Akira’s Play with Linux

labs.k7computing.com/index.php/akiras-play-with-linux/

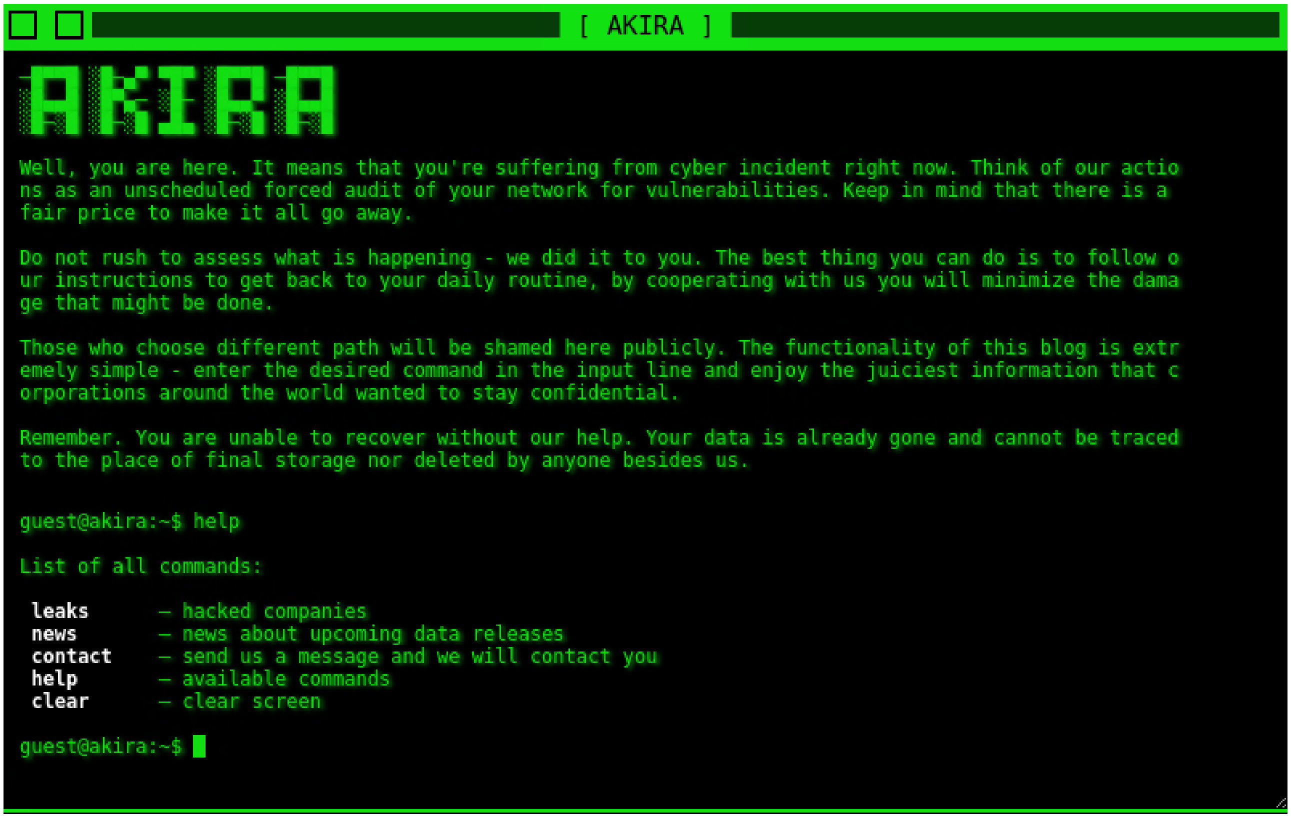
By Vigneshwaran P

July 25, 2023

The proliferation of Ransomware-as-a-Service (Raas) and the widespread availability of leaked source code from prominent ransomware strains have elevated ransomware attacks to a significant concern for individuals and organizations alike. As more threat actors adopt this modus operandi, it becomes imperative to acquire a comprehensive understanding of the Tactics, Techniques, and Procedures (TTPs) employed by these ransomware affiliates.

Recently we noticed that threat actors have been working on cross-platform malware for a wider attack surface. One such malware was a new ransomware variant named Akira that has emerged, making waves in the cybersecurity landscape from late March 2023. Notably, the ransomware group operates a Tor website imbued with a retro-themed aesthetic, where they publicly disclose pilfered data as a consequence of non-compliance with their ransom demands. Moreover, their website offers a chat feature, facilitating communication between victims and the perpetrators, utilizing the unique ID provided within the ransom note. Through this blog post, we will delve into the recent Akira ransomware Linux variant, unraveling its interconnectedness with the Windows variant of Akira ransomware and the Conti ransomware strain.

The Tor site of Akira ransomware is as shown below.

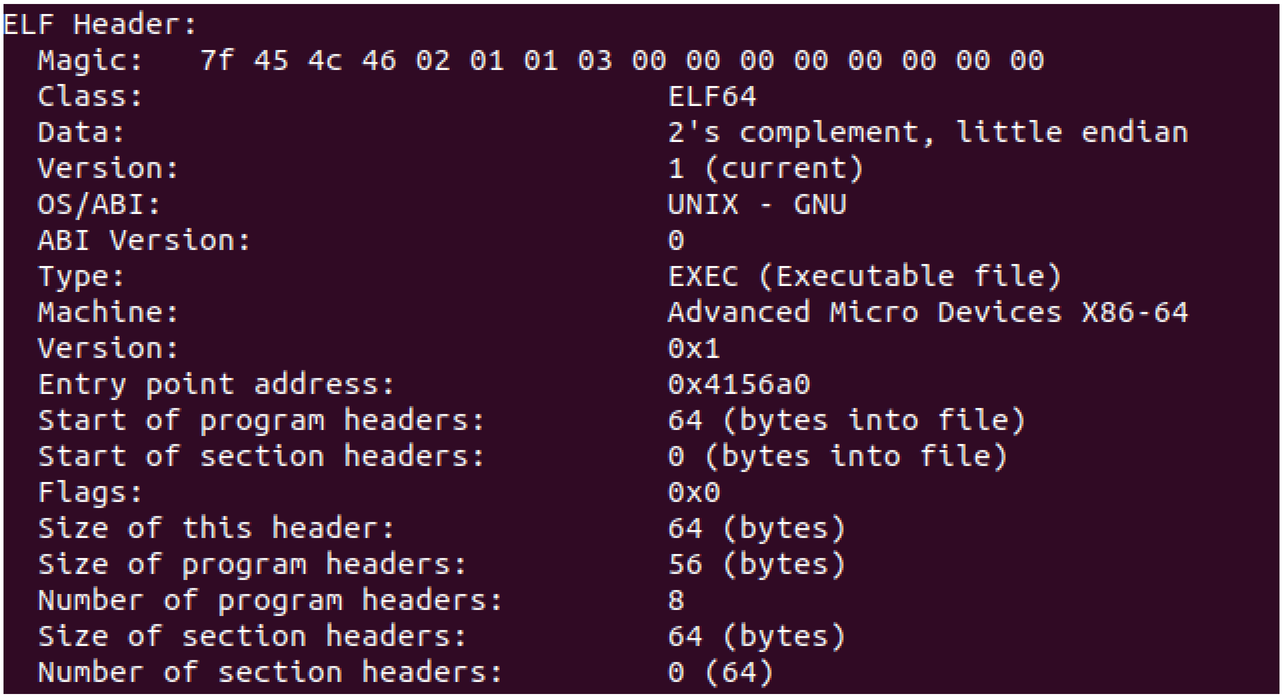


```
Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow o
ur instructions to get back to your daily routine, by cooperating with us you will minimize the dama
ge that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extr
emely simple - enter the desired command in the input line and enjoy the juiciest information that c
orporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced
to the place of final storage nor deleted by anyone besides us.


guest@akira:~$ help

List of all commands:

 leaks      – hacked companies
 news       – news about upcoming data releases
 contact    – send us a message and we will contact you
 help       – available commands
 clear      – clear screen

guest@akira:~$ 
```

Figure 1: Tor site of Akira ransomware

Binary analysis

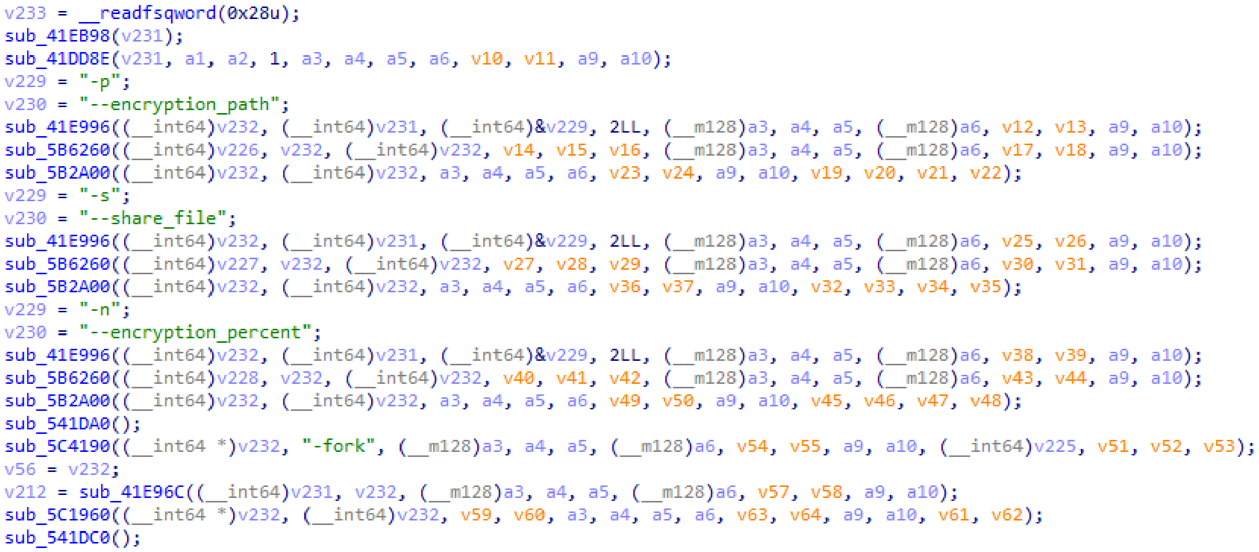
Let’s start with the header of the file. This file is 64 bit.



```
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 03 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - GNU
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x4156a0
  Start of program headers:          64 (bytes into file)
  Start of section headers:          0 (bytes into file)
  Flags:                             0x0
  Size of this header:               64 (bytes)
  Size of program headers:           56 (bytes)
  Number of program headers:         8
  Size of section headers:           64 (bytes)
  Number of section headers:         0 (64)
```

Figure 2: Binary Header

On analyzing the binary, we can see that this ransomware has the following command line arguments.

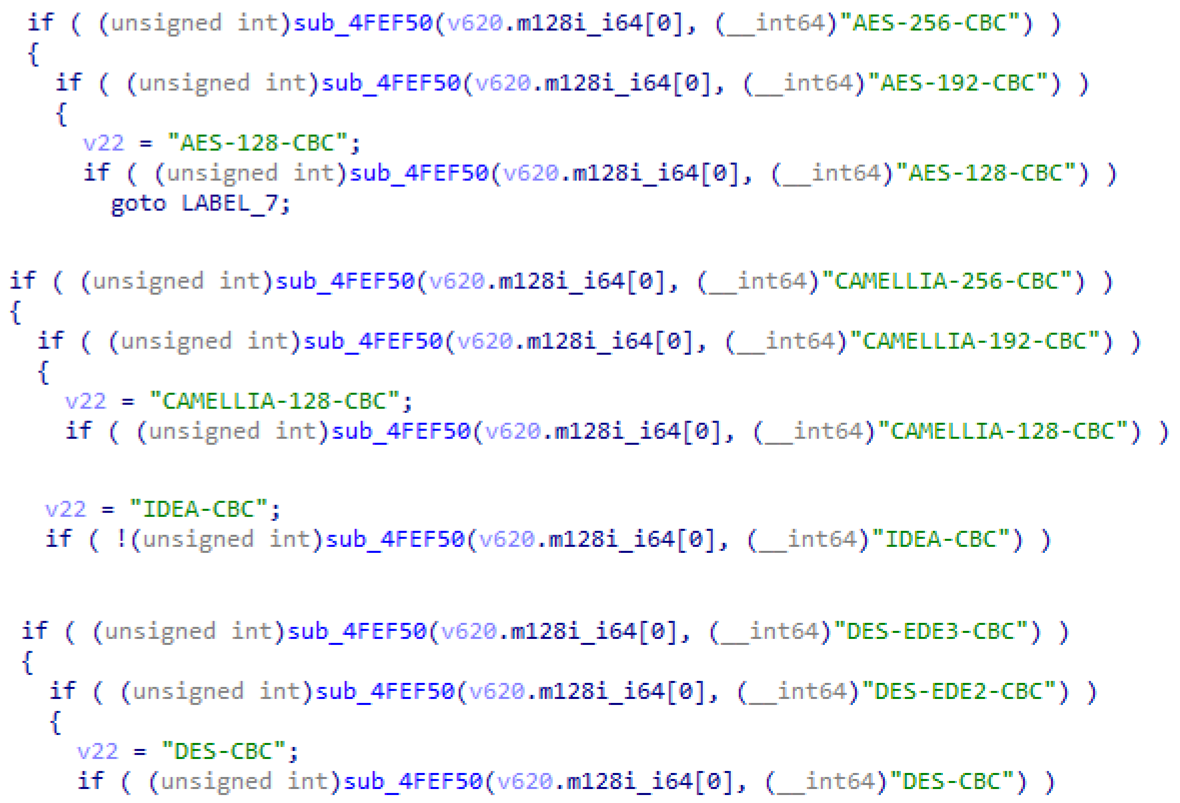


```
v233 = __readfsqword(0x28u);
sub_41EB98(v231);
sub_41DD8E(v231, a1, a2, 1, a3, a4, a5, a6, v10, v11, a9, a10);
v229 = "-p";
v230 = "--encryption_path";
sub_41E996((__int64)v232, (__int64)v231, (__int64)&v229, 2LL, (__m128)a3, a4, a5, (__m128)a6, v12, v13, a9, a10);
sub_5B6260((__int64)v226, v232, (__int64)v232, v14, v15, v16, (__m128)a3, a4, a5, (__m128)a6, v17, v18, a9, a10);
sub_5B2A00((__int64)v232, (__int64)v232, a3, a4, a5, a6, v23, v24, a9, a10, v19, v20, v21, v22);
v229 = "-s";
v230 = "--share_file";
sub_41E996((__int64)v232, (__int64)v231, (__int64)&v229, 2LL, (__m128)a3, a4, a5, (__m128)a6, v25, v26, a9, a10);
sub_5B6260((__int64)v227, v232, (__int64)v232, v27, v28, v29, (__m128)a3, a4, a5, (__m128)a6, v30, v31, a9, a10);
sub_5B2A00((__int64)v232, (__int64)v232, a3, a4, a5, a6, v36, v37, a9, a10, v32, v33, v34, v35);
v229 = "-n";
v230 = "--encryption_percent";
sub_41E996((__int64)v232, (__int64)v231, (__int64)&v229, 2LL, (__m128)a3, a4, a5, (__m128)a6, v38, v39, a9, a10);
sub_5B6260((__int64)v228, v232, (__int64)v232, v40, v41, v42, (__m128)a3, a4, a5, (__m128)a6, v43, v44, a9, a10);
sub_5B2A00((__int64)v232, (__int64)v232, a3, a4, a5, a6, v49, v50, a9, a10, v45, v46, v47, v48);
sub_541DA0();
sub_5C4190((__int64 *)v232, "-fork", (__m128)a3, a4, a5, (__m128)a6, v54, v55, a9, a10, (__int64)v225, v51, v52, v53);
v56 = v232;
v212 = sub_41E96C((__int64)v231, v232, (__m128)a3, a4, a5, (__m128)a6, v57, v58, a9, a10);
sub_5C1960((__int64 *)v232, (__int64)v232, v59, v60, a3, a4, a5, a6, v63, v64, a9, a10, v61, v62);
sub_541DC0();
```

Figure 3: Command line arguments

Arguments	Description
-p	Encryption Path used to only encrypt files in the given path
-s	Path to file containing list of shares to include in the encryption
-n	Encryption percentage on how much content of the files needs to be encrypted
-fork	To create new process or child process

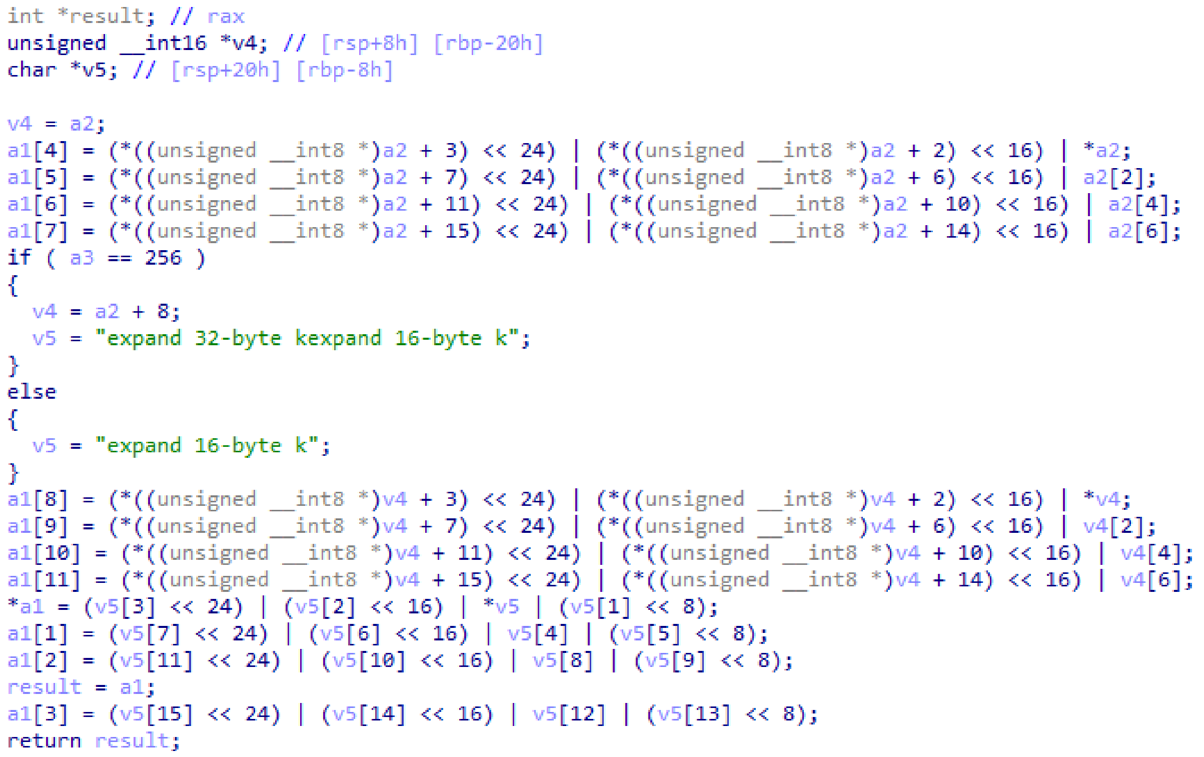
The ransomware integrates functionalities related to several symmetric key algorithms, such as AES, CAMELLIA, IDEA, and DES. Upon encountering a file possessing an extension from the aforementioned list, the ransomware proceeds with the encryption process of said file.



```
  if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"AES-256-CBC") )
  {
    if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"AES-192-CBC") )
    {
      v22 = "AES-128-CBC";
      if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"AES-128-CBC") )
        goto LABEL_7;

if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"CAMELLIA-256-CBC") )
{
  if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"CAMELLIA-192-CBC") )
  {
    v22 = "CAMELLIA-128-CBC";
    if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"CAMELLIA-128-CBC") )

   v22 = "IDEA-CBC";
   if ( !(unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"IDEA-CBC") )

 if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"DES-EDE3-CBC") )
 {
   if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"DES-EDE2-CBC") )
   {
     v22 = "DES-CBC";
     if ( (unsigned int)sub_4FEF50(v620.m128i_i64[0], (__int64)"DES-CBC") )
```

Figure 4: Algorithms referred in the binary

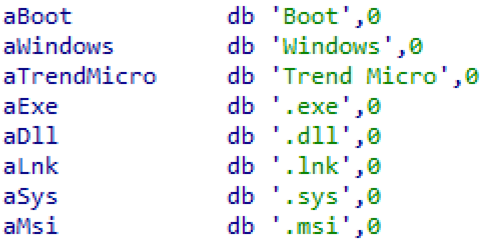
We found this ransomware is also using the CHACHA 20 encryption algorithm.



```
int *result; // rax
unsigned __int16 *v4; // [rsp+8h] [rbp-20h]
char *v5; // [rsp+20h] [rbp-8h]

v4 = a2;
a1[4] = (*((unsigned __int8 *)a2 + 3) << 24) | (*((unsigned __int8 *)a2 + 2) << 16) | *a2;
a1[5] = (*((unsigned __int8 *)a2 + 7) << 24) | (*((unsigned __int8 *)a2 + 6) << 16) | a2[2];
a1[6] = (*((unsigned __int8 *)a2 + 11) << 24) | (*((unsigned __int8 *)a2 + 10) << 16) | a2[4];
a1[7] = (*((unsigned __int8 *)a2 + 15) << 24) | (*((unsigned __int8 *)a2 + 14) << 16) | a2[6];
if ( a3 == 256 )
{
  v4 = a2 + 8;
  v5 = "expand 32-byte kexpand 16-byte k";
}
else
{
  v5 = "expand 16-byte k";
}
a1[8] = (*((unsigned __int8 *)v4 + 3) << 24) | (*((unsigned __int8 *)v4 + 2) << 16) | *v4;
a1[9] = (*((unsigned __int8 *)v4 + 7) << 24) | (*((unsigned __int8 *)v4 + 6) << 16) | v4[2];
a1[10] = (*((unsigned __int8 *)v4 + 11) << 24) | (*((unsigned __int8 *)v4 + 10) << 16) | v4[4];
a1[11] = (*((unsigned __int8 *)v4 + 15) << 24) | (*((unsigned __int8 *)v4 + 14) << 16) | v4[6];
*a1 = (v5[3] << 24) | (v5[2] << 16) | *v5 | (v5[1] << 8);
a1[1] = (v5[7] << 24) | (v5[6] << 16) | v5[4] | (v5[5] << 8);
a1[2] = (v5[11] << 24) | (v5[10] << 16) | v5[8] | (v5[9] << 8);
result = a1;
a1[3] = (v5[15] << 24) | (v5[14] << 16) | v5[12] | (v5[13] << 8);
return result;
```

Figure 5: CHACHA_20

If the directory and file shown in Figure 6 are present in the system, it excludes those from the encryption.

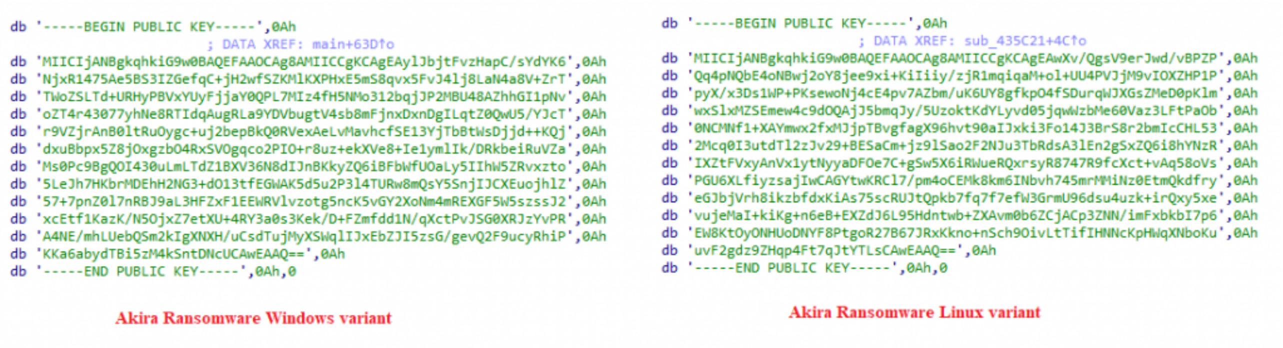


```
aBoot           db 'Boot',0
aWindows        db 'Windows',0
aTrendMicro     db 'Trend Micro',0
aExe            db '.exe',0
aDll            db '.dll',0
aLnk            db '.lnk',0
aSys            db '.sys',0
aMsi            db '.msi',0
```

Figure 6: Exclusion list

It then encrypts and adds the extension .akira for all the files.

During our analysis, we observed that the examined samples exhibited distinctive characteristics, specifically, a distinct Public RSA key and a Unique ID embedded in their Load section. These components were deliberately incorporated by the attacker to enable communication between the victim and the ransomware group.

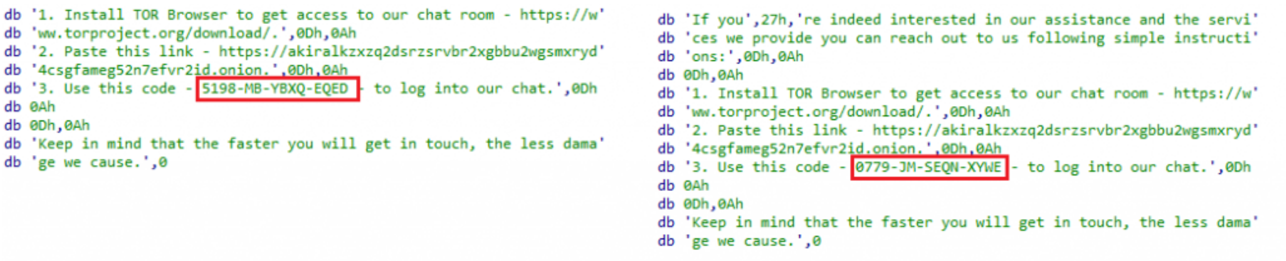


```
db '-----BEGIN PUBLIC KEY-----',0Ah
                        ; DATA XREF: main+63D↑o
db 'MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAylJbjtFvzHapC/sYdYK6',0Ah
db 'NjxR1475Ae5BS3IZGefqC+jH2wfSZKMlKXPHxE5mS8qvx5FvJ4lj8LaN4a8V+ZrT',0Ah
db 'TWoZSLTd+URHyPBVxYUyFjjaY0QPL7MIz4fH5NMo312bqjJP2MBU48AZhhGI1pNv',0Ah
db 'oZT4r43077yhNe8RTIdqAugRLa9YDVbugtV4sb8mFjnxDxnDgILqtZ0QwU5/YJcT',0Ah
db 'r9VZjrAnB0ltRuOygc+uj2bepBkQ0RVexAeLvMavhcfSE13YjTbBtWsDjjd++KQj',0Ah
db 'dxuBbpx5Z8jOxgzbO4RxSVOgqco2PIO+r8uz+ekXVe8+Ie1ymlIk/DRkbeiRuVZa',0Ah
db 'Ms0Pc9BgQOI430uLmLTdZ1BXV36N8dIJnBKkyZQ6iBFbWfUOaLy5IIhW5ZRvxzto',0Ah
db '5LeJh7HKbrMDEhH2NG3+dO13tfEGWAK5d5u2P3l4TURw8mQsY5SnjIJCXEuojhlZ',0Ah
db '57+7pnZ0l7nRBJ9aL3HFZxF1EEWRVlvzotg5ncK5vGY2XoNm4mREXGF5W5szssJ2',0Ah
db 'xcEtf1KazK/N5OjxZ7etXU+4RY3a0s3Kek/D+FZmfdd1N/qXctPvJSG0XRJzYvPR',0Ah
db 'A4NE/mhLUebQSm2kIgXNXH/uCsdTujMyXSWqlIJxEbZJI5zsG/gevQ2F9ucyRhiP',0Ah
db 'KKa6abydTBi5zM4kSntDNcUCAwEAAQ==',0Ah
db '-----END PUBLIC KEY-----',0Ah,0
```

```
db '-----BEGIN PUBLIC KEY-----',0Ah
                        ; DATA XREF: sub_435C21+4C↑o
db 'MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwXv/QgsV9erJwd/vBPZP',0Ah
db 'Qq4pNQbE4oNBwj2oY8jee9xi+KiIiiy/zjR1mqiqaM+ol+UU4PVJjM9vIOXZHP1P',0Ah
db 'pyX/x3Ds1WP+PKsewoNj4cE4pv7AZbm/uK6UY8gfkpO4fSDurqWJXGsZMeD0pKlm',0Ah
db 'wxSlxMZSEmew4c9dOQAjJ5bmqJy/5UzoktKdYLyvd05jqwWzbMe60Vaz3LFtPaOb',0Ah
db '0NCMNf1+XAYmwx2fxMJjpTBvgfagX96hvt90aIJxki3Fo14J3BrS8r2bmIcCHL53',0Ah
db '2Mcq0I3utdTl2zJv29+BESaCm+jz9lSao2F2NJu3TbRdsA3lEn2gSxZQ6i8hYNzR',0Ah
db 'IXZtFVxyAnVx1ytNyyaDFOe7C+gSw5X6iRWueRQxrsyR8747R9fcXct+vAq58oVs',0Ah
db 'PGU6XLfiyzsajIwCAGYtwKRCl7/pm4oCEMk8km6INbvh745mrMMiNz0EtmQkdfry',0Ah
db 'eGJbjVrh8ikzbfdxKiAs75scRUJtQpkb7fq7f7efW3GrmU96dsu4uzk+irQxy5xe',0Ah
db 'vujeMaI+kiKg+n6eB+EXZdJ6L95Hdntwb+ZXAvm0b6ZCjACp3ZNN/imFxbkbI7p6',0Ah
db 'EW8KtOyONHUoDNYF8PtgoR27B67JRxKkno+nSch9OivLtTifIHNNcKpHWqXNboKu',0Ah
db 'uvF2gdz9ZHqp4Ft7qJtYTLsCAwEAAQ==',0Ah
db '-----END PUBLIC KEY-----',0Ah,0
```

Figure 7: Comparison of public key

It appears that the ransomware operator dynamically constructs the ransomware with a fresh public RSA key for each target, along with a corresponding Unique ID appended in the ransomware note. The purpose of this Unique ID is to facilitate the attacker in determining the specific ransomware build that infected the victim, thereby identifying the corresponding private key required for decrypting the compromised files.

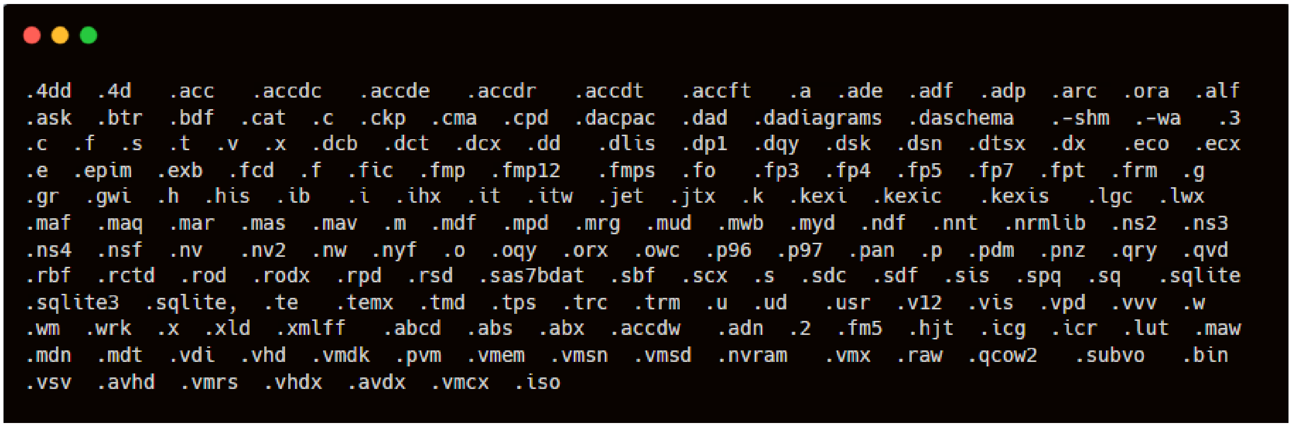


```
db '1. Install TOR Browser to get access to our chat room - https://w'
db 'ww.torproject.org/download/.',0Dh,0Ah
db '2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd'
db '4csgfameg52n7efvr2id.onion.',0Dh,0Ah
db '3. Use this code - 5198-MB-YBXQ-EQED - to log into our chat.',0Dh
db 0Ah
db 0Dh,0Ah
db 'Keep in mind that the faster you will get in touch, the less dama'
db 'ge we cause.',0
```

```
db 'If you',27h,'re indeed interested in our assistance and the servi'
db 'ces we provide you can reach out to us following simple instructi'
db 'ons:',0Dh,0Ah
db 0Dh,0Ah
db '1. Install TOR Browser to get access to our chat room - https://w'
db 'ww.torproject.org/download/.',0Dh,0Ah
db '2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd'
db '4csgfameg52n7efvr2id.onion.',0Dh,0Ah
db '3. Use this code - 0779-JM-SEQN-XYWE - to log into our chat.',0Dh
db 0Ah
db 0Dh,0Ah
db 'Keep in mind that the faster you will get in touch, the less dama'
db 'ge we cause.',0
```

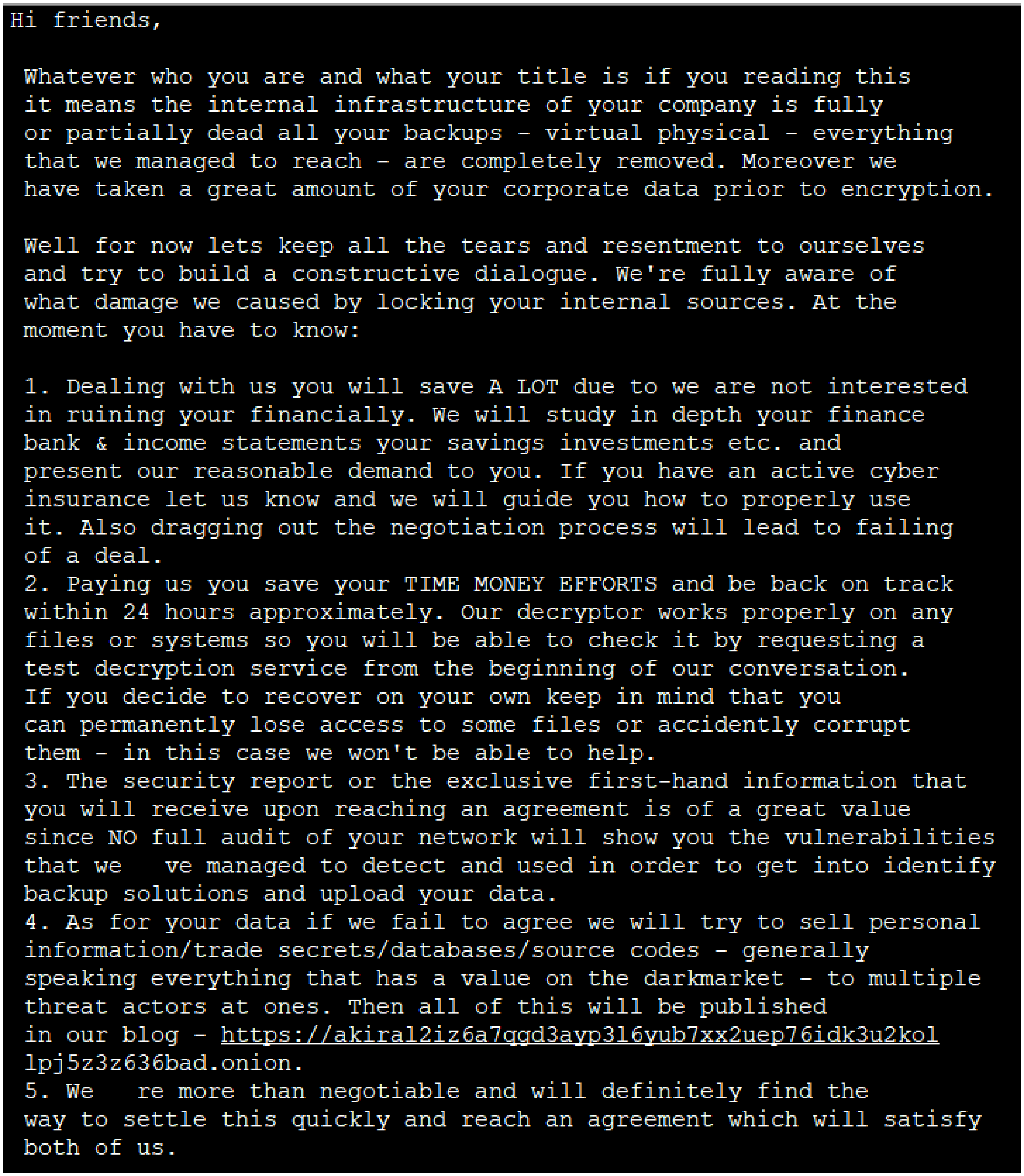
Figure 8: Unique ID for communication

Figure 9 lists around 190 file extensions that this binary encrypts.



```
.4dd  .4d   .acc   .accdc   .accde   .accdr   .accdt   .accft   .a  .ade  .adf  .adp  .arc  .ora  .alf
.ask  .btr  .bdf  .cat  .c  .ckp  .cma  .cpd  .dacpac  .dad  .dadiagrams  .daschema   .-shm  .-wa   .3
.c  .f  .s  .t  .v  .x  .dcb  .dct  .dcx  .dd   .dlis  .dp1  .dqy  .dsk  .dsn  .dtsx  .dx   .eco  .ecx
.e  .epim  .exb  .fcd  .f  .fic  .fmp  .fmp12   .fmps  .fo   .fp3  .fp4  .fp5  .fp7  .fpt  .frm  .g
.gr  .gwi  .h  .his  .ib   .i  .ihx  .it  .itw  .jet  .jtx  .k  .kexi  .kexic   .kexis   .lgc  .lwx
.maf  .maq  .mar  .mas  .mav  .m  .mdf  .mpd  .mrg  .mud  .mwb  .myd  .ndf  .nnt  .nrmlib  .ns2  .ns3
.ns4  .nsf  .nv   .nv2  .nw  .nyf  .o  .oqy  .orx  .owc  .p96  .p97  .pan  .p  .pdm  .pnz  .qry  .qvd
.rbf  .rctd  .rod  .rodx  .rpd  .rsd  .sas7bdat  .sbf  .scx  .s  .sdc  .sdf  .sis  .spq  .sq   .sqlite
.sqlite3  .sqlite,  .te   .temx  .tmd  .tps  .trc  .trm  .u  .ud   .usr  .v12  .vis  .vpd  .vvv  .w
.wm  .wrk  .x  .xld  .xmlff   .abcd  .abs  .abx  .accdw   .adn  .2  .fm5  .hjt  .icg  .icr  .lut  .maw
.mdn  .mdt  .vdi  .vhd  .vmdk  .pvm  .vmem  .vmsn  .vmsd  .nvram   .vmx  .raw  .qcow2   .subvo   .bin
.vsv  .avhd  .vmrs  .vhdx  .avdx  .vmcx  .iso
```

Figure 9: Files extension to be encrypted



```
Hi friends,

 Whatever who you are and what your title is if you reading this
 it means the internal infrastructure of your company is fully
 or partially dead all your backups - virtual physical - everything
 that we managed to reach - are completely removed. Moreover we
 have taken a great amount of your corporate data prior to encryption.

 Well for now lets keep all the tears and resentment to ourselves
 and try to build a constructive dialogue. We're fully aware of
 what damage we caused by locking your internal sources. At the
 moment you have to know:

 1. Dealing with us you will save A LOT due to we are not interested
 in ruining your financially. We will study in depth your finance
 bank & income statements your savings investments etc. and
 present our reasonable demand to you. If you have an active cyber
 insurance let us know and we will guide you how to properly use
 it. Also dragging out the negotiation process will lead to failing
 of a deal.
 2. Paying us you save your TIME MONEY EFFORTS and be back on track
 within 24 hours approximately. Our decryptor works properly on any
 files or systems so you will be able to check it by requesting a
 test decryption service from the beginning of our conversation.
 If you decide to recover on your own keep in mind that you
 can permanently lose access to some files or accidently corrupt
 them - in this case we won't be able to help.
 3. The security report or the exclusive first-hand information that
 you will receive upon reaching an agreement is of a great value
 since NO full audit of your network will show you the vulnerabilities
 that we   ve managed to detect and used in order to get into identify
 backup solutions and upload your data.
 4. As for your data if we fail to agree we will try to sell personal
 information/trade secrets/databases/source codes - generally
 speaking everything that has a value on the darkmarket - to multiple
 threat actors at ones. Then all of this will be published
 in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kol
 lpj5z3z636bad.onion.
 5. We   re more than negotiable and will definitely find the
 way to settle this quickly and reach an agreement which will satisfy
 both of us.
```

Figure 10: Ransom note

We at K7 Labs provide detection for Akira ransomware and all the latest threats. Users are advised to use a reliable security product such as “K7 Total Security” and keep it up-to-date to safeguard their devices.

Indicators of Compromise (IOCs)

Hash	Detection Name

177ACD248FC715A8B5E443BE38D3B204	Trojan (035562be1)
302f76897e4e5c8c98a52a38c4c98443	Trojan (035562be1)