VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Analysis and Audit

Course Code: CSE3501

Slot: L47-48

Faculty: Dr. Anil Kumar K

Assessment: 3

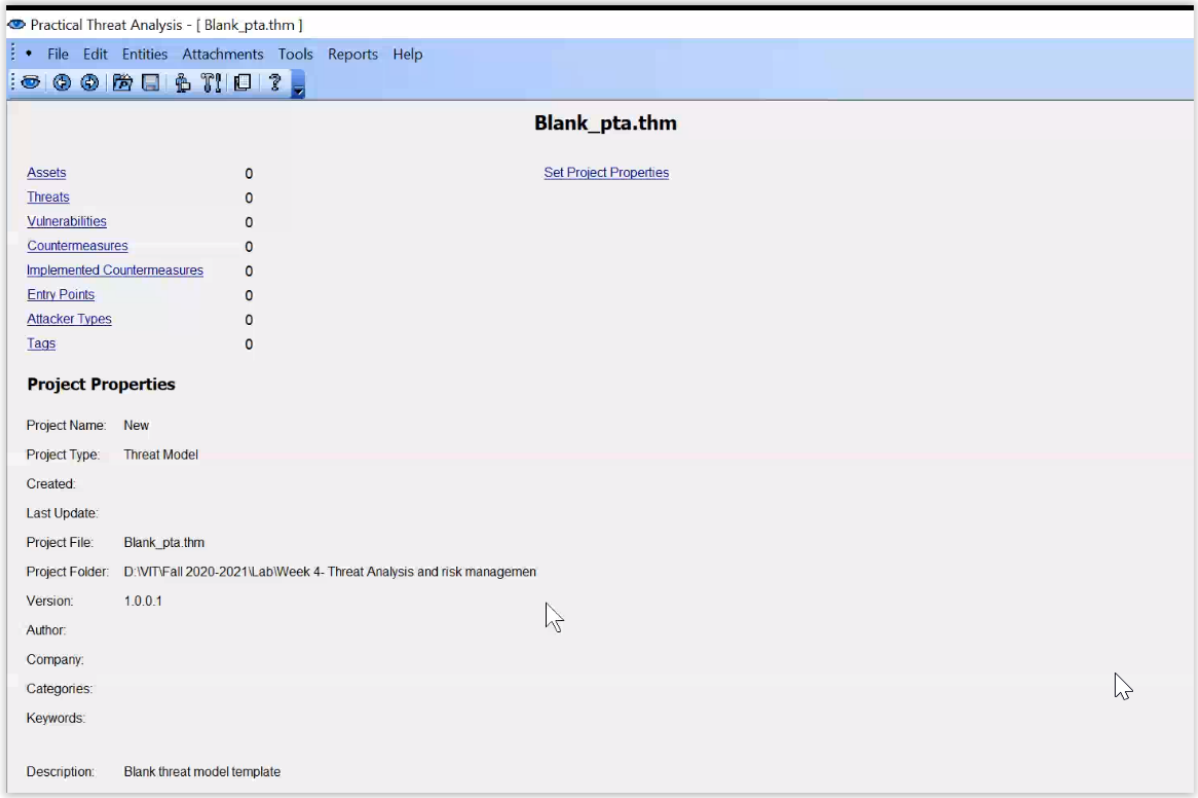
18BCI0247

Rohan Allen

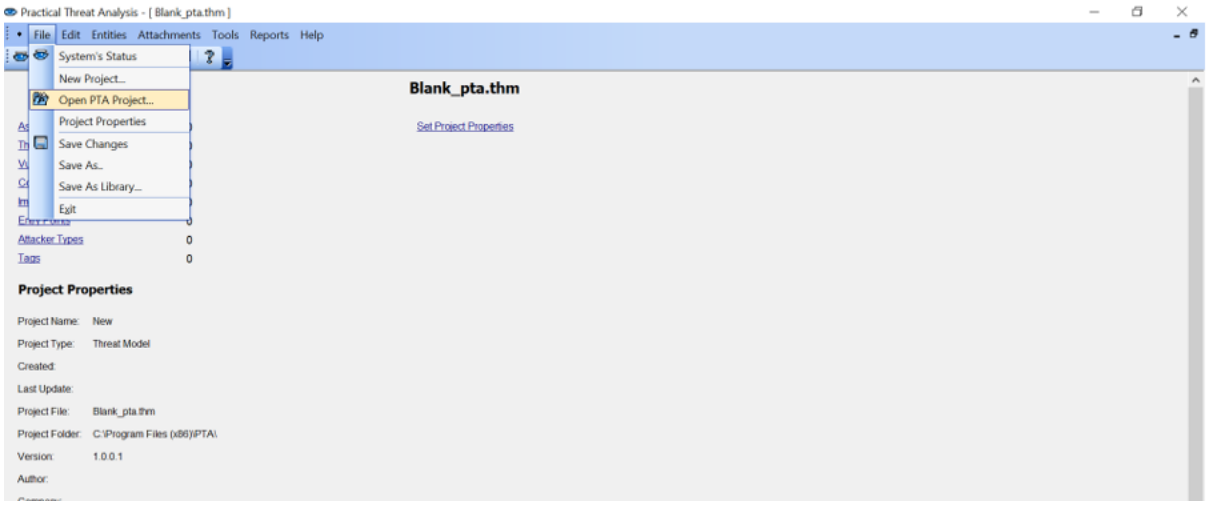
Exercise 1:

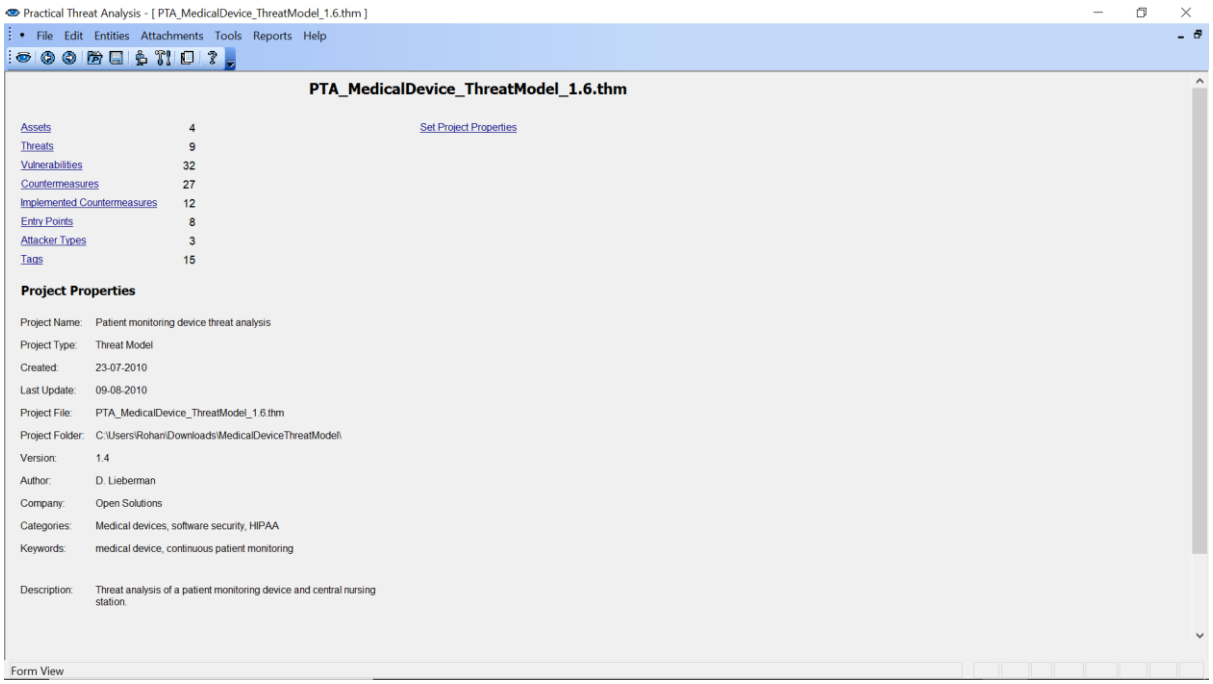
Experiments in Practical Threat Analysis(PTA) software.

Home page

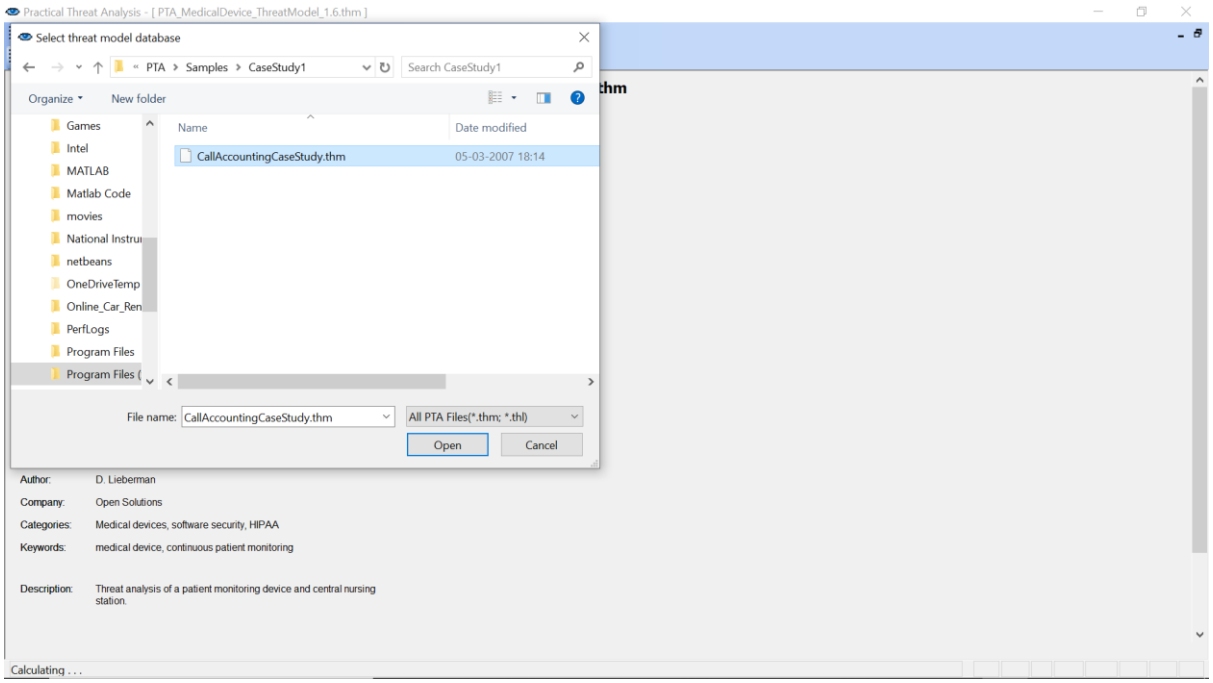


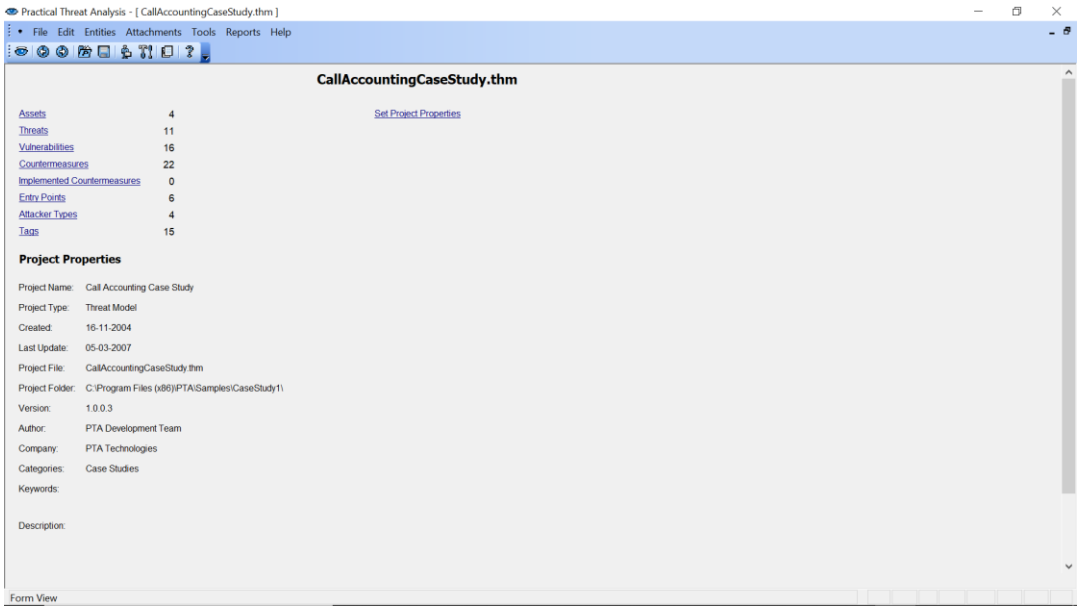
Adding Threat:



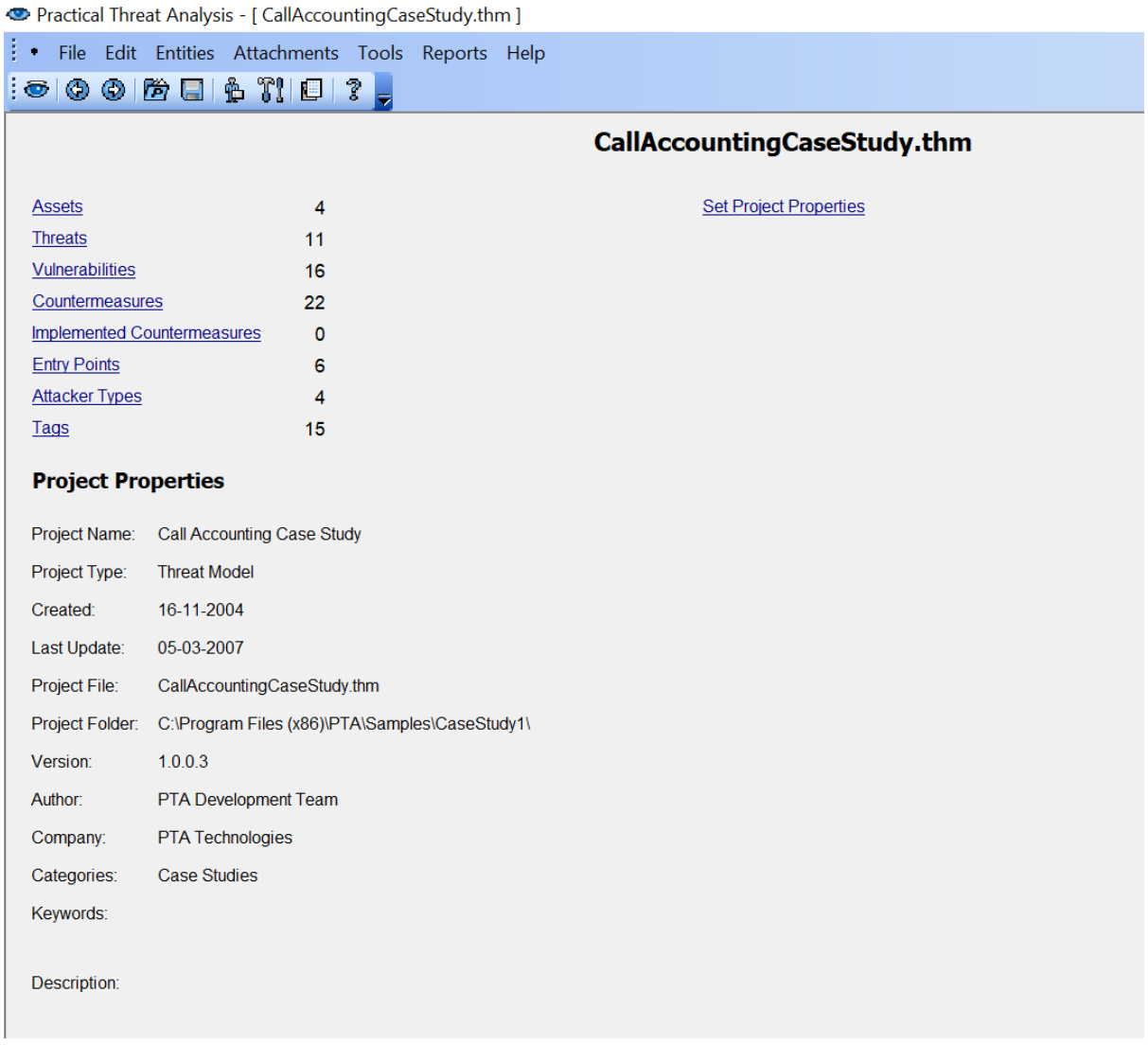


Adding another threat:




Practical Threat Analysis - [CallAccountingCaseStudy.thm]
File Edit Entities Attachments Tools Reports Help
CallAccountingCaseStudy.thm
Assets 4
Threats 11
Vulnerabilities 16
Countermeasures 22
Implemented Countermeasures 0
Entry Points 6
Attacker Types 4
Tags 15
Set Project Properties
Project Properties
Project Name: Call Accounting Case Study
Project Type: Threat Model
Created: 16-11-2004
Last Update: 05-03-2007
Project File: CallAccountingCaseStudy.thm
Project Folder: C:\Program Files (x86)\PTA\Samples\CaseStudy1\
Version: 1.0.0.3
Author: PTA Development Team
Company: PTA Technologies
Categories: Case Studies
Keywords:
Description:
Form View

Statistics:


Practical Threat Analysis - [CallAccountingCaseStudy.thm]
File Edit Entities Attachments Tools Reports Help
CallAccountingCaseStudy.thm
Assets 4
Threats 11
Vulnerabilities 16
Countermeasures 22
Implemented Countermeasures 0
Entry Points 6
Attacker Types 4
Tags 15
Set Project Properties
Project Properties
Project Name: Call Accounting Case Study
Project Type: Threat Model
Created: 16-11-2004
Last Update: 05-03-2007
Project File: CallAccountingCaseStudy.thm
Project Folder: C:\Program Files (x86)\PTA\Samples\CaseStudy1\
Version: 1.0.0.3
Author: PTA Development Team
Company: PTA Technologies
Categories: Case Studies
Keywords:
Description:

Assets:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Assets (4)

ID	Excluded	Name	Tags	Associated Threats	Fixed Value (?)	Recur. Value (?)	Annual Value (?)	Value (%)	Description
A002		**The privacy of call details information**	Data, Liability	T001, T002, T010, T011, T014	150,000	0	150,000	6.8	Calls details, especially the dialed and the caller numbers are considered private information that should be protected. The asset's value reflects the maximal liability according to the state's privacy-keeping regulations.
A003		**The availability / integrity of the system's passwords**	Data	T001	10,000	0	10,000	0.5	If passwords are disclosed then there is a need to run a password change procedure for users passwords as well as CDRs buffers passwords. Note that the asset in this case are the passwords themselves and not the damage that may be caused by a malicious use of the passwords.
A011		**The availability of the system's Web application and service**	Availability, Reputation	T001, T007, T009, T013, T016	0	50,000	50,000	2.3	If the Web application goes down, phone users and managers cannot view phone usage and utilization data. The value reflects the frustration, break of users confidence and cost of manual handling of users' queries.
A012		**The accuracy and integrity of the data in the system's database**	Data, Financial	T001, T004, T010, T011, T012, T013, T016	0	2,000,000	2,000,000	90.5	The database includes call records and pricing programs that affect the billing and has direct financial values. The value of the asset reflects the maximal annual loss of income caused by corrupted data.

Threats:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Threats (11)

ID	Excluded	Name	Tags	Probability	Threatened Assets	Exploited Vulnerabilities	Mitigation Plan	Risk (%)	Value At Risk (?)	Description
T001		**Intruder accesses the system's application and database servers directly from the Internet**	Networking, Application Servers	0.66	A002, A003, A011, A012	V001, V005	C001, C006, C013	66.0	1,458,600	An intruder gains access to the system's computers and database, steals or modifies data and disrupts system operation. This attack may damage most of the system's assets.
T002		**Insider accesses database via LAN for extruding private calls data**	Data, Networking, Users / Employees	0.49	A002	V003, V004, V005, V009	C002, C003, C004, C006, C007	3.3	73,500	The connection is established from a machine on the local area network.
T004		**Intruder corrupts database by injecting malicious SQLs in input fields of Web pages**	Data, Application Servers	0.49	A012	V010	C011, C012, C014	44.3	980,000	A sophisticated web attacker may reverse engineer the client side code of a web page and insert malicious sql statements to be submitted as the value of a page field assuming that it will be transferred to the database 'as is'. The code may include instructions for deleting database objects, altering the data itself or querying the information.
T007		**Denial of Service attack on the Web site**	Networking, Application Servers	0.66	A011	V013	C018	1.5	33,000	DoS attack prevents data from being available to public.
T009		**Intruder or an Internet worm uses HTTP vulnerabilities to break the Web server**	Application Servers, Operating System	0.95	A011	V011	C013, C014	1.4	31,350	The attack is performed using well-known exploits in the IIS Web server. The hacker or a worm may change the content of page, insert offensive texts etc…

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Threats (11)

ID	Excluded	Name	Tags	Probability	Threatened Assets	Exploited Vulnerabilities	Mitigation Plan	Risk (%)	Value At Risk (?)	Description
T010		**A malicious user with managerial rights manipulates calls data**	Data, Application Servers, Users / Employees	0.49	A002, A012	V004, V014, V027	C019, C021, C022, C033	23.9	528,710	e.g. malicious employee at ASP offices may join forces with other parties for faking calls data or selling private calls information.
T011		**Intruder sniffs CDR buffers passwords and then steals or corrupts calls data accumulated in buffers**	Data, Telephony Equipment	0.49	A002, A012	V016, V019	C026, C030	47.1	1,040,270	The attack is on the CDR buffers that stores the calls info obtained from the PBX before its transfer to the system's processing pipeline
T012		**Technician makes mistakes in scheduling call data collectors**	Operational, Data	0.33	A012	V020	C028	9.9	217,800	Calls are lost until the configuration problem is identified and fixed.
T013		**Intruder gets control of the call processing pipeline after hacking the Web server machine**	Operational, Data	0.49	A011, A012	V011, V012, V020, V026	C013, C014, C028, C032	30.0	662,970	Normal operation of data collection pipeline may be disrupted and calls may be lost. The intruder may stop pipeline service processes, turn off MSMQ, disconnect the database etc.
T014		**Managers abuse sensitive private call details**	Data, Users / Employees	1	A002	V025	C031, C034	6.8	150,000	This is against Campton privacy regulations.

Vulnerabilities:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Vulnerabilities (16)

ID	Excluded	Name	Tags	Associated Threats	Relevant Countermeasures	Description
V001		**Application servers are vulnerable to exploits via the Internet**	Networking, Application Servers	T001	C001, C013	Anyone can reach the server machines by scanning the organization network from the internet. This vulnerability can be mitigated by controlling incoming network traffic.
V003		**The database passwords may be sniffed from the LAN when establishing connection with the database server**	Networking, Application Servers	T002, T016	C003	Insider may learn passwords that are transferred in plain text by using sniffing equipment.
V004		**Insiders and power users can access or modify data**	Users / Employees	T002, T010	C019, C020, C021	Super-users such as technicians and administrators can modify data.
V005		**System data can be extruded via email/http/ftp protocols**	Data, Users / Employees	T001, T002	C006, C007	For example: since the application is managed in a campus-external site by an ASP (application service provider) party, there is always the possibility that ASP employee disclose calls sensitive information.
V009		**The Web server and the database server machines may be reached from the LAN**	Networking, Application Servers, Users / Employees	T002, T016	C002, C003, C004	Unauthorized personnel that have access to LAN can reach the server machines.

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Vulnerabilities (16)

ID	Excluded	Name	Tags	Associated Threats	Relevant Countermeasures	Description
V010		**MS SQL server is prone to injection of malicious code via Web pages**	Data, Application Servers	T004	C011, C012, C014	Malicious SQL code may be injected via input fields and may cause damage to the data and the structure of the database.
V011		**MS Server 2003 and IIS 6.0 have deficiencies that enable to exploit OS resources via HTTP protocol**	Application Servers	T009, T013	C013, C014	For example: security exploits such as buffer overrun, url canonicalization and other weaknesses that enable malicious activities through HTTP requests.
V012		**Web users can access the database**	Data, Application Servers, Users / Employees	T013	C014, C032	Without appropriate authentication and authorization mechanism, anyone connected to the Web site may have access to data.
V013		**Web servers are exposed to DoS attacks**	Networking, Application Servers	T007	C018	A well-known vulnerability.
V014		**Employee's personal weaknesses may be exploited by criminal elements**	Users / Employees	T010	C022	Especially when working with external ASP.

Countermeasures:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Countermeasures (22)

ID	Excluded	Name	Already Implemented	Tags	Mitigated Vulnerabilities	Mitigated Threats	Fixed Cost (?)	Recur. Cost (?)	Annual Cost (?)	Description
C001		**Install firewall**		Networking, Hardware	V001	T001	5,000	1,000	3,500	The network should be secured by using industry standard firewall, which is configured to block traffic from the internet to the local area network, excluding HTTP requests to the Web site. The cost of the implementation is based on the one time cost of the firewall purchase and deployment.
C002		**Enforce quality passwords policy for protecting each of the machines on the network**		Operational	V009	T002, T016	0	5,000	5,000	Network users should choose strong passwords that are hard to guess or discover by brute force means. The cost expresses the yearly effort of enforcing the password policy by system administration.
C003		**Use Windows integrated authentication policy**		Operational	V003, V009	T002, T016	5,000	1,000	3,500	This type of secured login protocol requires the installation of Windows domain controller + Active Directory + backup domain controller. The cost expresses the one time fee of purchasing the software and the deployment by system administration. Use windows integrated authentication for database logins and Web
C004		**Database login accounts should be given the minimal rights that are necessary for their functionality**		Operational	V009	T002, T016	0	2,500	2,500	Web application account that is used for retrieving the daily rates will be assigned with read only permissions. User account should be given update privileges only on relevant data. Database administrator account is the only account with full rights on the database that can access and modify the database and the data. The cost reflects the
C006		**Install content leakage prevention system**		Operational, Hardware	V005	T001, T002	20,000	0	10,000	Implement extrusion prevention policy to protect personally identifiable information and system configurations from being lost e.g. analyze email content and alert on unauthorized transfer of sensitive assets.

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Countermeasures (22)

ID	Excluded	Name	Already Implemented	Tags	Mitigated Vulnerabilities	Mitigated Threats	Fixed Cost (?)	Recur. Cost (?)	Annual Cost (?)	Description
C007		**Create acceptable use policy for email and Internet access**		Operational	V005	T002	0	2,500	2,500	Have acceptable use policy, sign all employees and contractors that they have read and understood the policy.
C011		**Implement validation of input fields in Web pages**		Software Modules	V010	T004	15,000	0	7,500	The cost expresses the one time effort for developing this software feature.
C012		**Enforce data access via stored procedures with formal parameters content validation**		Data, Software Modules	V010	T004	20,000	0	10,000	Data in database should be manipulated only via stored procedures. The parameters of the stored procedures should be validated before executing the stored procedure. The cost here is the one time effort for developing this software feature.
C013		**Enforce deployment of latest security patches for OS, database and Web server**		Operational	V001, V011	T001, T009, T013	0	5,000	5,000	The current security patches for all software infrastructures in the system should be maintained. The cost estimation is bases on the yearly effort for deploying the patches by system administration.
C014		**Enforce security code review**		Software Modules	V010, V011, V012	T004, T009, T013	35,000	0	17,500	Review all system's source codes according to 'secure code writing' industry standards. The cost here is the one time effort for implementing this software review.

Attacker Types:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Attacker Types (4)

ID	Name	Profile and Motivation	Available Tools and Accessibility
K002	**Insider**	Malicious insider may be an employee or a subcontractor.	Access to the LAN and calls database.
K003	**Hacker**		
K004	**Commercial Opponent**		
K005	**Internet Worm**		

Entry points:

Practical Threat Analysis - [CallAccountingCaseStudy.thm]

File Edit Entities Attachments Tools Reports Help

Entry Points (6)

ID	Name	Description
E001	**Page of Web application**	which is available to the public
E003	**Computer workstation on the LAN**	
E004	**Database Server**	
E005	**Network**	by intrusion
E006	**Telephony equipment and data buffers**	

Tags:

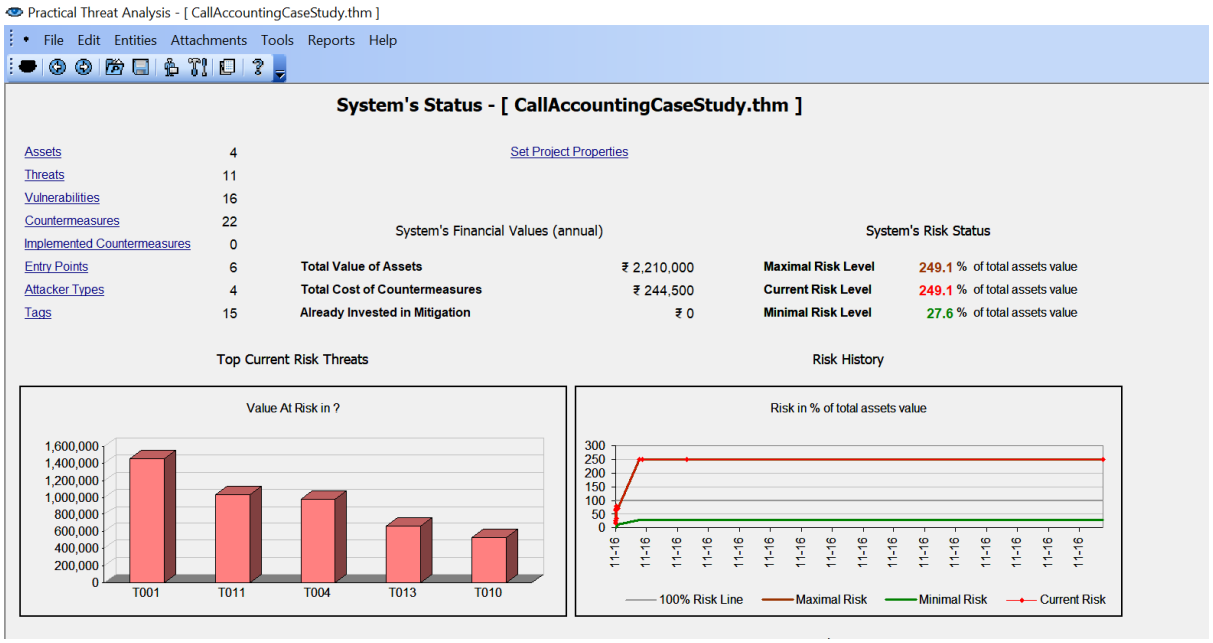
Practical Threat Analysis - [CallAccountingCaseStudy.thm]

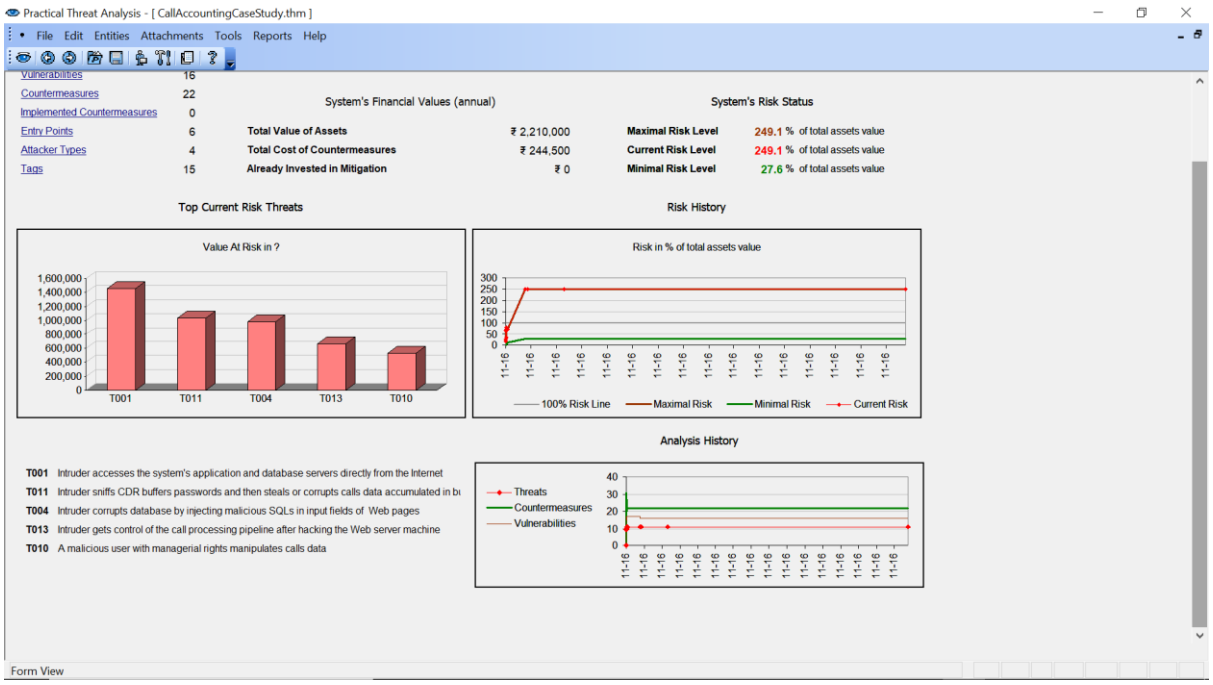
File Edit Entities Attachments Tools Reports Help

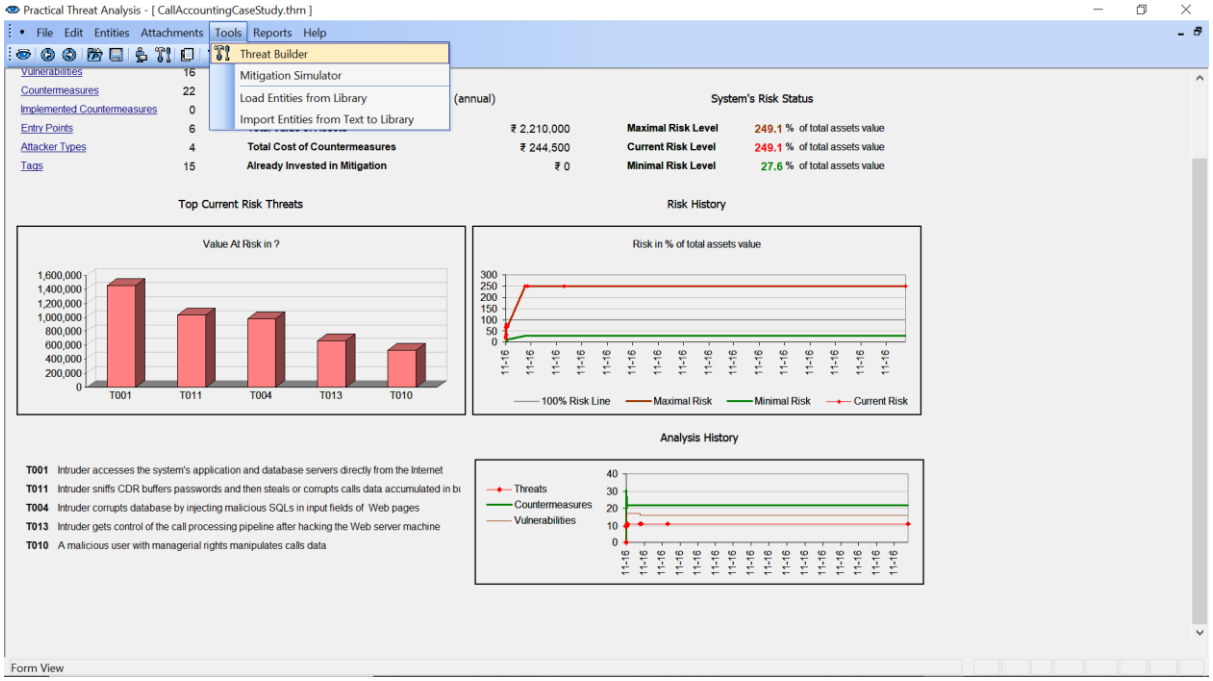
Tags (15)

ID	Name	Applicable to Assets	Applicable to Threats	Applicable to Vulnerabilities	Applicable to Countermeasures	Associated Entities
G001	**Operational**	V	V	V	V	T012, T013, C002, C003, C004, C006, C007, C013, C020, C022, C028, C033
G002	**Regulations**	V	V	V	V	C022, C034
G003	**Data**	V	V	V	V	T002, T004, T010, T011, T012, T013, T014, T016, V005, V010, V012, V025, V027, A002, A003, A012, C012, C032
G004	**Networking**		V	V	V	T001, T002, T007, V001, V003, V009, V013, V016, C001, C018
G005	**Application Servers**		V	V	V	T001, T004, T007, T009, T010, V001, V003, V009, V010, V011, V012, V013

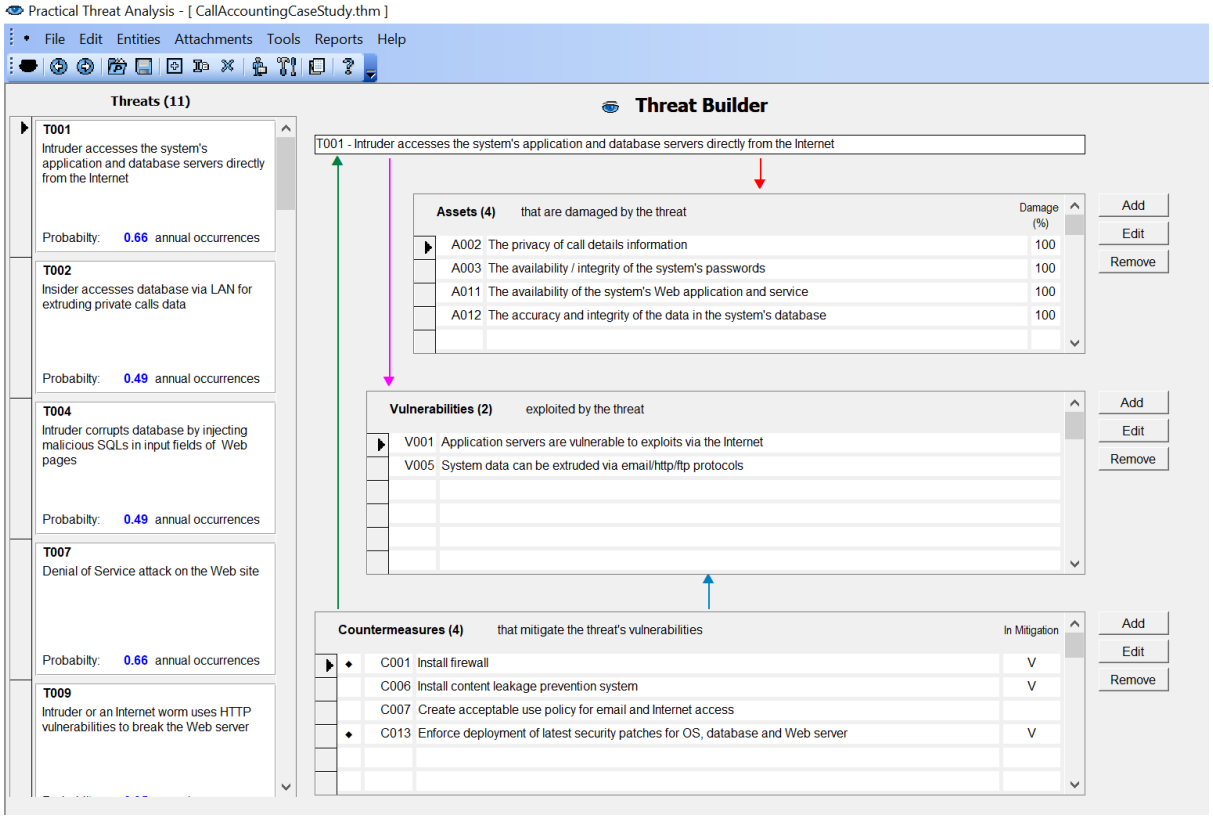
Threat Assessment:

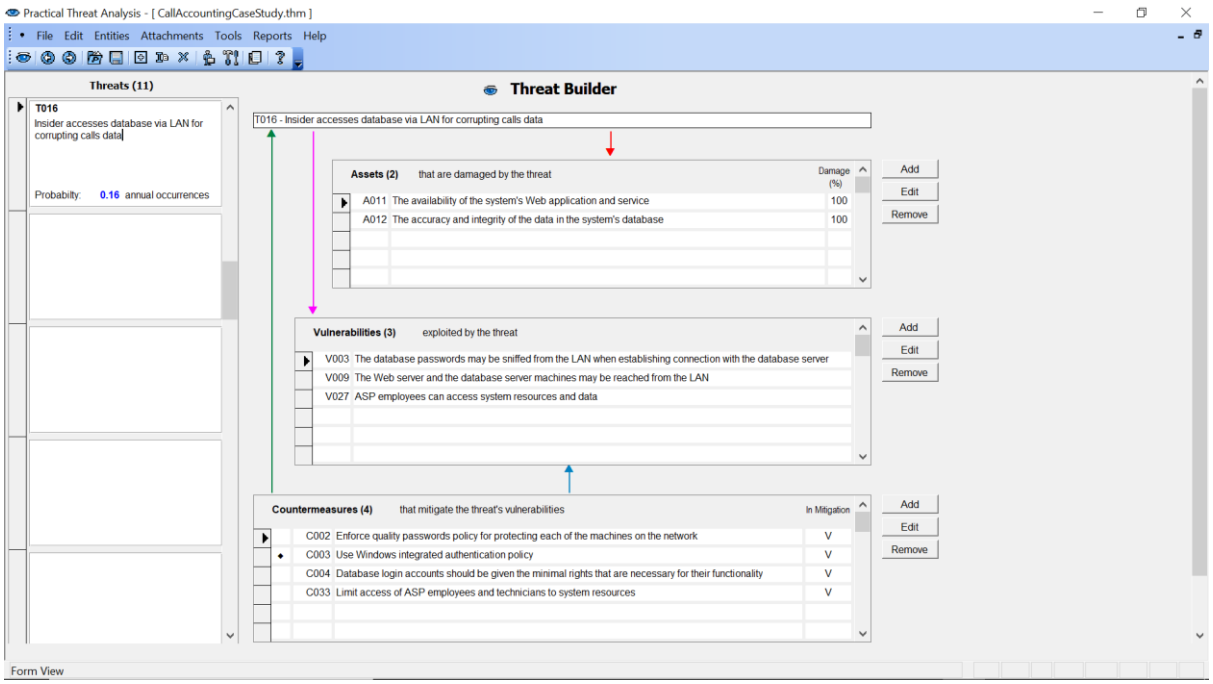




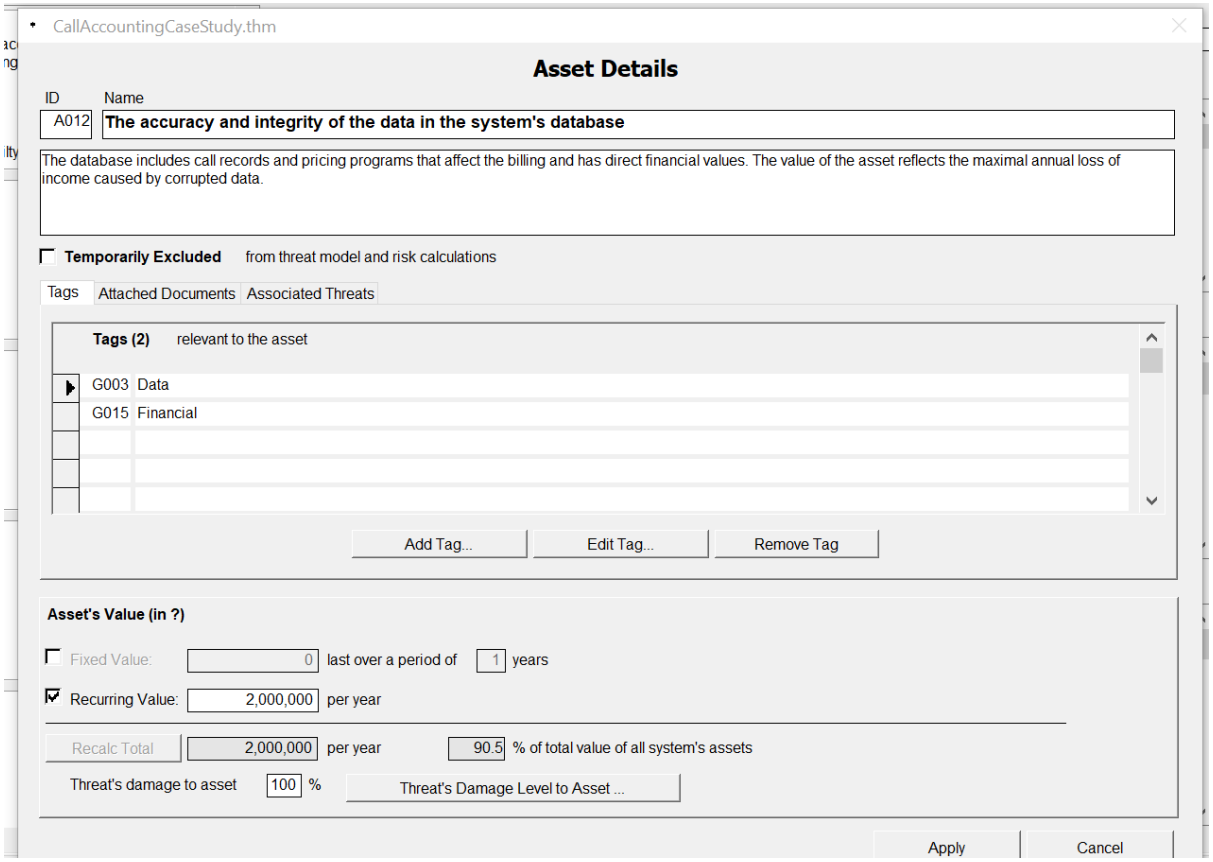


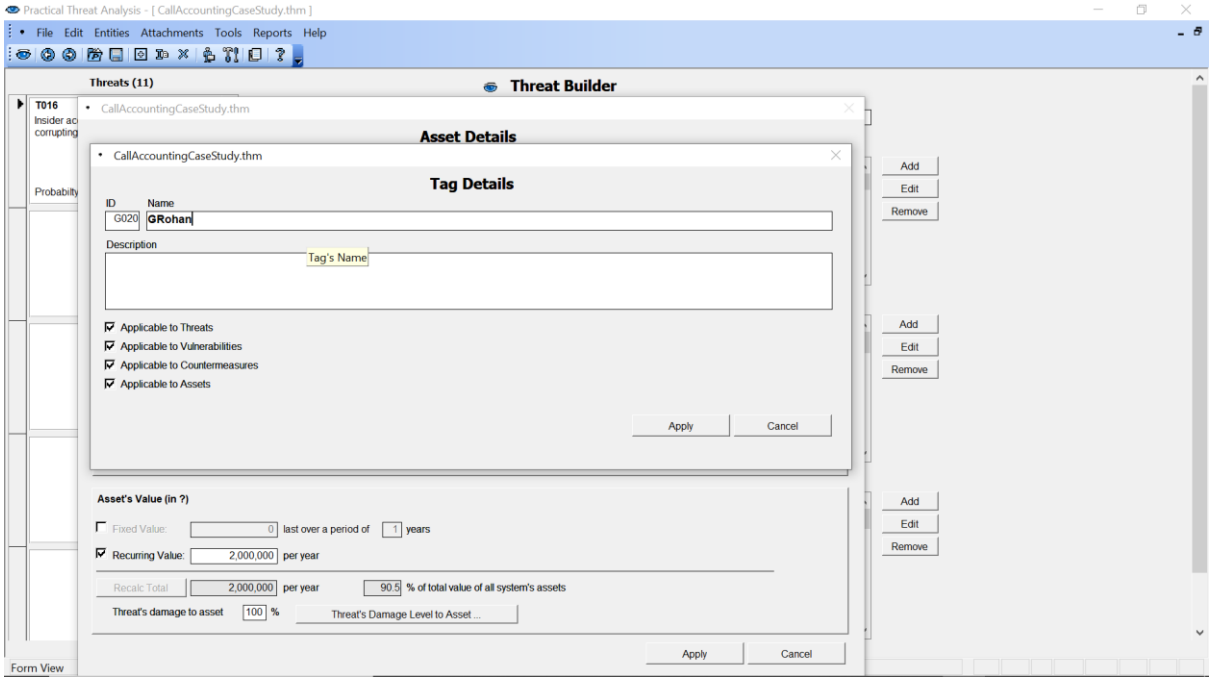
Creating new threat:

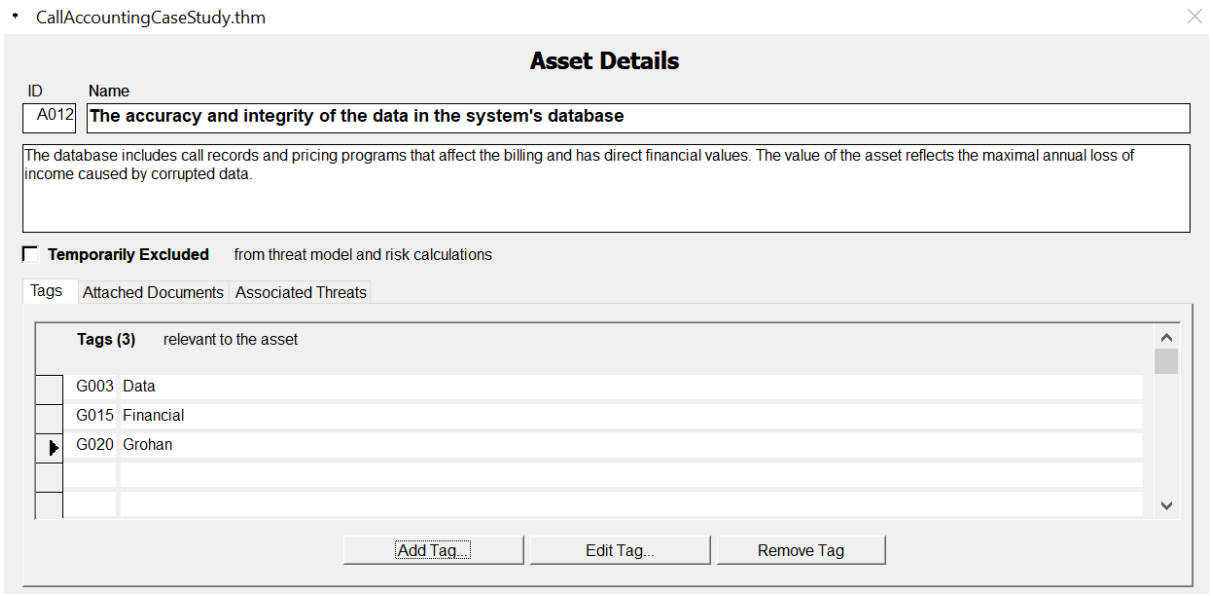


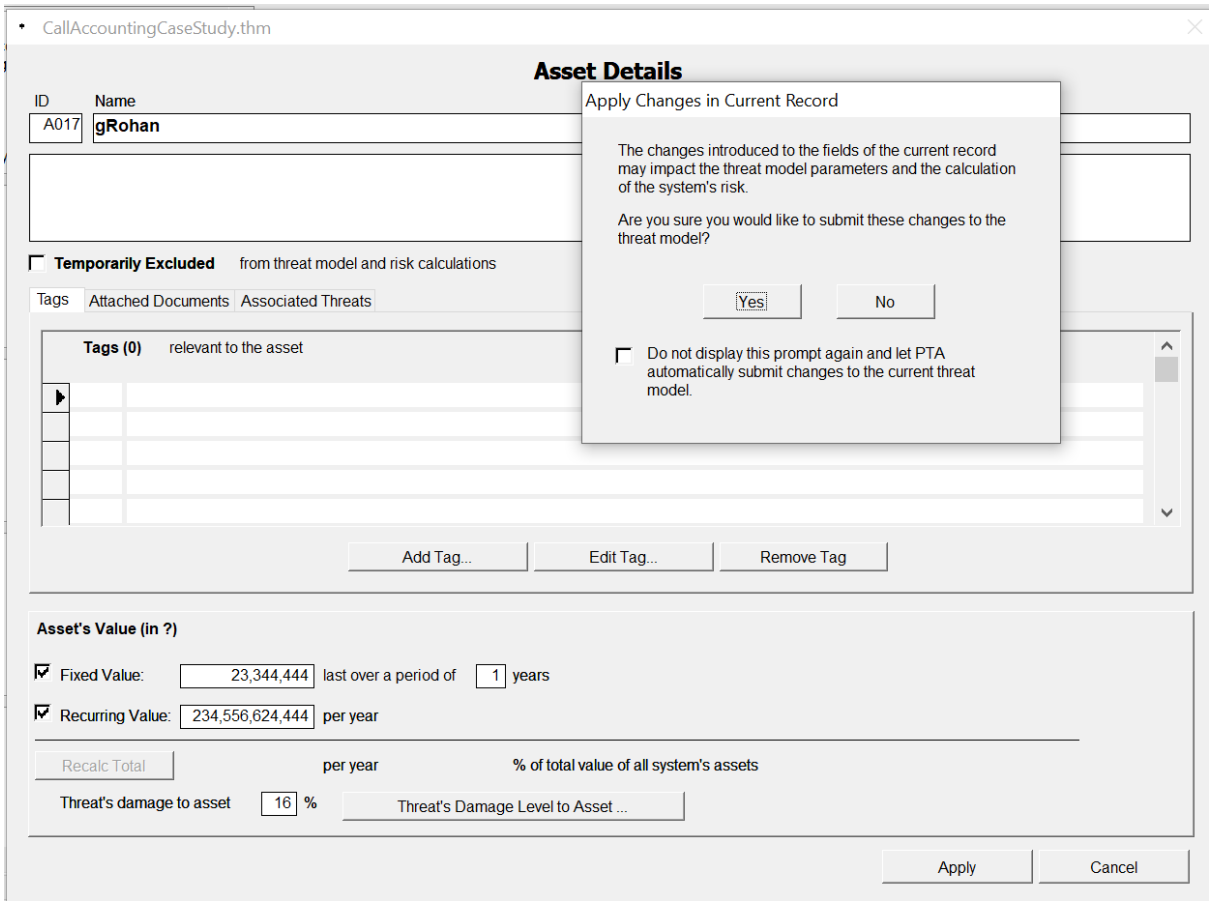


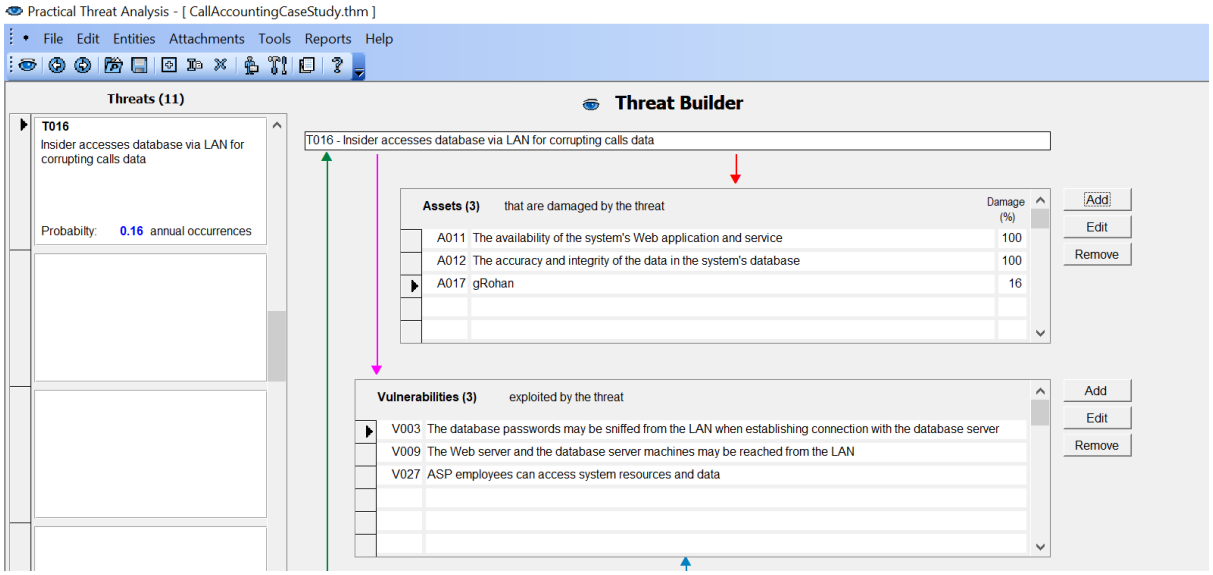
Creating new asset:

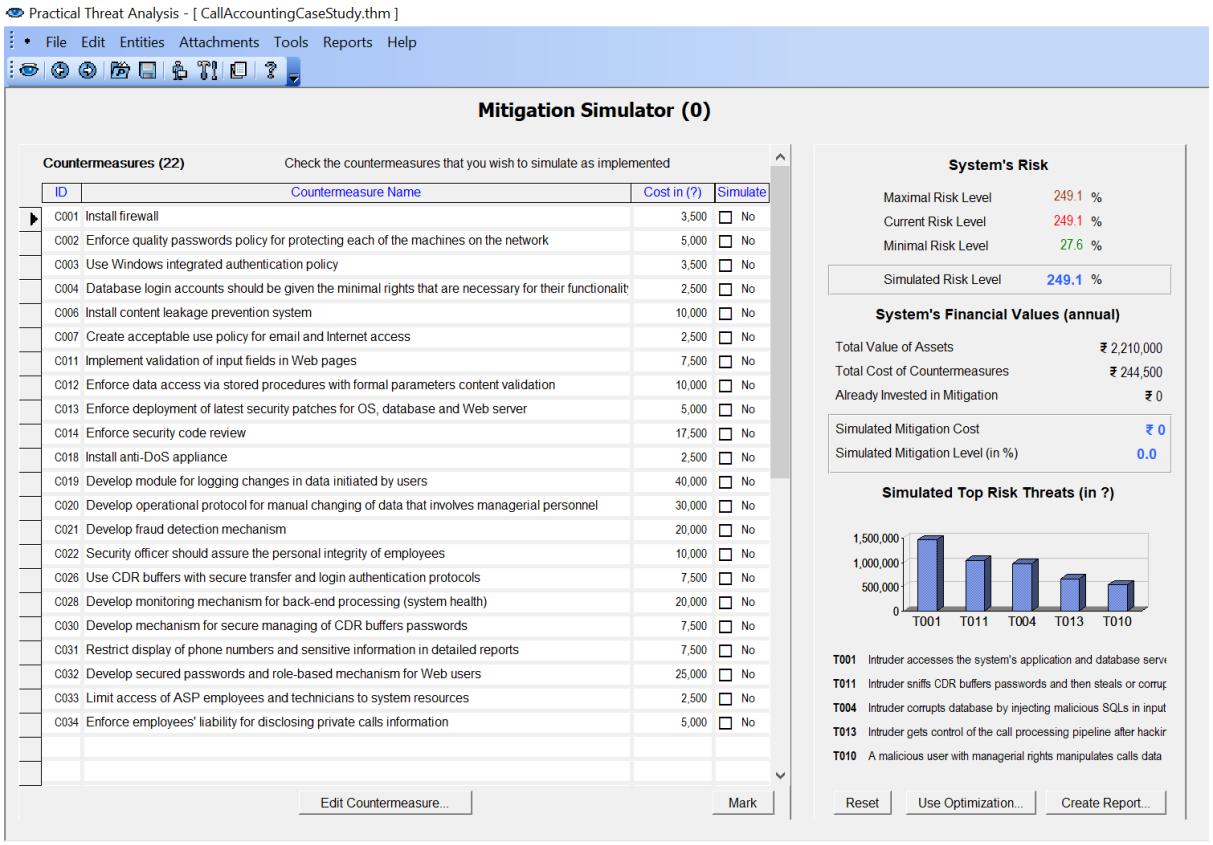


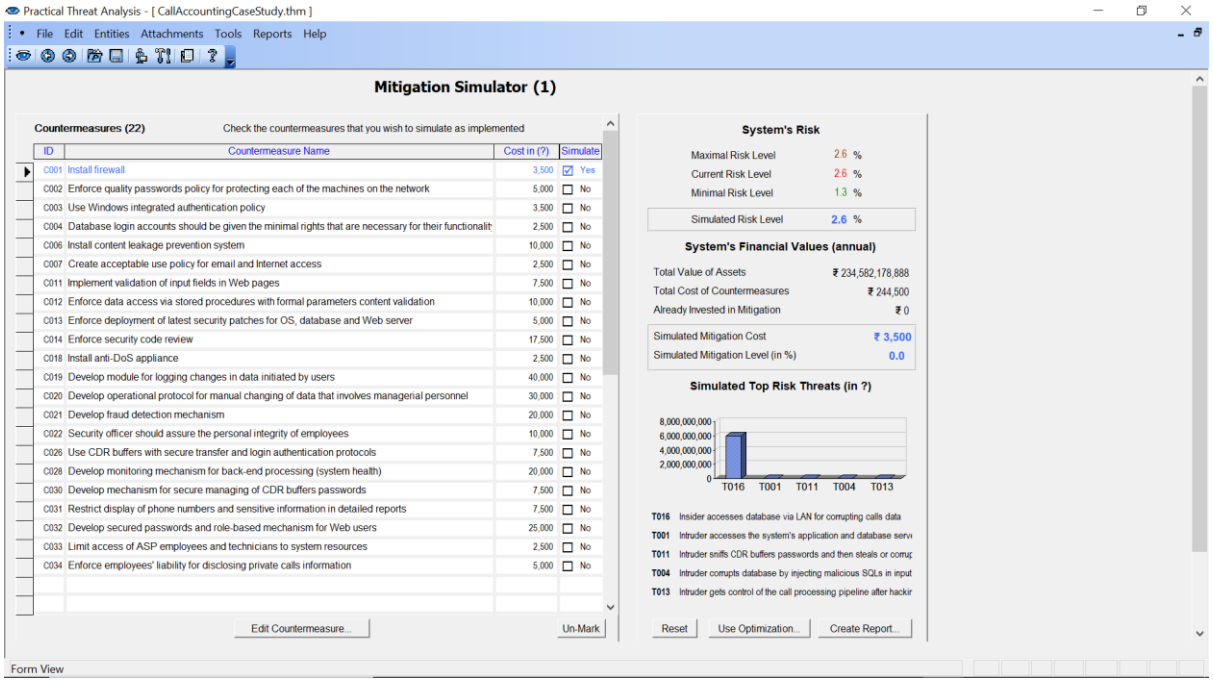

Practical Threat Analysis - [CallAccountingCaseStudy.thm]
File Edit Entities Attachments Tools Reports Help
Threats (11)
Threat Builder
T016
Insider ac
corrupting
Probability
CallAccountingCaseStudy.thm
Asset Details
CallAccountingCaseStudy.thm
Tag Details
ID
Name
G020
GRohan
Description
Tag's Name
Applicable to Threats
Applicable to Vulnerabilities
Applicable to Countermeasures
Applicable to Assets
Apply
Cancel
Add
Edit
Remove
Asset's Value (in ?)
Fixed Value:
0
last over a period of
1
years
Recurring Value:
2,000,000
per year
Recalc Total
2,000,000
per year
90.5
% of total value of all system's assets
Threat's damage to asset
100
%
Threat's Damage Level to Asset ...
Apply
Cancel
Form View


CallAccountingCaseStudy.thm
Asset Details
ID
Name
A012
The accuracy and integrity of the data in the system's database
The database includes call records and pricing programs that affect the billing and has direct financial values. The value of the asset reflects the maximal annual loss of income caused by corrupted data.
Temporarily Excluded
from threat model and risk calculations
Tags
Attached Documents
Associated Threats
Tags (3)
relevant to the asset
G003
Data
G015
Financial
G020
Grohan
Add Tag...
Edit Tag...
Remove Tag


CallAccountingCaseStudy.thm
Asset Details
ID
Name
A017
gRohan
Temporarily Excluded
from threat model and risk calculations
Tags
Attached Documents
Associated Threats
Tags (0)
relevant to the asset
Add Tag...
Edit Tag...
Remove Tag
Asset's Value (in ?)
Fixed Value:
23,344,444
last over a period of
1
years
Recurring Value:
234,556,624,444
per year
Recalc Total
per year
% of total value of all system's assets
Threat's damage to asset
16
%
Threat's Damage Level to Asset ...
Apply
Cancel
Apply Changes in Current Record
The changes introduced to the fields of the current record may impact the threat model parameters and the calculation of the system's risk.
Are you sure you would like to submit these changes to the threat model?
Yes
No
Do not display this prompt again and let PTA automatically submit changes to the current threat model.

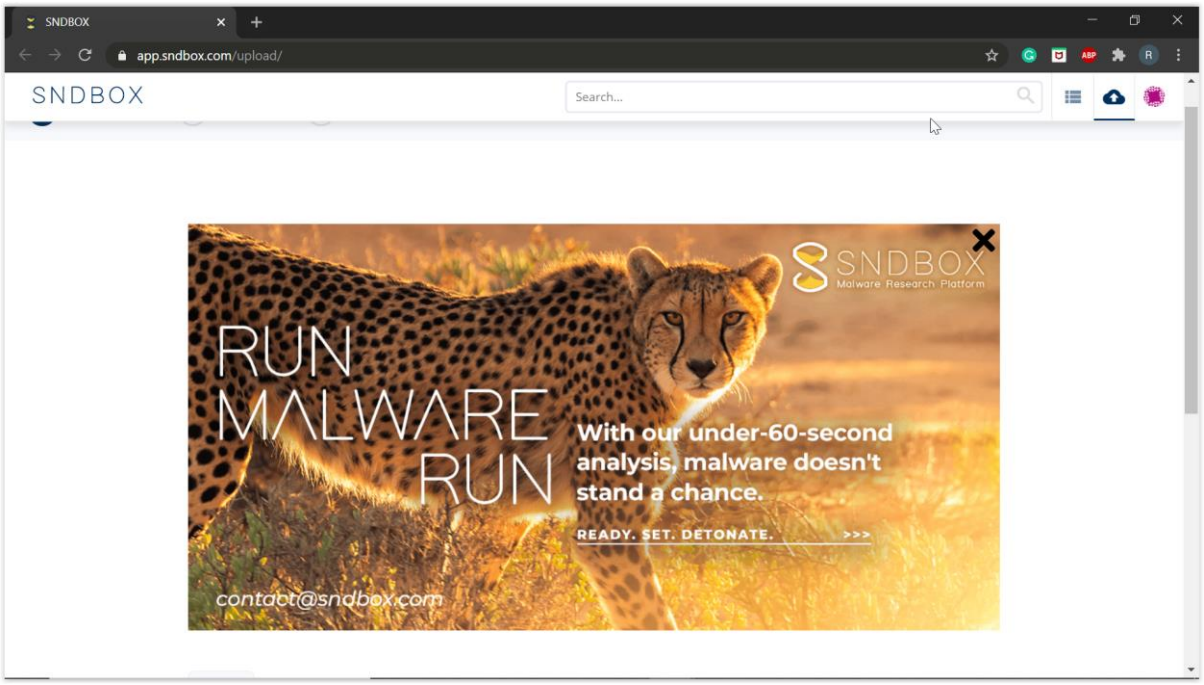

Practical Threat Analysis - [CallAccountingCaseStudy.thm]
File
Edit
Entities
Attachments
Tools
Reports
Help
Threats (11)
T016
Insider accesses database via LAN for corrupting calls data
Probabilty:
0.16
annual occurrences
Threat Builder
T016 - Insider accesses database via LAN for corrupting calls data
Assets (3)
that are damaged by the threat
Damage (%)
A011
The availability of the system's Web application and service
100
A012
The accuracy and integrity of the data in the system's database
100
A017
gRohan
16
Add
Edit
Remove
Vulnerabilities (3)
exploited by the threat
V003
The database passwords may be sniffed from the LAN when establishing connection with the database server
V009
The Web server and the database server machines may be reached from the LAN
V027
ASP employees can access system resources and data
Add
Edit
Remove


Practical Threat Analysis - [CallAccountingCaseStudy.thm]
File Edit Entities Attachments Tools Reports Help
Mitigation Simulator (0)
Countermeasures (22)
Check the countermeasures that you wish to simulate as implemented
ID | Countermeasure Name | Cost in (?) | Simulate
C001 Install firewall 3,500 No
C002 Enforce quality passwords policy for protecting each of the machines on the network 5,000 No
C003 Use Windows integrated authentication policy 3,500 No
C004 Database login accounts should be given the minimal rights that are necessary for their functionalit 2,500 No
C006 Install content leakage prevention system 10,000 No
C007 Create acceptable use policy for email and Internet access 2,500 No
C011 Implement validation of input fields in Web pages 7,500 No
C012 Enforce data access via stored procedures with formal parameters content validation 10,000 No
C013 Enforce deployment of latest security patches for OS, database and Web server 5,000 No
C014 Enforce security code review 17,500 No
C018 Install anti-DoS appliance 2,500 No
C019 Develop module for logging changes in data initiated by users 40,000 No
C020 Develop operational protocol for manual changing of data that involves managerial personnel 30,000 No
C021 Develop fraud detection mechanism 20,000 No
C022 Security officer should assure the personal integrity of employees 10,000 No
C026 Use CDR buffers with secure transfer and login authentication protocols 7,500 No
C028 Develop monitoring mechanism for back-end processing (system health) 20,000 No
C030 Develop mechanism for secure managing of CDR buffers passwords 7,500 No
C031 Restrict display of phone numbers and sensitive information in detailed reports 7,500 No
C032 Develop secured passwords and role-based mechanism for Web users 25,000 No
C033 Limit access of ASP employees and technicians to system resources 2,500 No
C034 Enforce employees' liability for disclosing private calls information 5,000 No
Edit Countermeasure...
Mark
System's Risk
Maximal Risk Level 249.1 %
Current Risk Level 249.1 %
Minimal Risk Level 27.6 %
Simulated Risk Level 249.1 %
System's Financial Values (annual)
Total Value of Assets ₹ 2,210,000
Total Cost of Countermeasures ₹ 244,500
Already Invested in Mitigation ₹ 0
Simulated Mitigation Cost ₹ 0
Simulated Mitigation Level (in %) 0.0
Simulated Top Risk Threats (in ?)
1,500,000
1,000,000
500,000
0
T001 T011 T004 T013 T010
T001 Intruder accesses the system's application and database serv
T011 Intruder sniffs CDR buffers passwords and then steals or corrup
T004 Intruder corrupts database by injecting malicious SQLs in input
T013 Intruder gets control of the call processing pipeline after hackir
T010 A malicious user with managerial rights manipulates calls data
Reset
Use Optimization...
Create Report...

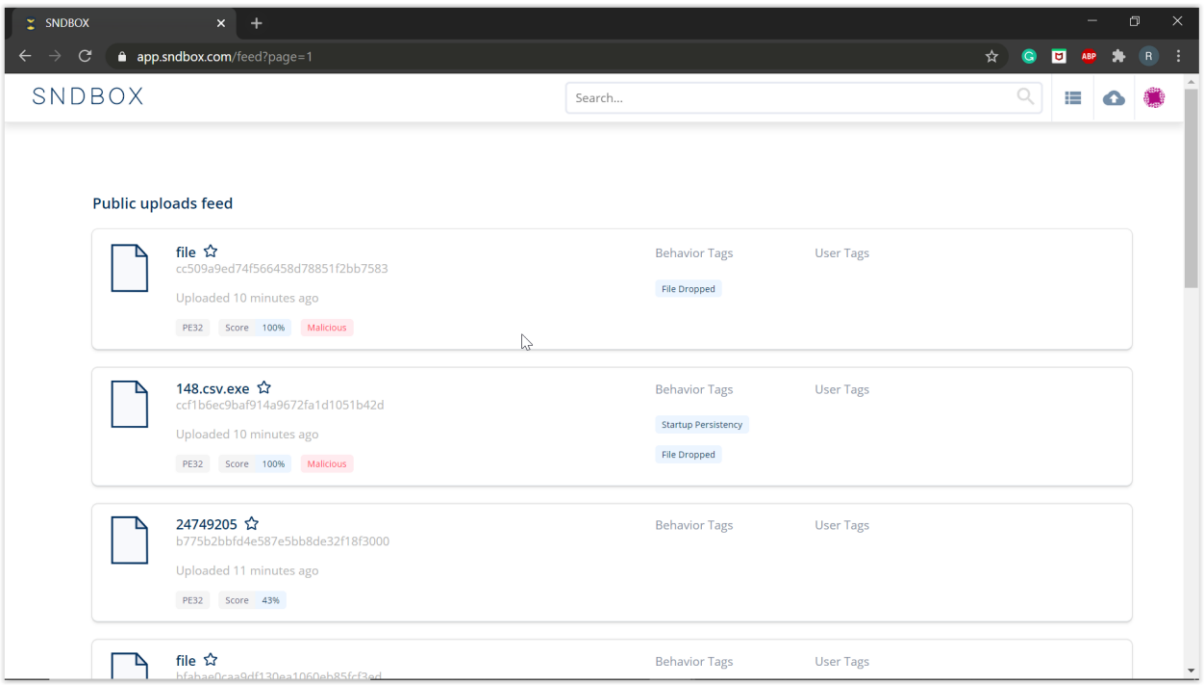

Practical Threat Analysis - [CallAccountingCaseStudy.thm]
File Edit Entities Attachments Tools Reports Help
Mitigation Simulator (1)
Countermeasures (22)
Check the countermeasures that you wish to simulate as implemented
ID | Countermeasure Name | Cost in (?) | Simulate
C001 Install firewall 3,500 Yes
C002 Enforce quality passwords policy for protecting each of the machines on the network 5,000 No
C003 Use Windows integrated authentication policy 3,500 No
C004 Database login accounts should be given the minimal rights that are necessary for their functionalit 2,500 No
C006 Install content leakage prevention system 10,000 No
C007 Create acceptable use policy for email and Internet access 2,500 No
C011 Implement validation of input fields in Web pages 7,500 No
C012 Enforce data access via stored procedures with formal parameters content validation 10,000 No
C013 Enforce deployment of latest security patches for OS, database and Web server 5,000 No
C014 Enforce security code review 17,500 No
C018 Install anti-DoS appliance 2,500 No
C019 Develop module for logging changes in data initiated by users 40,000 No
C020 Develop operational protocol for manual changing of data that involves managerial personnel 30,000 No
C021 Develop fraud detection mechanism 20,000 No
C022 Security officer should assure the personal integrity of employees 10,000 No
C026 Use CDR buffers with secure transfer and login authentication protocols 7,500 No
C028 Develop monitoring mechanism for back-end processing (system health) 20,000 No
C030 Develop mechanism for secure managing of CDR buffers passwords 7,500 No
C031 Restrict display of phone numbers and sensitive information in detailed reports 7,500 No
C032 Develop secured passwords and role-based mechanism for Web users 25,000 No
C033 Limit access of ASP employees and technicians to system resources 2,500 No
C034 Enforce employees' liability for disclosing private calls information 5,000 No
Edit Countermeasure...
Un-Mark
System's Risk
Maximal Risk Level 2.6 %
Current Risk Level 2.6 %
Minimal Risk Level 1.3 %
Simulated Risk Level 2.6 %
System's Financial Values (annual)
Total Value of Assets ₹ 234,582,178,888
Total Cost of Countermeasures ₹ 244,500
Already Invested in Mitigation ₹ 0
Simulated Mitigation Cost ₹ 3,500
Simulated Mitigation Level (in %) 0.0
Simulated Top Risk Threats (in ?)
8,000,000,000
6,000,000,000
4,000,000,000
2,000,000,000
0
T016 T001 T011 T004 T013
T016 Insider accesses database via LAN for corrupting calls data
T001 Intruder accesses the system's application and database serv
T011 Intruder sniffs CDR buffers passwords and then steals or corrup
T004 Intruder corrupts database by injecting malicious SQLs in input
T013 Intruder gets control of the call processing pipeline after hackir
Reset
Use Optimization...
Create Report...
Form View

Exercise 2:

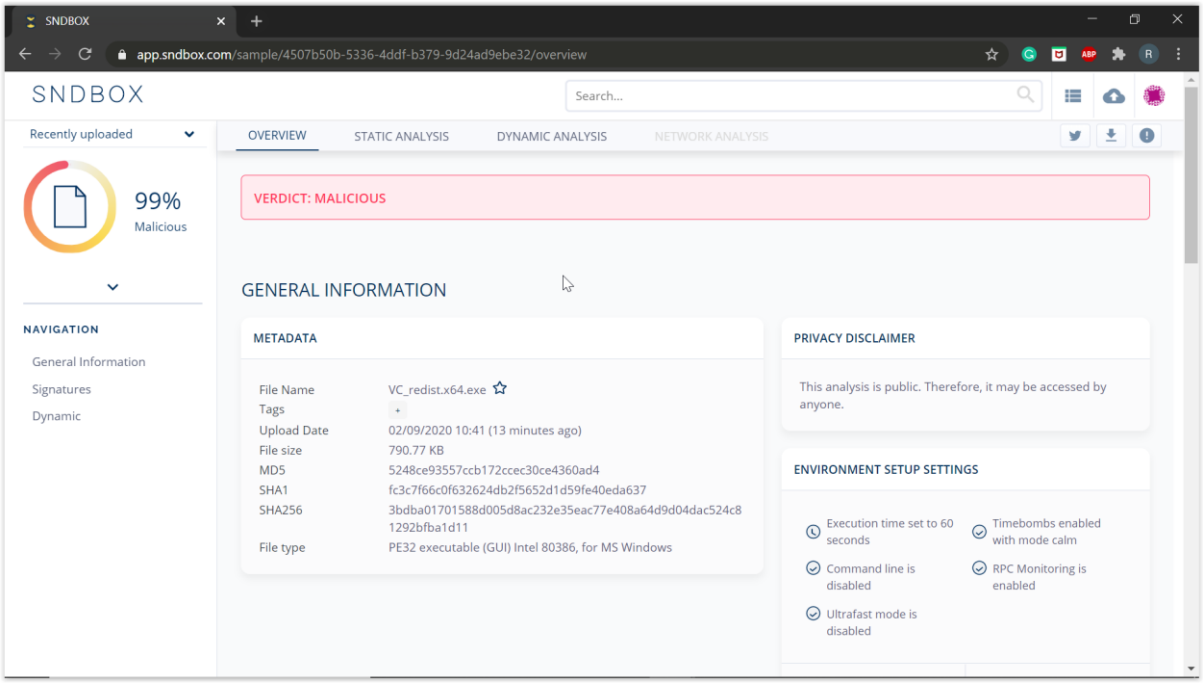
Malware Analysis on SNDBOX platform.

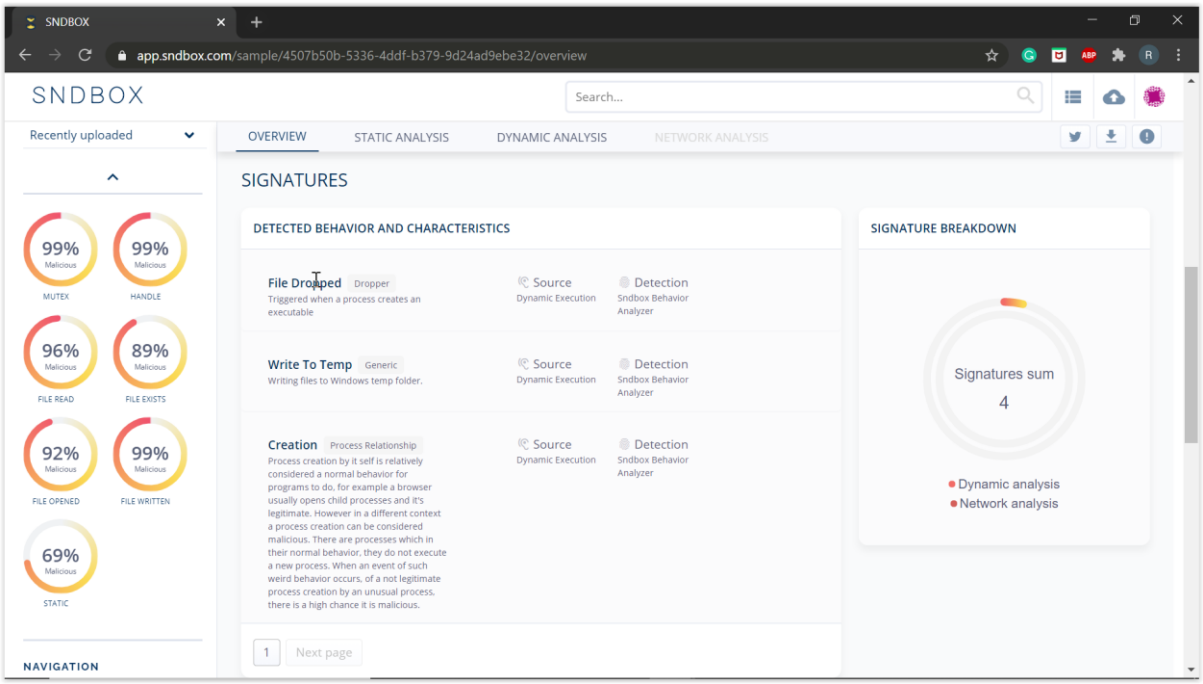


Choosing Malwares:

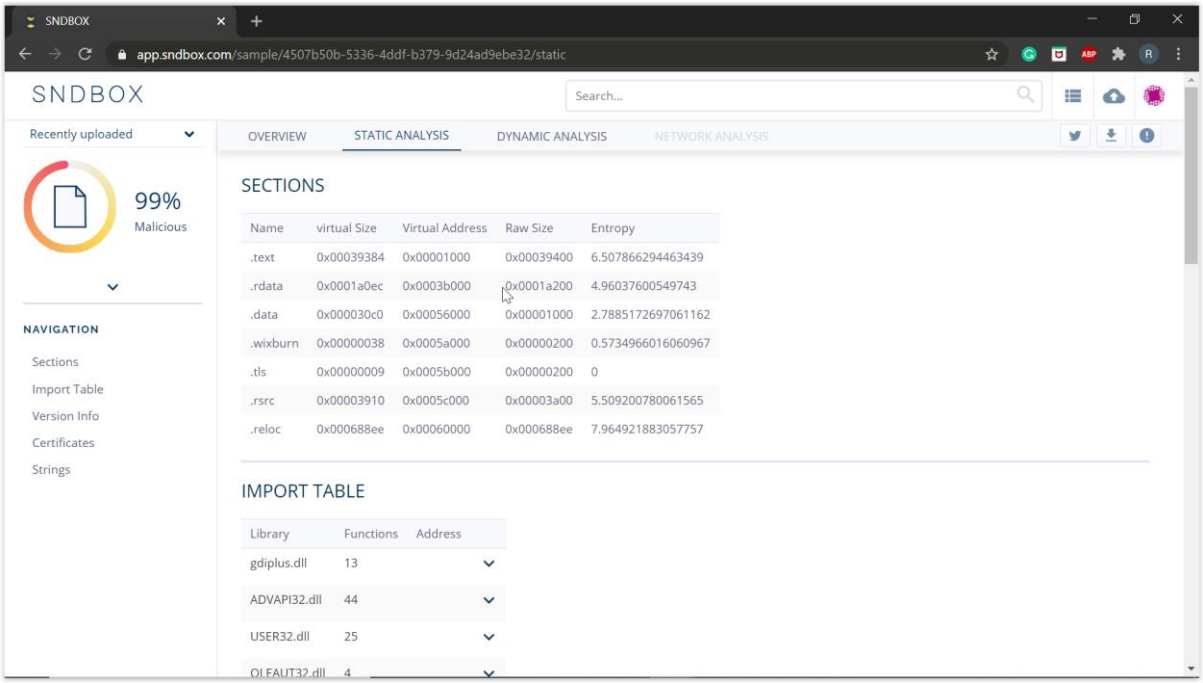


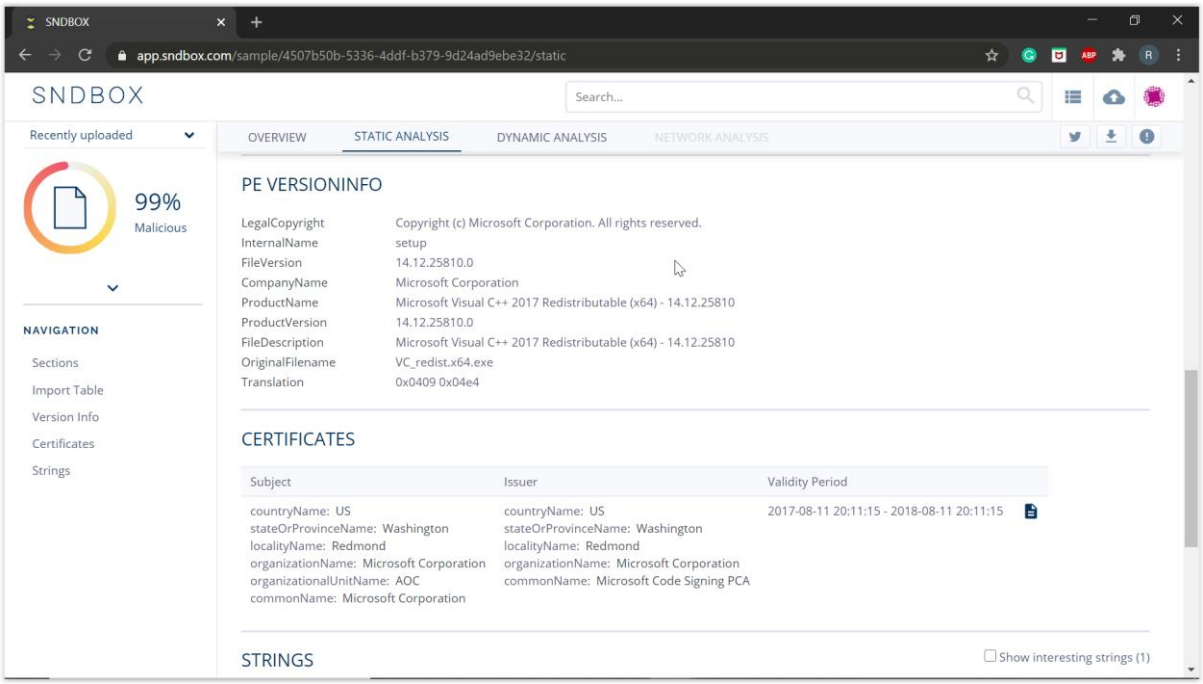
First Malware:



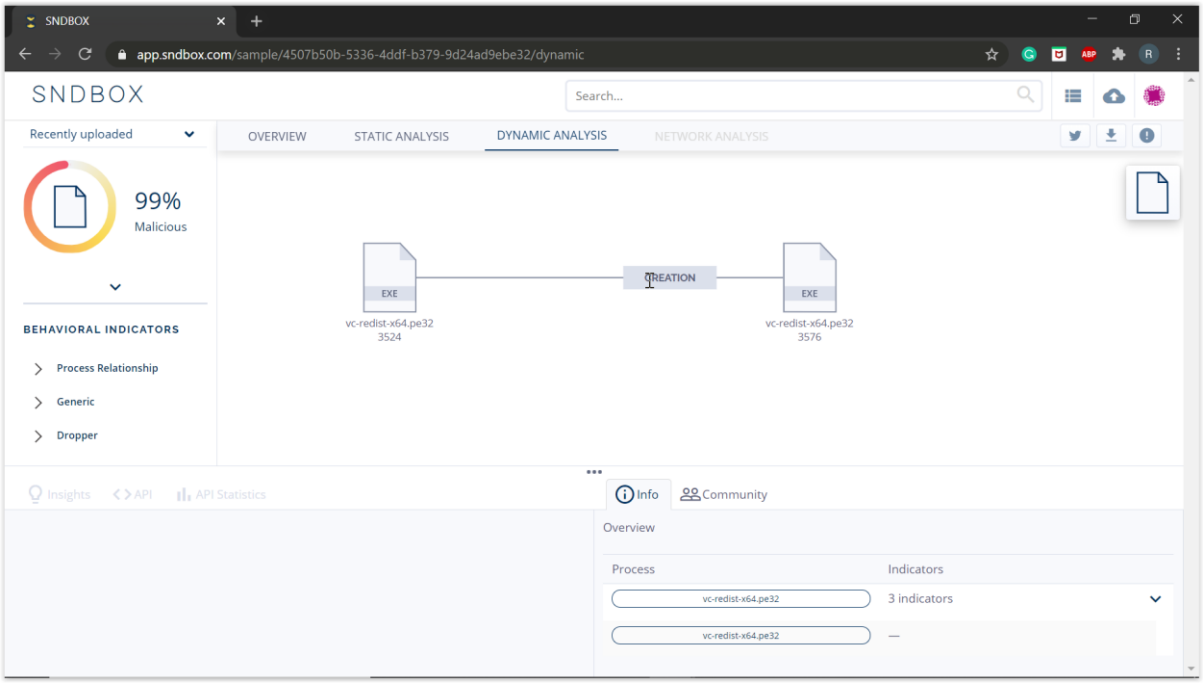


Static Analysis:

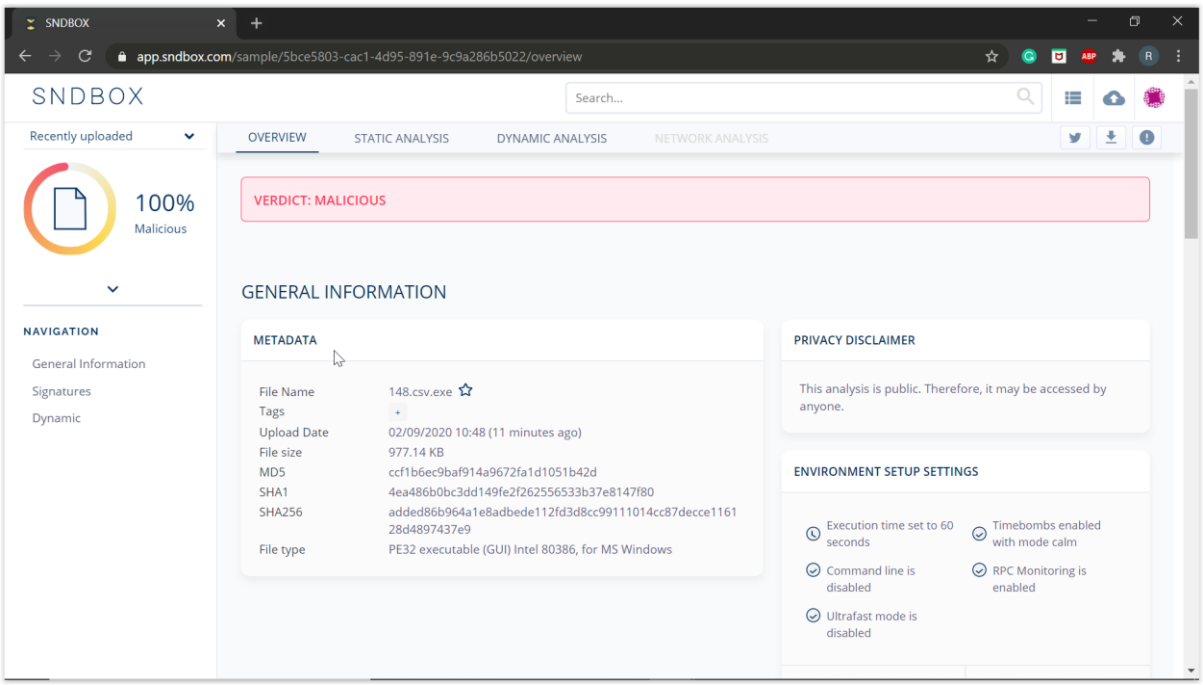


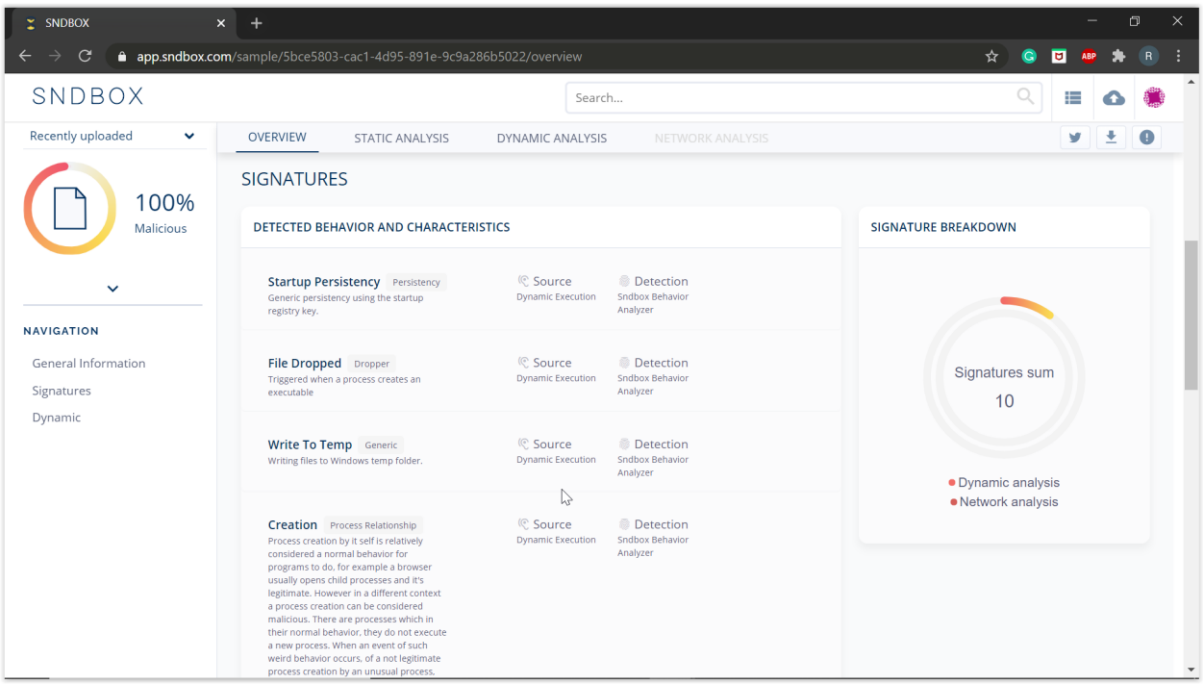


Dynamic Analysis:

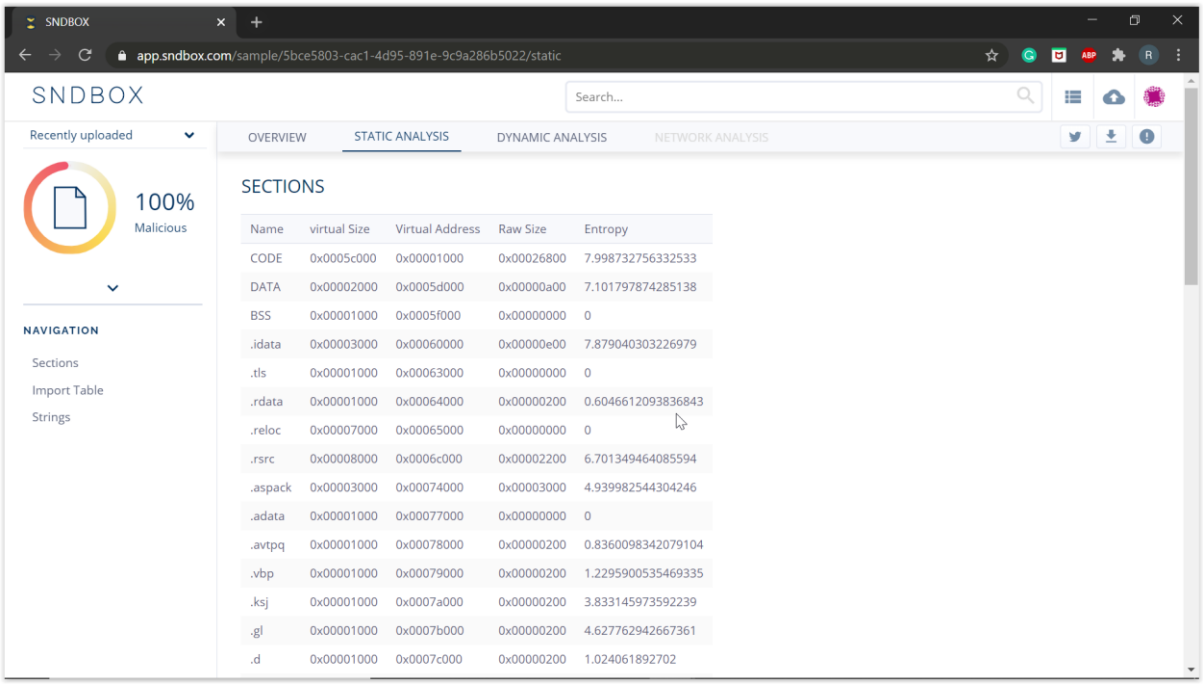


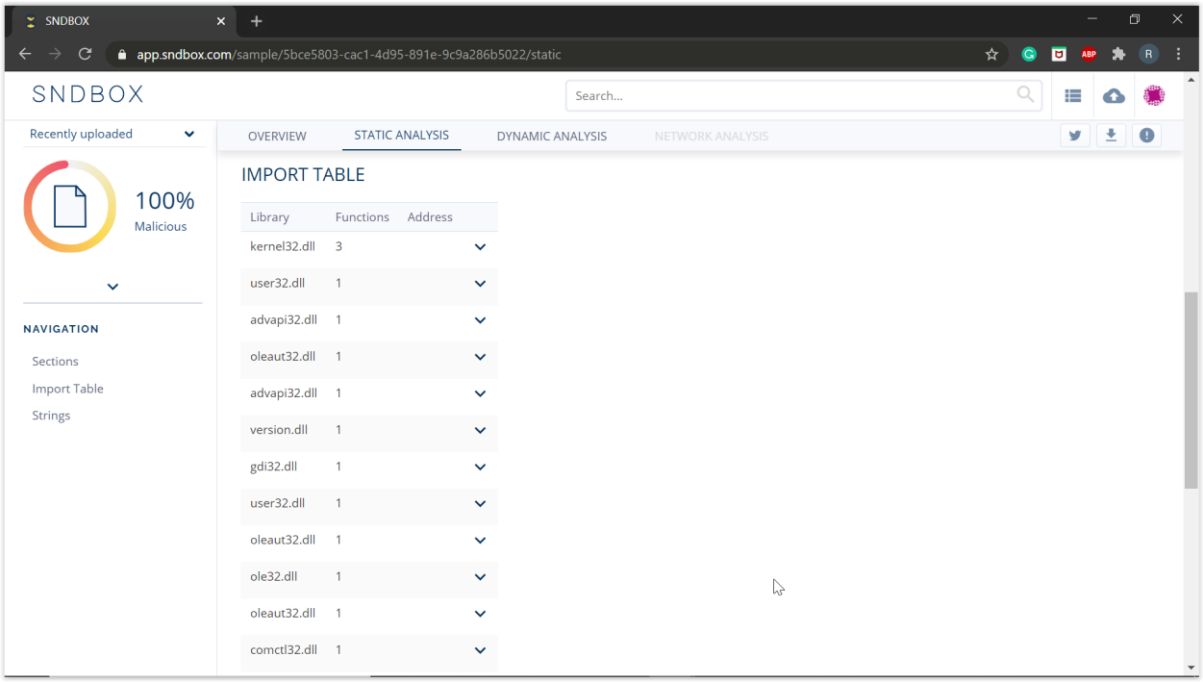
Second Malware:



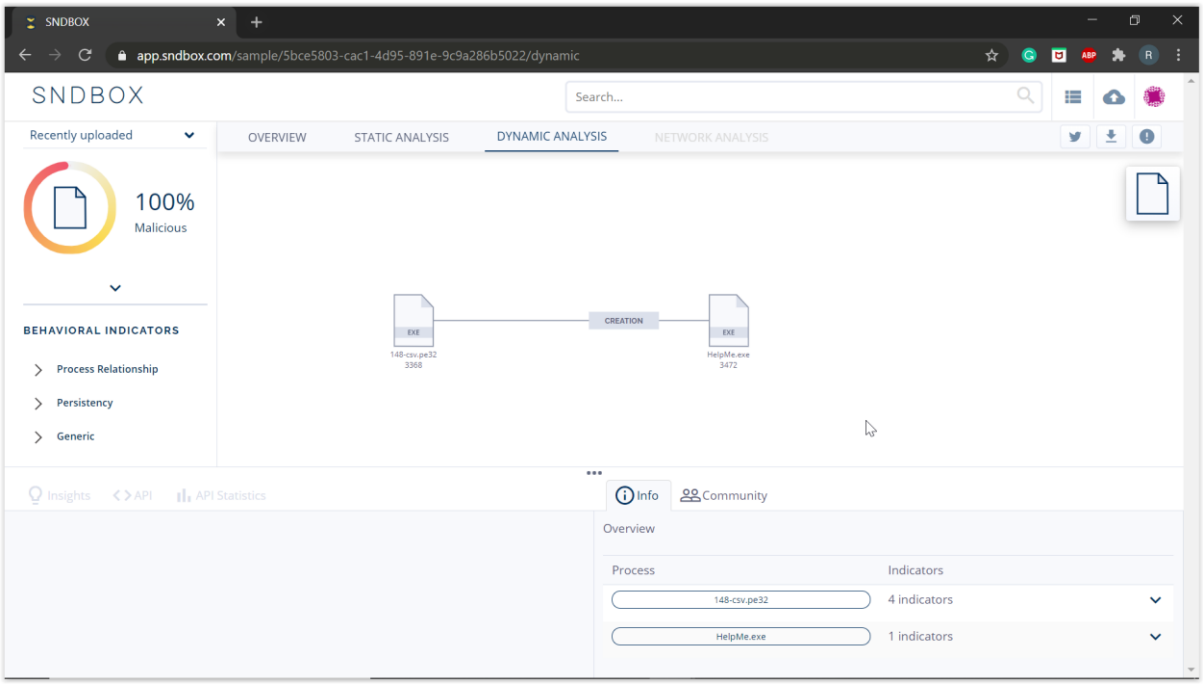


Static Analysis:

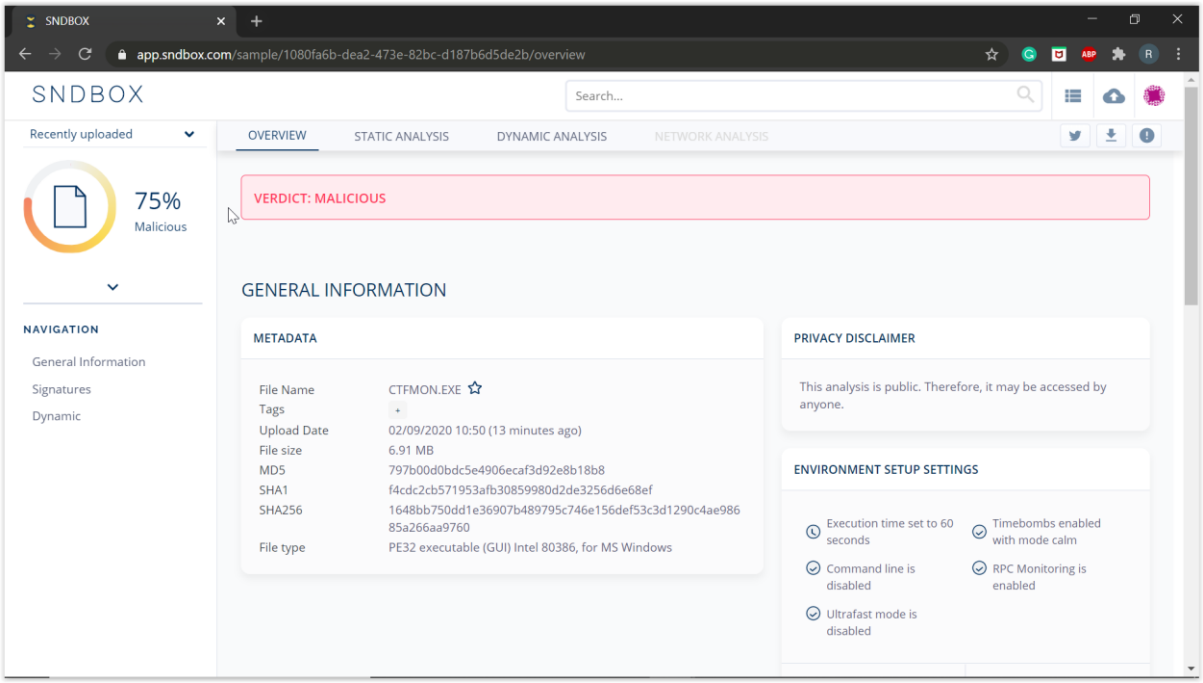


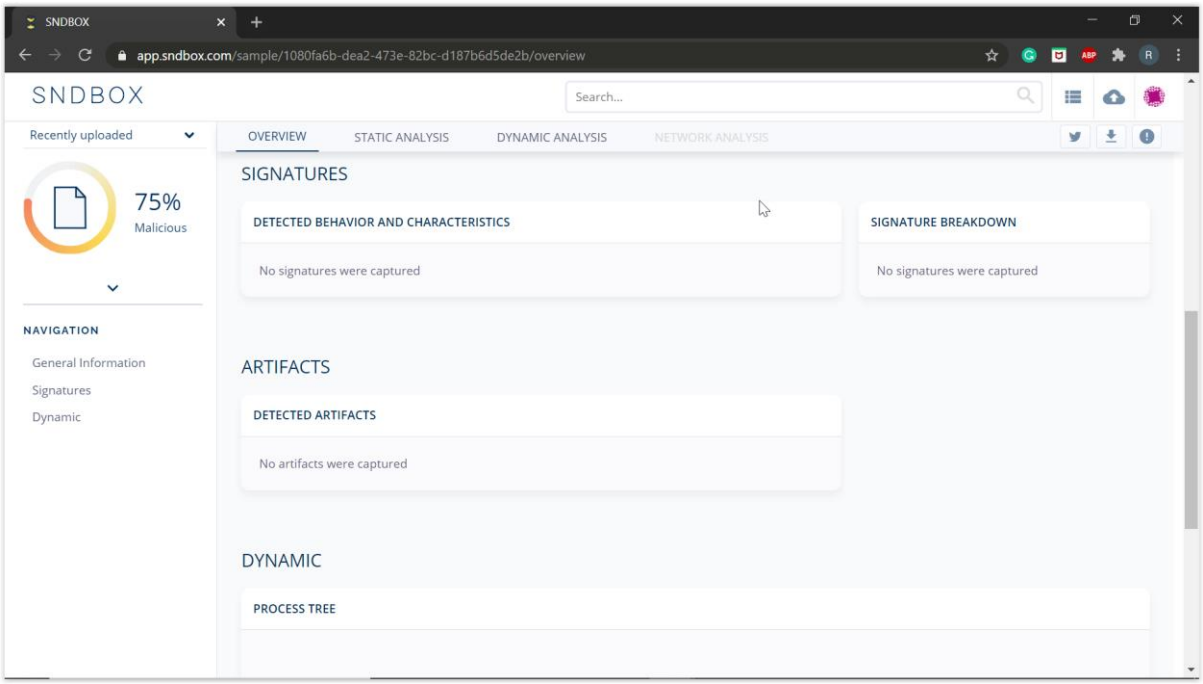


Dynamic Analysis:

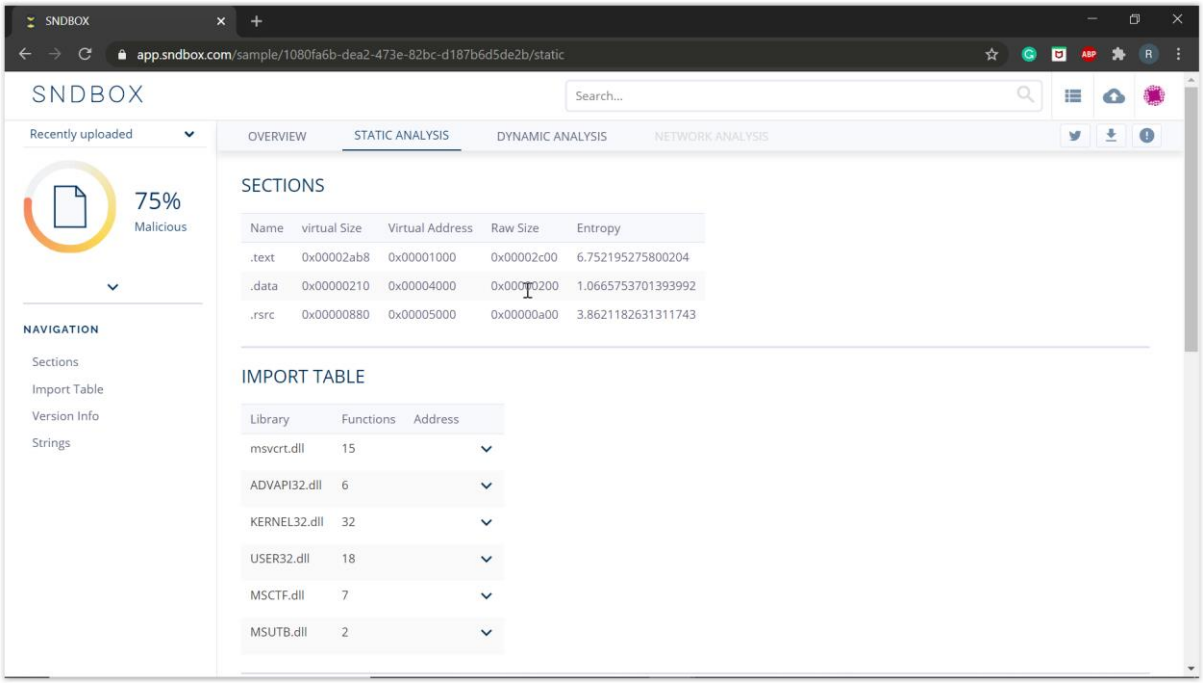


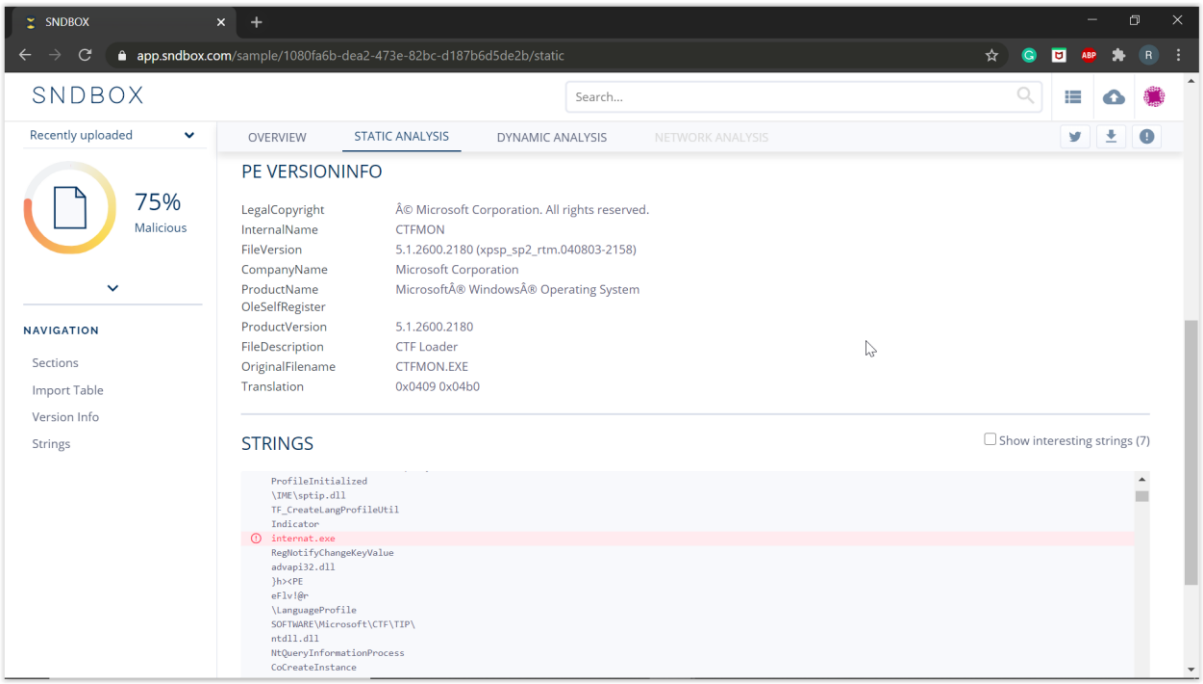
Third Malware:



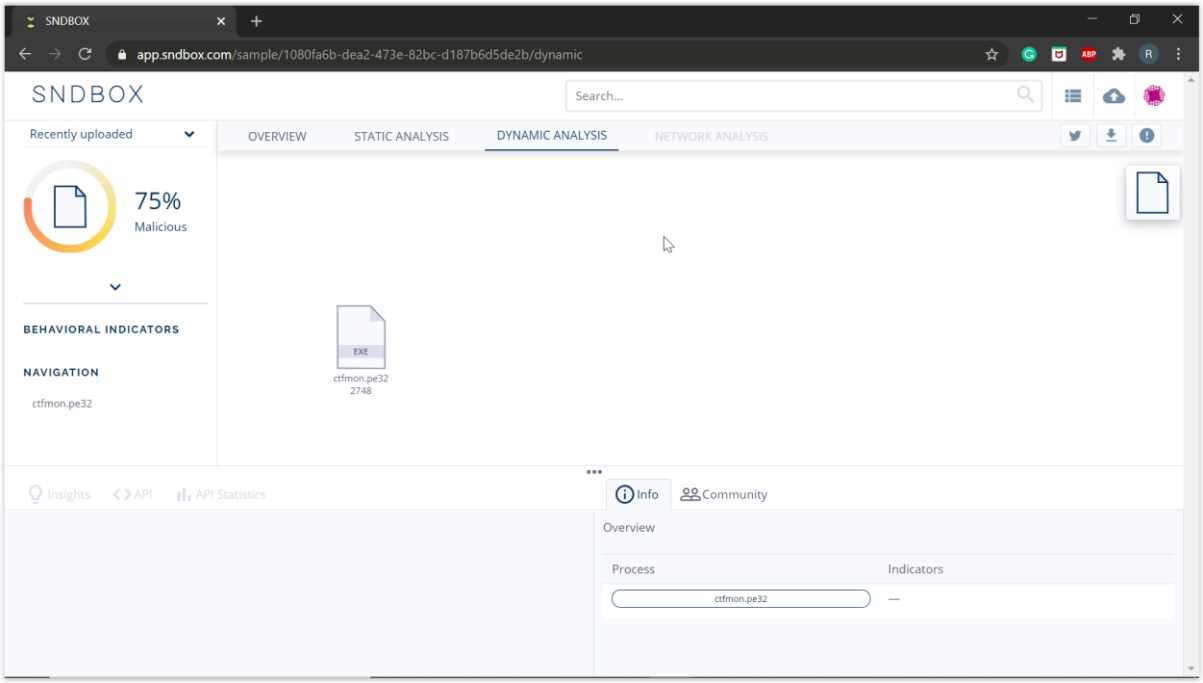


Static Analysis:

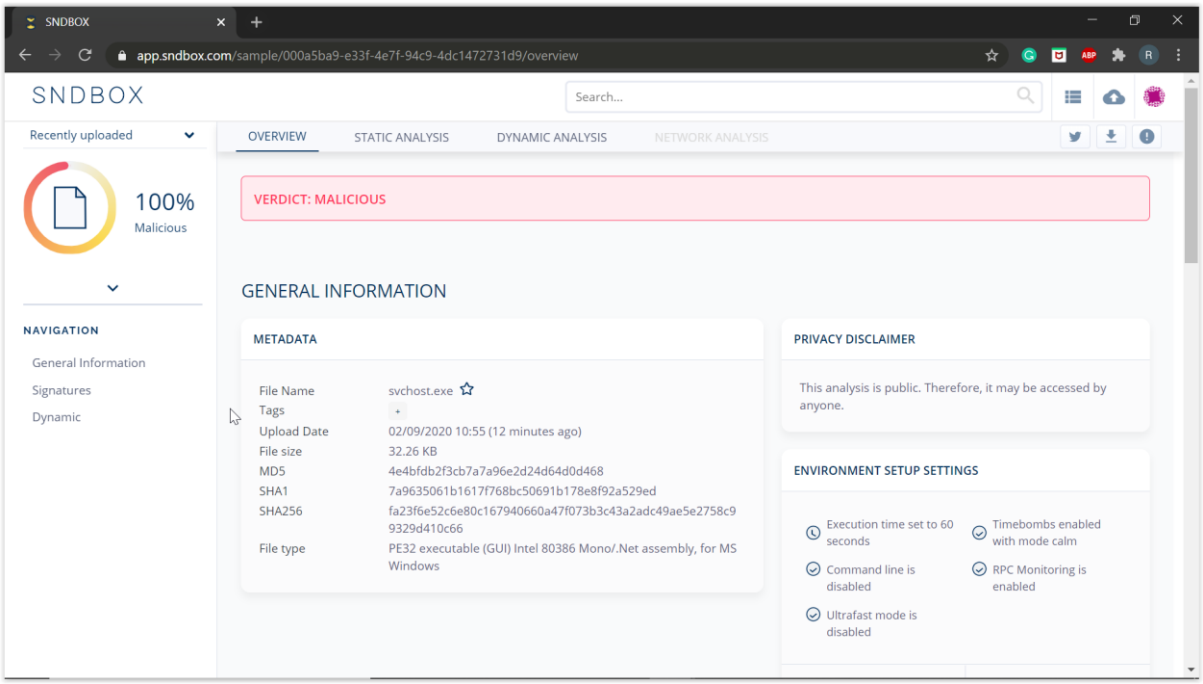


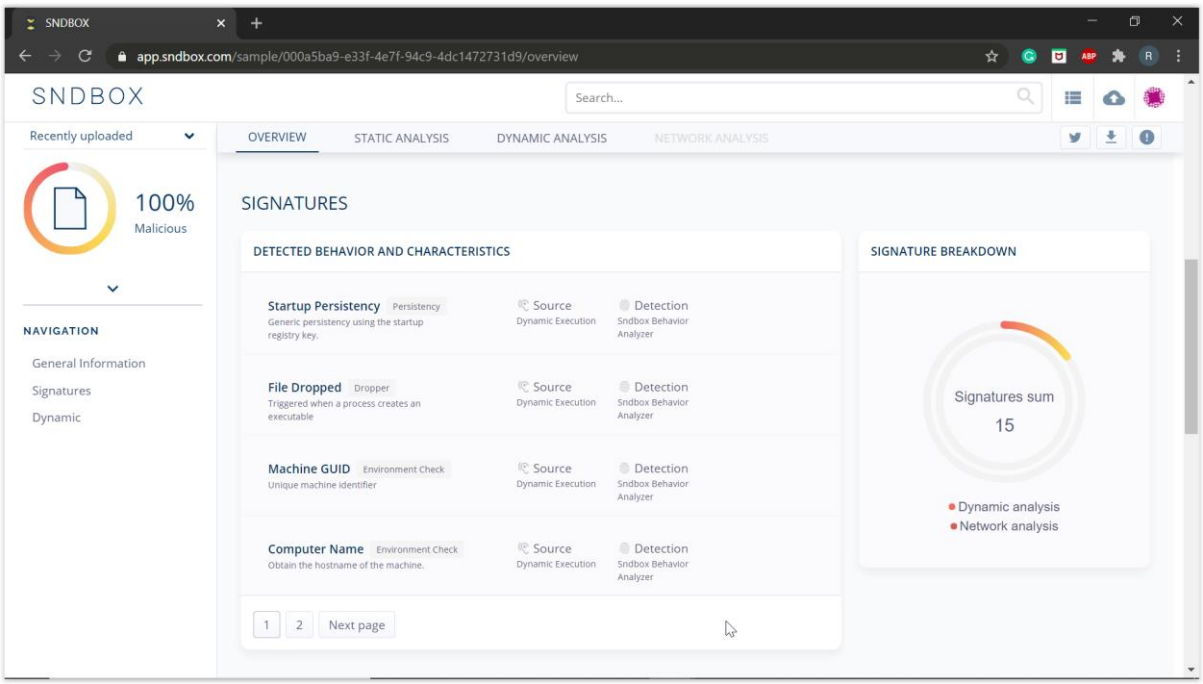


Dynamic Analysis:

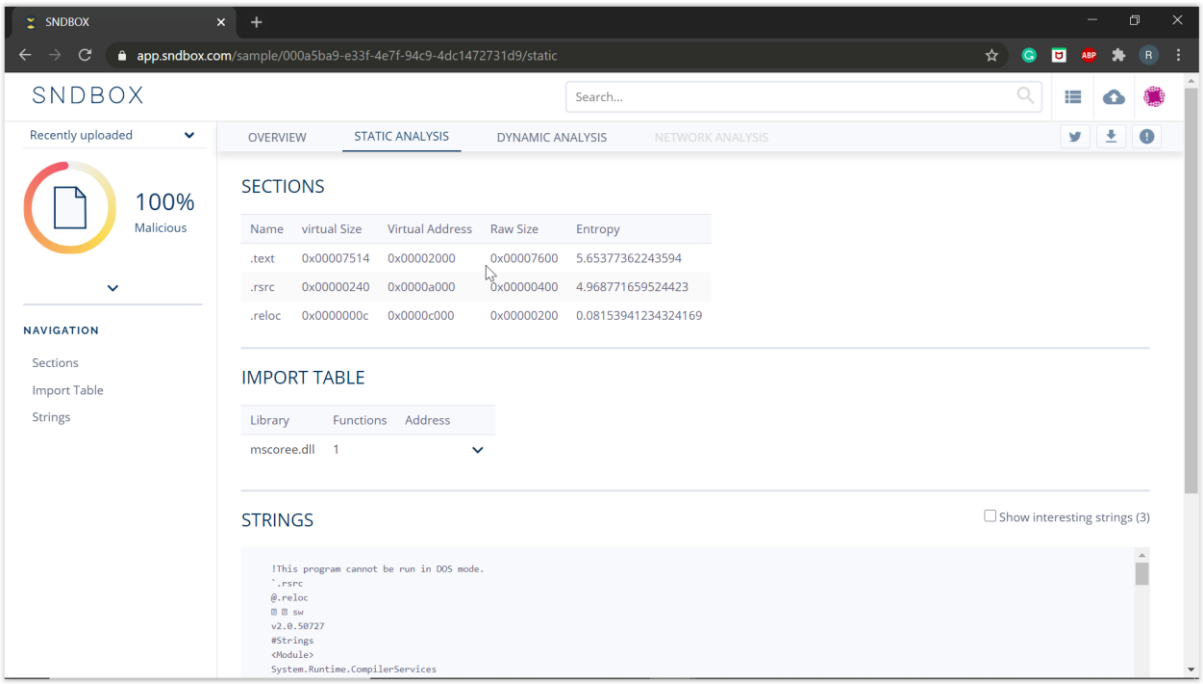


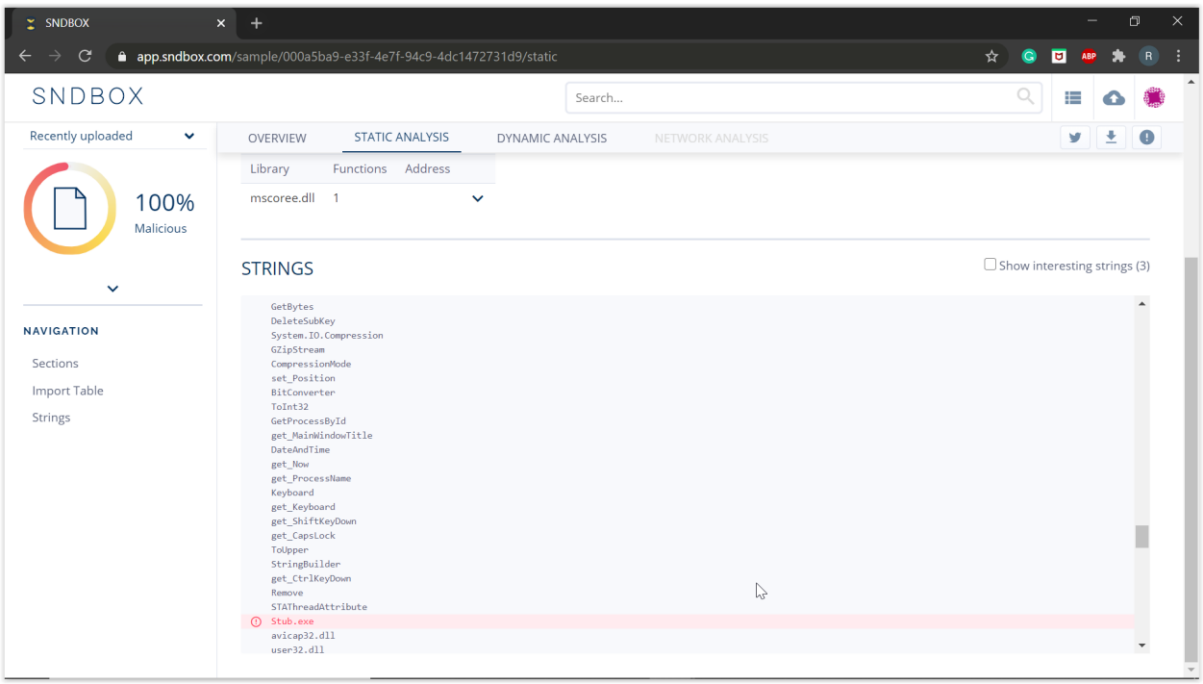
Fourth Malware:





Static Analysis:





Dynamic Analysis: