ISSN: 2456-9348
Vol (03) _Issue (08) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

# SECURITY ASSESSMENT OF MOBILE APPLICATIONS AND SECURITY AWARENESS FOR INFORMATION SYSTEMS BY MALWARE ANALYSIS

**Moh Moh**
Faculty of Information Science Department, University of Computer Studies (Mandalay)
Mandalay, Myanmar
dawmohmoh.mdy@gmail.com

**ABSTRACT**
Security analysis is the process of deciding which securities are sound investments. True investments keep the principal safe and deliver an acceptable return. Any purchase mobile applications that does not meet these criteria is speculation. This paper outcome display security assessment and analysis of mobile application for developers can identify security features which were not found to be up to mark based on the reviews, and thus work upon them to deliver better applications. Next point objective is the awareness of information security awareness is to take the message to the people who stakeholder's in information systems.

**KEYWORDS:**
Mobile Applications, Malware, Assessment, Analysis, Exploitation**,** **T**hreats, Integrity, Availability, Confidentiality

## INTRODUCTION

Information security is protecting information and information system from unauthorized access, use, disclosure, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability. It is a major issue for businesses information system. Confidentiality: means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Integrity: means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Availability: means ensuring timely and reliable access to and use of information.

**Information Security four major Components and different types**
Four major components are
1. Assets, 2. Vulnerability, 3. Threat and 4. Control
Different security types are:
1). Organization and infrastructure security
2). Policy, standards and procedures security
3). Baselines and risk assessments security
4). Awareness and training program security
5). Compliance security.
Security Requirements: Needs for information systems security and trust can be formulated in terms of several major Requirements:

- Data confidentiality
- Data integrity
- System availability
- Resources
- System configuration
- Authentication
- Authorization
- Auditing
- non-repudiation

iJETRM
International Journal of Engineering Technology Research & Management

The mobile application penetration testing methodology focuses on security analysis and it has been long considered that the end user is in control of the device. In this article, we shall provide an overview of this methodology and discuss its four main stages.

1) Discovery
2) Assessment /Analysis
3) Exploitation
4) Reporting

## WORK PLAN

In this section, we present step by step procedure of work plan.

(1) Searched and downloaded sample Myanmar Mobile Applications and sample of business information
(2) Collected a set of applications based on (attributes and a particular feature)
(3) Select Methods and search APK tools for security test with inclusive malware analysis.
(4) Experimental results
(6) Finally, Analysis report and awareness of security assessment results and display to message.

## EVALUATION METHODOLOGIES AND APPLY AUTOMATIC TOOLS

There are millions of mobile apps are available in market. But, most of the mobile users first prefer high ranked apps when downloading it. If the user wants to download application, to visit play store such as Google Play Store, Apples store etc. When users visit to play-store application, then he or she is able to see the various application lists. This list is built on the basis of promotion or advertisement. User doesn't have knowledge about the application (i.e. which applications are useful or useless). So user looks at the list and downloads the applications. But sometimes it happens that the downloaded application won't work or not useful. To avoid this, we are making application in which we are going to list the applications.

Table 1. Collected a set of applications based on (attributes and a particular feature) tools analysis report

| App Name | Login | Sensitive Info: | Confidential Info: | Financial |
|---|---|---|---|---|
| Buddhan | N | N | N | N |
| Doe Taung Thu | N | N | N | N |
| Hlwint Live | Y | Y | Y | N |
| iZayCho | Y | Y | Y | Y |
| MMEarn | Y | Y | Y | Y |
| Mom's talk | Y | Y | Y | N |
| Phoosar | Y | Y | Y | N |
| …. | | | | |
| ….. | | | | |

iJETRM
International Journal of Engineering Technology Research & Management

## METHODOLOGIES

In our system, some methodologies are used for security testing.

M1-Improper Platform Usage

- Check for permission apply to Apktool
- Check for permission from Google Playstore
- Check for permission apply to Drozer Module

M2-Insecure Data Storage

- Search for unencrypted user credentials
- Retrieve data from Database
- Search data from Temp file
- Search data as (file -type) from External Storage
- Search data from log

M3-Insecure Communication

- Check security feature to Burp Suite and Traffic
- SSL Certificate Printing Technique By Pass

M4-Insecure Authentication

- Check session Management

M5-Insufficient Cryptography

- Checking in secure cryptography implementation

M6-Insecure Authorization

- Use Activity apply adb shell
- Check Content Provider
- Receiver Exported Checking and By Pass Technique

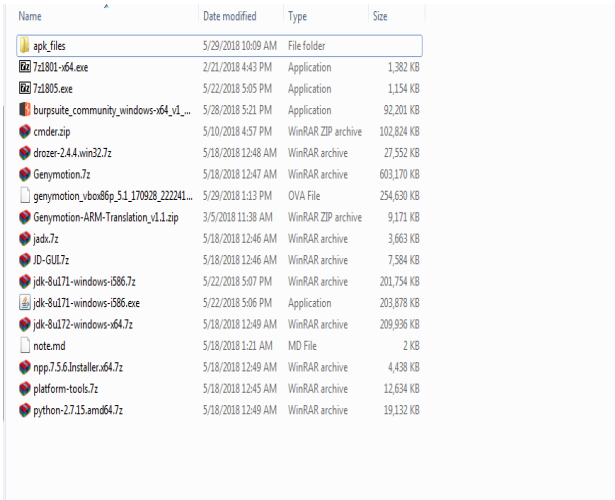
M9-Reverse Engineering

- Hardcoded Issue
- Hardcoded issue in native library file

**APK Tools**

Some of the security APK tools are described in the following figure.

iJETRM
International Journal of Engineering Technology Research & Management




**Fiugre 1 APK tools**

## EXPERIMENTAL RESULTS IN TESTING FOR MOBILE APPLICATIONS

Our case study invole three hundred user's feedback comments and sample hundred Mobile Applications and some methodologies and APK tools for security testing.

This system is analyzed the application by seven methods as shown in the following figures:

Method 1. Improper Platform Usage

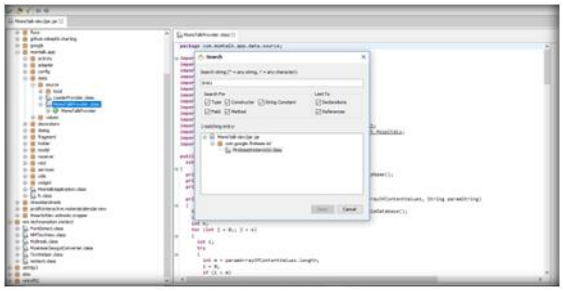


Figure 2. Permission List

Method 2. Insecure Data Storage

Fiugre 3. Log Files

Method 3. Insecure Communication

iJETRM
International Journal of Engineering Technology Research & Management

Figure 4. Communication and Traffic

Method 4. Insecure Authentication

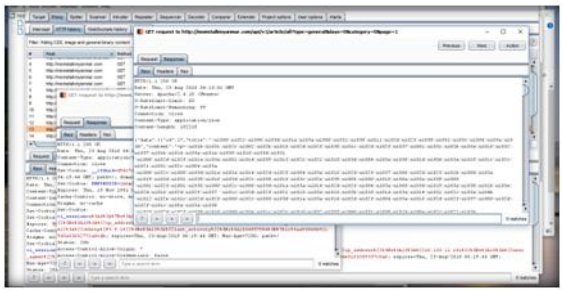


Figure 5. Authentication page

Method 5. Insufficient Cryptography

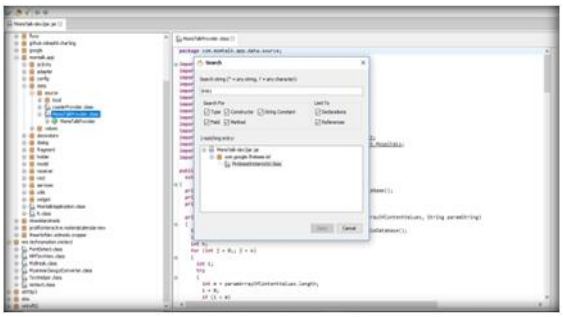


Figure 6. Security page

Method 6. Insecure Authorization

Figure 7. Authorization page

iJETRM
International Journal of Engineering Technology Research & Management

Method 9. Reverse Engineering

Figure 6. Hardcoded Issue page

ISSN: 2456-9348
Vol (03) _Issue (08) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

# EXPERIMENTAL RESULTS TESTING FOR BUSINESS INFORMATION SYSTEMS BY MALWARE

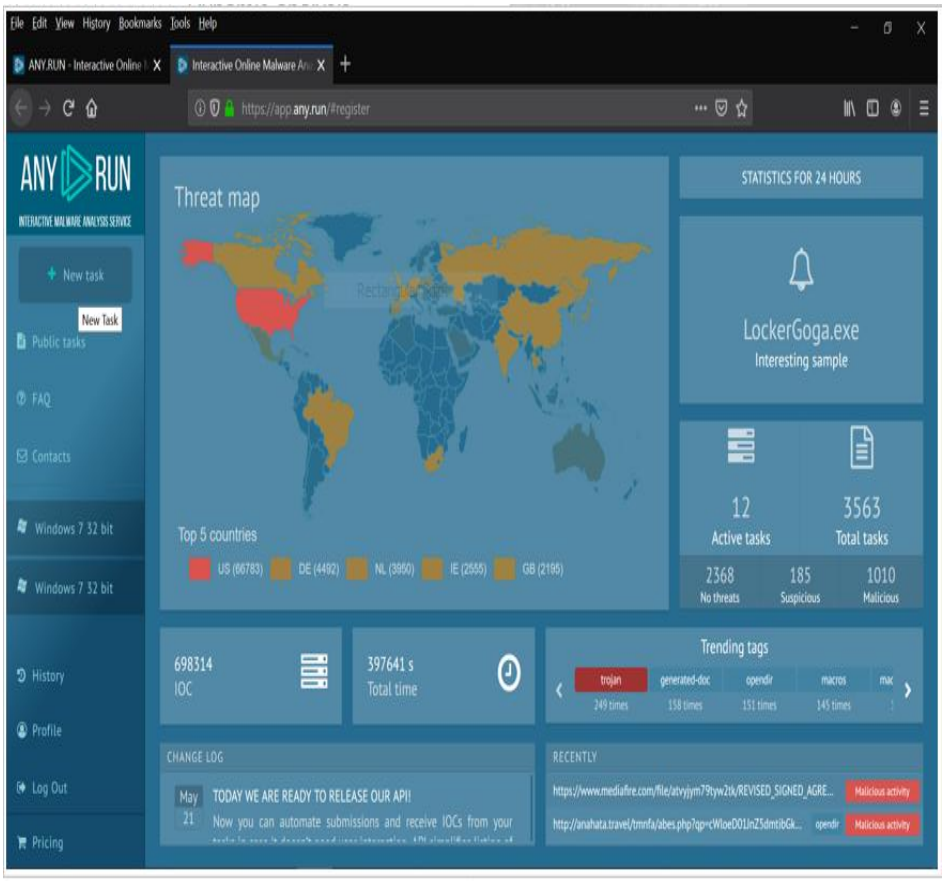



Fig**:** Malware analysis - dynamic analysis( run to https://any.run/ )

iJETRM
International Journal of Engineering Technology Research & Management


Fig: ‘Select ‘ Malware type

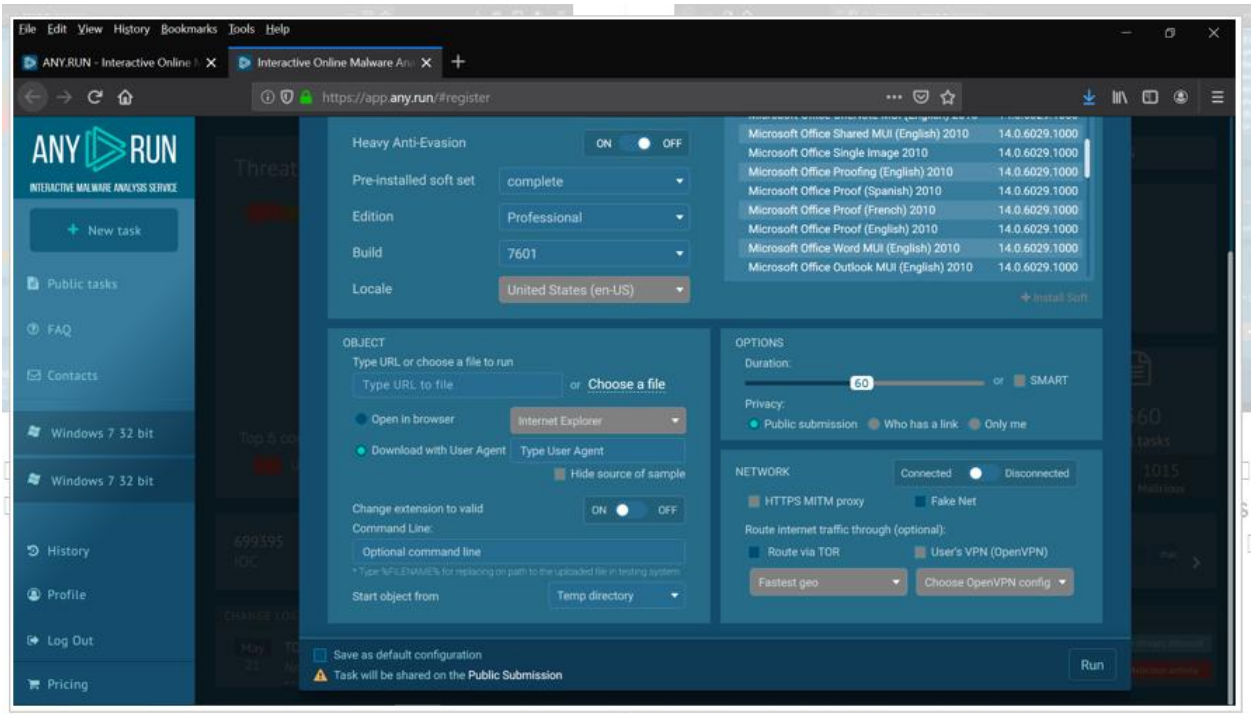



Fig: Run to start analysis and click add time,, to increase analysis time

iJETRM
International Journal of Engineering Technology Research & Management

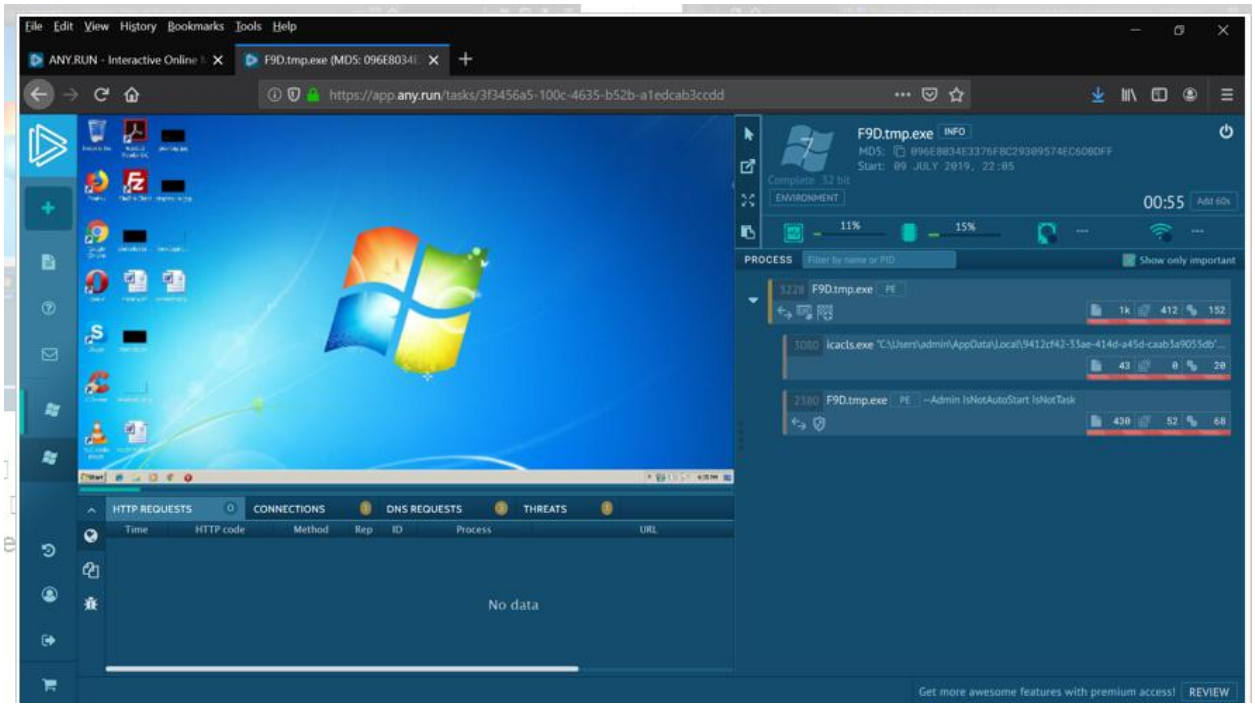



Fig: click text report to show result

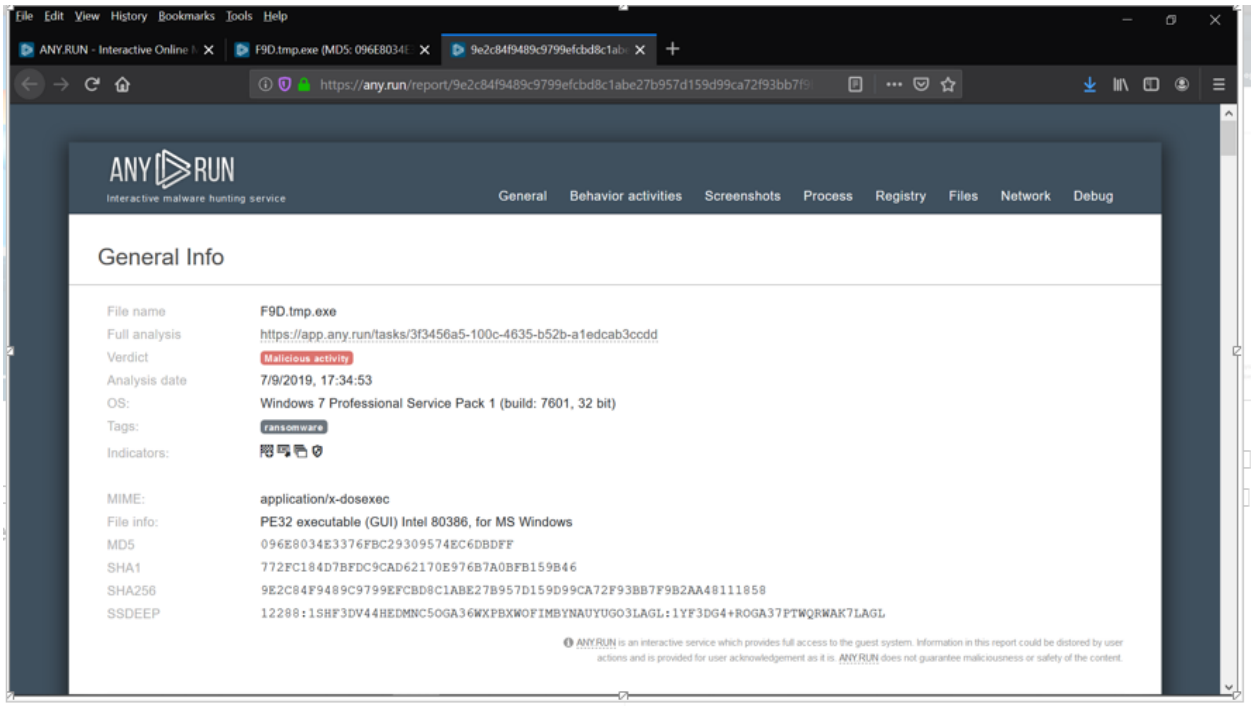



Fig: Show Malware infected process/ registry / exe……..

iJETRM
International Journal of Engineering Technology Research & Management

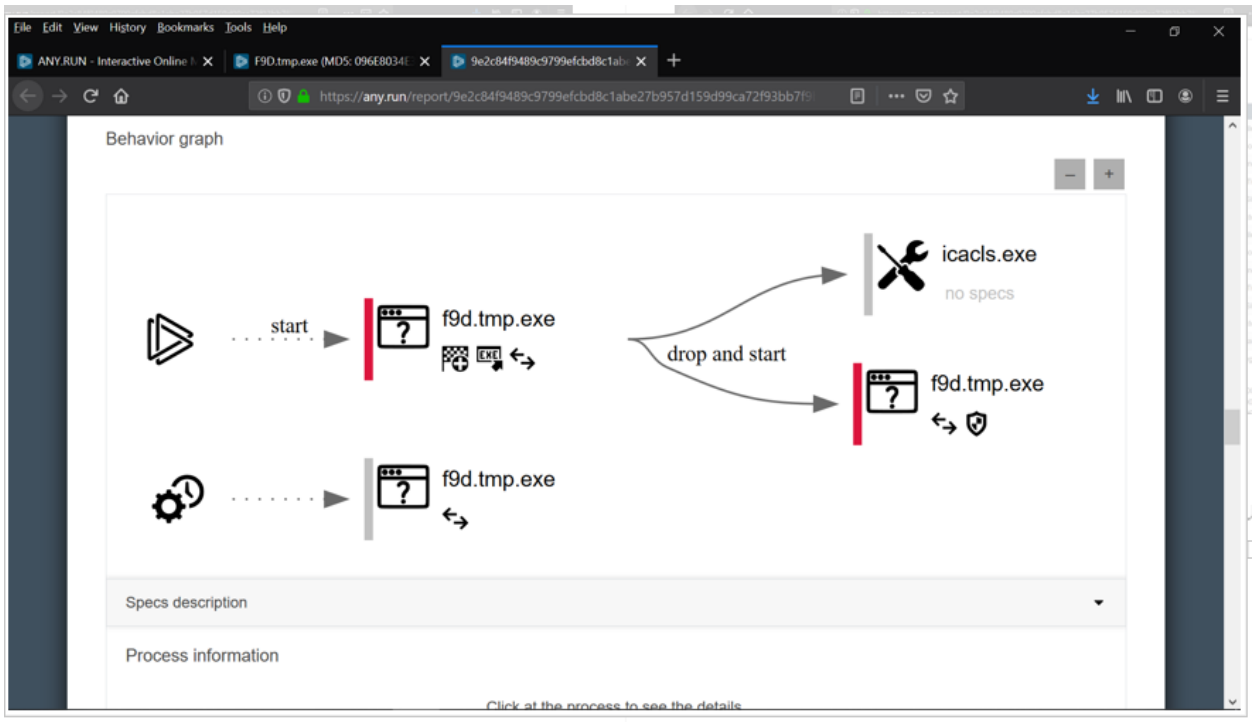



Fig: Run original exe,,, to create 2 child exe (first exe,,,, is no infected malicious code)

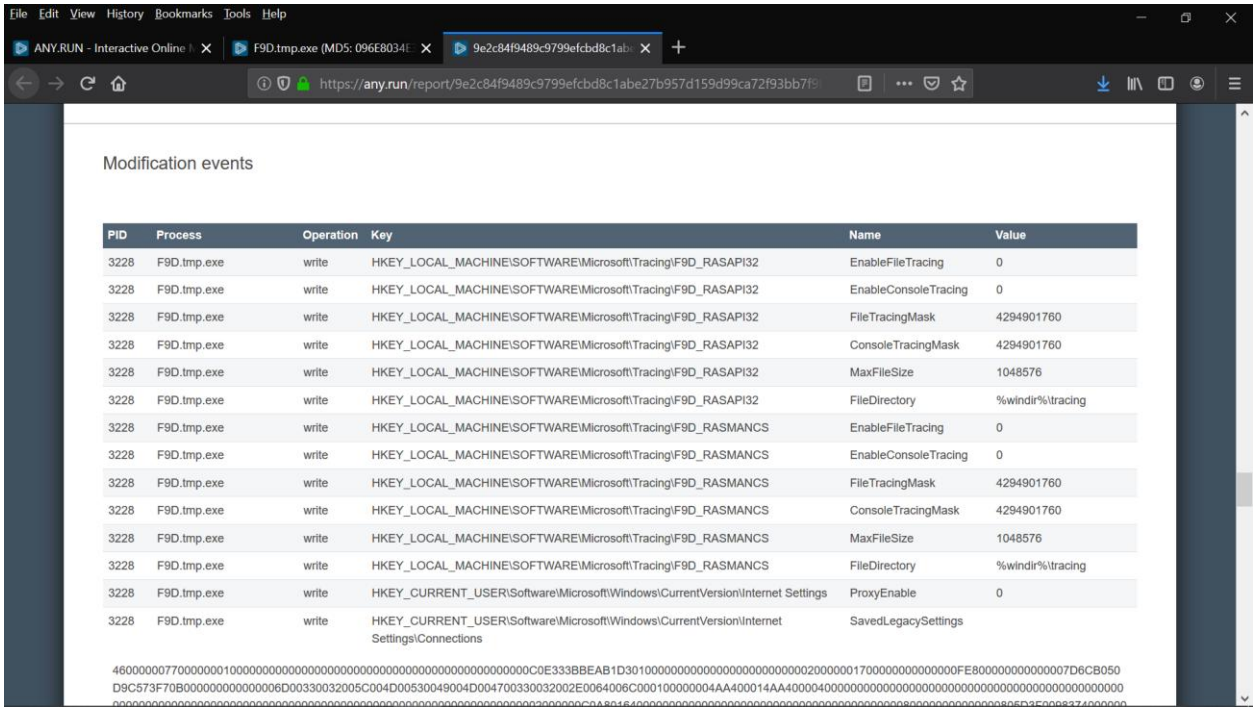



Fig: Run Second exe is found malware code

iJETRM
International Journal of Engineering Technology Research & Management

## CONCLUSION

Mobile application testing reduces risks, tests potential vulnerabilities, and examine software to ensure that an application is safe and meets adequate security compliance. Security experts use a variety of tests and strategies to monitor vulnerabilities to assess the security of a mobile application. Without through security testing, threat creators could infect your application with malware, spyware, and it could leave your user's financial account information and personal credentials exposed. Thus, this paper provides security awareness and Mobile Application users into applying the right application. This system presents analysis of Myanmar mobile applications for mobile devices that automatically discovered good security features.

## REFERENCES

[1] ENISA (European Network and Information Security Agency), "Risk Management /Risk Assessment " (available on-line at http://www.enisa.europa.eu/rmra)
[2] Walid Al-Ahmad and Bassil Mohammad. Addressing information security risks by adopting standards.
[3] International Journal of Information Security Science, 2(2):28_43, 2013.
[4] Tom Carlson, HF Tipton, and M Krause. Understanding Information Security Management Systems. Auerbach Publications Boca Raton, FL, 2008.
[5] Vladislav V Fomin, H Vries, and Y Barlette. Iso/iec 27001 information systems security management standard: exploring the reasons for low adoption. In Proceedings of The third European Conference on Management of Technology (EUROMOT), 2008.
[6] Kwo-Shing Hong, Yen-Ping Chi, Louis R Chao, and Jih-Hsing Tang. An integrated system theory of information security management. Information Management & Computer Security, 11(5):243_248, 2003.
[7] Ted Humphreys. State-of-the-art information security management systems with iso/iec 27001: 2005. ISO Management Systems, 6(1), 2006.
[8] G Pavlov and J Karakaneva. Information security management system in organization. Trakia Journal of Sciences, 9(4):20_25, 2011.
[9] Madhav Sinha and Alan Gillies. Improving the quality of information security management systems with iso27000. The TQM Journal, 23(4):367_376, 2011.
[10] The ISO Survey of Management System Standard Certi_cations 2015 http://www.iso.org/iso/the_iso_survey_of_management_system_standard_certi_cations_2015.pdf (Accessed: 11 December 2016).
[11] ISO/IEC 17799 (2005) _Information technology - Security techniques - Code of practice for information security management_.
[12] ISO/IEC 27001(2005) _Information technology - Security techniques - Information security management systems _ Requirements_.
[13] Debi Ashenden. Information security management: A human challenge? Information security technical report, 13(4):195_201, 2008.