Tespit aşamasında şunlar yapılabilir:

- ✓ Donanım üzerinde bulunan Firmware elde edilerek çeşitli forensics teknikleriyle analiz edilebilir. Bu analiz düşük seviyeli bir analiz olacağından konusunda uzman kişiler tarafından yapılması gerekmektedir ve kaynak/zaman olarak çok maliyetlidir.
- ✓ Donanım üzerinde bulunan Firmware elde edilerek dosya özeti (checksum) hesaplanarak üreticideki versiyonu ile kıyaslanabilir. Fakat eğer üretici tarafından üretilen firmware'de zararlı yazılım bulunuyorsa(çok düşük bir olasılık) yapılacak bu karşılaştırma hiçbir işe yaramayacaktır.
- ✓ Eğer donanım üzerinde zararlı yazılım tespit edilirse, donanımı reflash etmek çözüm olmayabilir. Bu sebepten dolayı, bu donanımın ve benzerlerinin kullanımı bırakılmalı ve tedarik edilen yer ile ilgili detaylı bir araştırma yapılmalıdır. Çünkü donanım ile beraber çalışan baska bir donanım, ilgili donanımın tekrar reflash edilerek enfekte olmasına sebep olabilir.
- ✓ Bu yazılımlarda amaç bilgi çalmak, finansal kazanç sağlamak gibi ana nedenler olduğundan dışarıyla bağlantıya geçmeye çalışacak, bunun için ya başka bir malware indirecek ya da kendisi direkt olarak bir bağlantı başlatacaktır. Çalışma ortamlarındaki bağlantı olanakları (LAN, WAN, dial-up, WİFİ, 3G/4G, usb, firewire, Bluetooth, vb) tespit edilmeli ve yetkisiz erişimler için bağlantılar izlenmelidir. Bunu yapabilmek için:
    - o Şirketlerde genelde 80 ve 443 portları dışarıya açık olduğundan HTTP ve SSL iletişimi gözlemlenmelidir. İç kullanıcıların bu sayede başka malware indirmeleri engelenebilecektir.
    - o Şirket içinden dışarıya yapılacak bağlantılar IBM X-Force, Symantec DeepSight, Mcafee threat intelligence, vb hizmetlerinin sunduğu IP güvenilirlik servisi ile bağlantıya geçilen IP adresleri control edilebilir.
    - o Kurum içinde kablosuz ağ olsun olmasın kablosuz ağlar için IPS sistemleri konumlandırılmalı ve bilgi dahilinde olmayan kablosuz ağlar zehirlenerek devre dışı bırakılmalıdır. Bu sayede çalışma ortamında bulunan yetkisiz herhangi bir erişim noktası (access point) göreviyle çalışan cihaz devre dışı bırakılmış olacaktır.
    - o İnternete çıkmayacak olan printer, scanner, vb donanımların firewall üzerinden dış dünyaya erişimleri kapatılmalıdır.
    - o Sunucuların sadece erişecekleri sitelere beyaz-liste(white list) olarak erişimleri tanımlanmalıdır.
    - o İçerik yönetim sunucuları konumlandırılmalıdır.
    - o Taşınabilir medyalar incelenmelidir.
    - o Mümkün olan cihazlar üzerinde şifreleme uygulanmalıdır. Bu sayede firmware malwareler sadece şifrelenmiş bilgilere erişebilecektir(malware'in kompleksliğine göre durum değişebilir)
    - o Ağ analiz araçları kullanılarak ağdaki anormal trafikler tespit edilebilir.
    - o Cihazlar üzerinde münkün oldukça şifreleme kullanılmalıdır.

- Hizmet alınan servis sağlayıcıya da güvenilmeyip mümkün olan tüm iletişimlerde şifreleme kullanılmalıdır.

6. SONUÇ

Derinlemesine güvenlik ilkesini benimseyip, uçtan uca güvenliği sağlayabilmek için öncelikle fiziksel güvenliği sağlamamız gerekmektedir. Fiziksel güvenlik süreci de donanımları tedarik ettikten sonra başlamaktadır. Donanımların üzerinde bulunan yazılımlar ise potansiyel tehdit oluşturmaktadır. Gömülü zararlı yazılımların tespit edilmesi zor olsa da alınacak önlemler ile potansiyel tehdidin riski azaltılabilmektedir. Böyle bir riskin farkında olup buna göre kurum politikalarını ve süreçlerini güncellemek ise kurumlar için son derece yararlı olacaktır. Aşağıda muhtemel bir süreç tanımlanmıştır:


Donanım Tedarik İsteği
Tedarik İsteği üzerinde donanım üzerindeki firmwarelerin, üreticinin son/uyumlu firmware'i ile reflash edilmesi gerektiği belirtilir.
Tedarikçi Reflash işlemini yapabiliyor mu?
H
Bu işlemi yapabilecek başka bir tedarikçi var mı?
E
H
E
Gereksinimi karşılayan tedarikçi seçilir
Tedarikçi donanım üzerindeki tüm firmware'i (PCI kartı gibi ek donanımlar dahil) gerekirse bir gözetmen eşliğinde reflash işlemi yapar
Reflash işleminde kullanılan yazılımın üreticiye ait olduğu ve dosya özeti kontrol edilir
Reflash işleminin yapılamama gerekleri araştırılır
Örnekleme metoduyla donanım seçilerek incelemeye tabi tutulur.
Tedarik Zincirinde yer alan paydaşlar incelenir, muhtemel zafiyetin olacağı kanallar incelenir
Donanım üzerindeki firmware çıkartılabiliyorsa çıkartılır üretici firma versiyonu ile kıyaslanır
Donanım üretim ortamına alınır
Gerekirse Davranışsal analiz yapılarak donanımın herhangi bir şekilde anomali gösterip göstermediği belirlenmeye çalışılır
TESPİT ETME
Muhtemel tehditlere karşı dış bağlantılar kısıtlanır
SSL trafiği şifresi çözülerek gözlemlenir, dışarıya herhangi bir şekide SSL tunneleme yapılması engellenir
Printer,vb internete çıkmayacak sistemler internetten bağları koparılır
Global Güvenlik Haber Alma Servisleri ile ağlar gözlemlenir, anormal hareketler tespit edilir
Sunucuların sadece erişecekleri web sistelerine erişimler verilir
Muhtemel WIFI erişim noktalarına karşı WIFI IPS konumlaması yapılır. Bilinmeyen erişim noktaları zehirlenerek erişilmez hale getirilir
Dial-Up,Bluetooth,firewire, usb, cdrom benzeri data transferinin yapılabileceği ekstra yerler kontrol altına alınır
Mümkün olan tüm heryerde ve her iletişimde şifreleme kullanılmalıdır

KAYNAKLAR

[1] http://en.wikipedia.org/wiki/Firmware

[2] https://media.blackhat.com/bh-us-12/Briefings/Brossard/BH_US_12_Brossard_Backdoor_Hacking_Slides.pdf

[3] http://www.theregister.co.uk/2010/07/21/dell_server_warning/

[4] http://www.computerworld.com/s/article/9231277/Microsoft_finds_new_computers_in_China_preinstalled_with_malware