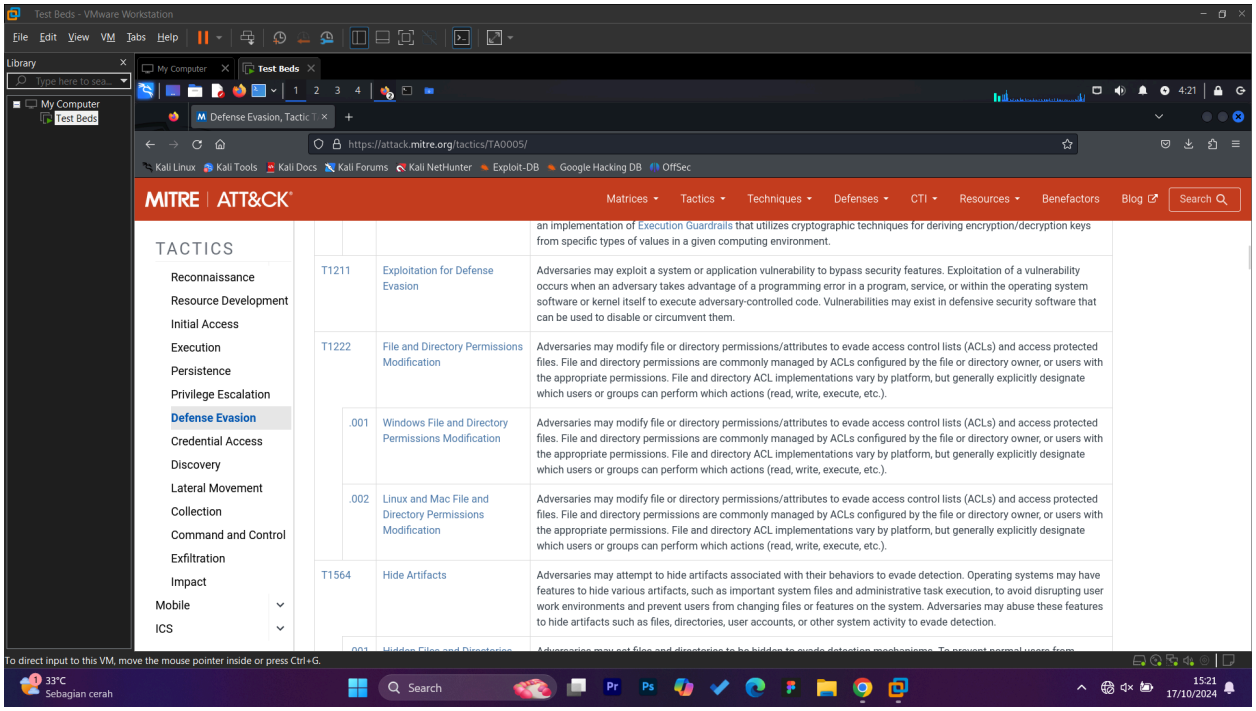
```
┌──(kalitestbeds㉿kalitestbed)-[/home/kalitestbeds]
└─PS> cd Downloads

┌──(kalitestbeds㉿kalitestbed)-[/home/kalitestbeds/Downloads]
└─PS> unzip capa-v7.4.0-linux.zip
Archive:  capa-v7.4.0-linux.zip
  inflating: capa
```

```
┌──(kalitestbeds㉿kalitestbed)-[/home/kalitestbeds/Downloads]
└─PS> chmod +x capa

┌──(kalitestbeds㉿kalitestbed)-[/home/kalitestbeds/Downloads]
└─PS> ./capa
main.py:1109: DeprecationWarning: This is the last capa version supporting Py
thon 3.8 and 3.9.
usage: capa [-h] [--version] [-v] [-vv] [-d] [-q]
            [--color {auto,always,never}]
            [-f {auto,pe,dotnet,elf,sc32,sc64,cape,drakvuf,vmray,freeze,binex
port2}]
            [-b {auto,vivisect,ida,pefile,binja,dotnet,binexport2,freeze,cape
,drakvuf,vmray}]
            [--restrict-to-functions RESTRICT_TO_FUNCTIONS]
            [--restrict-to-processes RESTRICT_TO_PROCESSES]
            [--os {auto,linux,macos,windows}] [-r RULES] [-s SIGNATURES]
            [-t TAG] [-j]
            input_file
capa: error: the following arguments are required: input_file
```



```
┌──(kalitestbeds㉿kalitestbed)-[/home/kalitestbeds/Downloads]
└─PS> ./capa ./ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41
aa.exe
main.py:1109: DeprecationWarning: This is the last capa version supporting Py
thon 3.8 and 3.9.
```

md5	84c82835a5d21bbcf75a61706d8ab549
sha1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
sha256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
analysis	static
os	windows
format	pe
arch	i386
path	/home/kalitestbeds/Downloads/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	File and Directory Permissions Modification [T1222]
	Obfuscated Files or Information [T1027]
DISCOVERY	File and Directory Discovery [T1083]
	Query Registry [T1012]
	System Information Discovery [T1082]
EXECUTION	Shared Modules [T1129]
	System Services::Service Execution [T1569.002]
PERSISTENCE	Create or Modify System Process::Windows Service [T1543.003]

MBC Objective	MBC Behavior
CRYPTOGRAPHY	Encrypt Data::AES [C0027.001]
	Encrypt Data::RC4 [C0027.009]
	Encryption Key::RC4 KSA [C0028.002]
	Generate Pseudo-random Sequence [C0021]
DATA	Checksum::CRC32 [C0032.001]
	Compression Library [C0060]
	Encode Data::XOR [C0026.002]
DEFENSE EVASION	Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02]
	Obfuscated Files or Information::Encryption-Standard Algorithm [E1027.m05]
DISCOVERY	Code Discovery::Enumerate PE Sections [B0046.001]
	File and Directory Discovery [E1083]
	System Information Discovery [E1082]
FILE SYSTEM	Copy File [C0045]
	Create Directory [C0046]
	Get File Attributes [C0049]
	Read File [C0051]

Capability	Namespace
hash data with CRC32 (2 matches)	data-manipulation/checksum/crc32
encode data using XOR (15 matches)	data-manipulation/encoding/xor
encrypt data using AES (5 matches)	data-manipulation/encryption/aes
reference AES constants (5 matches)	data-manipulation/encryption/aes
encrypt data using RC4 KSA (3 matches)	data-manipulation/encryption/rc4
generate random numbers using the Delphi LCG	data-manipulation/prng/lcg
extract resource via kernel32 functions	executable/resource
get common file path (3 matches)	host-interaction/file-system
set current directory (3 matches)	host-interaction/file-system
copy file	host-interaction/file-system/copy
create directory (2 matches)	host-interaction/file-system/create
check if file exists (4 matches)	host-interaction/file-system/exists
get file attributes (6 matches)	host-interaction/file-system/meta
get file size (2 matches)	host-interaction/file-system/meta
set file attributes	host-interaction/file-system/meta
read file on Windows (3 matches)	host-interaction/file-system/read
write file on Windows (2 matches)	host-interaction/file-system/write
check mutex	host-interaction/mutex
get hostname	host-interaction/os/hostname
create process on Windows	host-interaction/process/create
terminate process	host-interaction/process/terminate
query or enumerate registry value	host-interaction/registry
set registry value	host-interaction/registry/create
create service	host-interaction/service/create
start service	host-interaction/service/start
link many functions at runtime (2 matches)	linking/runtime-linking
linked against ZLIB	linking/static/zlib
enumerate PE sections (2 matches)	load-code/pe
parse PE header	load-code/pe
persist via Windows service	persistence/service

```
┌──(kalitestbeds㉿kalitestbed)-[/home/kalitestbeds/Downloads]
└─PS>
```

Hasil Analisis Malware

Att&ck Tactic

Defense Evasion
Discovery
Execution
Persistence

Att&ck Technique

T1222 File and Directory Permissions Modification
T1207 Obfuscated Files or Information
T1083 File and Directory Discovery
T1012 Query Registry
T1082 System Information Discovery
T1129 Shared Modules
T1569.002 System Services
T1543.003 Create or Modify System Process

Kasus T1222 merujuk ke serangan yang menyerang aspek Defense Evasion yang memodifikasi File & Directory Permission.
Dikutip dari website mitre att&ck

Musuh bisa memodifikasi izin/atribut file atau direktori untuk menghindari daftar kontrol akses (ACL) dan mengakses file yang dilindungi. Izin file dan direktori biasanya dikelola oleh ACL yang dikonfigurasi oleh pemilik file atau direktori, atau pengguna dengan izin yang sesuai. Implementasi ACL file dan direktori berbeda-beda di setiap platform, namun umumnya secara eksplisit menetapkan pengguna atau grup mana yang dapat melakukan tindakan apa (baca, tulis, eksekusi, dll.).

Kasus T1027 masih merujuk pada Defense Evasion yakni Obfuscated Files or Information
Musuh Informasi mungkin berusaha membuat file yang dapat dieksekusi atau file yang sulit ditemukan atau dianalisis dengan mengenkripsi, menyandikan, atau mengaburkan isinya di sistem atau saat transit. Ini adalah perilaku umum yang dapat digunakan di berbagai platform dan jaringan untuk menghindari pertahanan.

Kasus T1083 merujuk ke serangan yang menyerang aspek Discovery yang memodifikasi File and Directory Discovery dimana Musuh dapat menghitung file dan direktori atau dapat mencari di lokasi tertentu pada host atau berbagi jaringan untuk informasi tertentu dalam sistem file.

Musuh dapat menggunakan informasi dari Penemuan File dan Direktori selama penemuan otomatis untuk membentuk perilaku lanjutan, termasuk apakah musuh sepenuhnya menginfeksi target dan/atau mencoba tindakan tertentu.

Kasus T1012 masih merujuk pada aspek Discovery, Query Registry Musuh dapat berinteraksi dengan Windows Registry untuk mengumpulkan informasi tentang sistem, konfigurasi, dan perangkat lunak yang diinstal.

Kasus T1082 masih merujuk pada aspek Discovery, System Information Discovery, Musuh dapat mencoba mendapatkan informasi terperinci tentang sistem operasi dan perangkat keras, termasuk versi, tambalan, perbaikan terbaru, paket layanan, dan arsitektur. Musuh dapat menggunakan informasi dari Penemuan Informasi Sistem selama penemuan otomatis untuk membentuk perilaku lanjutan, termasuk apakah musuh sepenuhnya menginfeksi target dan/atau mencoba tindakan tertentu.

Kasus T1129 merujuk pada Execution, Shared Modules Musuh dapat mengeksekusi muatan berbahaya melalui pemuatan modul bersama. Modul bersama adalah file yang dapat dieksekusi yang dimuat ke dalam proses untuk menyediakan akses ke kode yang dapat digunakan kembali, seperti fungsi khusus tertentu atau memanggil fungsi API OS (misalnya, Native API).

Kasus T1569.002 masih merujuk pada Execution, System Services Musuh dapat menyalahgunakan layanan sistem atau daemon untuk menjalankan perintah atau program. Musuh dapat mengeksekusi konten berbahaya dengan berinteraksi atau membuat layanan baik secara lokal maupun jarak jauh. Banyak layanan yang diatur untuk berjalan saat boot, yang dapat membantu dalam mencapai persistensi (Membuat atau Memodifikasi Proses Sistem), tetapi musuh juga dapat menyalahgunakan layanan untuk eksekusi satu kali atau sementara.

Dan Service Execution pada poin 002, Musuh dapat menyalahgunakan manajer kontrol layanan Windows untuk menjalankan perintah atau muatan berbahaya. Manajer kontrol layanan Windows (services.exe) adalah antarmuka untuk mengelola dan memanipulasi layanan. Manajer kontrol layanan dapat diakses oleh pengguna melalui komponen GUI serta utilitas sistem seperti sc.exe dan Net.

Kasus T1543.003 merujuk pada Persistence. Merujuk pada Create or Modify System Process Musuh dapat membuat atau memodifikasi proses tingkat sistem untuk berulang kali mengeksekusi muatan berbahaya sebagai bagian dari persistensi. Ketika sistem operasi melakukan boot, mereka dapat memulai proses yang menjalankan fungsi sistem latar belakang. Di Windows dan Linux, proses sistem ini disebut sebagai layanan. Di macOS, proses peluncuran yang dikenal sebagai Launch Daemon dan Launch Agent dijalankan untuk menyelesaikan inisialisasi sistem dan memuat parameter spesifik pengguna.

Pada poin 003 Windows Service, Musuh dapat membuat atau memodifikasi layanan Windows untuk berulang kali mengeksekusi muatan berbahaya sebagai bagian dari kegigihan. Ketika Windows melakukan booting, ia memulai program atau aplikasi yang disebut layanan yang menjalankan fungsi sistem latar belakang. Informasi konfigurasi layanan Windows, termasuk jalur file ke program/perintah yang dapat dieksekusi atau program pemulihan layanan, disimpan di Windows Registry.