Malware Wars: DarkSide Strikes Back as ~~BlackMatter~~ ALPHV

Recorded Future®

Introduction

Lindsay Kaye

Senior Director, Operational Outcomes, Insikt Group
Recorded Future

James Niven

Principal Threat Researcher
Recorded Future

Same, same, but different

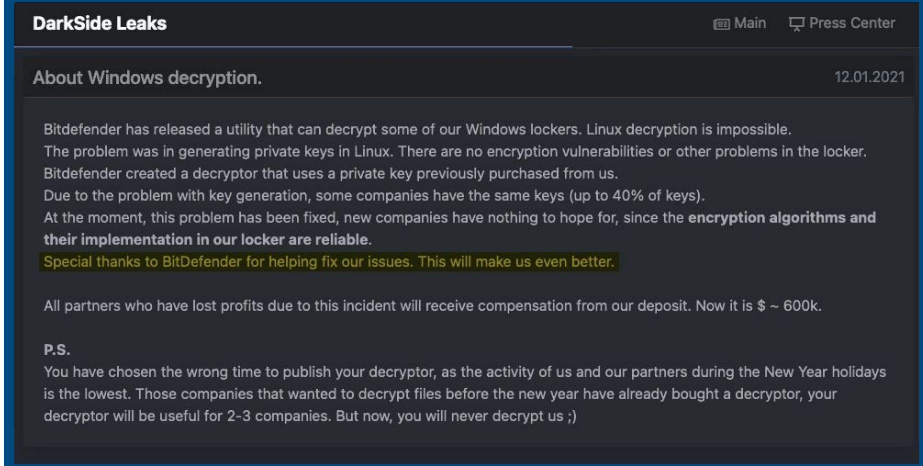
We're going to discuss how ransomware groups rebrand and transition in response to external factors, such as law enforcement pressure, technical flaws, and internal fallout.

Along the way, they'll iterate on their tools, carrying over technical (and tradecraft!) artifacts from version to version, and sometimes from old group to new group.

We'll talk about DarkSide's evolution to BlackMatter and later ALPHV

Discovery of BlackMatter

- DarkSide attacked Colonial Pipeline on May 6, 2021
- DarkSide decryption issues
- REvil Shutdown on July 12, 2021
- JBS Foods played a pivotal role in REvil disappearing
- Linux/ESXi locker needed after REvil/DarkSide gone



About Windows decryption. 12.01.2021

Bitdefender has released a utility that can decrypt some of our Windows lockers. Linux decryption is impossible.
The problem was in generating private keys in Linux. There are no encryption vulnerabilities or other problems in the locker.
Bitdefender created a decryptor that uses a private key previously purchased from us.
Due to the problem with key generation, some companies have the same keys (up to 40% of keys).
At the moment, this problem has been fixed, new companies have nothing to hope for, since the **encryption algorithms and their implementation in our locker are reliable.**
Special thanks to BitDefender for helping fix our issues. This will make us even better.

All partners who have lost profits due to this incident will receive compensation from our deposit. Now it is $ ~ 600k.

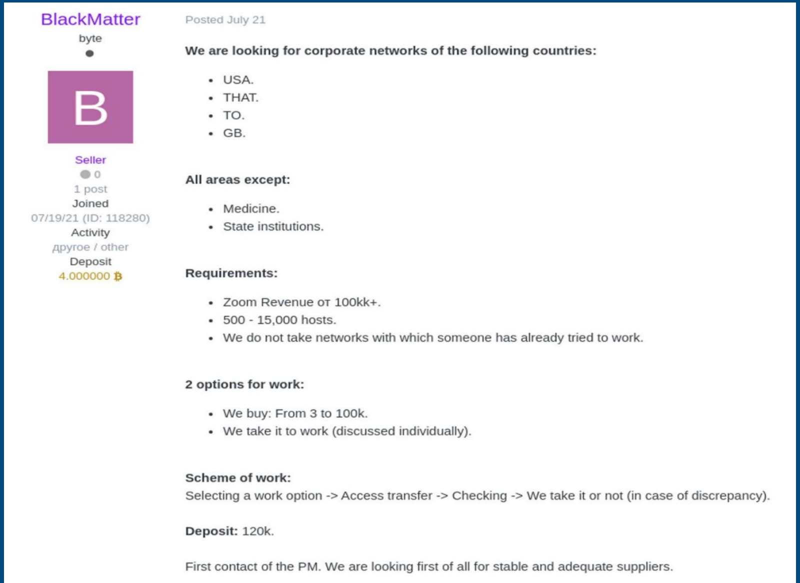
P.S.
You have chosen the wrong time to publish your decryptor, as the activity of us and our partners during the New Year holidays is the lowest. Those companies that wanted to decrypt files before the new year have already bought a decryptor, your decryptor will be useful for 2-3 companies. But now, you will never decrypt us ;)

DarkSide Announcement on Decryption Issues
(Source: Propublica)

Advertisement

BlackMatter looking for targets

- Exploit and XSS - Initial communications
- Communications move to Jabber, Tox, and Telegram
- Reputation is important
- Ransomware removed by admins after Colonial Pipeline attack



BlackMatter
byte
●

B

Seller
● 0
1 post
Joined
07/19/21 (ID: 118280)
Activity
другое / other
Deposit
4.000000 ₿

Posted July 21

We are looking for corporate networks of the following countries:

- USA.
- THAT.
- TO.
- GB.

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue от 100kk+.
- 500 - 15,000 hosts.
- We do not take networks with which someone has already tried to work.

2 options for work:

- We buy: From 3 to 100k.
- We take it to work (discussed individually).

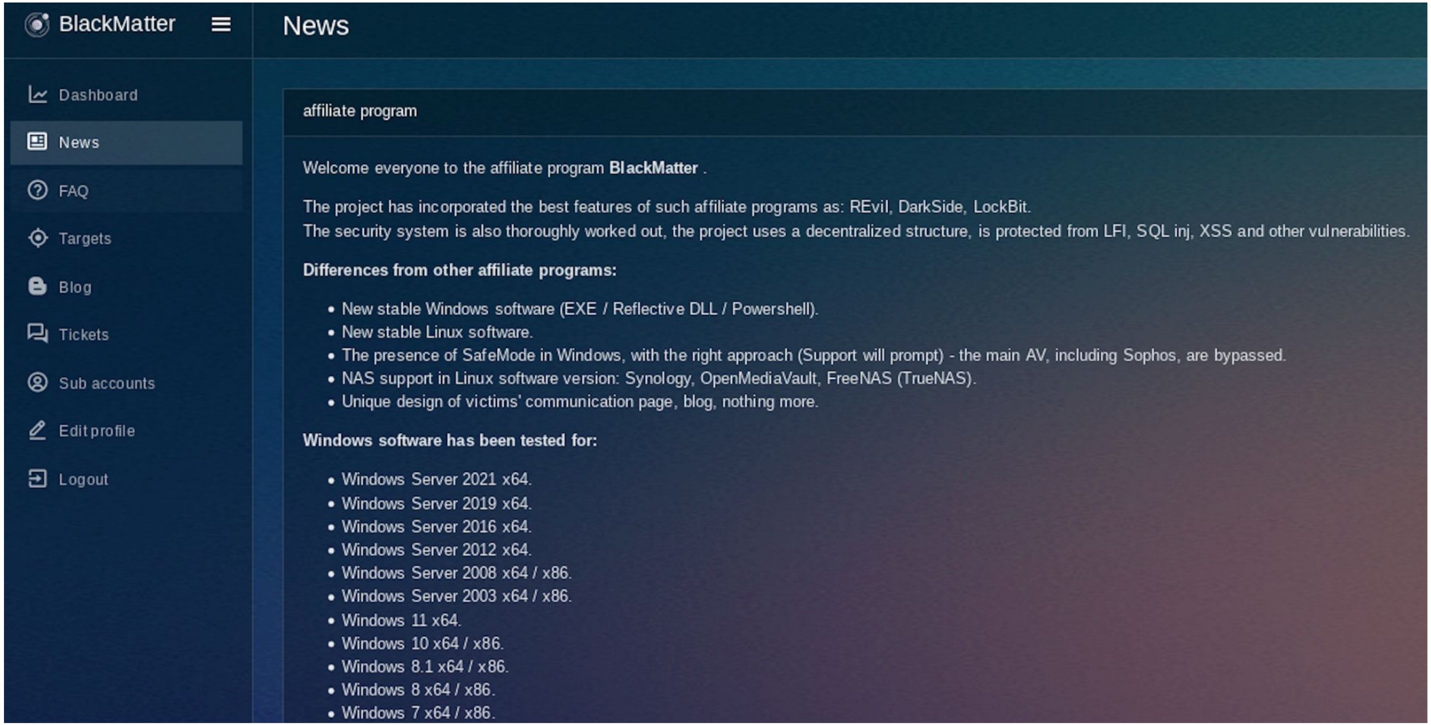
Scheme of work:
Selecting a work option -> Access transfer -> Checking -> We take it or not (in case of discrepancy).

Deposit: 120k.

First contact of the PM. We are looking first of all for stable and adequate suppliers.

Exploit Advertisement of BlackMatter

The Panel



affiliate program

Welcome everyone to the affiliate program **BlackMatter** .

The project has incorporated the best features of such affiliate programs as: REvil, DarkSide, LockBit.
The security system is also thoroughly worked out, the project uses a decentralized structure, is protected from LFI, SQL inj, XSS and other vulnerabilities.

Differences from other affiliate programs:

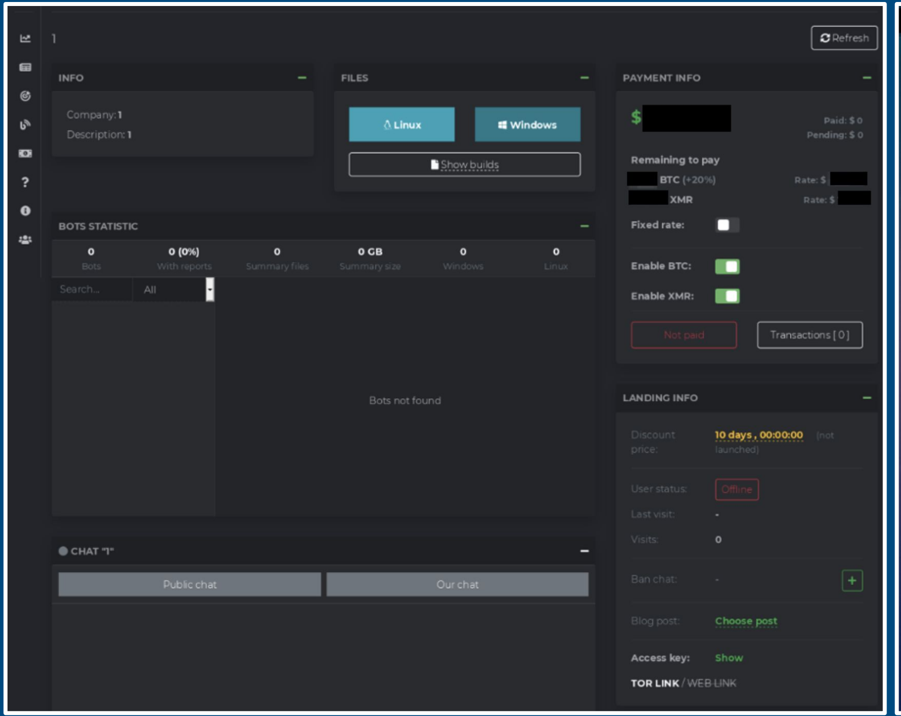
- New stable Windows software (EXE / Reflective DLL / Powershell).
- New stable Linux software.
- The presence of SafeMode in Windows, with the right approach (Support will prompt) - the main AV, including Sophos, are bypassed.
- NAS support in Linux software version: Synology, OpenMediaVault, FreeNAS (TrueNAS).
- Unique design of victims' communication page, blog, nothing more.

Windows software has been tested for:

- Windows Server 2021 x64.
- Windows Server 2019 x64.
- Windows Server 2016 x64.
- Windows Server 2012 x64.
- Windows Server 2008 x64 / x86.
- Windows Server 2003 x64 / x86.
- Windows 11 x64.
- Windows 10 x64 / x86.
- Windows 8.1 x64 / x86.
- Windows 8 x64 / x86.
- Windows 7 x64 / x86.

BlackMatter Affiliate News Panel

DarkSide vs BlackMatter



1

Refresh

INFO

Company: 1
Description: 1

FILES

Linux | Windows

Show builds

PAYMENT INFO

$ [redacted]

Paid: $ 0
Pending: $ 0

Remaining to pay

[redacted] BTC (+20%) Rate: $ [redacted]
[redacted] XMR Rate: $ [redacted]

Fixed rate: ☐
Enable BTC: ☑
Enable XMR: ☑

Not paid | Transactions [0]

BOTS STATISTIC

0	0 (0%)	0	0 GB	0	0
Bots	With reports	Summary files	Summary size	Windows	Linux

Search... All

Bots not found

LANDING INFO

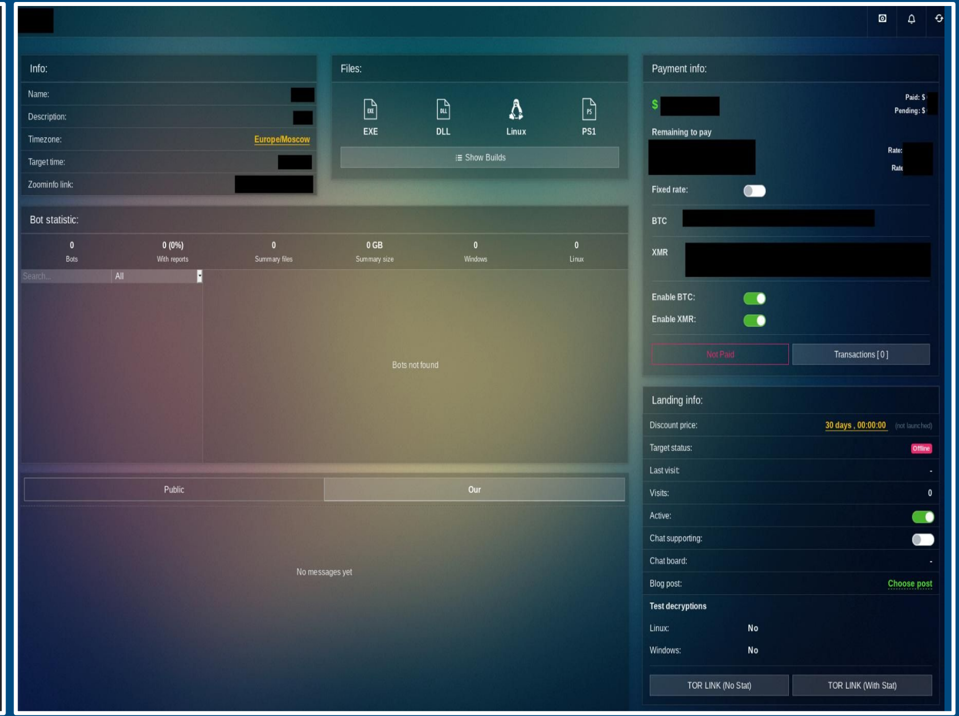
Discount price: 10 days , 00:00:00 (not launched)
User status: Offline
Last visit: -
Visits: 0
Ban chat: -
Blog post: Choose post
Access key: Show
TOR LINK / WEB LINK

CHAT "1"

Public chat | Our chat

DarkSide Panel

(Source: Mandiant)



[redacted]

Info:

Name: [redacted]
Description: [redacted]
Timezone: Europe/Moscow
Target time: [redacted]
Zoominfo link: [redacted]

Files:

EXE | DLL | Linux | PS1

Show Builds

Bot statistic:

0	0 (0%)	0	0 GB	0	0
Bots	With reports	Summary files	Summary size	Windows	Linux

Search... All

Bots not found

Public | Our

No messages yet

Payment info:

$ [redacted]

Paid: $ [redacted]
Pending: $ [redacted]

Remaining to pay

[redacted]

Rate: [redacted]
Rate [redacted]

Fixed rate: ☐
BTC [redacted]
XMR [redacted]
Enable BTC: ☑
Enable XMR: ☑

Not Paid | Transactions [0]

Landing info:

Discount price: 30 days , 00:00:00 (not launched)
Target status: Offline
Last visit: -
Visits: 0
Active: ☑
Chat supporting: ☐
Chat board: -
Blog post: Choose post

Test decryptions
Linux: No
Windows: No

TOR LINK (No Stat) | TOR LINK (With Stat)

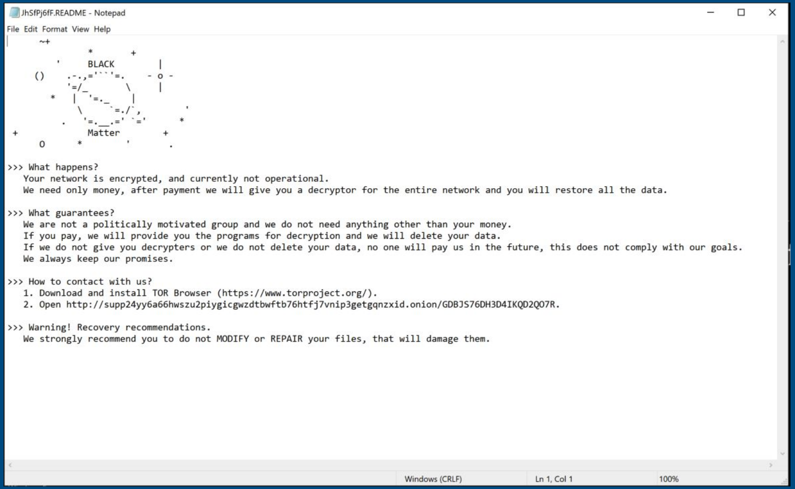
BlackMatter Panel

(Source: Recorded Future)

Recorded Future®

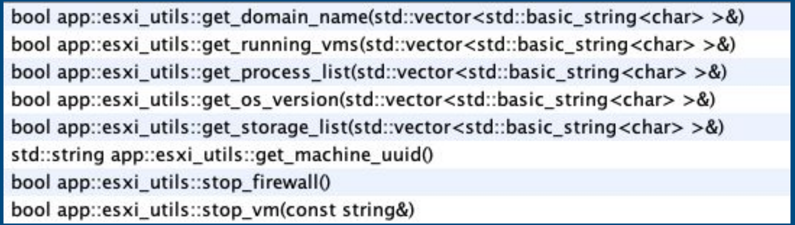
The Malware

- Two variants released initially: Windows, Linux/ESXi
- Windows ransomware implemented extensive anti-RE/anti-analysis capabilities
- Linux/ESXi was more straightforward - included function names, deobfuscated config



```
      ~+
               *       +
         '     BLACK        |
     ()    .-.,='``'=.    - o -
           '=/_       \     |
        *   |  '=._    |
             \     `=./`,        '
          .   '=.__.=' `='      *
 +             Matter        +
      O      *        '       .

>>> What happens?
   Your network is encrypted, and currently not operational.
   We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.

>>> What guarantees?
   We are not a politically motivated group and we do not need anything other than your money.
   If you pay, we will provide you the programs for decryption and we will delete your data.
   If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals.
   We always keep our promises.

>>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open http://supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnzxid.onion/GDBJS76DH3D4IKQD2QO7R.

>>> Warning! Recovery recommendations.
   We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them.
```

Windows Ransom Note



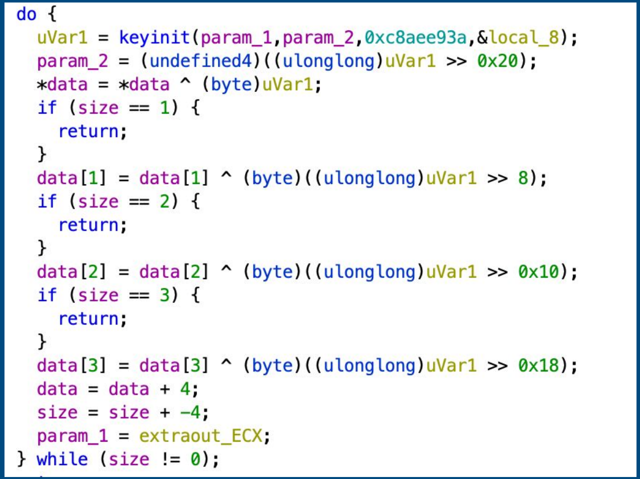
```
bool app::esxi_utils::get_domain_name(std::vector<std::basic_string<char> >&)
bool app::esxi_utils::get_running_vms(std::vector<std::basic_string<char> >&)
bool app::esxi_utils::get_process_list(std::vector<std::basic_string<char> >&)
bool app::esxi_utils::get_os_version(std::vector<std::basic_string<char> >&)
bool app::esxi_utils::get_storage_list(std::vector<std::basic_string<char> >&)
std::string app::esxi_utils::get_machine_uuid()
bool app::esxi_utils::stop_firewall()
bool app::esxi_utils::stop_vm(const string&)
```

Linux/ESXi Function Names

Windows Ransomware

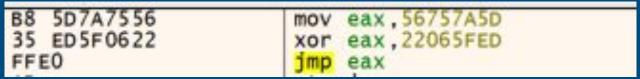
BlackMatter implemented some techniques that made their malware signaturable

- Cryptographic routines (more on this later)
- String obfuscation
- Function call obfuscation
- Magic numbers (0X22065FED, here)



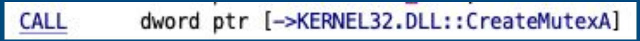
```
do {
  uVar1 = keyinit(param_1,param_2,0xc8aee93a,&local_8);
  param_2 = (undefined4)((ulonglong)uVar1 >> 0x20);
  *data = *data ^ (byte)uVar1;
  if (size == 1) {
    return;
  }
  data[1] = data[1] ^ (byte)((ulonglong)uVar1 >> 8);
  if (size == 2) {
    return;
  }
  data[2] = data[2] ^ (byte)((ulonglong)uVar1 >> 0x10);
  if (size == 3) {
    return;
  }
  data[3] = data[3] ^ (byte)((ulonglong)uVar1 >> 0x18);
  data = data + 4;
  size = size + -4;
  param_1 = extraout_ECX;
} while (size != 0);
```

BlackMatter string decryption routine



```
B8 5D7A7556     mov eax,56757A5D
35 ED5F0622     xor eax,22065FED
FFE0            jmp eax
```

BlackMatter call obfuscation

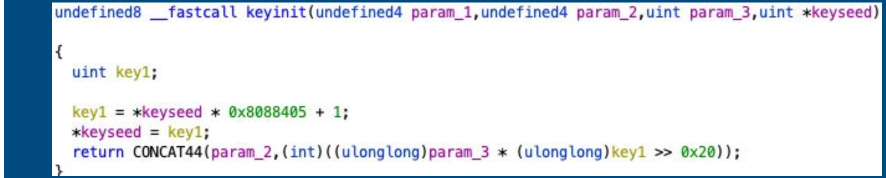


```
CALL       dword ptr [->KERNEL32.DLL::CreateMutexA]
```

“Normal” call

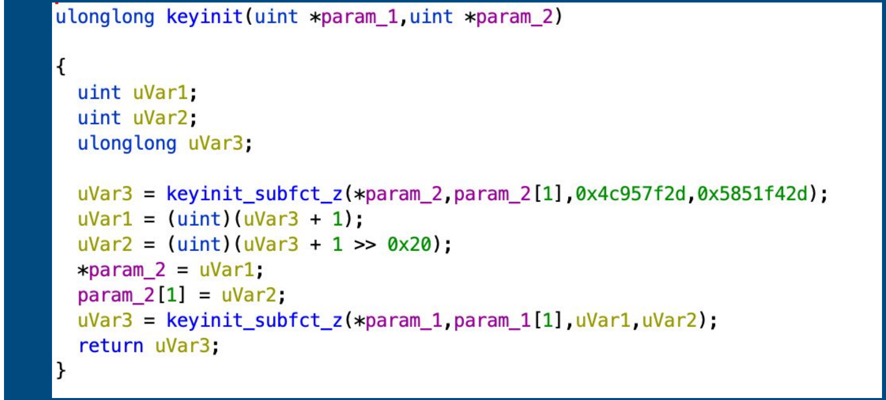
The Malware Evolves!

- After we released our report, new versions of the Windows ransomware began appearing
  - Simple changes, such as magic XOR key
  - More complex, like some new features
- We never saw another Linux/ESXi one
- Ultimately, BlackMatter released 6 versions (1.2-3.0) of their malware between July 2021 and September 2021



```
undefined8 __fastcall keyinit(undefined4 param_1,undefined4 param_2,uint param_3,uint *keyseed)

{
  uint key1;

  key1 = *keyseed * 0x8088405 + 1;
  *keyseed = key1;
  return CONCAT44(param_2,(int)((ulonglong)param_3 * (ulonglong)key1 >> 0x20));
}
```

String encryption key initialization v1.2



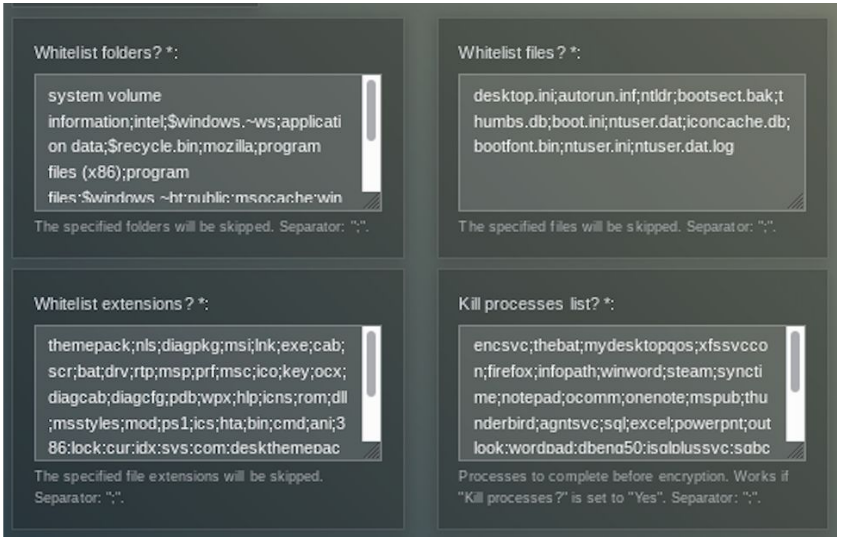
```
ulonglong keyinit(uint *param_1,uint *param_2)

{
  uint uVar1;
  uint uVar2;
  ulonglong uVar3;

  uVar3 = keyinit_subfct_z(*param_2,param_2[1],0x4c957f2d,0x5851f42d);
  uVar1 = (uint)(uVar3 + 1);
  uVar2 = (uint)(uVar3 + 1 >> 0x20);
  *param_2 = uVar1;
  param_2[1] = uVar2;
  uVar3 = keyinit_subfct_z(*param_1,param_1[1],uVar1,uVar2);
  return uVar3;
}
```

String encryption key initialization v2.0

The Malware Evolves!

Feature Additions

- Print the ransom note on local printers
- Encrypt additional file types
  (eg: Microsoft Exchange files)
- Computers not to encrypt
- Implementation of cryptographic algorithm
- Checking for “large” files and encrypting them differently



Whitelist folders? *:

system volume
information;intel;$windows.~ws;applicati
on data;$recycle.bin;mozilla;program
files (x86);program
files;$windows.~bt;public;msocache;win

The specified folders will be skipped. Separator: ";".

Whitelist files ? *:

desktop.ini;autorun.inf;ntldr;bootsect.bak;t
humbs.db;boot.ini;ntuser.dat;iconcache.db;
bootfont.bin;ntuser.ini;ntuser.dat.log

The specified files will be skipped. Separator: ";".

Whitelist extensions ? *:

themepack;nls;diagpkg;msi;lnk;exe;cab;
scr;bat;drv;rtp;msp;prf;msc;ico;key;ocx;
diagcab;diagcfg;pdb;wpx;hlp;icns;rom;dll
;msstyles;mod;ps1;ics;hta;bin;cmd;ani;3
86;lock;cur;idx;sys;com;deskthemepac

The specified file extensions will be skipped. Separator: ";".

Kill processes list? *:

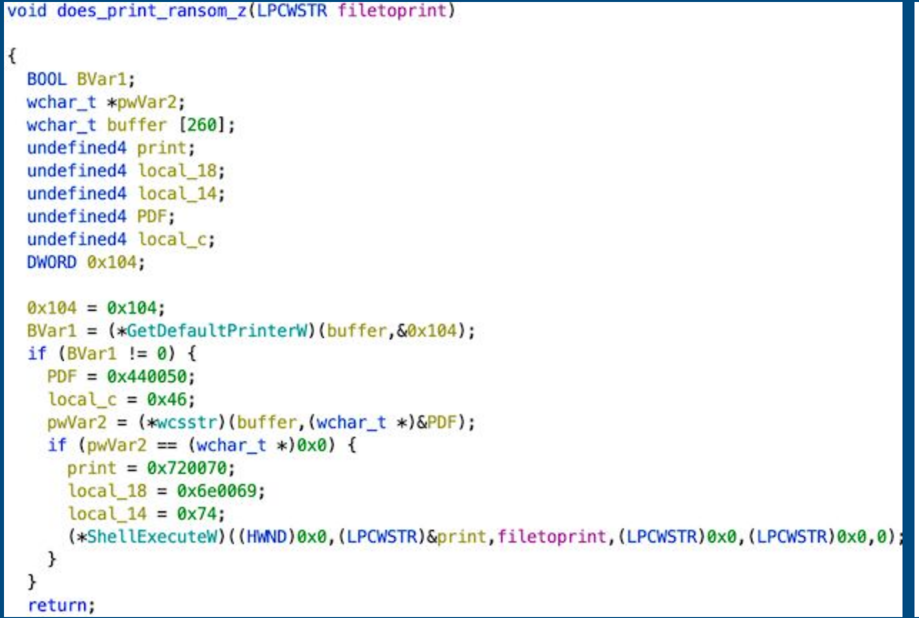
encsvc;thebat;mydesktopqos;xfssvcco
n;firefox;infopath;winword;steam;syncti
me;notepad;ocomm;onenote;mspub;thu
nderbird;agntsvc;sql;excel;powerpnt;out
look;wordpad;dbeng50;isqlplussvc;sqbc

Processes to complete before encryption. Works if "Kill processes ?" is set to "Yes". Separator: ";".

BlackMatter Affiliate Panel

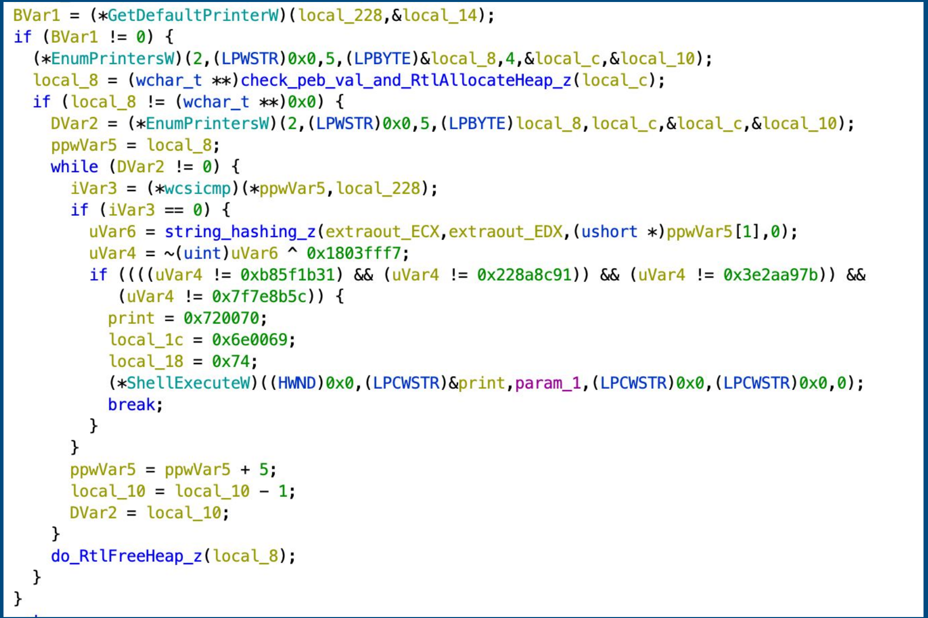
The Malware Evolves!

Between version 1.6 and 2.0, added additional “virtual printers” to ignore in printing ransom note



```
void does_print_ransom_z(LPCWSTR filetoprint)

{
  BOOL BVar1;
  wchar_t *pwVar2;
  wchar_t buffer [260];
  undefined4 print;
  undefined4 local_18;
  undefined4 local_14;
  undefined4 PDF;
  undefined4 local_c;
  DWORD 0x104;

  0x104 = 0x104;
  BVar1 = (*GetDefaultPrinterW)(buffer,&0x104);
  if (BVar1 != 0) {
    PDF = 0x440050;
    local_c = 0x46;
    pwVar2 = (*wcsstr)(buffer,(wchar_t *)&PDF);
    if (pwVar2 == (wchar_t *)0x0) {
      print = 0x720070;
      local_18 = 0x6e0069;
      local_14 = 0x74;
      (*ShellExecuteW)((HWND)0x0,(LPCWSTR)&print,filetoprint,(LPCWSTR)0x0,(LPCWSTR)0x0,0);
    }
  }
  return;
```

Print function v1.6-1.9 - Do not print to printer containing “PDF”

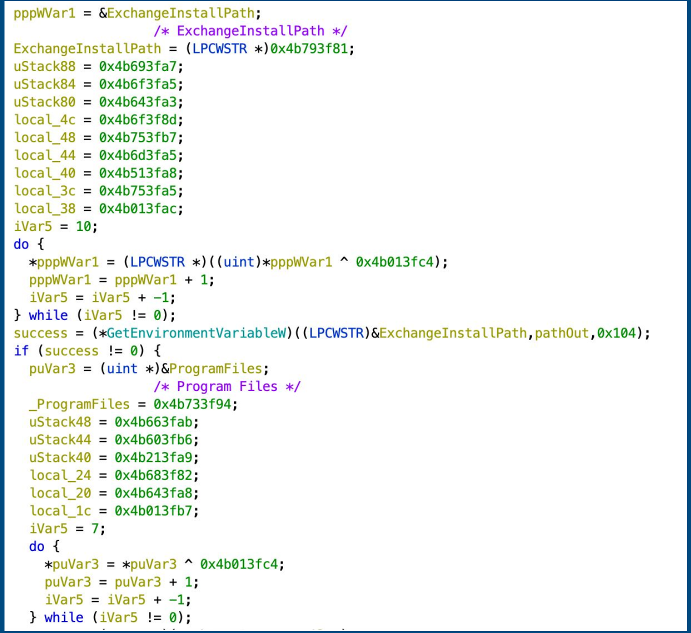


```
BVar1 = (*GetDefaultPrinterW)(local_228,&local_14);
if (BVar1 != 0) {
  (*EnumPrintersW)(2,(LPWSTR)0x0,5,(LPBYTE)&local_8,4,&local_c,&local_10);
  local_8 = (wchar_t **)check_peb_val_and_RtlAllocateHeap_z(local_c);
  if (local_8 != (wchar_t **)0x0) {
    DVar2 = (*EnumPrintersW)(2,(LPWSTR)0x0,5,(LPBYTE)local_8,local_c,&local_c,&local_10);
    ppwVar5 = local_8;
    while (DVar2 != 0) {
      iVar3 = (*wcsicmp)(*ppwVar5,local_228);
      if (iVar3 == 0) {
        uVar6 = string_hashing_z(extraout_ECX,extraout_EDX,(ushort *)ppwVar5[1],0);
        uVar4 = ~(uint)uVar6 ^ 0x1803fff7;
        if ((((uVar4 != 0xb85f1b31) && (uVar4 != 0x228a8c91)) && (uVar4 != 0x3e2aa97b)) &&
           (uVar4 != 0x7f7e8b5c)) {
          print = 0x720070;
          local_1c = 0x6e0069;
          local_18 = 0x74;
          (*ShellExecuteW)((HWND)0x0,(LPCWSTR)&print,param_1,(LPCWSTR)0x0,(LPCWSTR)0x0,0);
          break;
        }
      }
      ppwVar5 = ppwVar5 + 5;
      local_10 = local_10 - 1;
      DVar2 = local_10;
    }
    do_RtlFreeHeap_z(local_8);
  }
}
```

Print function v2.0+ - Do not print if printer port for virtual printers SHRFAX, FILE, XPSPort, PORTPROMPT

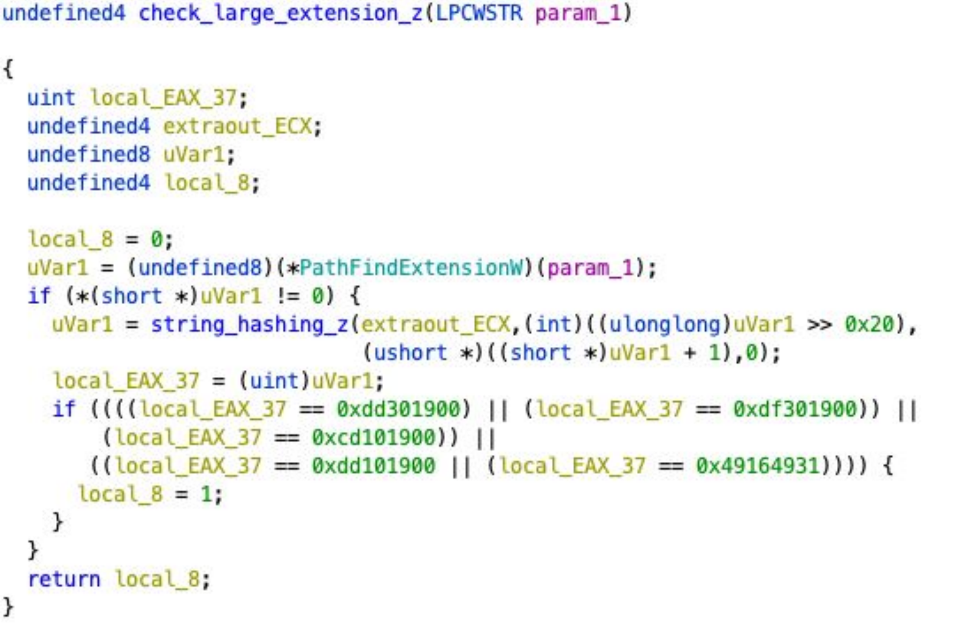
The Malware Evolves!

First added capability to encrypt Exchange files, then to handle “large” Microsoft files differently



```
pppWVar1 = &ExchangeInstallPath;
                    /* ExchangeInstallPath */
ExchangeInstallPath = (LPCWSTR *)0x4b793f81;
uStack88 = 0x4b693fa7;
uStack84 = 0x4b6f3fa5;
uStack80 = 0x4b643fa3;
local_4c = 0x4b6f3f8d;
local_48 = 0x4b753fb7;
local_44 = 0x4b6d3fa5;
local_40 = 0x4b513fa8;
local_3c = 0x4b753fa5;
local_38 = 0x4b013fac;
iVar5 = 10;
do {
  *pppWVar1 = (LPCWSTR *)((uint)*pppWVar1 ^ 0x4b013fc4);
  pppWVar1 = pppWVar1 + 1;
  iVar5 = iVar5 + -1;
} while (iVar5 != 0);
success = (*GetEnvironmentVariableW)((LPCWSTR)&ExchangeInstallPath,pathOut,0x104);
if (success != 0) {
  puVar3 = (uint *)&ProgramFiles;
                    /* Program Files */
  _ProgramFiles = 0x4b733f94;
  uStack48 = 0x4b663fab;
  uStack44 = 0x4b603fb6;
  uStack40 = 0x4b213fa9;
  local_24 = 0x4b683f82;
  local_20 = 0x4b643fa8;
  local_1c = 0x4b013fb7;
  iVar5 = 7;
  do {
    *puVar3 = *puVar3 ^ 0x4b013fc4;
    puVar3 = puVar3 + 1;
    iVar5 = iVar5 + -1;
  } while (iVar5 != 0);
```

Part of function to find and traverse Microsoft Exchange mailbox path and later encrypt files - v1.4+



```
undefined4 check_large_extension_z(LPCWSTR param_1)

{
  uint local_EAX_37;
  undefined4 extraout_ECX;
  undefined8 uVar1;
  undefined4 local_8;

  local_8 = 0;
  uVar1 = (undefined8)(*PathFindExtensionW)(param_1);
  if (*(short *)uVar1 != 0) {
    uVar1 = string_hashing_z(extraout_ECX,(int)((ulonglong)uVar1 >> 0x20),
                             (ushort *)((short *)uVar1 + 1),0);
    local_EAX_37 = (uint)uVar1;
    if ((((local_EAX_37 == 0xdd301900) || (local_EAX_37 == 0xdf301900)) ||
        (local_EAX_37 == 0xcd101900)) ||
       ((local_EAX_37 == 0xdd101900 || (local_EAX_37 == 0x49164931)))) {
      local_8 = 1;
    }
  }
  return local_8;
}
```

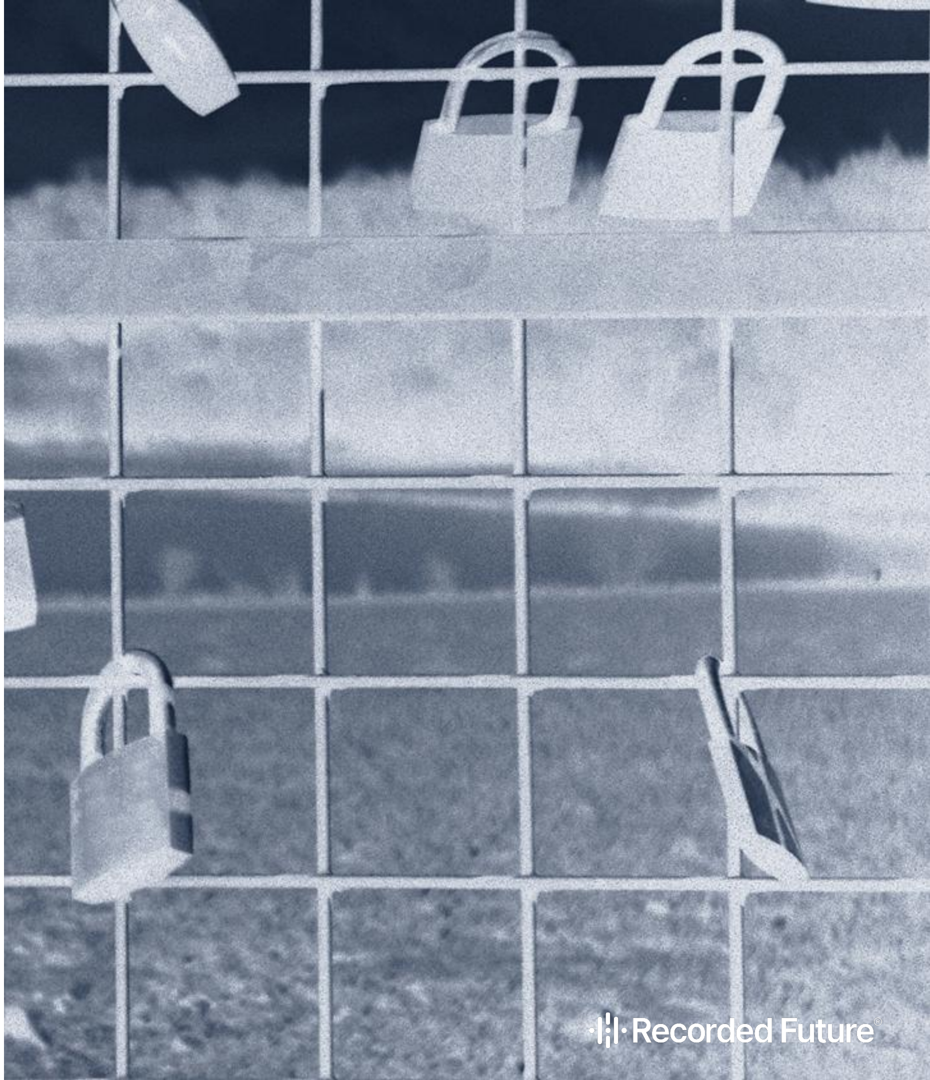
Check if file extension is .mdb, .mdf, .edb, .accdb and encrypt as “large file” by default - v1.9+

Recorded Future®

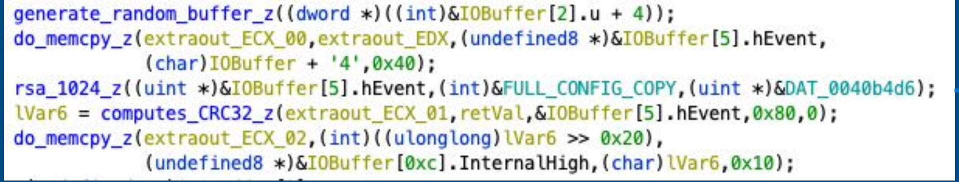
DarkSide vs BlackMatter

"There is some evidence to suggest that DarkSide, or at least some members of DarkSide, may have returned under the BlackMatter moniker. After investigating a leaked BlackMatter decryptor, Emsisoft analysts determined that BlackMatter uses the same encryption routines that DarkSide formerly used in their attacks, including a custom Salsa20 matrix that was unique to DarkSide."

Source: Emsisoft

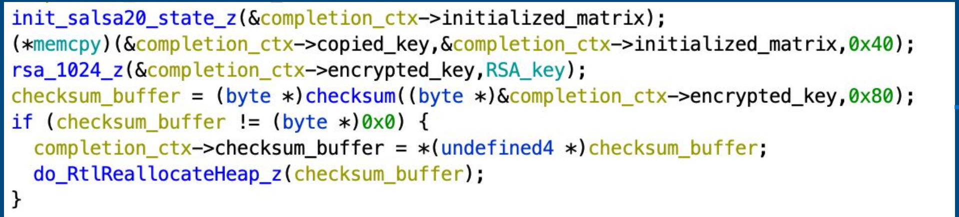


DarkSide vs BlackMatter

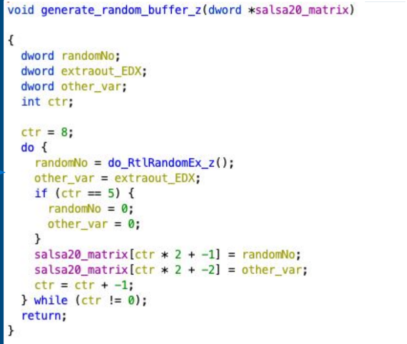


```
generate_random_buffer_z((dword *)((int)&IOBuffer[2].u + 4));
do_memcpy_z(extraout_ECX_00,extraout_EDX,(undefined8 *)&IOBuffer[5].hEvent,
            (char)IOBuffer + '4',0x40);
rsa_1024_z((uint *)&IOBuffer[5].hEvent,(int)&FULL_CONFIG_COPY,(uint *)&DAT_0040b4d6);
lVar6 = computes_CRC32_z(extraout_ECX_01,retVal,&IOBuffer[5].hEvent,0x80,0);
do_memcpy_z(extraout_ECX_02,(int)((ulonglong)lVar6 >> 0x20),
            (undefined8 *)&IOBuffer[0xc].InternalHigh,(char)lVar6,0x10);
```

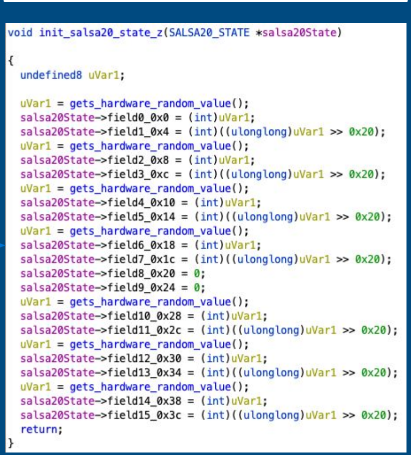
DarkSide (top) random buffer (salsa20 matrix init) followed by RSA 1024 encryption and **BlackMatter (bottom)** random buffer (salsa 20 matrix init) followed by RSA 1024 encryption



```
init_salsa20_state_z(&completion_ctx->initialized_matrix);
(*memcpy)(&completion_ctx->copied_key,&completion_ctx->initialized_matrix,0x40);
rsa_1024_z(&completion_ctx->encrypted_key,RSA_key);
checksum_buffer = (byte *)checksum((byte *)&completion_ctx->encrypted_key,0x80);
if (checksum_buffer != (byte *)0x0) {
  completion_ctx->checksum_buffer = *(undefined4 *)checksum_buffer;
  do_RtlReallocateHeap_z(checksum_buffer);
}
```



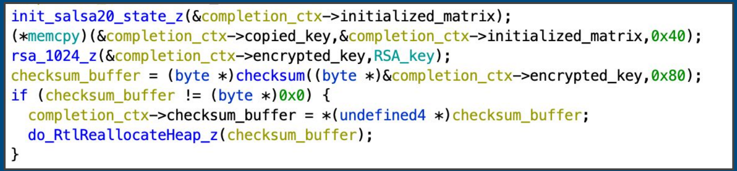
```
void generate_random_buffer_z(dword *salsa20_matrix)

{
  dword randomNo;
  dword extraout_EDX;
  dword other_var;
  int ctr;

  ctr = 8;
  do {
    randomNo = do_RtlRandomEx_z();
    other_var = extraout_EDX;
    if (ctr == 5) {
      randomNo = 0;
      other_var = 0;
    }
    salsa20_matrix[ctr * 2 + -1] = randomNo;
    salsa20_matrix[ctr * 2 + -2] = other_var;
    ctr = ctr + -1;
  } while (ctr != 0);
  return;
}
```



```
void init_salsa20_state_z(SALSA20_STATE *salsa20State)

{
  undefined8 uVar1;

  uVar1 = gets_hardware_random_value();
  salsa20State->field0_0x0 = (int)uVar1;
  salsa20State->field1_0x4 = (int)((ulonglong)uVar1 >> 0x20);
  uVar1 = gets_hardware_random_value();
  salsa20State->field2_0x8 = (int)uVar1;
  salsa20State->field3_0xc = (int)((ulonglong)uVar1 >> 0x20);
  uVar1 = gets_hardware_random_value();
  salsa20State->field4_0x10 = (int)uVar1;
  salsa20State->field5_0x14 = (int)((ulonglong)uVar1 >> 0x20);
  uVar1 = gets_hardware_random_value();
  salsa20State->field6_0x18 = (int)uVar1;
  salsa20State->field7_0x1c = (int)((ulonglong)uVar1 >> 0x20);
  salsa20State->field8_0x20 = 0;
  salsa20State->field9_0x24 = 0;
  uVar1 = gets_hardware_random_value();
  salsa20State->field10_0x28 = (int)uVar1;
  salsa20State->field11_0x2c = (int)((ulonglong)uVar1 >> 0x20);
  uVar1 = gets_hardware_random_value();
  salsa20State->field12_0x30 = (int)uVar1;
  salsa20State->field13_0x34 = (int)((ulonglong)uVar1 >> 0x20);
  uVar1 = gets_hardware_random_value();
  salsa20State->field14_0x38 = (int)uVar1;
  salsa20State->field15_0x3c = (int)((ulonglong)uVar1 >> 0x20);
  return;
}
```

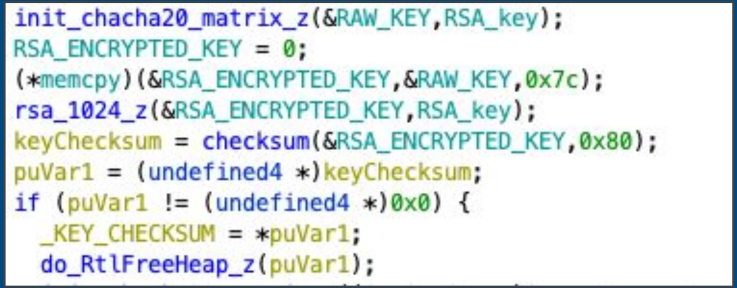
Broken Again?

Emsisoft released a decryptor for BlackMatter ransomware → the threat actor is said to have fixed the issue in late September 2021. Can’t speak to the specific cryptographic issue at hand, however, interesting to notice slight changes in key init code, among others



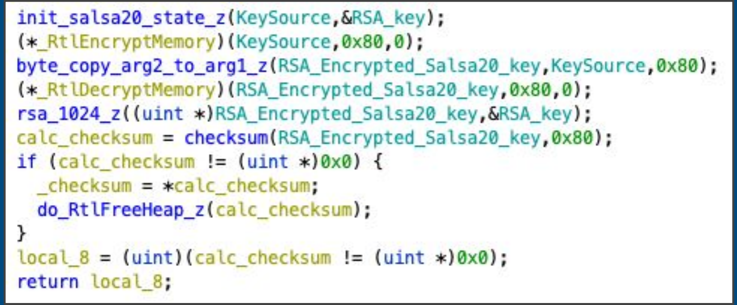
```
init_salsa20_state_z(&completion_ctx->initialized_matrix);
(*memcpy)(&completion_ctx->copied_key,&completion_ctx->initialized_matrix,0x40);
rsa_1024_z(&completion_ctx->encrypted_key,RSA_key);
checksum_buffer = (byte *)checksum((byte *)&completion_ctx->encrypted_key,0x80);
if (checksum_buffer != (byte *)0x0) {
  completion_ctx->checksum_buffer = *(undefined4 *)checksum_buffer;
  do_RtlReallocateHeap_z(checksum_buffer);
}
```

Key initialization in v1.2



```
init_chacha20_matrix_z(&RAW_KEY,RSA_key);
RSA_ENCRYPTED_KEY = 0;
(*memcpy)(&RSA_ENCRYPTED_KEY,&RAW_KEY,0x7c);
rsa_1024_z(&RSA_ENCRYPTED_KEY,RSA_key);
keyChecksum = checksum(&RSA_ENCRYPTED_KEY,0x80);
puVar1 = (undefined4 *)keyChecksum;
if (puVar1 != (undefined4 *)0x0) {
  _KEY_CHECKSUM = *puVar1;
  do_RtlFreeHeap_z(puVar1);
```

Key initialization in v2.0

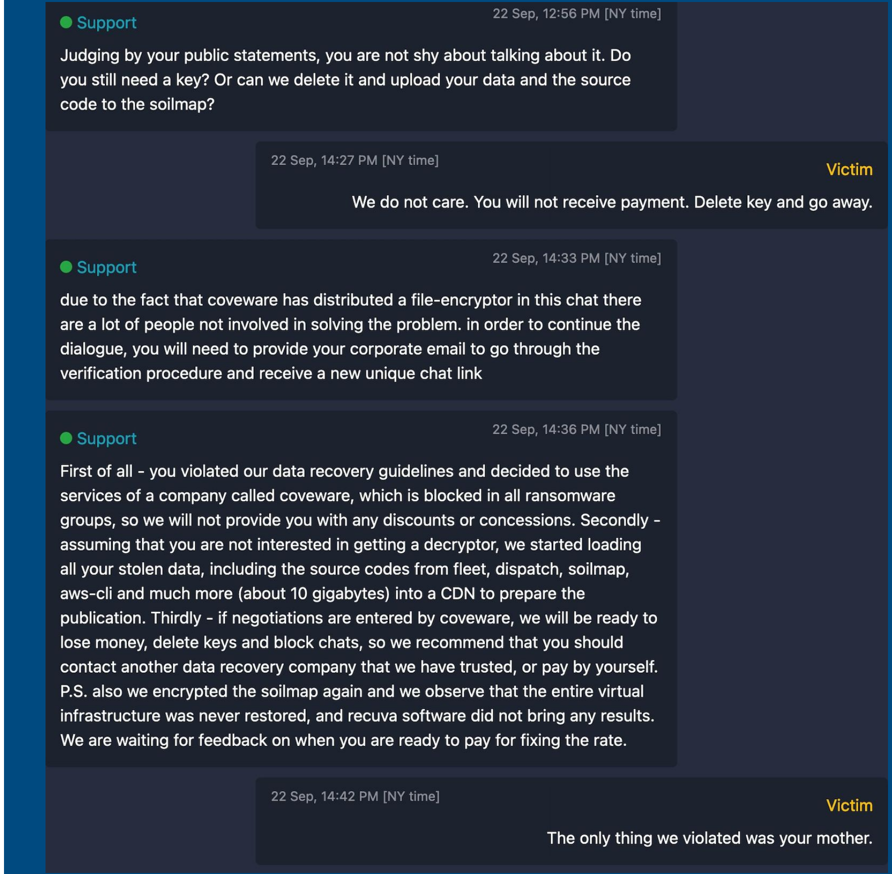


```
init_salsa20_state_z(KeySource,&RSA_key);
(*_RtlEncryptMemory)(KeySource,0x80,0);
byte_copy_arg2_to_arg1_z(RSA_Encrypted_Salsa20_key,KeySource,0x80);
(*_RtlDecryptMemory)(RSA_Encrypted_Salsa20_key,0x80,0);
rsa_1024_z((uint *)RSA_Encrypted_Salsa20_key,&RSA_key);
calc_checksum = checksum(RSA_Encrypted_Salsa20_key,0x80);
if (calc_checksum != (uint *)0x0) {
  _checksum = *calc_checksum;
  do_RtlFreeHeap_z(calc_checksum);
}
local_8 = (uint)(calc_checksum != (uint *)0x0);
return local_8;
```

Key initialization in v3.0

Downfall

- Decryption Issues
- Chat Hijacking
- Requirements for victim chat
- Domain Controller name
- Domain Admins
- Chat Access Codes (discussed later)



Support 22 Sep, 12:56 PM [NY time]

Judging by your public statements, you are not shy about talking about it. Do you still need a key? Or can we delete it and upload your data and the source code to the soilmap?

22 Sep, 14:27 PM [NY time] Victim

We do not care. You will not receive payment. Delete key and go away.

Support 22 Sep, 14:33 PM [NY time]

due to the fact that coveware has distributed a file-encryptor in this chat there are a lot of people not involved in solving the problem. in order to continue the dialogue, you will need to provide your corporate email to go through the verification procedure and receive a new unique chat link

Support 22 Sep, 14:36 PM [NY time]

First of all - you violated our data recovery guidelines and decided to use the services of a company called coveware, which is blocked in all ransomware groups, so we will not provide you with any discounts or concessions. Secondly - assuming that you are not interested in getting a decryptor, we started loading all your stolen data, including the source codes from fleet, dispatch, soilmap, aws-cli and much more (about 10 gigabytes) into a CDN to prepare the publication. Thirdly - if negotiations are entered by coveware, we will be ready to lose money, delete keys and block chats, so we recommend that you should contact another data recovery company that we have trusted, or pay by yourself. P.S. also we encrypted the soilmap again and we observe that the entire virtual infrastructure was never restored, and recuva software did not bring any results. We are waiting for feedback on when you are ready to pay for fixing the rate.

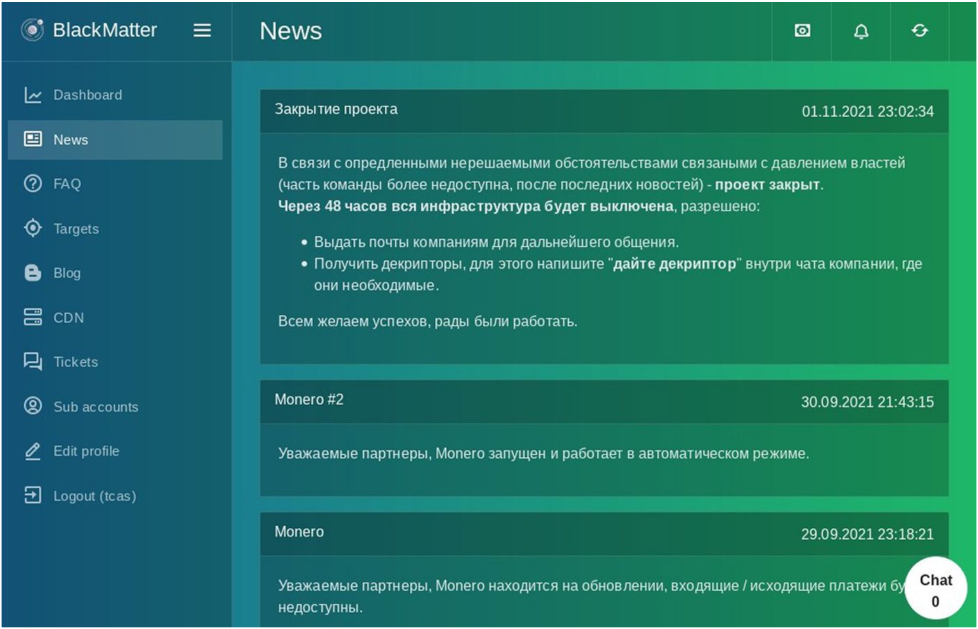
22 Sep, 14:42 PM [NY time] Victim

The only thing we violated was your mother.

BlackMatter Victim Chat

The End

Blackmatter **claims** to be shutting down due to local law enforcement pressure



Закрытие проекта 01.11.2021 23:02:34

В связи с опредленными нерешаемыми обстоятельствами связаными с давлением властей (часть команды более недоступна, после последних новостей) - **проект закрыт**.
Через 48 часов вся инфраструктура будет выключена, разрешено:

- Выдать почты компаниям для дальнейшего общения.
- Получить декрипторы, для этого напишите "**дайте декриптор**" внутри чата компании, где они необходимые.

Всем желаем успехов, рады были работать.

Monero #2 30.09.2021 21:43:15

Уважаемые партнеры, Монеро запущен и работает в автоматическом режиме.

Monero 29.09.2021 23:18:21

Уважаемые партнеры, Монеро находится на обновлении, входящие / исходящие платежи бу недоступны.

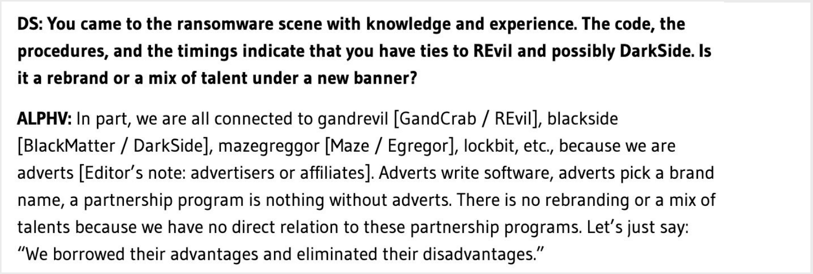
BlackMatter announcing retirement

(Source: VX Underground)

So It's Over, Right?

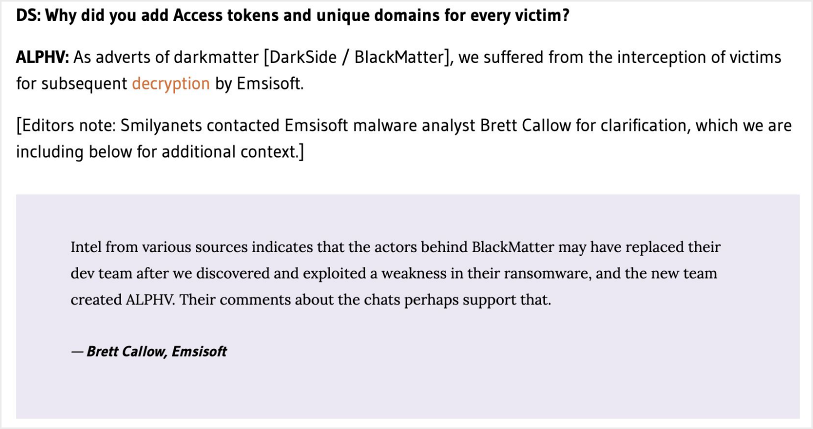
Well, no, not quite.

- Rebranding does happen
- Affiliates move from one program to another
- BlackMatter and REvil affiliates rebranded to ALPHV



DS: You came to the ransomware scene with knowledge and experience. The code, the procedures, and the timings indicate that you have ties to REvil and possibly DarkSide. Is it a rebrand or a mix of talent under a new banner?

ALPHV: In part, we are all connected to gandrevil [GandCrab / REvil], blackside [BlackMatter / DarkSide], mazegreggor [Maze / Egregor], lockbit, etc., because we are adverts [Editor's note: advertisers or affiliates]. Adverts write software, adverts pick a brand name, a partnership program is nothing without adverts. There is no rebranding or a mix of talents because we have no direct relation to these partnership programs. Let's just say: "We borrowed their advantages and eliminated their disadvantages."



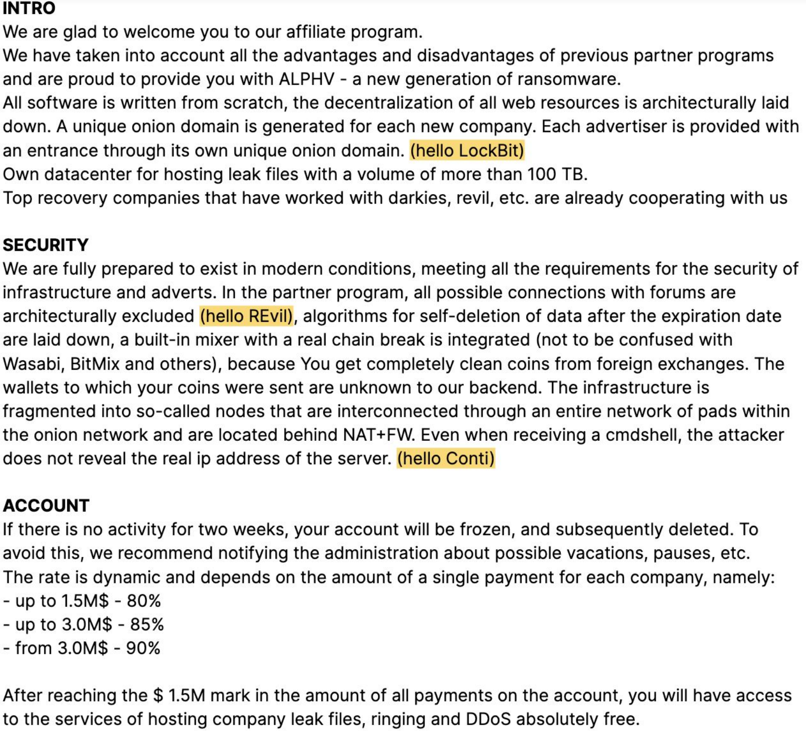
DS: Why did you add Access tokens and unique domains for every victim?

ALPHV: As adverts of darkmatter [DarkSide / BlackMatter], we suffered from the interception of victims for subsequent decryption by Emsisoft.

[Editors note: Smilyanets contacted Emsisoft malware analyst Brett Callow for clarification, which we are including below for additional context.]

> Intel from various sources indicates that the actors behind BlackMatter may have replaced their dev team after we discovered and exploited a weakness in their ransomware, and the new team created ALPHV. Their comments about the chats perhaps support that.
>
> — ***Brett Callow, Emsisoft***

Everyone else sucks (hello BlackMatter)



INTRO

We are glad to welcome you to our affiliate program.

We have taken into account all the advantages and disadvantages of previous partner programs and are proud to provide you with ALPHV - a new generation of ransomware.

All software is written from scratch, the decentralization of all web resources is architecturally laid down. A unique onion domain is generated for each new company. Each advertiser is provided with an entrance through its own unique onion domain. (hello LockBit)

Own datacenter for hosting leak files with a volume of more than 100 TB.

Top recovery companies that have worked with darkies, revil, etc. are already cooperating with us

SECURITY

We are fully prepared to exist in modern conditions, meeting all the requirements for the security of infrastructure and adverts. In the partner program, all possible connections with forums are architecturally excluded (hello REvil), algorithms for self-deletion of data after the expiration date are laid down, a built-in mixer with a real chain break is integrated (not to be confused with Wasabi, BitMix and others), because You get completely clean coins from foreign exchanges. The wallets to which your coins were sent are unknown to our backend. The infrastructure is fragmented into so-called nodes that are interconnected through an entire network of pads within the onion network and are located behind NAT+FW. Even when receiving a cmdshell, the attacker does not reveal the real ip address of the server. (hello Conti)

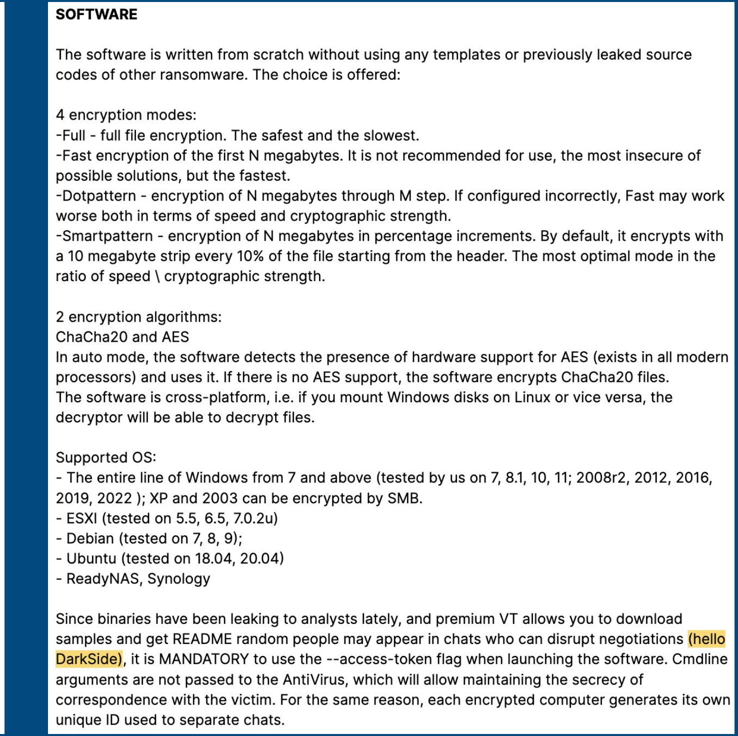
ACCOUNT

If there is no activity for two weeks, your account will be frozen, and subsequently deleted. To avoid this, we recommend notifying the administration about possible vacations, pauses, etc.

The rate is dynamic and depends on the amount of a single payment for each company, namely:

- up to 1.5M$ - 80%
- up to 3.0M$ - 85%
- from 3.0M$ - 90%

After reaching the $ 1.5M mark in the amount of all payments on the account, you will have access to the services of hosting company leak files, ringing and DDoS absolutely free.



SOFTWARE

The software is written from scratch without using any templates or previously leaked source codes of other ransomware. The choice is offered:

4 encryption modes:

-Full - full file encryption. The safest and the slowest.

-Fast encryption of the first N megabytes. It is not recommended for use, the most insecure of possible solutions, but the fastest.

-Dotpattern - encryption of N megabytes through M step. If configured incorrectly, Fast may work worse both in terms of speed and cryptographic strength.

-Smartpattern - encryption of N megabytes in percentage increments. By default, it encrypts with a 10 megabyte strip every 10% of the file starting from the header. The most optimal mode in the ratio of speed \ cryptographic strength.

2 encryption algorithms:

ChaCha20 and AES

In auto mode, the software detects the presence of hardware support for AES (exists in all modern processors) and uses it. If there is no AES support, the software encrypts ChaCha20 files.

The software is cross-platform, i.e. if you mount Windows disks on Linux or vice versa, the decryptor will be able to decrypt files.

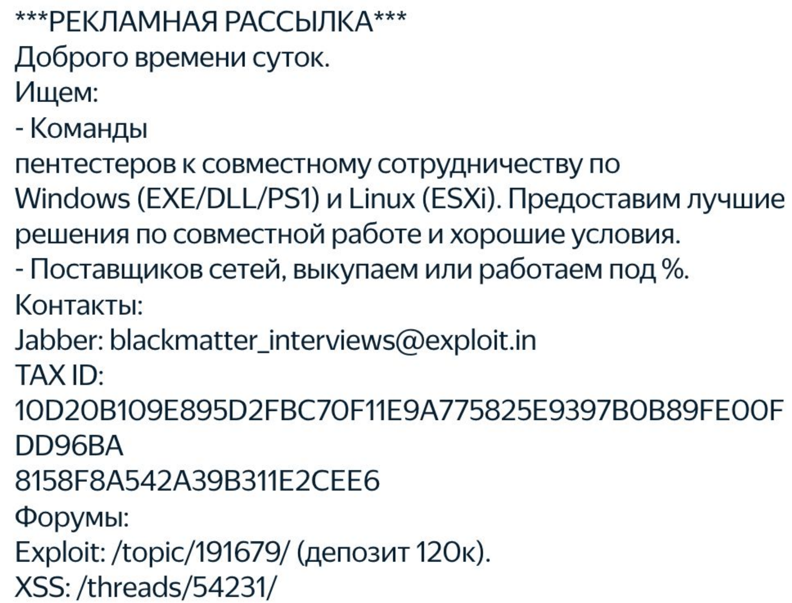
Supported OS:

- The entire line of Windows from 7 and above (tested by us on 7, 8.1, 10, 11; 2008r2, 2012, 2016, 2019, 2022); XP and 2003 can be encrypted by SMB.
- ESXI (tested on 5.5, 6.5, 7.0.2u)
- Debian (tested on 7, 8, 9);
- Ubuntu (tested on 18.04, 20.04)
- ReadyNAS, Synology

Since binaries have been leaking to analysts lately, and premium VT allows you to download samples and get README random people may appear in chats who can disrupt negotiations (hello DarkSide), it is MANDATORY to use the --access-token flag when launching the software. Cmdline arguments are not passed to the AntiVirus, which will allow maintaining the secrecy of correspondence with the victim. For the same reason, each encrypted computer generates its own unique ID used to separate chats.

ALPHV Affiliate Introduction and Rules

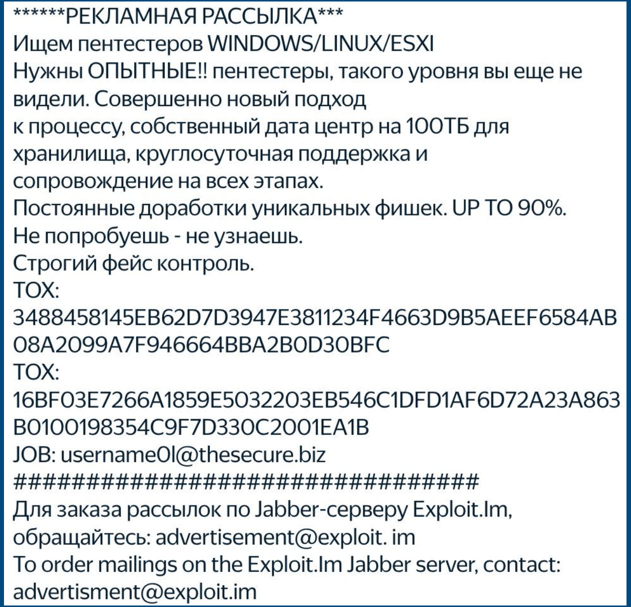
Advertisements



РЕКЛАМНАЯ РАССЫЛКА
Доброго времени суток.
Ищем:
- Команды
пентестеров к совместному сотрудничеству по Windows (EXE/DLL/PS1) и Linux (ESXi). Предоставим лучшие решения по совместной работе и хорошие условия.
- Поставщиков сетей, выкупаем или работаем под %.

Контакты:
Jabber: blackmatter_interviews@exploit.in
TAX ID:
10D20B109E895D2FBC70F11E9A775825E9397B0B89FE00F
DD96BA
8158F8A542A39B311E2CEE6
Форумы:
Exploit: /topic/191679/ (депозит 120к).
XSS: /threads/54231/

BlackMatter Advertisement on Exploit Jabber Service



******РЕКЛАМНАЯ РАССЫЛКА***
Ищем пентестеров WINDOWS/LINUX/ESXI
Нужны ОПЫТНЫЕ!! пентестеры, такого уровня вы еще не видели. Совершенно новый подход
к процессу, собственный дата центр на 100ТБ для хранилища, круглосуточная поддержка и сопровождение на всех этапах.
Постоянные доработки уникальных фишек. UP TO 90%.
Не попробуешь - не узнаешь.
Строгий фейс контроль.
TOX:
3488458145EB62D7D3947E3811234F4663D9B5AEEF6584AB
08A2099A7F946664BBA2B0D30BFC
TOX:
16BF03E7266A1859E5032203EB546C1DFD1AF6D72A23A863
B0100198354C9F7D330C2001EA1B
JOB: username0l@thesecure.biz

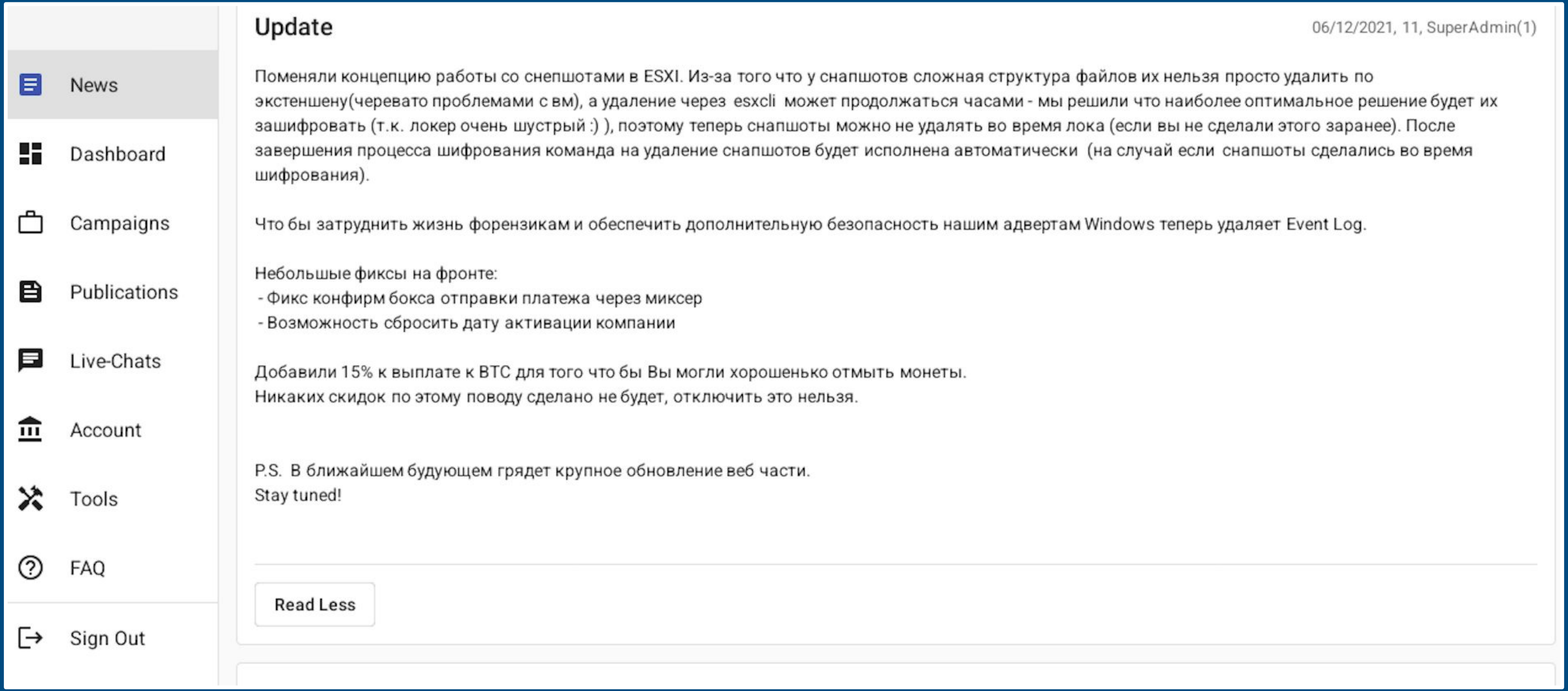
##################################

Для заказа рассылок по Jabber-серверу Exploit.Im, обращайтесь: advertisement@exploit. im
To order mailings on the Exploit.Im Jabber server, contact:
advertisment@exploit.im

ALPHV Advertisement on Exploit Jabber Service

Recorded Future®

ALPHV



Update

06/12/2021, 11, SuperAdmin(1)

Поменяли концепцию работы со снепшотами в ESXI. Из-за того что у снапшотов сложная структура файлов их нельзя просто удалить по экстеншену(черевато проблемами с вм), а удаление через esxcli может продолжаться часами - мы решили что наиболее оптимальное решение будет их зашифровать (т.к. локер очень шустрый :)), поэтому теперь снапшоты можно не удалять во время лока (если вы не сделали этого заранее). После завершения процесса шифрования команда на удаление снапшотов будет исполнена автоматически (на случай если снапшоты сделались во время шифрования).

Что бы затруднить жизнь форензикам и обеспечить дополнительную безопасность нашим адвертам Windows теперь удаляет Event Log.

Небольшые фиксы на фронте:
- Фикс конфирм бокса отправки платежа через миксер
- Возможность сбросить дату активации компании

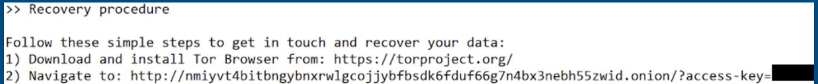
Добавили 15% к выплате к BTC для того что бы Вы могли хорошенько отмыть монеты.
Никаких скидок по этому поводу сделано не будет, отключить это нельзя.

P.S. В ближайшем будующем грядет крупное обновление веб части.
Stay tuned!

ALPHV Affiliate Panel

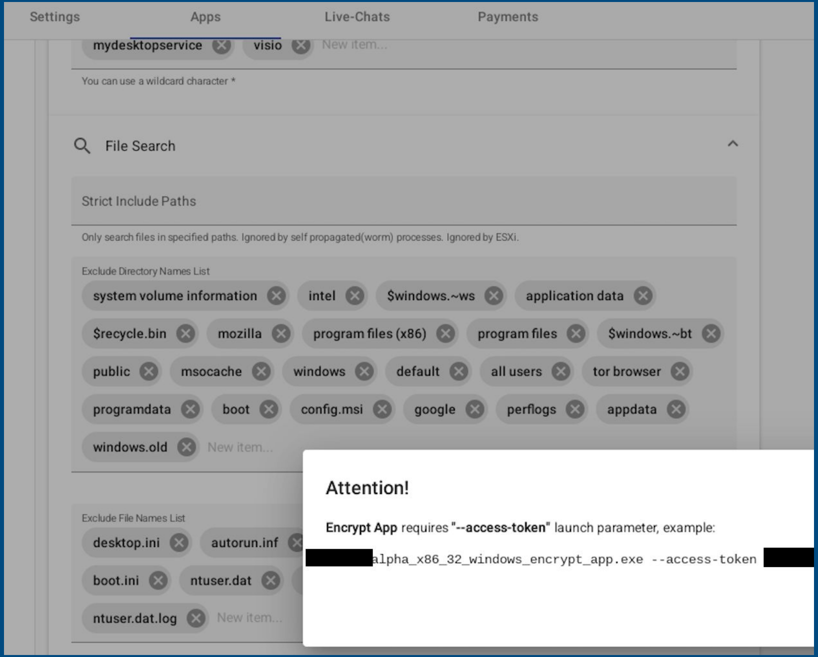
What’s New?

- Rust
- New panel
- Access code for victim chat
- Better support
- BTC Mixer
- MORPH



```
>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://nmiyvt4bitbngybnxrwlgcojjybfbsdk6fduf66g7n4bx3nebh55zwid.onion/?access-key=[redacted]
```

ALPHV Ransom Note
Source: Recorded Future



mydesktopservice, visio

You can use a wildcard character *

File Search

Strict Include Paths

Only search files in specified paths. Ignored by self propagated(worm) processes. Ignored by ESXi.

Exclude Directory Names List

system volume information, intel, $windows.~ws, application data, $recycle.bin, mozilla, program files (x86), program files, $windows.~bt, public, msocache, windows, default, all users, tor browser, programdata, boot, config.msi, google, perflogs, appdata, windows.old

Exclude File Names List

desktop.ini, autorun.inf, boot.ini, ntuser.dat, ntuser.dat.log

Attention!

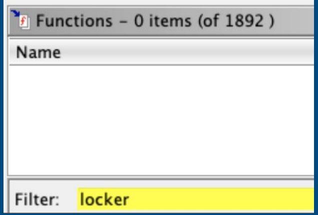
Encrypt App requires "**--access-token**" launch parameter, example:

```
[redacted]alpha_x86_32_windows_encrypt_app.exe --access-token [redacted]
```

ALPHV Ransomware Build Panel

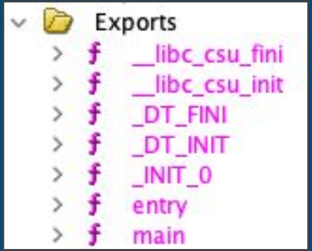
ALPHV MORPH - Linux

No string obfuscation was present, but the Linux x64 Morph-obfuscated samples appear to now have the name-mangled function names, versus the unobfuscated ones with scrubbed names



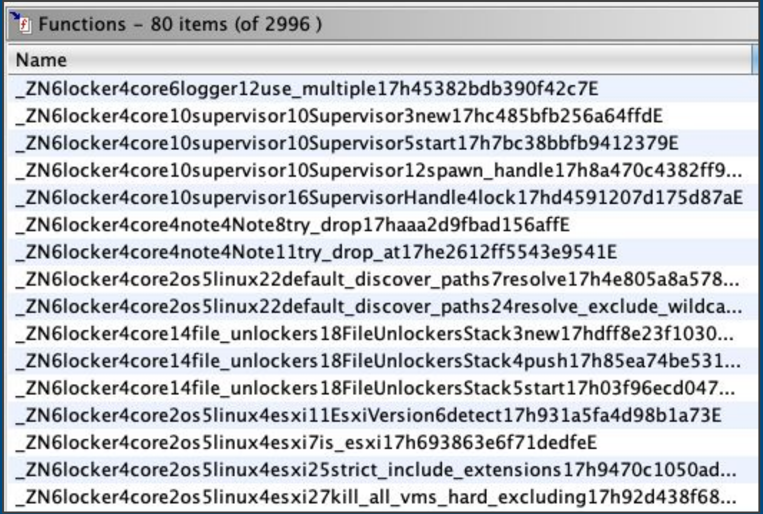
```
Functions – 0 items (of 1892 )
Name

Filter: locker
```

Function names from “unobfuscated” x64 Linux/ESXi Samples



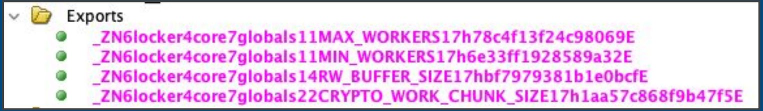
```
Exports
  __libc_csu_fini
  __libc_csu_init
  _DT_FINI
  _DT_INIT
  _INIT_0
  entry
  main
```

Exported variables from “unobfuscated” x64 Linux/ESXi Samples



```
Functions – 80 items (of 2996 )
Name
_ZN6locker4core6logger12use_multiple17h45382bdb390f42c7E
_ZN6locker4core10supervisor10Supervisor3new17hc485bfb256a64ffdE
_ZN6locker4core10supervisor10Supervisor5start17h7bc38bbfb9412379E
_ZN6locker4core10supervisor10Supervisor12spawn_handle17h8a470c4382ff9...
_ZN6locker4core10supervisor16SupervisorHandle4lock17hd4591207d175d87aE
_ZN6locker4core4note4Note8try_drop17haaa2d9fbad156affE
_ZN6locker4core4note4Note11try_drop_at17he2612ff5543e9541E
_ZN6locker4core2os5linux22default_discover_paths7resolve17h4e805a8a578...
_ZN6locker4core2os5linux22default_discover_paths24resolve_exclude_wildca...
_ZN6locker4core14file_unlockers18FileUnlockersStack3new17hdff8e23f1030...
_ZN6locker4core14file_unlockers18FileUnlockersStack4push17h85ea74be531...
_ZN6locker4core14file_unlockers18FileUnlockersStack5start17h03f96ecd047...
_ZN6locker4core2os5linux4esxi11EsxiVersion6detect17h931a5fa4d98b1a73E
_ZN6locker4core2os5linux4esxi7is_esxi17h693863e6f71dedfeE
_ZN6locker4core2os5linux4esxi25strict_include_extensions17h9470c1050ad...
_ZN6locker4core2os5linux4esxi27kill_all_vms_hard_excluding17h92d438f68...
```

Function names from “obfuscated” x64 Linux/ESXi Samples



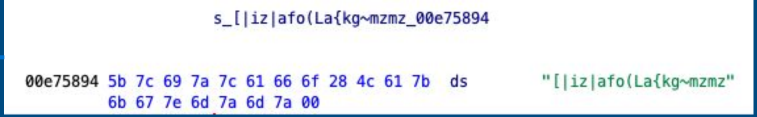
```
Exports
  _ZN6locker4core7globals11MAX_WORKERS17h78c4f13f24c98069E
  _ZN6locker4core7globals11MIN_WORKERS17h6e33ff1928589a32E
  _ZN6locker4core7globals14RW_BUFFER_SIZE17hbf7979381b1e0bcfE
  _ZN6locker4core7globals22CRYPTO_WORK_CHUNK_SIZE17h1aa57c868f9b47f5E
```

Exported variables from “obfuscated” x86 Linux/ESXi Samples

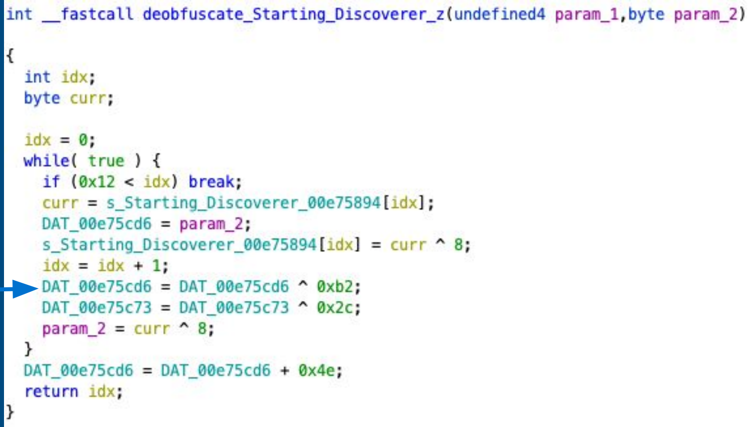
Recorded Future®

ALPHV MORPH - Windows

Strings deobfuscated with 1-byte XOR using “randomly generated” functions (with garbage code)



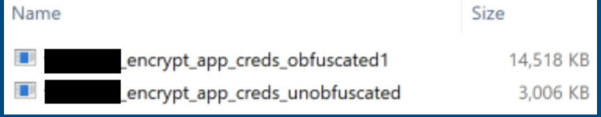
```
                         s_[|iz|afo(La{kg~mzmz_00e75894


00e75894 5b 7c 69 7a 7c 61 66 6f 28 4c 61 7b   ds        "[|iz|afo(La{kg~mzmz"
         6b 67 7e 6d 7a 6d 7a 00
```



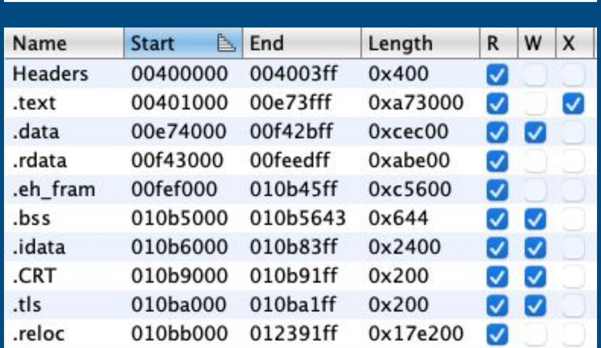
```
int __fastcall deobfuscate_Starting_Discoverer_z(undefined4 param_1,byte param_2)

{
  int idx;
  byte curr;

  idx = 0;
  while( true ) {
    if (0x12 < idx) break;
    curr = s_Starting_Discoverer_00e75894[idx];
    DAT_00e75cd6 = param_2;
    s_Starting_Discoverer_00e75894[idx] = curr ^ 8;
    idx = idx + 1;
    DAT_00e75cd6 = DAT_00e75cd6 ^ 0xb2;
    DAT_00e75c73 = DAT_00e75c73 ^ 0x2c;
    param_2 = curr ^ 8;
  }
  DAT_00e75cd6 = DAT_00e75cd6 + 0x4e;
  return idx;
}
```

Deobfuscation function for “Starting Discoverer”

Windows binaries over 4 times the size of the “unobfuscated” versions - biggest increase in .text, .data and .reloc sections



Name	Size
[redacted]_encrypt_app_creds_obfuscated1	14,518 KB
[redacted]_encrypt_app_creds_unobfuscated	3,006 KB

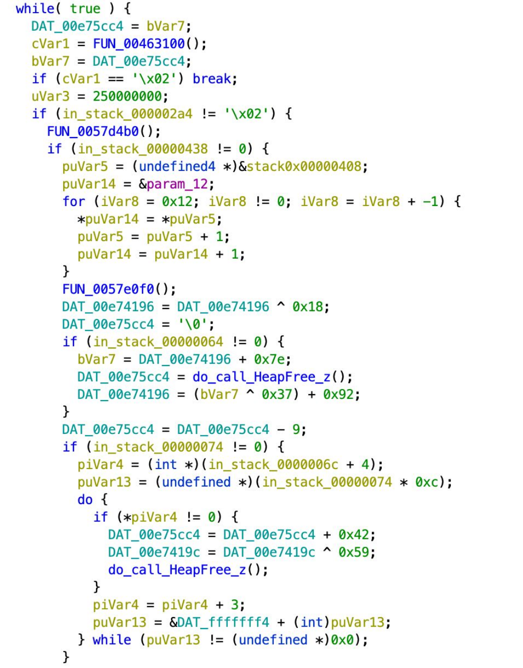


Name	Start	End	Length	R	W	X
Headers	00400000	004003ff	0x400	☑	□	□
.text	00401000	00e73fff	0xa73000	☑	□	☑
.data	00e74000	00f42bff	0xcec00	☑	☑	□
.rdata	00f43000	00feedff	0xabe00	☑	□	□
.eh_fram	00fef000	010b45ff	0xc5600	☑	□	□
.bss	010b5000	010b5643	0x644	☑	☑	□
.idata	010b6000	010b83ff	0x2400	☑	☑	□
.CRT	010b9000	010b91ff	0x200	☑	☑	□
.tls	010ba000	010ba1ff	0x200	☑	☑	□
.reloc	010bb000	012391ff	0x17e200	☑	□	□

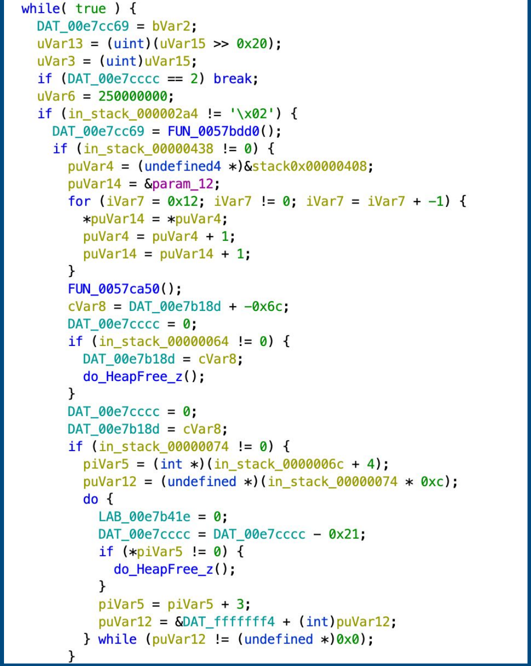
Morph-Obfuscated Binary Section Information

Recorded Future®

ALPHV MORPH - Windows



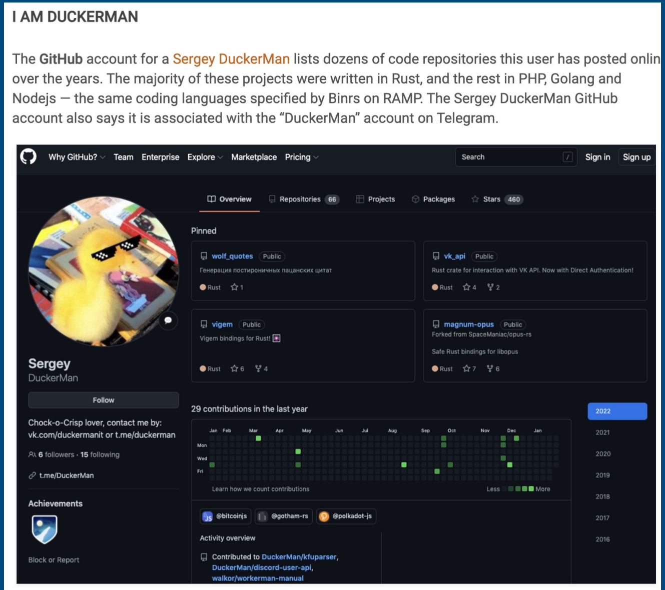
```c
while( true ) {
  DAT_00e75cc4 = bVar7;
  cVar1 = FUN_00463100();
  bVar7 = DAT_00e75cc4;
  if (cVar1 == '\x02') break;
  uVar3 = 250000000;
  if (in_stack_000002a4 != '\x02') {
    FUN_0057d4b0();
    if (in_stack_00000438 != 0) {
      puVar5 = (undefined4 *)&stack0x00000408;
      puVar14 = &param_12;
      for (iVar8 = 0x12; iVar8 != 0; iVar8 = iVar8 + -1) {
        *puVar14 = *puVar5;
        puVar5 = puVar5 + 1;
        puVar14 = puVar14 + 1;
      }
      FUN_0057e0f0();
      DAT_00e74196 = DAT_00e74196 ^ 0x18;
      DAT_00e75cc4 = '\0';
      if (in_stack_00000064 != 0) {
        bVar7 = DAT_00e74196 + 0x7e;
        DAT_00e75cc4 = do_call_HeapFree_z();
        DAT_00e74196 = (bVar7 ^ 0x37) + 0x92;
      }
      DAT_00e75cc4 = DAT_00e75cc4 - 9;
      if (in_stack_00000074 != 0) {
        piVar4 = (int *)(in_stack_0000006c + 4);
        puVar13 = (undefined *)(in_stack_00000074 * 0xc);
        do {
          if (*piVar4 != 0) {
            DAT_00e75cc4 = DAT_00e75cc4 + 0x42;
            DAT_00e7419c = DAT_00e7419c ^ 0x59;
            do_call_HeapFree_z();
          }
          piVar4 = piVar4 + 3;
          puVar13 = &DAT_fffffff4 + (int)puVar13;
        } while (puVar13 != (undefined *)0x0);
      }
```



```c
while( true ) {
  DAT_00e7cc69 = bVar2;
  uVar13 = (uint)(uVar15 >> 0x20);
  uVar3 = (uint)uVar15;
  if (DAT_00e7cccc == 2) break;
  uVar6 = 250000000;
  if (in_stack_000002a4 != '\x02') {
    DAT_00e7cc69 = FUN_0057bdd0();
    if (in_stack_00000438 != 0) {
      puVar4 = (undefined4 *)&stack0x00000408;
      puVar14 = &param_12;
      for (iVar7 = 0x12; iVar7 != 0; iVar7 = iVar7 + -1) {
        *puVar14 = *puVar4;
        puVar4 = puVar4 + 1;
        puVar14 = puVar14 + 1;
      }
      FUN_0057ca50();
      cVar8 = DAT_00e7b18d + -0x6c;
      DAT_00e7cccc = 0;
      if (in_stack_00000064 != 0) {
        DAT_00e7b18d = cVar8;
        do_HeapFree_z();
      }
      DAT_00e7cccc = 0;
      DAT_00e7b18d = cVar8;
      if (in_stack_00000074 != 0) {
        piVar5 = (int *)(in_stack_0000006c + 4);
        puVar12 = (undefined *)(in_stack_00000074 * 0xc);
        do {
          LAB_00e7b41e = 0;
          DAT_00e7cccc = DAT_00e7cccc - 0x21;
          if (*piVar5 != 0) {
            do_HeapFree_z();
          }
          piVar5 = piVar5 + 3;
          puVar12 = &DAT_fffffff4 + (int)puVar12;
        } while (puVar12 != (undefined *)0x0);
      }
```

Two builds of MORPH-obfuscated Windows samples showing junk code inserted

And The Story Continues…



I AM DUCKERMAN

The **GitHub** account for a Sergey DuckerMan lists dozens of code repositories this user has posted onlin over the years. The majority of these projects were written in Rust, and the rest in PHP, Golang and Nodejs — the same coding languages specified by Binrs on RAMP. The Sergey DuckerMan GitHub account also says it is associated with the "DuckerMan" account on Telegram.

Sergey
DuckerMan

Chock-o-Crisp lover, contact me by: vk.com/duckermanit or t.me/duckerman

6 followers · 15 following

t.me/DuckerMan

Achievements

Pinned

wolf_quotes Public
Генерация постироничных пацанских цитат
Rust ☆ 1

vk_api Public
Rust crate for interaction with VK API. Now with Direct Authentication!
Rust ☆ 4 2

vigem Public
Vigem bindings for Rust!
Rust ☆ 6 4

magnum-opus Public
Forked from SpaceManiac/opus-rs
Safe Rust bindings for libopus
Rust ☆ 7 6

29 contributions in the last year

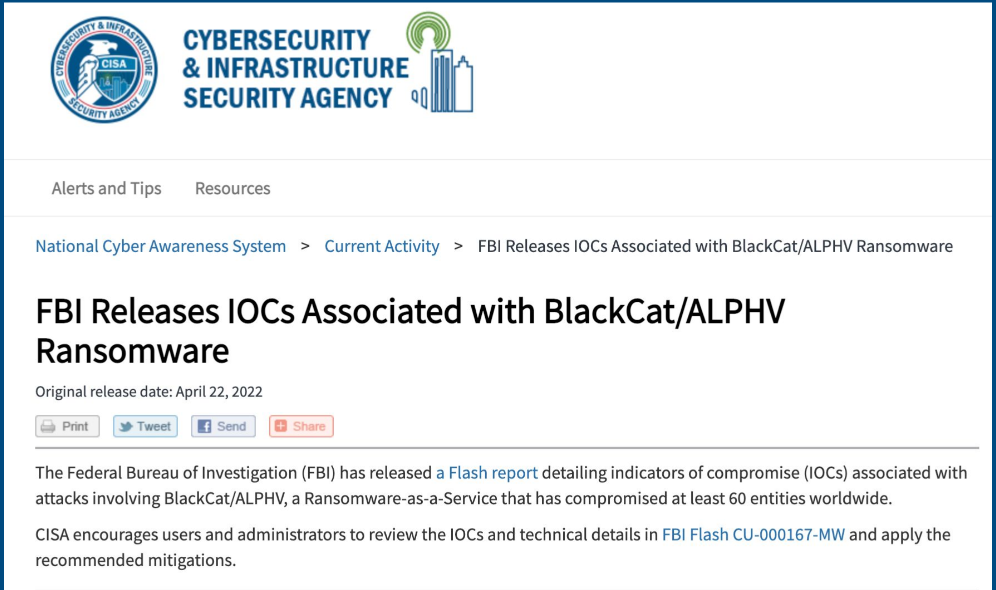
Learn how we count contributions

@bitcoinjs @gotham-rs @polkadot-js

Activity overview

Contributed to DuckerMan/kfuparser, DuckerMan/discord-user-api, walkor/workerman-manual

(Source: Krebs on Security)



National Cyber Awareness System > Current Activity > FBI Releases IOCs Associated with BlackCat/ALPHV Ransomware

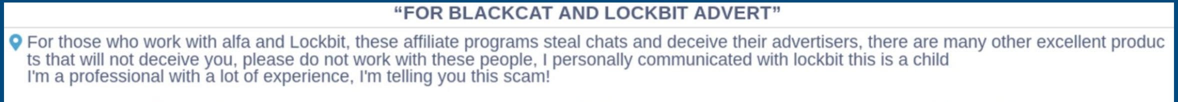
FBI Releases IOCs Associated with BlackCat/ALPHV Ransomware

Original release date: April 22, 2022

The Federal Bureau of Investigation (FBI) has released a Flash report detailing indicators of compromise (IOCs) associated with attacks involving BlackCat/ALPHV, a Ransomware-as-a-Service that has compromised at least 60 entities worldwide.

CISA encourages users and administrators to review the IOCs and technical details in FBI Flash CU-000167-MW and apply the recommended mitigations.

(Source: CISA)



"FOR BLACKCAT AND LOCKBIT ADVERT"

For those who work with alfa and Lockbit, these affiliate programs steal chats and deceive their advertisers, there are many other excellent products that will not deceive you, please do not work with these people, I personally communicated with lockbit this is a child
I'm a professional with a lot of experience, I'm telling you this scam!

(Source: Conti Blog)

Thank You!

Recorded Future®

Lindsay Kaye @TheQueenofELF
James Niven @stuffedinlocker