Ransome

Related resources

minifilter

ransom analysis1

unveil : protection

hardware protection

hardware protection

Attack Defense Paradigm

I attack your computer based on your OS source code

I protect my computer based on your attack source code

...

Never end

`Testing Frame Work` $\longrightarrow$ `Statisitcs`

OK, if system A fails at 5 different virus and system B only fails at 1, who is better? You can't tell.

Need an index that's independent from protection method and attack method.

- Ideal defense $\rightarrow$ no ransomware anymore
- k-lag defense, let ransomware run $k\ \mu s$ and see the destruction.
  - Destruction means the unrecoverable data in mapped disk(target storage region which stores targeted files to ransomware)

Question :

How generic should this testing framework be?

Generic

Generic meeans the testing framework should be independent of variables. But what are those variables. If storage system types isn't one of these variable, then I think the way is to widely test upon GFS, XFS, mySQL, postgreSQL ...

Variable can also include the type of ransomware :

Observation

- Current ransomware are hard to work with because
  - server might be off-line (20 / 20 aren't working when I randomly fetch ransomwares from virus set).
  - only available on windows, hard to probe
  - some ransomware destorys the system(not the entire system, just ban the other ransomwares and applications), hard to test, need to **reload** the system every time, reload windows takes ~10 minutes

- With working ransomware, still
  - hard to standardize, why choose this one over other ransomwares?
  - not summable (fs lost 70% data over ransomware1, 80% data over ransomware2, another file system fs' lost 90% data over ransomware1 50% data over ransomware2), which is better? Can we take sum over any data?
  - Most of ransomwares disregard remote backups, while having access to credential manager.

Standardized ransomware

- Healthy : do nothing except for encryption data
- Transparent : can be adjusted for testing framework
- Working : can encryt data without the existence of server.
- Flexible : can do batch test.

How does storage systems do their journal?

- Many of the storage systems don't do data journal, they do metadata journal only for performance.
- Some systems do coW, but that's per transaction, the amount of recoverable files are limited.

Data backup

Generic way to defend against ransomware.

So need to study journal and logging behavior...

The most important problem is frequency and expiration rate of those backups, I think.

Now I think those can be omitted because index should be from "stationary" data backups and calculate their ratios.

Remote backups : crisis on credential manager

The following 3 slides are from https://www.nirsoft.net/utils/credentials_file_view.html

Data Stored In Credentials Files

Windows operating system stores the following information inside Credentials files:

- Login passwords of remote computers on your LAN.
- Passwords of mail accounts on exchange server (stored by Microsoft Outlook)
- Windows Live session information.

- Remote Desktop 6 user\password information.
- Internet Explorer 7.x and 8.x: passwords of password-protected Web sites ("Basic Authentication" or "Digest Access Authentication")
- Password of MSN Messenger / Windows Messenger accounts

Credentials File Location

You can find the Credentials files of Windows in the following locations:

```
C:\Users\[User Profile]\AppData\Roaming\Microsoft\Credentials (Windows Vista and later)
C:\Users\[User Profile]\AppData\Local\Microsoft\Credentials (Windows Vista and later)
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Credentials (Windows 8 and later)
C:\Documents and Settings\[User Profile]\Application Data\Microsoft\Credentials (Windows XP)
C:\Documents and Settings\[User Profile]\Local Settings\Application Data\Microsoft\Credentials (Windows XP)
```

Those are no valid locations, but I duplicated `.crd` file to desktop and find the encrypted results.

And there are ways to decryt those account / password

> CredentialsFileView is a simple tool for Windows that decrypts and displays the passwords and other data stored inside Credentials files of Windows.

Ransomware operates at your comp. Message protection will be likely to fail.

You logged in to onedrive today, so your cached verification will bypass the text-message-verification.

Then you have a ransomware.

But in testing framework's perspective, what are we testing against? The expiration rate of cloud service?

Are we testing subject storage system or the cloud backup sub-system?

Remote storage

summary (might expire)

GFS

Implementation

Need this tool to be portable, probably have to encapsulate the code and provide some APIs. However, the probes within BIOs should be enforced (not optional).

~~Ideas, now I don't think these are going to help~~:

- Patch :
  - kernel patch1
  - kernel patch2
  - kernel patch3
  - kernel patch4

Windows & IO

- Windows7 iso
- Windows 10 ISO should be available...

Current obstacles

1. NTFS does NOT have data journal. Typical ransomwares don't exist on linux.
2. Don't really know how to trace journals and logs(def unable to do it in block level) in **Windows** and with storage systems that I **can't access source code**.
    - Implicit problem, layering : how to trace data backups ?
3. Might need to build a standardized ransomware(may need to study the repos on github a little bit)
4. False positive : it happens to many Filesystem Filters based detecting tools.

Current obstacles (cont.)

5. I don't think logal backups have any meaning because backups essentially are files.