Technion – Israel Institute of Technology

Faculty of Computer Science

236499 – Projects in Ransomware

Winter 2018-2019

In this project we will develop several projects in ransomware, that will deepen our understanding how ransomware works, and how to protect against it.

The course will be supervised by experts from Microsoft, along with Technion staff.

Each pair of students will choose one of the listed projects below and will submit an initial report within a week from the beginning of the semester proposing the content of the project, the schedule, main issues to be researched or solved, material to be studied, and relevant issues. The report needs to be approved by the course staff before submission to the course web site.

The course will have about 5 frontal lectures, as listed below. (Dates and content may change).

Grades will be given based on the development along the semester, success of the project, initiative and particularly **innovation**, and all activities during the course.

The projects will be performed by pairs of students.

Prerequisites

- Network Security (236350) or Computer Security (recently given as 236607) or equivalent.
- Operating systems (234123 or 046209) or equivalent (no exceptions).
- Priority will be given to knowledge in Reverse Engineering (recently given as 236653)
- Basic knowledge in cryptography is required (e.g., from 236350 or 236506)
- Some projects may require additional prior knowledge and expertise.

  Required material on Windows 10 and Azure cloud will be taught in class.

Background

(Source: https://en.wikipedia.org/wiki/Ransomware)

Ransomware is computer malware that installs covertly on a victim's computer, executes a cryptovirology attack that adversely affects it, and demands a ransom payment to decrypt it or not publish it. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable

person to reverse, and display a message requesting payment to unlock it. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

While initially popular in Russia, the use of ransomware scams has grown internationally; in June 2013, security software vendor McAfee released data showing that it had collected over 250,000 unique samples of ransomware in the first quarter of 2013, more than double the number it had obtained in the first quarter of 2012. Wide-ranging attacks involving encryption-based ransomware began to increase through Trojans, which had procured millions of US Dollars.

File encrypting ransomware was invented and implemented by Young and Yung at Columbia University and was presented at the 1996 IEEE Security & Privacy conference. It is called *cryptoviral extortion* and is the following 3-round protocol carried out between the attacker and the victim.

1. *[attacker→victim]* The attacker generates a key pair and places the corresponding public key in the malware. The malware is released.
2. *[victim→attacker]* To carry out the cryptoviral extortion attack, the malware generates a random symmetric key and encrypts the victim's data with it. It uses the public key in the malware to encrypt the symmetric key. This is known as hybrid encryption and it results in a small asymmetric ciphertext as well as the symmetric ciphertext of the victim's data. It zeroizes the symmetric key and the original plaintext data to prevent recovery. It puts up a message to the user that includes the asymmetric ciphertext and how to pay the ransom. The victim sends the asymmetric ciphertext and e-money to the attacker.
3. *[attacker→victim]* The attacker receives the payment, deciphers the asymmetric ciphertext with his private key, and sends the symmetric key to the victim. The victim deciphers the encrypted data with the needed symmetric key thereby completing the cryptovirology attack.

References

Ransomware and detection

- https://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf
- https://www.blackhat.com/docs/us-15/materials/us-15-Kirda-Most-Ransomware-Isn%E2%80%99t-As-Complex-As-You-Might-Think.pdf
- https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf
- https://www.sans.org/reading-room/whitepapers/malicious/enterprise-survival-guide-ransomware-attacks-36962

Real Ransomware (be careful: open only in a VM)

- CryptoLocker – https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/CryptoLocker_22Jan2014
- Locky – https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.Locky

Open Source Ransomware Implementations

- https://github.com/mauri870/ransomware
    - https://github.com/goliate/hidden-tear/tree/master/hidden-tear/hidden-tear, and https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/hidden-tear-project-forbidden-fruit-is-the-sweetest/

Projects Scope

1. **Project #1 – Write a desktop Ransomware, where the command and control section is in the cloud**
    a. Project Goals
        i. Write a desktop application that communicates with a cloud service over HTTP (REST). This application, residing on the victim's desktop, will serve as the ransomware client that will encrypt the user machine as part of an extortion attack. The encryption can be for a specific file type, location, etc., inhibiting the victim from accessing or use. Once in action, the victim gets an extortion message with all details on how he should act in order to gain back access to his files.
        The application will enable the victim to decrypt the affected files, once the attacker enabled that by communicating (in-band or out-of-band) with the victim.
        ii. Write a cloud service, used by the attacker, that will manage the ransomware clients, or the victims (pre-infection and post-infection). That is, manage the full life cycle of a victim, including; for example: generate asymmetric encryption keys, manage key-victim pairs, implement in-band or out-of-band "payment" process, etc..
    b. Skills needed for the project:
        i. Develop cloud service
        ii. Develop an app for Windows 10
            1. Low CPU consumption
            2. Encrypt selected files (by: type, location, time stamp, etc.)
            3. Efficient encryption per file type, e.g. PDF, Media files, DOC, etc.
        iii. Basic cryptography
            1. AES
            2. Public Key Encryption
            3. Key management
2. **Project #2 – Detect and response to ransomware infection via cloud service**
    a. Project Goals
        i. In this project you will need develop a cloud service that detects and responds to a ransomware infection. The service will connect to an active storage service (e.g. One Drive, installed and running on the potentially infected machine), and listen to file notification events, to monitor for possible infections.

ii. The detection mechanism can be based on: https://www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf. It will use events and logs collected from step i above.
iii. Once a ransomware infection is detected, the cloud-based protection service will orchestrate the storage service to extract a previous revision of the affected file/files from the storage account and sync back to the user machine (make sure that the extracted versions are indeed infection free). In addition, the service should notify the victim (e.g. mail, message, etc.), and from his or hers perspective, files will be only temporarily unavailable (i.e. encrypted).
iv. Remember that the ransomware is running in the victim's machine independently of the service, make sure you address all implications

b. Skills needed for the project:
   i. Develop a cloud service
   ii. Basic anomaly detection capabilities

3. **Project #3 – End-point Ransomware detection and remediation**
   a. Project Goals
      i. Write an application, running standalone on the potential victim's machine, that will hook to core OS functions in order to detect ransomware activity
      ii. You will need to globally hook specific system process to identify anomalies related to specific types of ransomware.
      iii. Once hooks have been set, a detection mechanism should be implemented. See: https://www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf as an example of detecting ransomware activity
      iv. In case the application has detected a ransomware infection on the victim's machine, it will respond by using the built-in Windows mechanisms, e.g. Shadow-Copy to recover one or more corrupted files.
   b. Skills needed for the project:
      i. Develop win32 desktop app in .NET or C++.
      ii. Understanding Windows OS internals – system call APIs, hooking, process injection.
      iii. Process profiling
      iv. Determine what process behavior is of a ransomware pattern.
      v. Improve on false-positive rate - differentiate between real ransomware and process that behaves similarly (e.g. Dropbox).
4. **Optional Project #4 – Write a mobile Ransomware, where the command and control section is in the cloud**
   a. Project Goals
      i. Same as Project #1, but the victim here is an Android mobile device.
   b. Skills needed for the project:
      i. Same as Project #1
      ii. Required: deep knowledge in the development of an Android apps and relevant cloud services
5. **Project #5 – Ransomware Detonation**
   a. Project Goals

i. Write a sandbox based ransomware detection solution that protects from a malicious mail infection vector
ii. The ransomware can be hidden within an attachment, e.g. a Word document, or a link
iii. You will create a cloud application that will use Microsoft Graph API (https://developer.microsoft.com/en-us/graph/) that will scan the user's new mails and do the following:
    a. Register for notification on new emails
    b. When an email contains an attachment (or link), take a VM (from a predefined pool), execute the file, and look for unexpected behavior. You can use the honeypots concept, and monitor the files, network, and processes running to identify ransomware alike activities (be creative)
    c. Alert the user and block (bonus) infected attachments

b. Skills needed for the project:
    i. Develop a cloud service
    ii. Basic anomaly detection capabilities

6. Project #6 – Cloud Ransomware that uses identity thefts to infect a full cloud environment

a. Project Goals
    i. PC based malware that deploys a new cloud based Ransomware service, based on the stolen user credentials
    ii. Cloud based Ransomware service that:
        1. Scan for all the user's Azure services
        2. Corrupt each service – reversibly
            a. Azure Storage (File, Blob, Disk, Table)
            b. AzureSQL
            c. VM's
        3. Notify the user
    iii. Recovery service
    iv. Command & control
        1. Manage victims keys/PINs
        2. Manage the victim's lifecycle

Schedule and Syllabus

Week*	Topic	Lecture/task/comments
1 **23.10.2018**	Introduction to ransomware	Frontal
2 **06.11.2018**	Azure and developing a cloud service	Frontal & initial project report submission
3 **13.11.2018**	Windows 10 internals	Frontal
4 **20.11.2018**	Advanced topics in Windows 10 and Azure	Frontal
5 **27.11.2018**	Project status and review	With each team individually
6 **04.12.2018**		
7 **11.12.2018**	Peer project review	Frontal presentations to all teams
8 **18.12.2018**	Q&A with Alon	Frontal
9 **25.12.2018**		
10 **01.01.2018**		
11 **08.01.2018**		
12 **TBD**		**Poster submission**
13 **TBD**	Poster review	With each team individually
14 **TBD**	Demo day	Presentations in the faculty lobby & **final project report submission**

15 **TBD**	Project review	Each team will present their work to the course staff & **presentation submission**