Everything happens for a reason

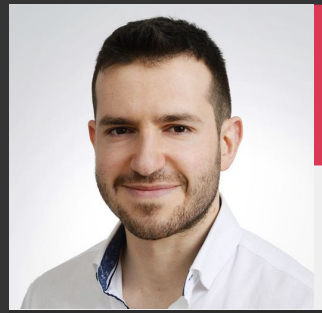
The choices made by ransomware operators

PwC Threat Intelligence

TLP:WHITE

October 2023

Introductions



Jono Davis

Technical Analyst
PwC

Been in the team for 4 years focusing on Ransomware-as-a-Service threat actors

- Malware reverse engineering
- Confuses International Relations with Incident Response
- Always happy to discuss the Rugby World Cup
- Sorry for all the coughing

@Katechondic

PwC Threat Intelligence

Strategic and Technical roles
Global

Threat research used by public and private sector organisations to protect networks, defend nations, provide situational awareness & inform strategy.

- Team members spread across 8 countries and 3 continents
- Focus on both technical and strategic analysis
- Cross-collaboration alongside intel partners
- Support to IR, red teams, threat hunting teams etc.

Why are we here?

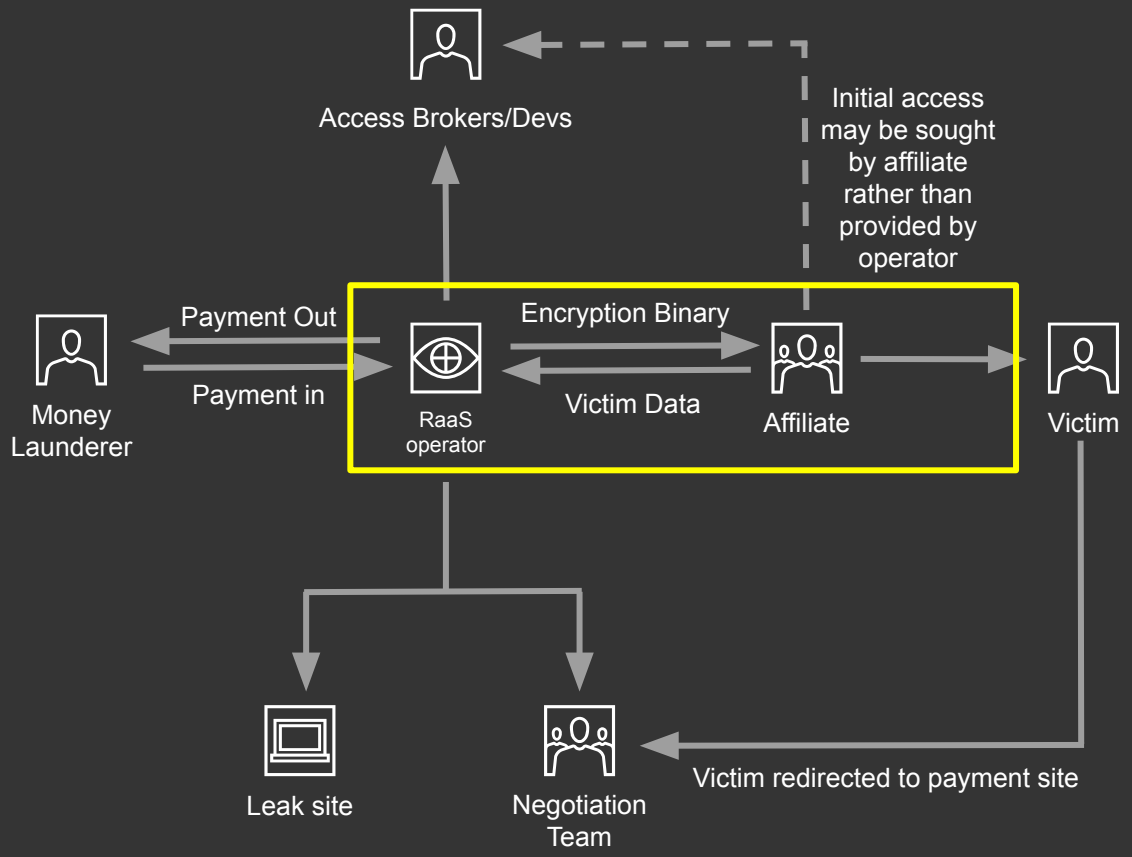
The agenda of this presentation

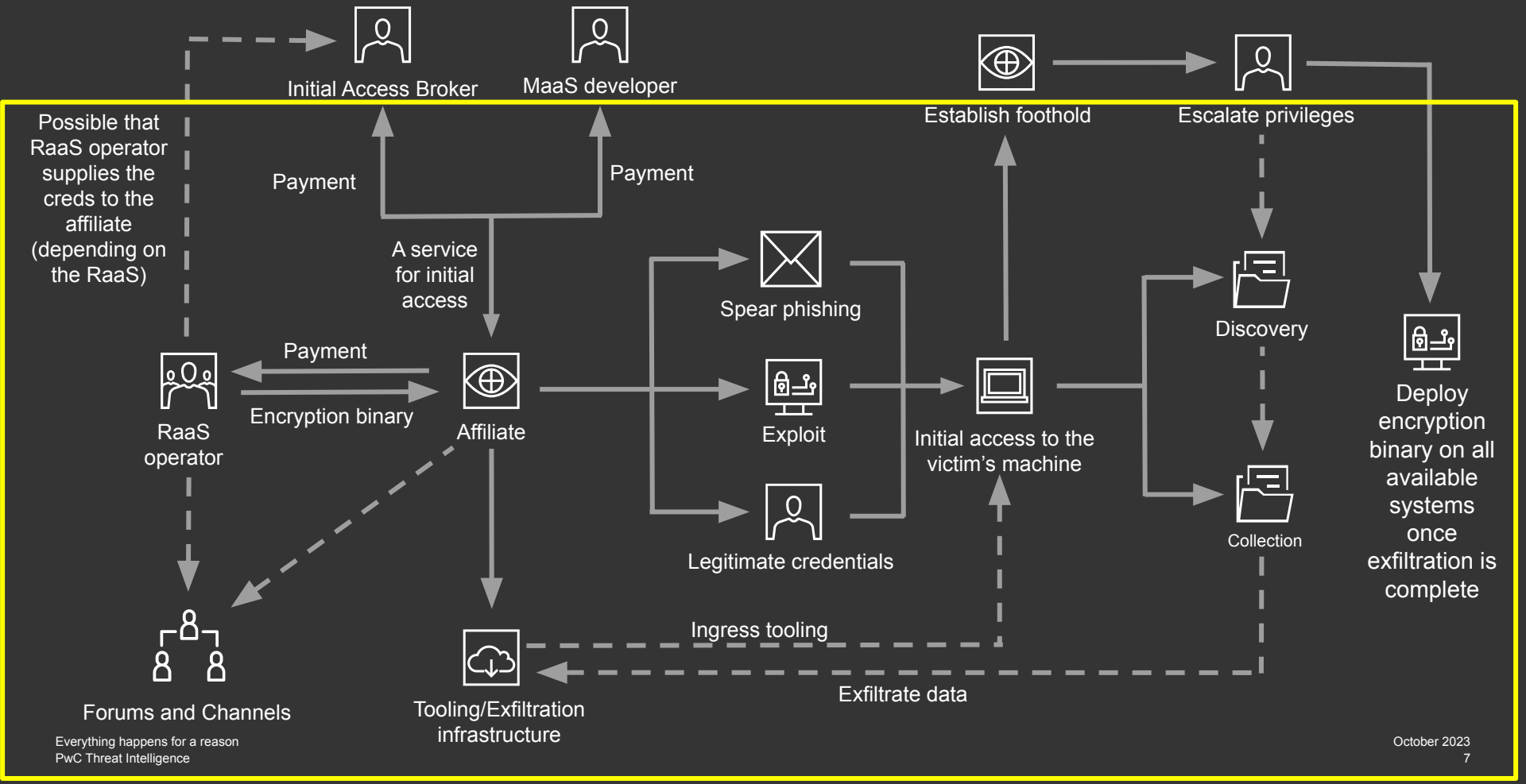
The-Ransomware-as-a service universe

The Exosphere

A top down view of our world (the RaaS ecosystem)

Framing the RaaS Space - perspective




Initial Access Broker
MaaS developer
Establish foothold
Escalate privileges
Possible that RaaS operator supplies the creds to the affiliate (depending on the RaaS)
Payment
Payment
A service for initial access
Spear phishing
Discovery
Payment
Encryption binary
RaaS operator
Affiliate
Exploit
Initial access to the victim's machine
Deploy encryption binary on all available systems once exfiltration is complete
Collection
Legitimate credentials
Ingress tooling
Forums and Channels
Tooling/Exfiltration infrastructure
Exfiltrate data

Things are bad…real bad

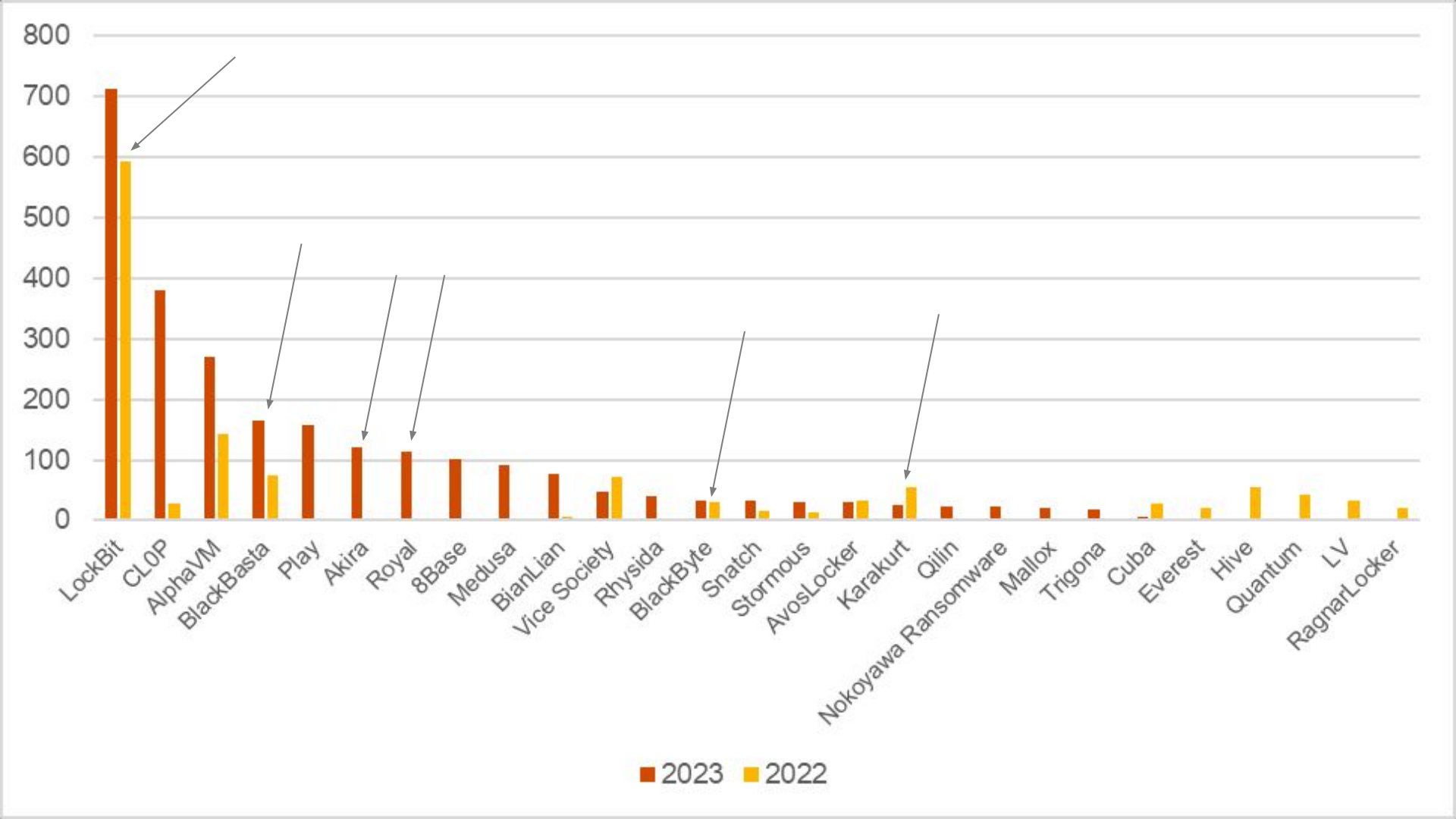
01
Lack of law enforcement presence
Law Enforcement has not been the omnipotent presence it once was to criminals - there is an emboldened sense of untouchability

02
More actors than ever before
The number of consolidated actors in this space has grown by double (depending on how one measures “consolidated”)

2023 RaaS ecosystem

03
Experience is transferred
Even as new programmes are created as older ones are closed down, the experience of the members involved does not disappear

04
Extortion is king
Whilst encryption is still a large part of the RaaS ecosystem, operators are starting to make a turn towards the “data” element being most important

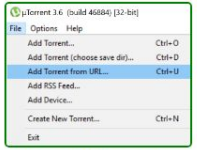

800
700
600
500
400
300
200
100
0
LockBit
CL0P
AlphaVM
BlackBasta
Play
Akira
Royal
8Base
Medusa
BianLian
Vice Society
Rhysida
BlackByte
Snatch
Stormous
AvosLocker
Karakurt
Qilin
Nokoyawa Ransomware
Mallox
Trigona
Cuba
Everest
Hive
Quantum
LV
RagnarLocker
2023
2022

STEP 1

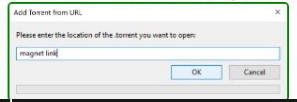
Download and install free **uTorrent** client
(if you don't already have it)
https://www.utorrent.com/downloads/
Or any other **torrent** client that you prefer

STEP 2

Run **uTorrent** and select File > Add Torrent from URL



Paste magnet URL to the Add Torrent from URL dialog box and click **OK** button



COMPANY	LOGO
tjx.com	TJX
synlab.fr	SYNLAB
rhenus.group	RHENUS LOGISTICS
pbinfo.com	pbi
payback.group	PAYBACK GR
mesvision.com	MES Vision
informa.com	informa

ALPHV Blog Collections Api

List of available calls

Route	Descrption	Notice
GET /api/robot/blog/updates/{epoch_millis}	Brief information about articles created or updated since {epoch_millis}	size <= 1000
GET /api/blog/{id}	Article with {id}	
GET /api/blog/attachment?id={id}	Article attachment with {id}	
GET /api/blog/all/{from}/{size}	Articles starting {from} with page {size}	size <= 9
GET /api/blog/brief/{from}/{size}	Brief information about articles starting {from} with page {size}	size <= 1000

Usage

Fetch updates since the beginning and synchronize each article with your database.
After that any subsequent updates call should supply the most recent `updatedDt` from previously synchronized articles + 1 millisecond.

Migration

We have introduced `updatedDt` field to the article, combine it with new updates call to make your crawler updates aware.
As a temporary quick fix you can simply replace the route `/api/blog/all-brief` with `/api/blog/brief/0/1000`.
Also notice that we have limited page size of `/api/blog/all` call to 9 articles.

Example

Download simple crawler implementation written in Python.

```
import datetime
import http
import json
import logging
import time
import urllib.parse
from http import client
from typing import *
```

Basta News

1 2 ... 31 >

BION_2

*Launched in 2014, **BionPharma** was founded by a team of executives and professionals with years of cumulative experience in the generics industry.*
Bionpharma's goals are to develop and commercialize affordable quality generics and building strong and effective partnerships.
Based in Princeton, New Jersey, and with offices in Raleigh, North Carolina
BionPharma is licensed to do business in the United States and is accomplished in the areas of

Published	Visits
0%	14771

Read more

EDVMS

*Als **BSB-Steuerberatungsgesellschaft mbH** betreuen wir seit über 30 Jahren Unternehmen und Privatpersonen. Dabei fokussieren wir uns vor allem auf gewerbliche Steuerberatung, Lohnbuchhaltung sowie die Betreuung von land- und forstwirtschaftlichen Betrieben. Die enge Zusammenarbeit mit unseren Mandanten ist uns besonders wichtig. Durch unseren Verwaltungssitz mitten in Münster sowie 25 Niederlassungen, in Münster, im Münsterland und in*

Published	Visits
0%	13756

Read more

TWINTOWER

*Since its inception in 1993 when it was located in New York City, **Twin Towers Trading** has been setting the standard in the field of live demonstrations. Whether on television or in retail environments, TTT has garnered a well-deserved reputation for presenting unique products with dynamic and engaging presentations referred to as "retailtainment." Millions of people are enthralled yearly, and today, in addition to its corporate headquarters in Manalapan, New Jersey, TTT's offices in Sarasota, Las*

Published	Visits
0%	8648

Read more

VDVEN

***Van der Ven Auto's** is marktleider in milieuvriendelijke autorecycling. En daar zijn we best trots op. Elke sloopauto wordt vakkundig ontdaan van onder meer aanwezige vloeistoffen en accu, en vervolgens nog verder minutieus gestript. In samenwerking met Auto Recycling Nederland (ARN) wordt dankzij deze highend werkwijze een recyclingpercentage behaald van 95% op het totaalgewicht van een demontagevoertuig. Samen streven we naar een groene automotive. Wij betalen een marktconforme prijs*

Published	Visits
0%	8558

Read more

DEUTSCHELEASING

Deutsche Leasing - your partner for asset finance and leasing. Whether you need a new company car – with or without fleet management –, are looking for help in expanding abroad, require machinery with the right insurance, a building with construction management or have a whole IT project to deal with, we can help you!
As the asset finance partner of small and medium-sized businesses, we can offer you investment solutions that are right

Published	Visits
0%	8870

Read more


3 auctions online
47 Companies
RHYSIDA
Token
Enter Token and press Enter key

[AKIRA]

AKIRA

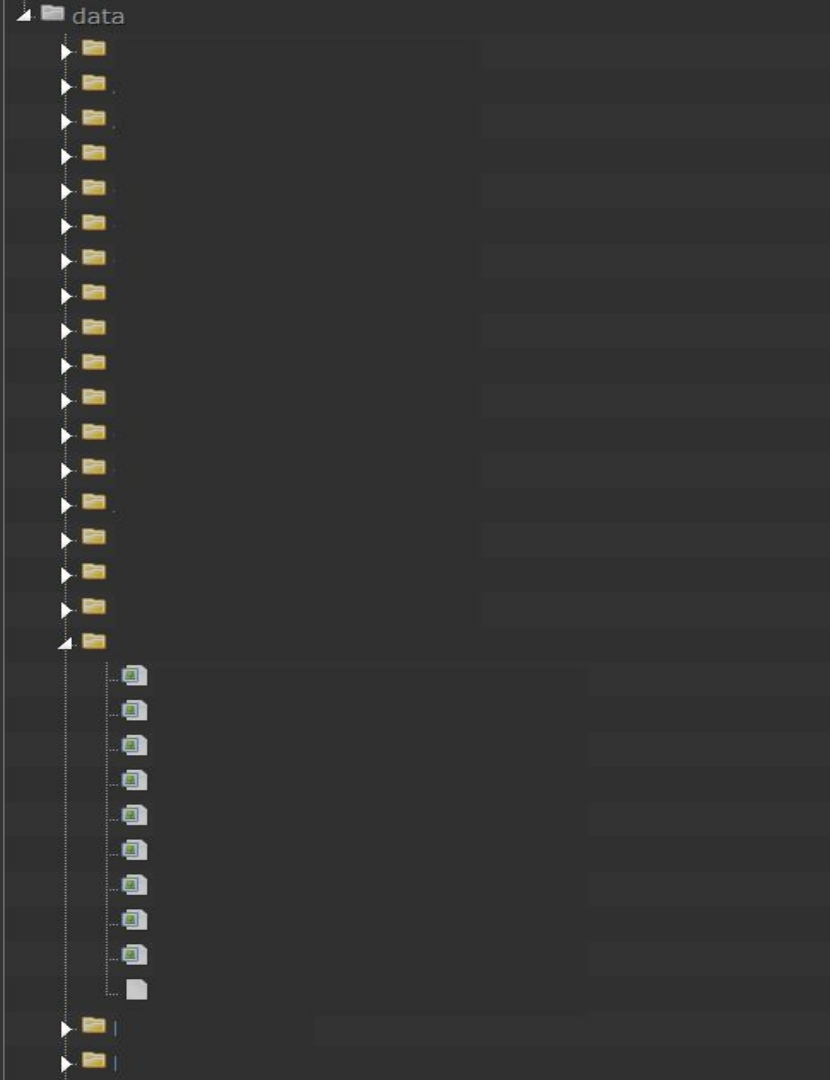
Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
fair price to make it all go away.

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.

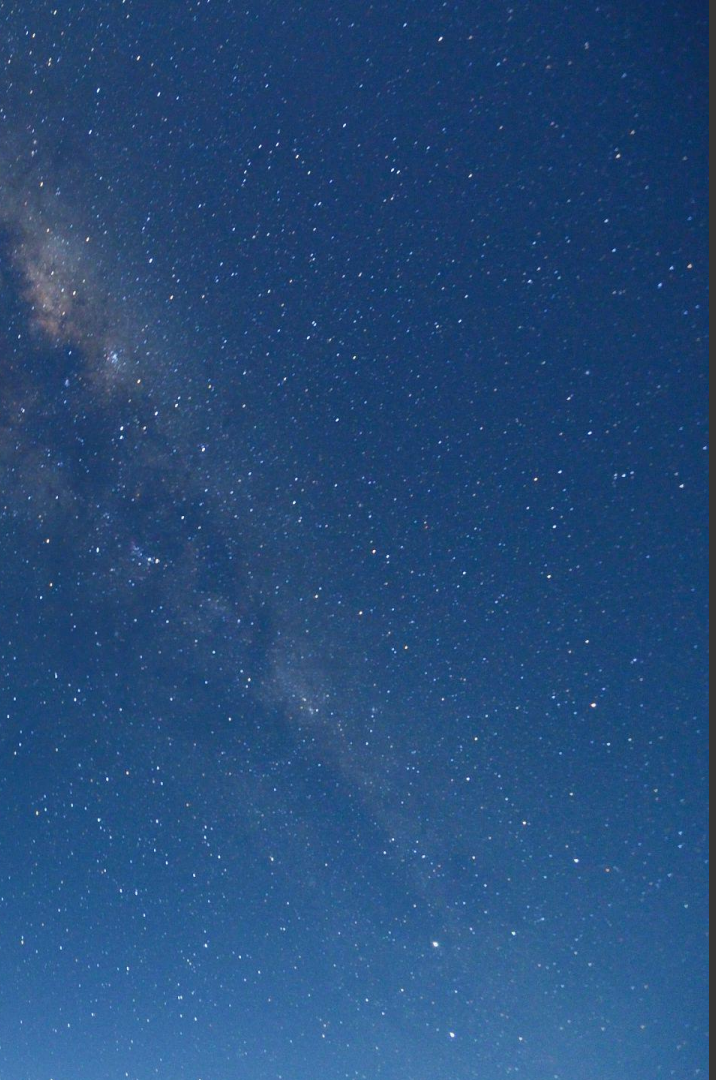
```
guest@akira:~$ help

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:~$
```



Everything happens for a reason
PwC Threat Intelligence

The Thermosphere

RaaS encryption binaries and what we can learn



What makes a RaaS binary?

- RaaS binaries are a product, requiring a modicum of flexibility and ease of use
- The malware is a representation of a developer’s thought process
- Things I watch out for:
  - Flags
  - Filesize delimiters
  - Trial and error “unique” functions
  - Always start with version 1.0 of any binary

```
text:0040304C                 cmp     bx, di
text:0040304F                 jnz     short loc_403056 ; Ukraine
text:00403051
text:00403051 loc_403051:                              ; CODE XREF: LanguageCheck+39
text:00403051                 jmp     one
text:00403056 ; ---------------------------------------------------------------
text:00403056
text:00403056 loc_403056:                              ; CODE XREF: LanguageCheck+3E
text:00403056                 xor     bl, 3Bh          ; Ukraine
text:00403059                 cmp     bx, si
text:0040305C                 jz      short loc_403063
text:0040305E                 cmp     bx, di
text:00403061                 jnz     short loc_403068 ; Belarus
text:00403063
text:00403063 loc_403063:                              ; CODE XREF: LanguageCheck+4B
text:00403063                 jmp     one
text:00403068 ; ---------------------------------------------------------------
text:00403068
text:00403068 loc_403068:                              ; CODE XREF: LanguageCheck+50
text:00403068                 inc     bl               ; Belarus
text:0040306A                 cmp     bx, si
text:0040306D                 jz      short loc_403074
text:0040306F                 cmp     bx, di
text:00403072                 jnz     short loc_403079 ; Tajikistan
text:00403074
text:00403074 loc_403074:                              ; CODE XREF: LanguageCheck+5C
text:00403074                 jmp     one
text:00403079 ; ---------------------------------------------------------------
text:00403079
text:00403079 loc_403079:                              ; CODE XREF: LanguageCheck+61
text:00403079                 xor     bl, 0Bh          ; Tajikistan
text:0040307C                 cmp     bx, si
text:0040307F                 jz      short loc_403086
```

```
loc_49309C:                 ; ulRID
push    220h
push    0                   ; hToken
call    SHTestTokenMembership
cmp     eax, 1
setz    byte ptr [esp+8]
mov     eax, ds:set_flag_logging
cmp     eax, 3
jb      loc_493183
```

```
lea     eax, [esp+8]
mov     ecx, offset aCargoRegistryS ; "/cargo/registry/src/github.com-1ecc6299"...
lea     edx, [esp+0C0h]
mov     [esp+0C0h], eax
mov     dword ptr [esp+0C4h], offset sub_45ED20
mov     eax, ds:dword_6EE078
mov     dword ptr [esp+18h], 3
mov     dword ptr [esp+1Ch], offset aLockerCoreOsWi_5 ; "locker::core::os::windows::privilege_es"...
mov     dword ptr [esp+20h], 2Fh ; '/'
mov     dword ptr [esp+24h], offset off_680360 ; "token_is_admin="
mov     dword ptr [esp+28h], 1
mov     dword ptr [esp+2Ch], 0
```

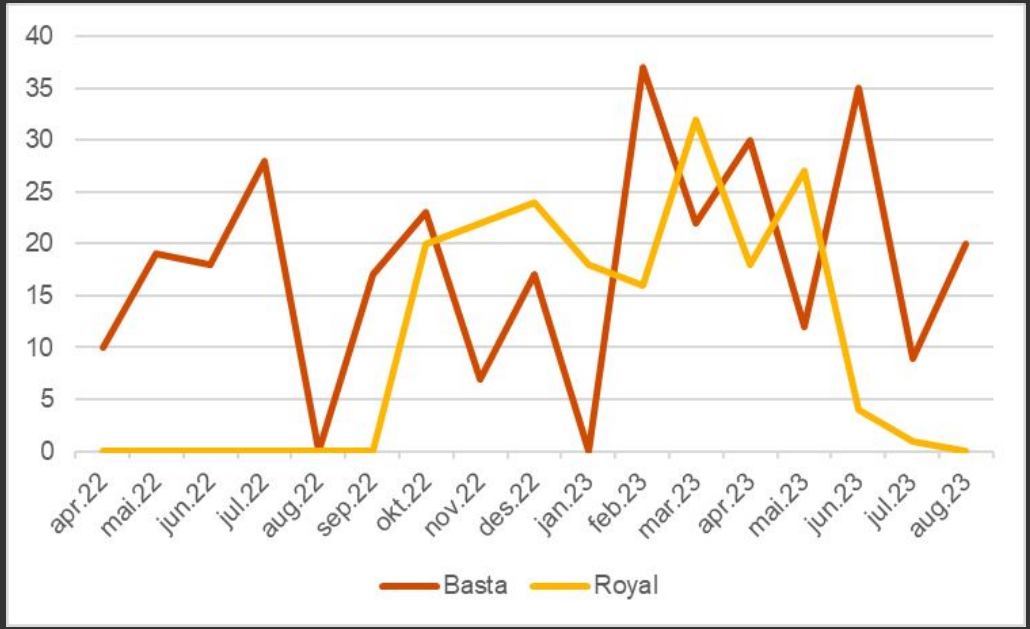
```
; BOOL mw_test_token_memberhsip()
mw_test_token_memberhsip proc near
push    220h                ; ulRID
push    0                   ; hToken
call    SHTestTokenMembership
retn
mw_test_token_memberhsip endp
```

BlackBasta

A consistent middle-of-the-pack RaaS binary

BlackBasta, a fully fledged programme

- BlackBasta first appeared in April of 2022 after Conti collapse
- Conti and Basta highly likely share leadership (at least in 2022)
- Basta leak site victims peak and trough over time, but have averaged 23.5 victims per month since Feb 2023
  - Compare that with:
    - Alphv: 34.9
    - LockBit: 94.4
    - Royal/Blacksuit: 14.0
    - Karakurt: 3.4



Relation between Conti and Basta

B

BlackBasta

Paid registration

0

JOINED	CONTENT COUNT
April 15	1

kurva

byte

K

Paid registration

0

20 posts

Joined

02/15/21 (ID: 114110)

Activity

вирусология / malware

Posted February 15, 2021

Написал данный мембер, обещал делать 200-300 ботов в стуки, по факту сделал только 12 ботов за две недели))) по факту меня больше отвлекал от дела, чем сам делал.

Я ему даже предоплату за в размере $3000. Прошу данного мембера привлечь и сделать возврат. лог ниже:

++++++++++++++

sputnik.0ne@exploit.im: Я вспомнил кто нас знакомил

sputnik.0ne@exploit.im: jedith

sputnik.0ne@exploit.im: придет спишусь с ним.

sputnik.0ne@exploit.im: Файл будет сегодня ?

tramp@*******: да

tramp@*******: фаил готов

tramp@*******: сейчас посчитаю зелененьких и сделаю тебе скрины по ним

tramp@*******: Закинь биток, Я буду молча и покорно ждать. - уже закидывал , результат был нулевой

tramp@*******: https://privatlab.com/s/v/VDb4BOQ5rxiXAmRyY2WJ

tramp@*******: https://privatlab.com/s/d/VDb4BOQ5rxiXAm*****p#delete

tramp@*******: 123123

kurva

byte

K

Paid registration

0

20 posts

Joined

02/15/21 (ID: 114110)

Activity

вирусология / malware

Posted October 19, 2021

куплю акки https://app.avention.com

от $300

[redacted] | 106 SRV | 2VCentr/8EsxI | 18M(avention) | [redacted]

[redacted] | AV | 9.2gb DW |

CONTI | 25.11.21 | адвокаты - нужно по ним блог сделать и ссылку им скинуть

```
  first_char_cmd_line = v3[i];
  if ( *first_char_cmd_line == 45 )
  {
    if ( argc <= i + 1 )
    {
      mw_memmove(v18, first_char_cmd_line);
      LOBYTE(v19) = 2;
      *sub_102AEA0(v18) = byte_1090C84;
      LOBYTE(v19) = 0;
      sub_1029610(v18);
    }
    else
    {
      mw_memmove(v17, first_char_cmd_line);
      LOBYTE(v19) = 1;
      v6 = sub_102AEA0(v17);
      *v6 = *(v16 + v15 + 4);
      LOBYTE(v19) = 0;
      sub_1029610(v17);
      ++i;
    }
    v5 = v16;
  }
}
v7 = mw_memmove(v18, "-forcepath");
LOBYTE(v19) = 3;
sub_1024AA0(v14, &v18, v7);
LOBYTE(v19) = 0;
sub_1029610(v18);
v8 = sub_1036F10(v14, &v15);
if ( unknown_libname_1(v8) )
{
  v9 = sub_102AF20(&v16);
  sub_102A410(dword_10A724C, *(v9 + 24));
  v10 = mw_memmove_maybe(dword_10A9670, "Forced path: ");
  v11 = sub_10226A0(v10, dword_10A724C);
  sub_102A8D0(v11, sub_1024910);
}
mw_make_new_service_fax_restart(v12, v13);
```

```
if ( !StartServiceCtrlDispatcherW(&ServiceStartTable) )
{
  v5 = OpenSCManagerW(0, 0, 0xF003Fu);
  if ( !v5 )
  {
    v5 = GetLastError;
    if ( GetLastError() == 5 )
    {
      v6 = mw_memmove_maybe(dword_10A9670, "Please run program as admin");
    }
    else
    {
      LastError = GetLastError();
      mw_memmove_maybe(dword_10A9670, "Cant open scm manager: ");
      v6 = sub_102A700(LastError);
    }
    sub_102A8D0(v6, sub_1024910);
    _loaddll(0);
  }
  mw_delete_shadow_copies();
  phkResult = &v18;
  mw_maths_and_memmove(&v18, &xmmword_10A71D4);
  v31 = 0;
  v28 = v17;
  mw_maths_and_memmove(v17, &lpServiceName);
  v31 = -1;
  if ( mw_service_stuff(v5, v17[0], v17[1], v17[2], v17[3], v17[4], v17[5],
  {
    SystemMetrics = GetSystemMetrics(SM_CLEANBOOT);
    bootMode = SystemMetrics;
    boot_option_string = mw_memmove_maybe(dword_10A9670, "Boot option: ");
    printedBootMode = makePretty(boot_option_string, bootMode);
    v10 = sub_103D330(&printedBootMode[*(*printedBootMode + 4)], 10);
    sub_103AB20(printedBootMode, v10);
    sub_10376E0(printedBootMode);
    if ( !SystemMetrics )
    {
```

ILSpy

File Home Share View

This PC > Local Disk (C:) > Program Files > ILSpy >

Search ILSpy

Quick access
- Desktop
- Downloads
- Documents
- Program Files
- Program Files (x86)

Name	Date modified	Type	Size
zh-Hans	5/17/2022 6:08 PM	File folder	
AvalonDock.dll.basta	5/17/2022 6:08 PM	BASTA File	472 KB
AvalonDock.Themes.VS2013.dll.basta	5/17/2022 6:08 PM	BASTA File	125 KB
DataGridExtensions.dll.basta	5/17/2022 6:08 PM	BASTA File	112 KB
Iced.dll.basta	5/17/2022 6:11 PM	BASTA File	1,606 KB
ICSharpCode.AvalonEdit.dll.basta	5/17/2022 6:08 PM	BASTA File	605 KB

This PC > Local Disk (C:) > Program Files > ILSpy > zh-Hans

Search zh

nts
Files
Files (x86)
)

Name	Date modified	Type	Size
ILSpy.ReadyToRun.Plugin.resources.dll	5/30/2021 7:04 PM	Application extens...	3 KB
ILSpy.resources.dll	5/30/2021 7:04 PM	Application extens...	31 KB
readme.txt	5/17/2022 4:19 AM	TXT File	1 KB

V2.0 improved features substantially

```
v5 = nNumberOfBytesToRead;
v12 = 0;
v6 = unknown_libname_58(nNumberOfBytesToRead);
Overlapped.hEvent = 0;
Overlapped.8 = a2;
*&Overlapped.Internal = 0i64;
NumberOfBytesRead = 0;
ReadFile(hFile, v6, v5, &NumberOfBytesRead, &Overlapped);
mw_CryptFile(v6, v6, v5);
WriteFile(hFile, v6, v5, &NumberOfBytesRead, &Overlapped);
j_j__free(v6);
nNumberOfBytesToRead += *&a2;
*&v9.Internal = 0i64;
v9.hEvent = 0;
v9.8 = (a4 + 292);
a2.OffsetHigh = 0;
WriteFile(hFile, &nNumberOfBytesToRead, 8u, &a2.OffsetHigh, &v9);
v7 = a5;
*a5 = &CryptoPP::SymmetricCipherFinal<CryptoPP::ConcretePolicyHolder<CryptoPP::
v7[1] = &CryptoPP::SymmetricCipherFinal<CryptoPP::ConcretePolicyHolder<CryptoPP
v7[2] = &CryptoPP::SymmetricCipherFinal<CryptoPP::ConcretePolicyHolder<CryptoPP
v7[8] = &CryptoPP::SymmetricCipherFinal<CryptoPP::ConcretePolicyHolder<CryptoPP
return sub_1000EFA0();
```

```
    sub_100111B0(v25, FileW, &v45);
    highPart = v66;
    if ( v66 <= 0 )
    {
      if ( v66 < 0 || LowPart < 5000 )
      {
        *v57 = 0x4059000000000000i64;
fileOver1GB:
        v86 = 0i64;
        howBigIsFile = 0;
        goto encryptionSections;
      }
      if ( LowPart <= 0x40000000 )
        goto fileOver1GB;
    }
    *v57 = 0x3FF0000000000000i64;
    v32 = sub_1000DB90(v49, &v67);
    mw_encrypt(FileW, 0i64, 5000i64, __SPAIR64__(v66, LowPart), v32);
    highPart = v66;
    howBigIsFile = 5000;
encryptionSections:
    v59 = 0;
    v29 = (__PAIR64__(highPart, LowPart) - howBigIsFile) / 64;
    v63 = HIDWORD(v29);
    v65 = v29;
    *v57 = *v57 * 0.01;
    v30 = (v29 * *v57);
    if ( v30 )
    {
      v62 = (__SPAIR64__(v63, v65) / v30) >> 32;
      *&v57[4] = __SPAIR64__(v63, v65) / v30;
      if ( __SPAIR64__(v63, v65) / v30 )
```

```
C:\Users\Cyber\Desktop>"Basta ransomware October.exe" -encryptionpercent
File encription percent: 0
RELEASE BUILD
ENCRYPTION
```

Flag	Functionality
`-bomb`	Active Directory access only, proliferates malware through wldap32.lib library
`-killservices`	Kill specific services
`-forceprivate` <key>	Allows for the choice of a private key
`-forcepath` <folderpath>	Encrypt files within a specific folder path
`-nomutex`	Skips creation of the mutex
`-disablewhitelist`	Not fully functional; removed from newest version
`-file` <filepath>	Encrypt a specific file
`-threads` <number>	Launch with a specific number of threads

But wait there’s more - ESXi and “3.0”

```
  std::basic_string<>::basic_string(local_48,"-forcepath");
  uVar8 = std::_Hash_bytes(local_48[0],*(local_48[0] + -0x18),0xc70f6907);
  uVar10 = DAT_0062c708;
  uVar7 = uVar8 % DAT_0062c708;
  pplVar2 = *(argList + uVar7 * 8);
  if (pplVar2 != 0x0) {
    plVar9 = *pplVar2;
    uVar6 = plVar9[3];
    do {
      if (uVar6 == uVar8) {
        if ((*(local_48[0] + -0x18) == *(plVar9[1] + -0x18)) &&
           (iVar3 = memcmp(local_48[0],plVar9[1],*(local_48[0] + -0x18)), iVar3 == 0)) {
          if (local_48[0] != &DAT_0062c5d8) goto LAB_004045f9;
          goto LAB_0040459f;
        }
      }
      plVar9 = *plVar9;
    } while ((plVar9 != 0x0) && (uVar6 = plVar9[3], uVar7 == uVar6 % uVar10));
  }
  if (local_48[0] != &DAT_0062c5d8) {
    plVar9 = 0x0;
LAB_004045f9:
    std::basic_string<>::_Rep::_M_dispose(local_48[0] + -0x18);
    if (plVar9 != 0x0) {
LAB_0040459f:
      std::basic_string<>::assign(&forcedPath);
      pbVar5 = std::operator<<(&std::cout,"Forced path: ");
      pbVar5 = std::__ostream_insert<>(pbVar5,forcedPath,*(forcedPath + -0x18));
      std::endl<>(pbVar5);
    }
  }
  AutoBuilderProcess();
  return 0;
}
```

```
  std::basic_string<>::basic_string(local_48,"-forcepath");
  uVar8 = std::_Hash_bytes(local_48[0],*(local_48[0] + -0x18),0xc70f6907);
  uVar10 = DAT_0062c708;
  uVar7 = uVar8 % DAT_0062c708;
  pplVar2 = *(arglist + uVar7 * 8);
  if (pplVar2 != 0x0) {
    plVar9 = *pplVar2;
    uVar6 = plVar9[3];
    do {
      if (uVar6 == uVar8) {
        if ((*(local_48[0] + -0x18) == *(plVar9[1] + -0x18)) &&
           (iVar3 = memcmp(local_48[0],plVar9[1],*(local_48[0] + -0x18)), iVar3 == 0)) {
          if (local_48[0] != &DAT_0062c5d8) goto LAB_004045f9;
          goto LAB_0040459f;
        }
      }
      plVar9 = *plVar9;
    } while ((plVar9 != 0x0) && (uVar6 = plVar9[3], uVar7 == uVar6 % uVar10));
  }
  if (local_48[0] != &DAT_0062c5d8) {
    plVar9 = 0x0;
LAB_004045f9:
    std::basic_string<>::_Rep::_M_dispose(local_48[0] + -0x18);
    if (plVar9 != 0x0) {
LAB_0040459f:
      std::basic_string<>::assign(&forcedPath);
      pbVar5 = std::operator<<(&std::cout,"Forced path: ");
      pbVar5 = std::__ostream_insert<>(pbVar5,forcedPath,*(forcedPath + -0x18));
      std::endl<>(pbVar5);
    }
  }
  AutoBuilderProcess();
  return 0;
}
```

```
  first_char_cmd_line = v3[i];
  if ( *first_char_cmd_line == 45 )
  {
    if ( argc <= i + 1 )
    {
      mw_memmove(v18, first_char_cmd_line);
      LOBYTE(v19) = 2;
      *sub_102AEA0(v18) = byte_1090C84;
      LOBYTE(v19) = 0;
      sub_1029610(v18);
    }
    else
    {
      mw_memmove(v17, first_char_cmd_line);
      LOBYTE(v19) = 1;
      v6 = sub_102AEA0(v17);
      *v6 = *(v16 + v15 + 4);
      LOBYTE(v19) = 0;
      sub_1029610(v17);
      ++i;
    }
    v3 = v16;
  }
}
v7 = mw_memmove(v18, "-forcepath");
LOBYTE(v19) = 3;
sub_1024AA0(v14, &v16, v7);
LOBYTE(v19) = 0;
sub_1029610(v18);
v8 = sub_1036F10(v14, &v15);
if ( unknown_libname_1(v8) )
{
  v9 = sub_102AF20(&v16);
  sub_102A410(dword_10A724C, *(v9 + 24));
  v10 = mw_memmove_maybe(dword_10A9670, "Forced path: ");
  v11 = sub_10226A0(v10, dword_10A724C);
  sub_102A8D0(v11, sub_1024910);
}
mw_make_new_service_fax_restart(v12, v13);
```

```
TickCount = GetTickCount();
mw_args(v26, v27);
mw_mutex();
sub_40B760(L"Checking arguments\n", v26);
if ( dword_4C0254 )
{
  HIDWORD(v25) = &dword_4C0244;
  if ( dword_4C5BF0 == dword_4C5BF4 )
  {
    sub_401EC0(dword_4C5BF0, HIDWORD(v25));
  }
  else
  {
    mw_confirmICOExists(HIDWORD(v25));
    dword_4C5BF0 += 24;
  }
}
else
{
  v0 = sub_407950(0x20u);
  v39 = 21;
  v40 = 31;
  strcpy(v0, "c:/users/public/music");
  Block = v0;
  v41 = 1;
  sub_403250(v26, v27);
  sub_408EF0(&Src, Block, Block + 21);
  sub_403FD0(v32);
  v1 = dword_4C5BF0;
  LOBYTE(v41) = 2;
  if ( dword_4C5BF0 == dword_4C5BF4 )
  {
```

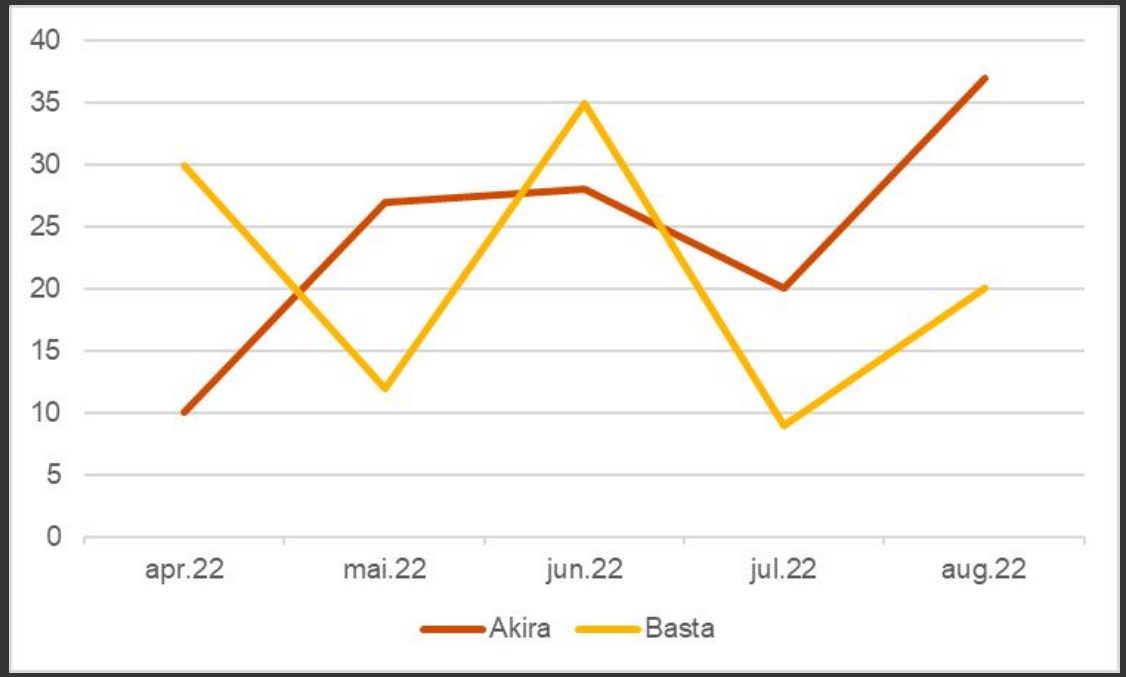
```
tickCount = GetTickCount();
mw_loadArgs();
mw_CreateMutex();
mw_createICOTemp(Src);
mw_confirmICOExists(&v37, Src);
mw_SetICOAsDefaultIcon(v37, v38, v39, v40, v41, HIDWORD(v41));
sub_1000BDD0(L"Checking arguments\n");
if ( dword_100C2254 )
{
  HIDWORD(v41) = &dword_100C2244;
  if ( dword_100C7D60 == dword_100C7D64 )
  {
    sub_10001EF0(&::Src, dword_100C7D60, HIDWORD(v41));
  }
  else
  {
    mw_confirmICOExists(dword_100C7D60, HIDWORD(v41));
    dword_100C7D60 += 24;
  }
}
else
{
  mw_GetVolumeInfo(&v63);
  v0 = v63;
  v1 = 0;
  if ( (v64 - v63) / 24 )
  {
    v2 = 0;
    do
    {
      HIDWORD(v41) = &v0[v2];
      if ( dword_100C7D60 == dword_100C7D64 )
      {
        sub_10001EF0(&::Src, dword_100C7D60, HIDWORD(v41));
      }
      else
      {
```

Akira

The new darling child of the RaaS landscape

Akira – too successful to be new?

- Akira first appeared in April of 2023 seemingly out of nowhere
- Akira highly likely makes use of Conti developer/leadership
- Akira has become a “consolidated” ransomware programme with a potential political leaning
- Akira has reactive codebase developers, altering encryption mechanisms once it is proven to be flawed.



Affiliate Management and political leanings

[AKIRA]

```
guest@akira:~$ news

+------------+
| date       |
+------------+
| 2023-06-22 |
```

[AKIRA]

```
guest@akira:~$ news
```

date	title	content
2023-09-29	Vertical Development	Vertical Development has helped companies design parts catalogs for over 30 years, both in paper and digital formats. Numerous contracts and agreement, NDAs, confidential docs and employee information of the company will be available soon.
2023-09-27	Civic San Diego	CCDC is the public, non-profit corporation created by the City of San Diego to staff and implement Downtown redevelopment projects and programs. Almost 200Gb of files. Confidential documents, personal information etc. Uploading soon.
2023-09-27	The Polish American Association	Have you ever been interested in the US-Poland friendship details ? The Polish American Association is ready to share it's internal live secrets. 185GB SQL will be available for downloading soon. Who cares of immigrants, right?

Akira’s codebase links to Conti

```
_BYTE *__fastcall mw_stringDecrypt(_BYTE *string)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v1 = string + 1;
  if ( *string )
    return v1;
  string_plus_1 = string + 1;
  v3 = 16i64;
  do
  {
    v4 = *string_plus_1++;
    *(string_plus_1 - 1) = (7 * (v4 - 47) % 127 + 127) % 127;
    --v3;
  }
  while ( v3 );
```

Akira’s codebase links to Conti

```
  string[16] = 7;
  string[17] = 29;
  string[18] = 0;
  for ( i = 0i64; i < 0x12; ++i )
    string[i] = (41 * (string[i] - 29) % 127 + 127) % 127;
  if ( !sub_180001B10(qword_180007018, dword_180003004, string) )
    break;
  ++v0;
}
while ( v0 < dword_180007014 );
return 1i64;
```

IcedID

Akira's codebase links to Conti

Trickbot

```
while ( 1 )
{
  v67[3] = 0;
  qmemcpy(string, "}\nKKy_@tu*5@J\adt", 16);
  string[16] = 22;
  string[17] = 12;
  string[18] = 43;
  string[19] = 1;
  qmemcpy(v69, "dL", sizeof(v69));
  for ( i = 0i64; i < 0x16; ++i )
  {
    v5 = 12 * (string[i] - 76) % 127 + 127;
    string[i] = v5
              - 127 * (((((2164392969i64 * v5) >> 32) & 0x80000000) != 0i64) + (((2164392969i64 * v5) >> 32) >> 6));
  }
  v6 = sub_18001753C(v83, string, 21i64);
  v7 = sub_1800175D0(v6);
  v8 = sub_1800175D0(a2);
  v9 = sub_1800113F4();
  v10 = v9(v8, v7);
  sub_1800175AC(v83);
  if ( v10 )
    break;
  alsoString[2] = 0;
  alsoString[3] = 11;
  qmemcpy(&alsoString[4], "/IQ/Ic", 6);
  for ( j = 0i64; j < 7; ++j )
  {
    v12 = 63 * (99 - alsoString[j + 3]) % 127 + 127;
    alsoString[j + 3] = v12
                      - 127
                      * (((((2164392969i64 * v12) >> 32) & 0x80000000) != 0i64) + (((2164392969i64 * v12) >> 32) >> 6));
  }
```

Akira's codebase links to Conti

Conti

```
string[11] = 13;
string[12] = 13;
string[13] = 13;
for ( i = 0i64; i < 0xE; ++i )
{
  v11 = (unsigned int)(unsigned __int8)string[i] - 13;
  string[i] = (15 * (int)v11 % 127 + 127) % 127;
}
v12 = *(_QWORD *)v7;
v13 = (unsigned int (__fastcall *)(__int64, char *))sub_180004B40(v11, 15i64, 3446876362i64, 81i64);
if ( v13(v12, string) )
{
  v27[7] = 0;
  qmemcpy(v28, "%%%%%%", 6);
  for ( j = 0i64; j < 6; ++j )
  {
    alsoString = (unsigned int)((35 * (36 - (unsigned __int8)v28[j]) % 127 + 127) % 127);
    v28[j] = alsoString;
  }
```

Akira’s codebase links to Conti

```
string[16] = 7;
string[17] = 29;
string[18] = 0;
for ( i = 0i64; i < 0x12; ++i )
  string[i] = (41 * ((unsigned __int8)string[i] - 29) % 127 + 127) % 127;
if ( !(unsigned int)sub_180001B10(qword_180007018, (unsigned int)dword_180003004, string) )
  break;
```

Bazar

Akira has proven a malleable developer

```
if ( !CryptAcquireContextW(&phProv, 0i64, L"Microsoft Enhanced RSA and AES Cryptographic Provide
  goto LABEL_101;
if ( !CryptStringToBinaryA(pszString, 0, CRYPT_STRING_BASE64HEADER, pbBinary, &pcbBinary, 0i64,
  goto LABEL_101;
v34 = X509_ASN_ENCODING;
if ( !CryptDecodeObjectEx(
        X509_ASN_ENCODING,
        8,
        pbBinary,
        pcbBinary,
        CRYPT_DECODE_ALLOC_FLAG,
        0i64,
        &pInfo,
        &pcbStructInfo)
  || !CryptImportPublicKeyInfo(phProv, X509_ASN
  || (v35 = phProv, CGPGenKey = phKey, !phProv)
  || !phKey
  || (memset(v136, 0, 0x234ui64), !CryptGenRanc
  || !CryptGenRandom(v35, 8u, v136)
  || (*&v136[40] = *&v136[8],
      *&v136[56] = *&v136[24],
      *&v136[72] = *v136,
      pdwDataLen = 40,
      !CryptEncrypt(CGPGenKey, 0i64, X509_ASN_E
{
```

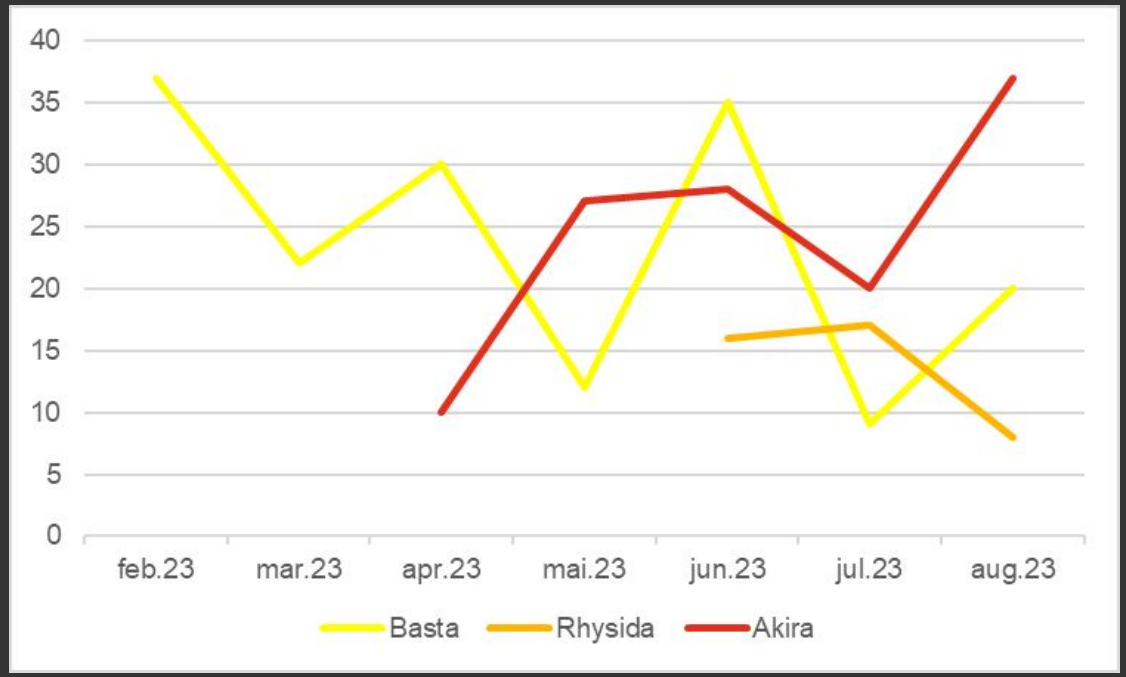
```
memset(a1->key_0x20C, 0, 0x20Cui64);
CPAcquireContext = a1->field_69;
v131 = CPAcquireContext;
if ( !CPAcquireContext )
{
  if ( *p_encryptSize )
    (**p_memset_address)(&a1->field_80);
  v10 = &a1->field_7C;
  goto LABEL_301;
}
if ( !CryptGenRandom(*CPAcquireContext, 32u, &a1->_0)
  || !CryptGenRandom(*v131, 8u, &a1->_0)  // 40 bytes total
  || (v130 = *&a1->field_148,
      *a1->key_0x20C = *&a1->_0,
      a1->field_168 = v130,
      a1->field_178 = a1->_0,
      a1->_40 = 40,
      !CryptEncrypt(v131[1], 0i64, 1, 0, a1->key_0x20C, &a1->_40, 0x20Cu)) )
```

Rhysida

A good example of a zero-to-ugh story

Rhysida - the reality of the 2023 landscape

- A private RaaS appearing in May 2023
- Has observed success based on the leak site numbers
- The leak site itself displays victim data in a user friendly format; but bulk collection is not immediately possible.
- The codebase is not advanced, but proof that one merely needs a functional encryptor.



```
*a3->mallocd_mem_also = 0;
a3->delete_sef = 1;
a3->no_wallpaper = 1;
a3->md5 = 0;
a3->scheduled_task = 0;
strcpy(v6, "-d");
strcpy(&v5[6], "-sr");
strcpy(v5, "-nobg");
strcpy(&v4[3], "-md5");
strcpy(v4, "-S");
for ( *&v6[7] = 0; ; ++*&v6[7] )
{
  result = *&v6[7];
  if ( *&v6[7] >= argc )
    break;
  if ( *&v6[7] )
  {
    if ( !strcmp(argv[*&v6[7]], v6) )
    {
      ++*&v6[7];
      if ( argv[*&v6[7]] )
      {
        strcpy(a3->mallocd_mem_also, argv[*&v6[7]]);
        *&v6[3] = 0;
        while ( *&v6[3] < strlen(a3->mallocd_mem_also) )
        {
          if ( *(a3->mallocd_mem_also + *&v6[3]) == '\\' )
            *(a3->mallocd_mem_also + *&v6[3]) = 47;
          ++*&v6[3];
        }
        if ( *(a3->mallocd_mem_also + strlen(a3->mallocd_mem_also) - 1) == '/' )
          *(a3->mallocd_mem_also + strlen(a3->mallocd_mem_also) - 1) = 0;
      }
```

Very few customisable options

```
*a3->mallocd_mem_also = 0;
a3->delete_sef = 1;
a3->no_wallpaper = 1;
a3->md5 = 0;
a3->scheduled_task = 0;
strcpy(v6, "-d");
strcpy(&v5[6], "-sr");
strcpy(v5, "-nobg");
strcpy(&v4[3], "-md5");
strcpy(v4, "-S");
for ( *&v6[7] = 0; ; ++*&v6[7] )
{
  result = *&v6[7];
  if ( *&v6[7] >= argc )
    break;
  if ( *&v6[7] )
  {
    if ( !strcmp(argv[*&v6[7]], v6) )
    {
      ++*&v6[7];
      if ( argv[*&v6[7]] )
      {
        strcpy(a3->mallocd_mem_also, argv[*&v6[7]]);
        *&v6[3] = 0;
        while ( *&v6[3] < strlen(a3->mallocd_mem_also) )
        {
          if ( *(a3->mallocd_mem_also + *&v6[3]) == '\\' )
            *(a3->mallocd_mem_also + *&v6[3]) = 47;
          ++*&v6[3];
        }
        if ( *(a3->mallocd_mem_also + strlen(a3->mallocd_mem_also) - 1) == '/' )
          *(a3->mallocd_mem_also + strlen(a3->mallocd_mem_also) - 1) = 0;
      }
```

Flags set in a very “1.0” way

The Troposphere

How the affiliates are behaving and what we can do

Affiliate TTPs - the good, the bad, and the worrying

Depending on the initial access vector, execution is being conducted through Domain/Local Account (i.e. scheduled tasks and modified GPOs).

This phase is often completed with the help of tooling; often offensive security tools (several entities will use their own tooling, but there is a lot of opportunity for detection here)

Initial access methods are becoming oriented away from phishing (sorry vishing stans). 0days, externally facing vulns, legitimate credentials, third party compromise, and information stealers

Persistence is often achieved through legitimate accounts - either previously established or created during this phase.

This phase is often completed with the help of tooling; often often offensive security tools (several entities will use their own tooling, but there is a lot of opportunity for detection here)

Initial Access

Externally facing technology

- Open ports should be closed
- Multi factor authentication implemented across all logins
- Automated and continuous vulnerability scanning of internet-facing infrastructure

Exploit

- Oof, this one is tricky
- Patching at the instruction of the relevant vendor
- The following phases are easier to defend

Special mention to Phishing/Vishing:

- Cybersecurity will always be a human problem
- It is the responsibility of the employer to ensure protocol is enforced, and that a sense of skepticism is given to all unknown requests

Legitimate credentials

- Strong/phishing resistant MFA to be implemented across all logins (including third parties)
- Monitoring for anomalous account logins
- Reducing session time
- Moving to passwordless authentication

Initial Access

Special mention to Phishing/Vishing:

- Cybersecurity will always be a human problem
- It is the responsibility of the employer to ensure protocol is enforced, and that a sense of skepticism is given to all unknown requests

Execution

Scheduled task/service

- EDR tools can monitor for newly created users that initiate a scheduled task
- Detection in place for users creating scheduled tasks on remote systems

Command and Scripting Interpreter

- Antivirus goes a long way to detecting malicious bad
- Tamper protection in place to prevent the switching off of anti-virus
- Restrictions in place for tools like PowerShell or certain file extensions from downloading files / WDAC and SmartScreen

Valid Accounts

- New accounts performing certain action - such as interacting with newly created files or “known bad registries” - should be flagged

Discovery/Credential Access

Account Discovery

- Known offensive security tools should be denied on-disk for User Groups
- Monitoring for access to known Password directories/registry hives with EDR

Brute Force

- Ensure that there is a limited number of password attempts for logins, especially services that by default have set credentials
- Monitoring for anomalous account logins
- Long, complex passwords on all accounts

OS Credential Dumping

- Files used as password stores - especially in Cloud environments - must be either encrypted or removed entirely (secret scanning)
- Implementation of Privileged Access Workstations, or PAM tools that provide session management
- Removing local admin privileges from standard users, and implementing tiering in AD

Command & Control

Application Layer Protocol

- Outbound internet access for all servers restricted to an allow list by firewalls / web filtering tooling
- Alerts in place for known offensive exfiltration tools (e.g. WinSCP, RClone).

Data encoding

- Base64 encoded Headers to be flagged as severe
- Network detection in place for “common” malware traffic
- Significant one-way traffic flagged as severe

Ransomware Protection Framework

Reduce your attack surface

Prevent Internet-facing weaknesses

- Automated and continuous vulnerability scanning of Internet-facing infrastructure with effective remediation processes
- Multi-factor authentication configured for all email and remote access accounts

Reduce the threat of phishing

- Web security tooling that restricts content and blocks malicious downloads
- Email tooling that restricts attachments and scans for malicious content
- Hardened endpoints to restrict execution of untrusted scripts and executables
- Restrictions that prevent the execution of untrusted Microsoft Office macros
- Prevent standard day-to-day accounts from having local administrator privileges

Reduce attackers' dwell time

- Endpoint detection and response tooling deployed on workstations and servers
- Continuous monitoring capability that rapidly investigates and contains alerts, including out of hours
- Regular 'red teaming' to validate detection and response capabilities
- Centralised log collection and rules configured to detect common techniques used by ransomware groups
- Security tooling (or detection rules) that monitors for anomalous use of privilege accounts
- Antivirus tooling that automatically remediates 'commodity malware' and is monitored for critical detections
- Ability to remotely perform forensics analysis and take containment actions

Limit blast radius of unauthorised access

Increase the cost of escalating privileges

- Controls to restrict and secure the use of accounts with domain administrator privileges
- Internal vulnerability scanning with effective remediation processes
- Proactive hunting and remediation of Active Directory hygiene issues

- Host-based firewalls on workations configured by default to block inbound traffic
- Network segmentation that restricts lateral movement from workstations
- Outbound internet access for all servers should be restricted to an allow list by firewalls / web filtering tooling
- Cloud-based SaaS services for employee email and file-sharing

Prepare to respond to and recover

- Endpoint protection tooling that detects and blocks ransomware behaviours
- Exercised cyber incident response and crisis management plans
- Playbooks for rapidly isolating parts of network and managing the impact

IT Resilience (for ransomware failure mode)

- Validated backups with tested recovery of infrastructure (e.g. Active Directory)
- Verified protection of backups to prevent corruption or deletion by an attacker
- Prioritised recovery plans for key business systems and applications
- Playbooks for mass rebuilding of endpoints and servers at scale

Thank you