

Analyzing Indicator of compromises for Ransomware: Leveraging IOCs with Machine Learning Techniques

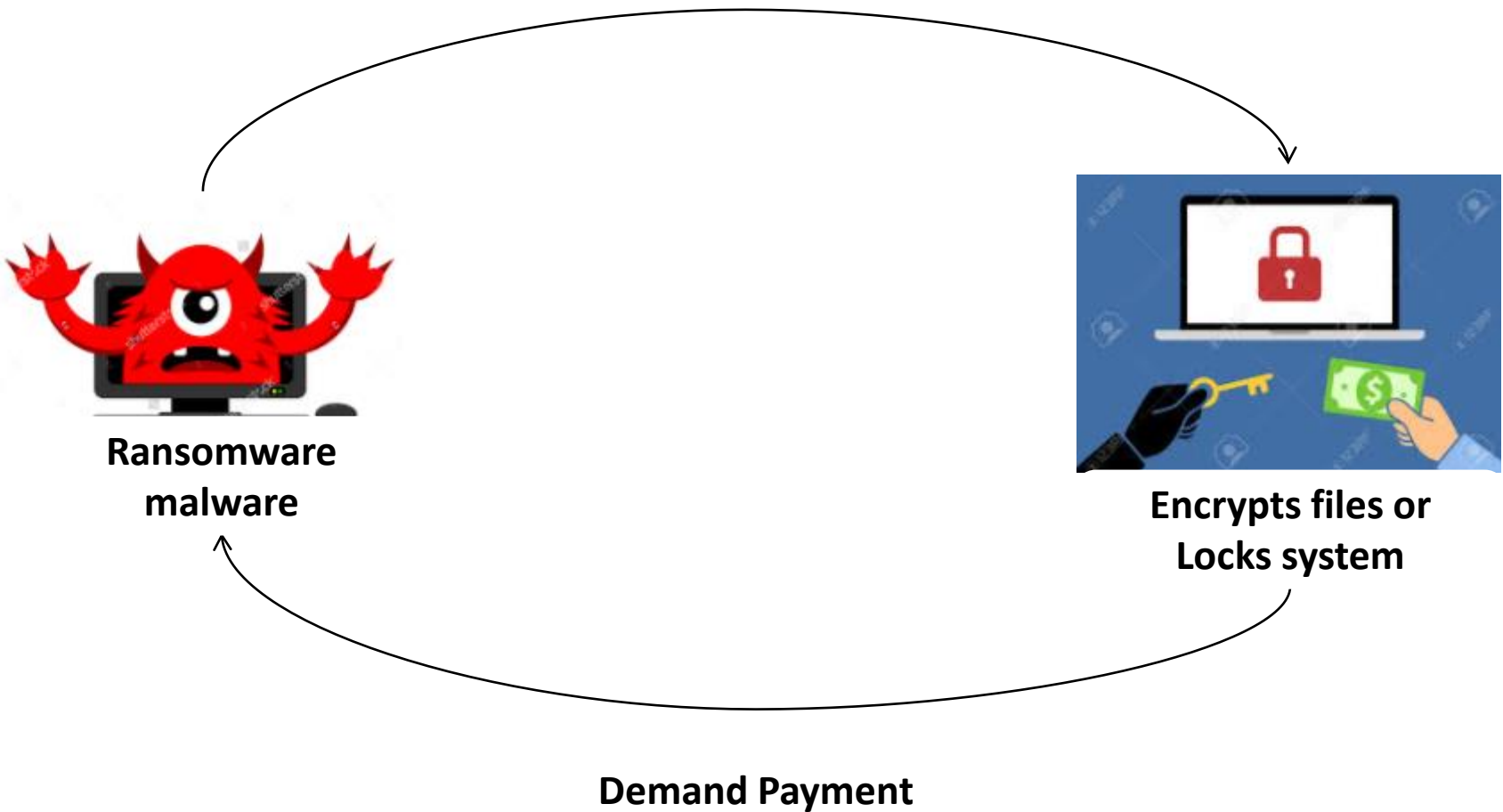
By:
Mayank Verma
9915314019

Advisors:

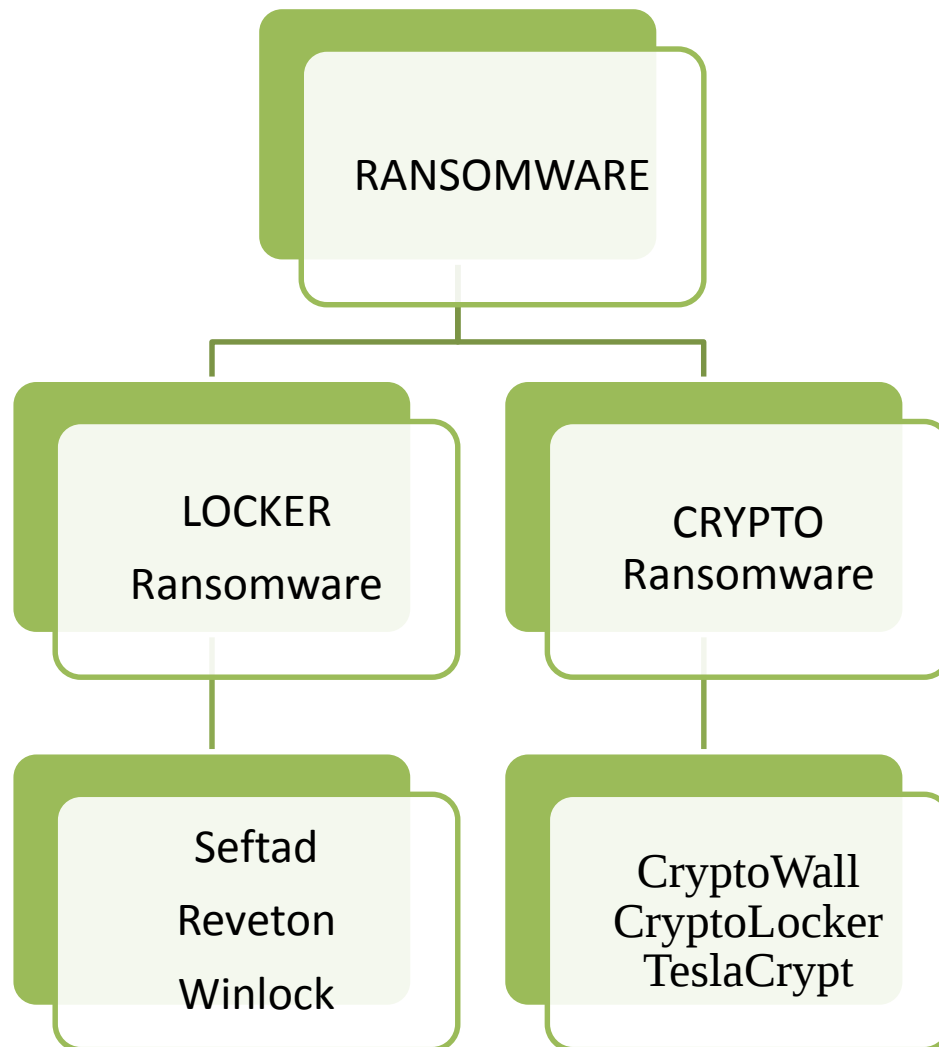
- Ms. Anuradha Gupta
- Mr. Ponnurangam Kumaragura

Ransomware

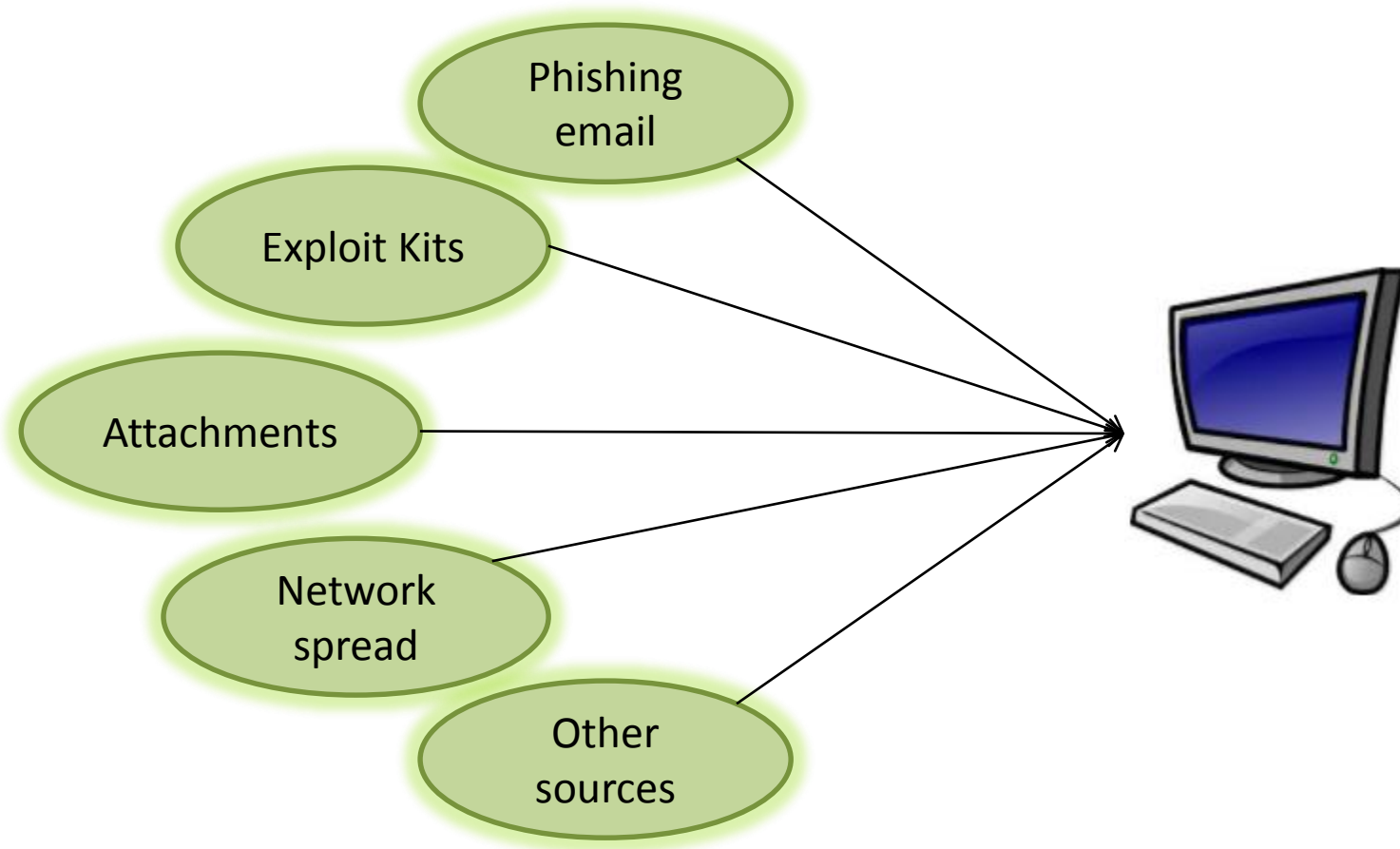
Hijack User System



Types of Ransomware



Propagation



Affected Areas

Looking at the past 5 years, governmental entities bore the **largest share** of ransomware attacks.



Motivation

University pays **\$20,000** to ransomware hackers



NEWS ANALYSIS

Hollywood hospital hit with ransomware: Hackers demand **\$3.6 million** as ransom

By Darlene Storm, Computerworld | FEB 15, 2016 6:39 AM PT

Ransomware attack on Red Deer College thwarted

University of Calgary recently paid a \$20K ransom

By Robson Fletcher, Jennifer Lee, CBC News | Posted: Jun 21, 2016 3:49 PM MT | Last Updated: Jun 21, 2016 3:49 PM MT

The spread of the WannaCry ransomware attack slowed over the weekend but the respite might only be brief, experts have said. More than 200,000 computers have been affected so far.

Global cyber attack isn't over yet, your phone could be ransomware's next target

THE ECONOMIC TIMES

UPDATED: MAY 18, 2017, 01.46 PM IST

48,000 ransomware attack attempts seen in India: Quick Heal Tech

Quick Heal says 60% of the ransomware attack attempts by WannaCry virus in India were targeted at enterprises, while the rest were on individual customers

BBC

BBC iD

News

Sport

Weather

Shop

Earth

Travel

NEWS

Home

Video

World

Asia

UK

Business

Tech

Science

Magazine

Entertainment

Technology

Microsoft warns ransomware cyber-attack is a wake-up call

© 15 May 2017 | Technology

f t b e Share

Problem Statement



To Identify Indicator of Compromises (IOCs) for ransomware

Classification of unknown ransomware samples using machine learning classifiers

Related Work

Static & Dynamic

- Signature based approach (Static): signatures like code, frequency of occurrence, executable processes and cryptographic operations
- UNVEIL (Dynamic): desktop attribute change, Input Output file buffers and entropy change in file system

Network

- Connection-Monitor & Connection- Breaker: communication of victims system with C&C server
- HTTP Traffic characteristics (HTTP POST messages): between the infected host and a proxy server to detect ransomware data exchange, for Cryptowall, Locky ransomware

Others

- Specific to Cryptolocker ransomware: payment mode
- Specific to android platform: .APK Files structures of android application, critical path and data flow, malicious domain access, malicious charges, and android permissions.

Related Work



Generalised Malwares

- Interactions between malware and sensitive system resources
- File, Registry, Process, Network
- Prototype based clustering technique is used for malware clustering

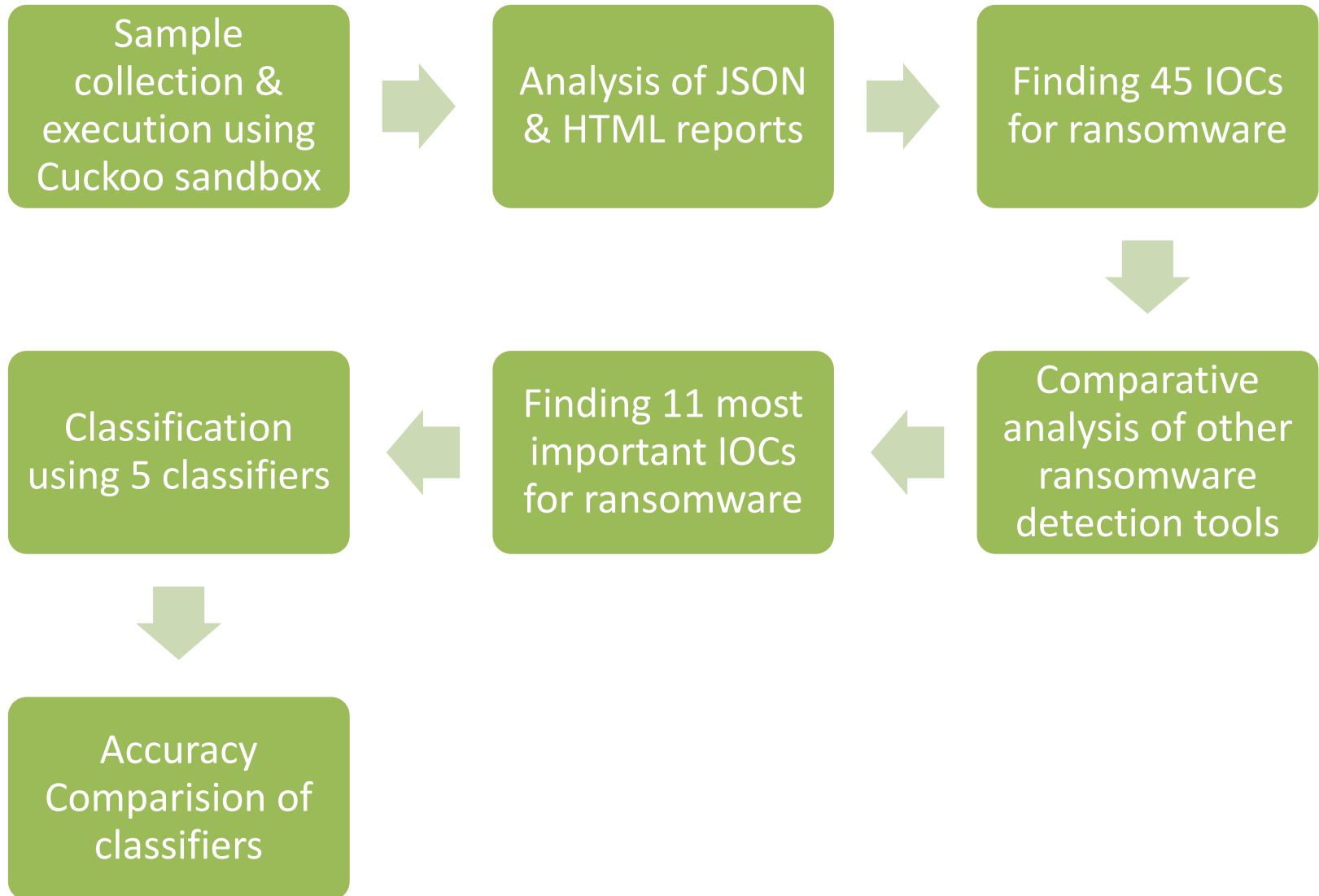
Similar work

- For all malwares
- Based on Network related features
- IP Address, Port number, & dependencies between network activities
- Modelled as Graph
- WEKA tool used for malware classification into their respective families.

Similar Work

- Ransomware & goodwillware
- Registry Keys
Operation, API Stats, Strings, File Extensions, Files Operations, Directory Operations. Dropped Files Extensions
- Analysis with limited application on VM
- Logistic Regression Classifier

Work Flow



Data Set



- virusshare.com
- malwr.com
- Ransomware samples - 848

Ransomware Variants	Number of samples
CryptoLocker	239
TorrentLocker	186
Cryptowall	181
Locky	149
TeslaCrypt	50
CTB Locker	36
Winlocker	7

Tools Used

Sample Execution

- Cuckoo Sandbox[1]

Comparative Analysis

- Bitdefender [2]
- Cryptoprevent [3]
- Cryptomonitor [4]
- CryptoDrop [5]
- HitmanPro [6]

System Automation

- MATLAB

Identified IOC's

45 Ransomware Specific IOC's identified

Static IOC (6)

System IOC (14)

Network IOC (6)

Behavioural IOC (19)

Static IOC



- Compiled recently
- Recently downloaded
- Packed/obfuscated
- Reported infected by YARA
- Imports crypto libraries
- Process signature

System IOC



- Browser security setting changed
- Deletes shadow copies
- Disable windows error recovery startup
- Disables startup repairs
- Disables UAC
- Disable Task Manager
- Stops windows security center service and prevents it from starting up on boot

System IOC



- Stops windows defender service and prevents it from starting up on boot
- Stops windows update service and prevent it from starting up on boot
- Stops Error reporting service and prevents it from starting up on boot
- Firewall disabled
- Antivirus disabled
- Stops background intelligence transfer service and prevents it from starting up on boot
- Renames file to executable

Network IOC



- Performs HTTP requests
- Connects to tor2web
- Too many DNS requests
- Too many non existent domain name responses.
- Requests to high entropy domain name
- I2P requests

Behavioural IOC



- Fingerprints the system (SystemBiosDate, Machine GUID, Digital Product ID)
- Tries to unhook windows function
- Tries to detect virtual environment
- Dropped files (downloads exe's and dll's)
- Periodic Activity
- Untrusted Processes spawning/injecting into OS processes (explorer.exe, svchost.exe)
- Temp Directory

Behavioural IOC



- Appdata Roaming
- AppData Local Directory
- Program Data Directory
- Links to crypto libraries during runtime
- WinCrypt API used- BOOL WINAPI CryptDecrypt()
- Create RWX memory
- Create hidden files
- Delete original files from disk
- Suspicious registry entry
- Mimics file times of a windows system files
- OS process encryption – writes to target files
- File/File name Encryption

Comparative Analysis with other ransomware specific tools for identification, detection & prevention

- Not all 45 IOC we used together with any of the ransomware detection tools
- Can be seen in the table*

Solution Approach

Dataset

- Training Dataset (678 samples)
- Testing Dataset (170 samples)

Feature set

- 11 most important IOCs
- Delete Shadow Copy,
- I2P Anonymity Network,
- Connect to tor2web,
- Request to high Entropy Domain Name,
- File Encryption,
- Encrypts File Name,
- Locks Screen,
- Deletes original Files from disk,
- Import and Links to Crypto Libraries,
- Packed/obfuscated,
- Create RWX memory

Classifiers

- 5 classifiers are used for classification
- Support Vector Machine (SVM)
- Linear Discriminant Analysis (LDA)
- Quadratic Discriminant Analysis (QDA)
- K- nearest neighbour (KNN)
- Complex Tree

Results and Observations

Observation for winlocker ransomware



Desktop snapshot before ransomware execution



Desktop snapshot after ransomware execution with no applications available

Snapshot of cuckoo sandbox HTML report for winlocker ransomware, showing no network related behaviour

Domains (0)

Hosts (0)

HTTP (0)

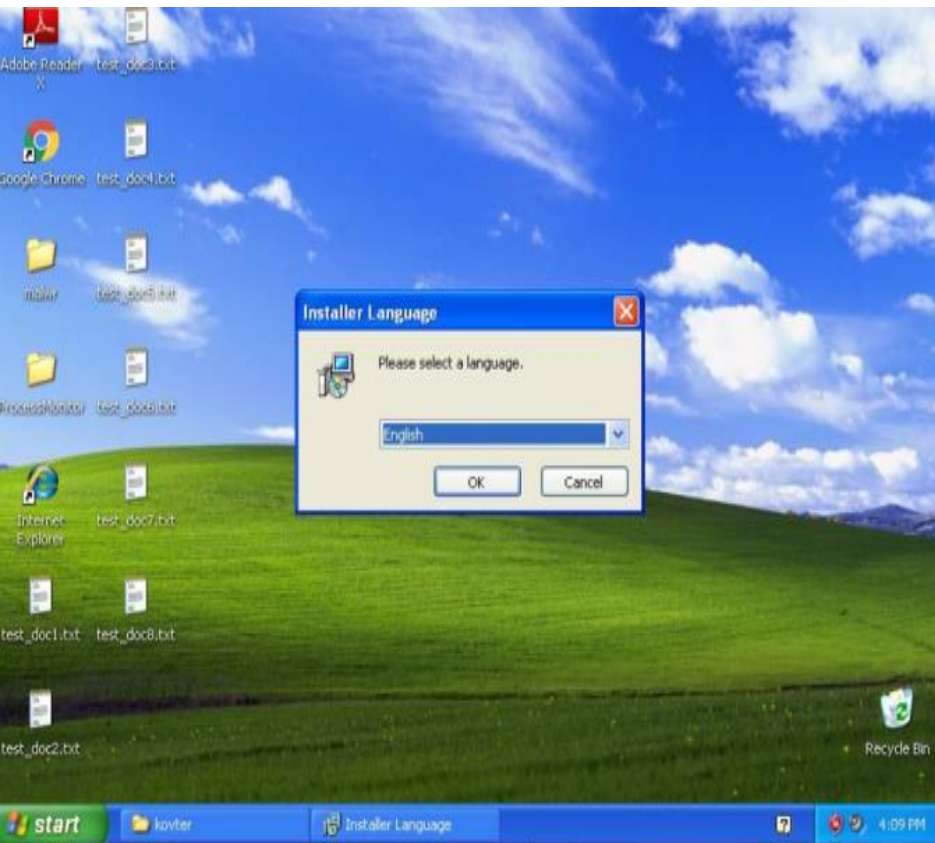
IRC (0)

SMTP (0)

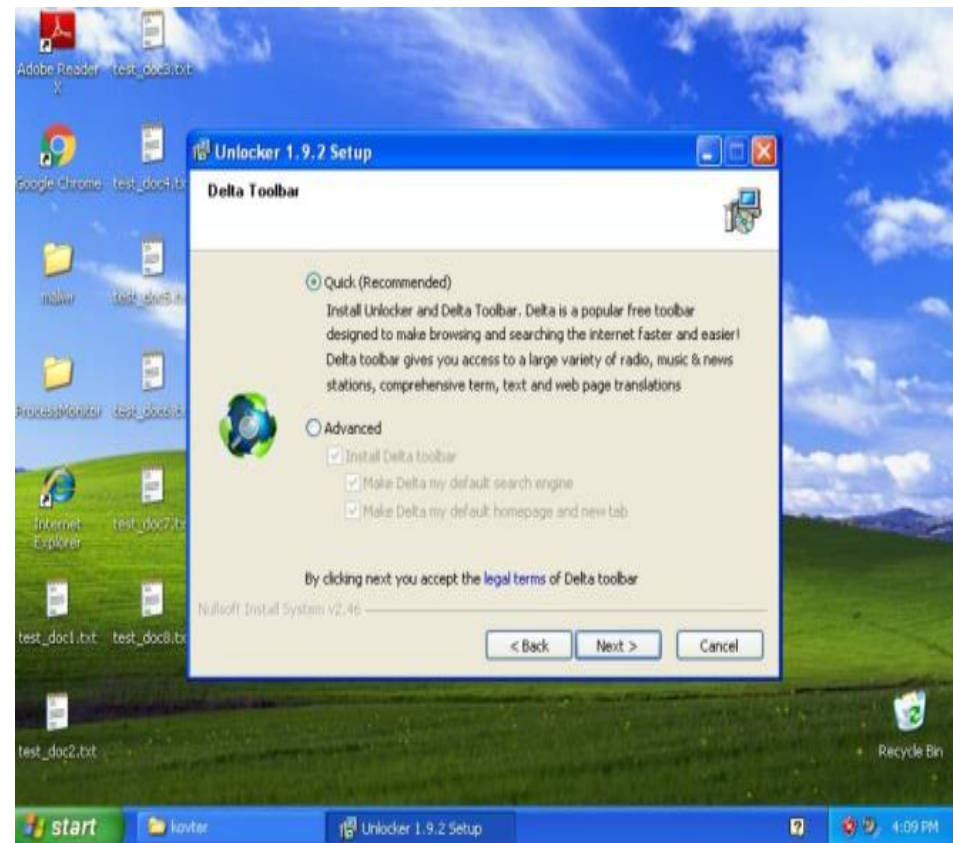
Domains

No domains contacted.

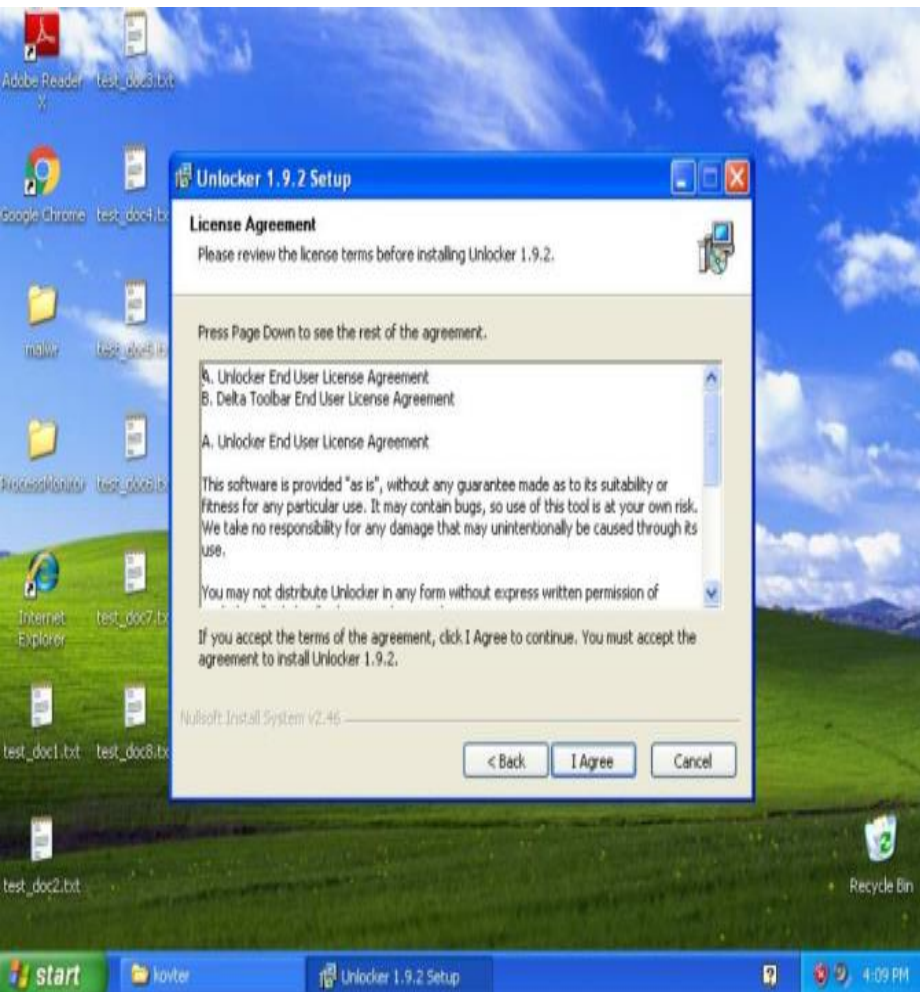
Observation for crypto ransomware, Installing Unlocker for files deletion



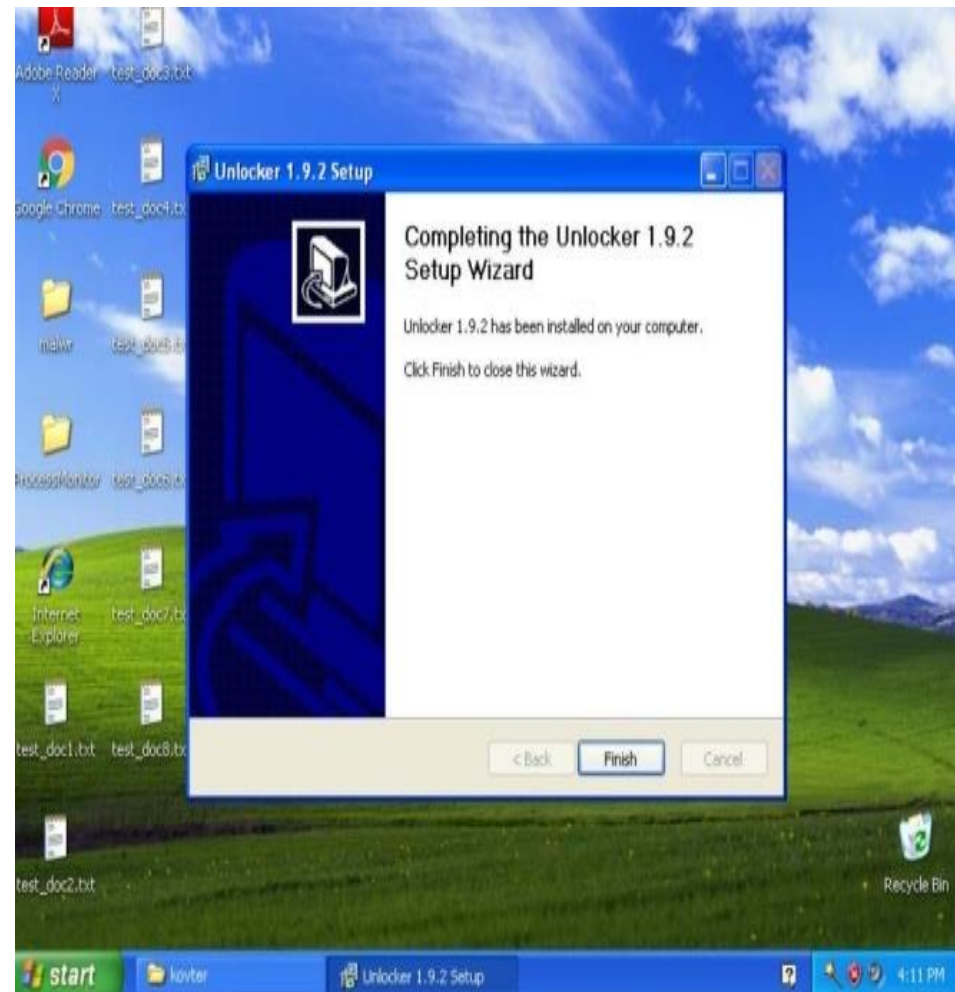
Desktop snapshot after crypto ransomware execution, showing language selection



Desktop snapshot after crypto ransomware execution, showing quick installation feature selection for unlocker installation

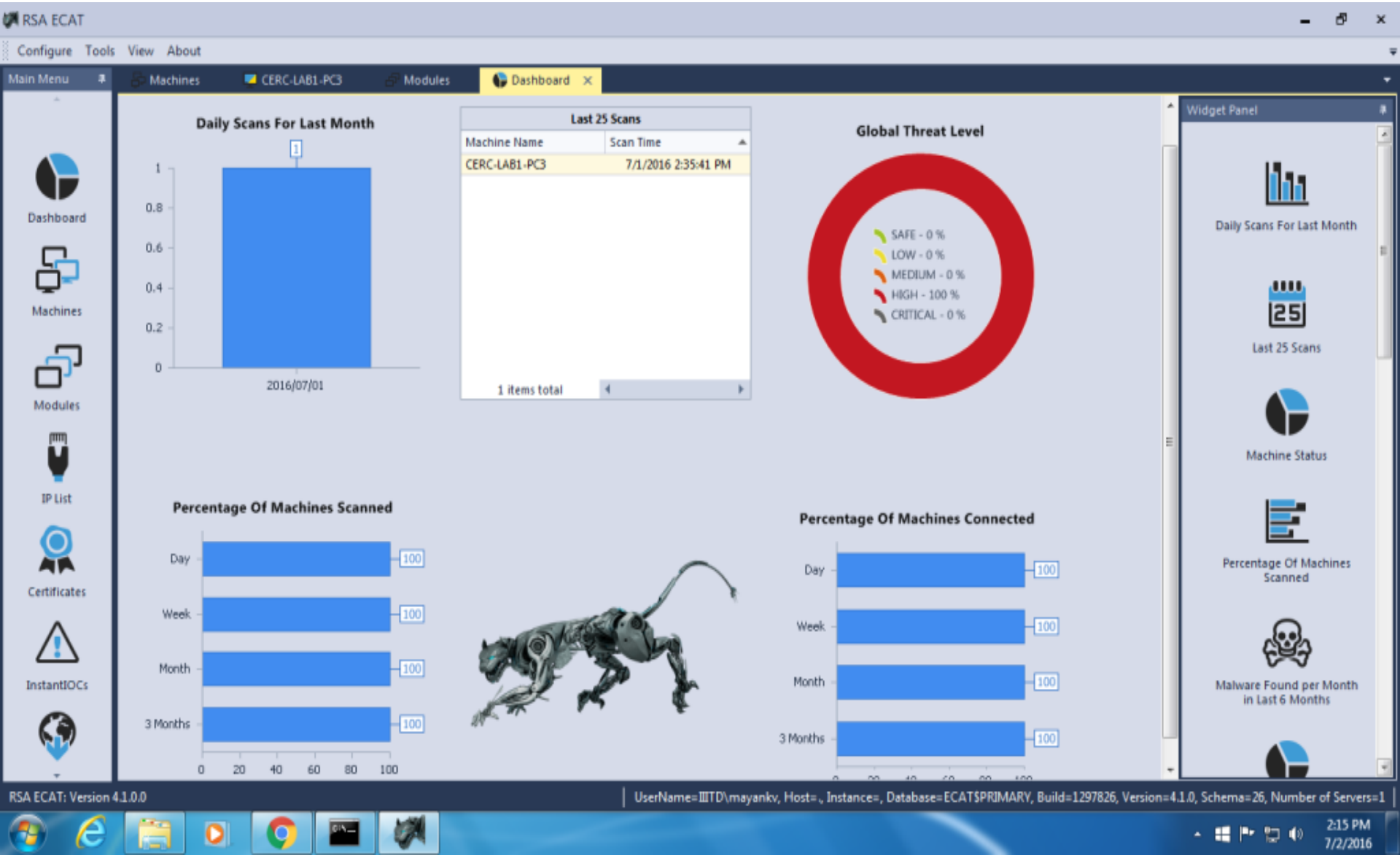


Desktop snapshot after crypto ransomware execution, showing ransomware agreement to all the terms and conditions as a legitimate user



Desktop snapshot after crypto ransomware execution, showing successful installation of unlocker for files deletion

Installed malware detection tool showing global threat level



Malware detection tool showing global threat level before ransomware execution

RSA ECAT

Configure Tools View About

Main Menu Machines CERC-LAB1-PC3

Dashboard Machines Modules IP List Certificates InstantIOCs

CERC-LAB1-PC3

135 Score Administrative Status | Last Seen | 4 mins ago

Show Whitelisted Hide Good Files Hide Valid Signature

Summary Blocked Modules History Downloaded Agent Log Scan Data More Info

Drag a column header here to group by that column

Filename	IIOC Score	Risk Score	Machine Count	Signature	Hash Lookup	Status Comment
uTorrent.exe	132	0	1	Need Revoke Update: BitTorrent Inc	Unknown	
TeamViewer_Service.exe	130	0	1	Need Revoke Update: TeamViewer	Unknown	
chrome.exe	129	1	1	Need Revoke Update: Google Inc	Unknown	
ConsoleServer.exe	129	0	1	Need Revoke Update: RSA Security LLC	Unknown	
acpi.sys	2	0	1	Need Revoke Update: Microsoft Wind...	Unknown	

683 items total

[Status] <> 'Whitelisted' Edit Filter

Machine Instant IOCs

Description	IOC Level	Bias Status
Modifies services ImagePath	1	Neutral
Duplicate section name	3	Neutral
Compiled in last month	3	Neutral
No file description	3	Neutral
Autorun	3	Neutral

10 items total

Tracking (1)

Event Time	Source Filename	Event	Target Filename
------------	-----------------	-------	-----------------

0 items total

Tracking (1) Network (28) Paths Machines Autoruns Diagram

Machine Properties

Summary All

ECAT.Components

Machine.ECAT

Agent ID	b1d44926-745a...
Blocking Ac	True
Driver Error	0xe0010014
ECAT Driver	7/20/2015 11:0...
ECAT Packa	7/1/2016 2:24:3...
ECAT Server	CERC-LAB1-PC3
ECAT Serv	7/20/2015 11:0...
Group	Default
Idle	True
Included in	True
Included in	True
Install Time	7/1/2016 2:26:1...
Last Conne	7/1/2016 3:12:0...
Last Scan	7/1/2016 2:35:4...
Online	True
Roaming A	True
Scan Start	7/1/2016 2:29:1...
Start Time	7/1/2016 2:25:5...
Version Inf	4.1.0.0

Machine.Network

DNS	192.168.1.7
Gateway	192.168.16.11
Local IP	192.168.20.136
MAC	6C:3B:E5:1D:07...
Network Se	192.168.20.0
Remote IP	192.168.20.136

Machine.OperatingSystem

Boot Time	7/1/2016 1:24:1...
Country	USA

(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

RSA ECAT: Version 4.1.0.0

UserName=III\TD\mayankv, Host=., Instance=, Database=ECAT\$PRIMARY, Build=1297826, Version=4.1.0, Schema=26, Number of Servers=1

3:20 PM 7/1/2016

Malware detection tool showing global threat level after cryptowall ransomware execution

RSA ECAT

Configure Tools View About

Main Menu Machines MAYANK x Modules - 1 Modules - 1 Modules - 1

Dashboard

Machines

Modules

IP List

Certificates

InstantIOCs

MAYANK

967 Score Last Seen | 9 mins ago

Show Whitelisted Hide Good Files Hide Valid Signature

Summary Blocked Modules History Downloaded Agent Log Scan Data More Info

Drag a column header here to group by that column

File Name	IIOC Score	Risk Score	Machine Count	Signature	Hash Lookup	Status Comment
Cryptowall-v4.exe	405	8	1	Not Signed: TRENDY Corporation	-	
bootmgr	266	3	1	Not Signed	-	
bkjyoskhf2.exe	173	5	1	Not Signed: UltraVNC	-	
svchost.exe	140	0	2	Valid: Microsoft Windows	-	
how_recover+std.txt	132	2	1	Not Signed	-	
how_recover+std.html	132	2	1	Not Signed	-	
svchost.exe	17	0	0	Not Signed	-	
1335 items total						

☒ [Status] <> 'Whitelisted' Edit Filter

Machine Instant IOCs

Description	IIOC Level	Bias Status	Event Time	Source File Name	Event	Target File Name
In root of AppDataRoaming directory	1	Neutral	9/8/2016 2:57:42.775 PM	WmiPrvSE.exe	Open System Pro...	wininit.exe
Non-Microsoft & System attributes	1	Neutral	9/8/2016 2:57:42.760 PM	WmiPrvSE.exe	Open System Pro...	csrss.exe
Autorun unsigned only executable in directory	1	Neutral				
37 items total						

Tracking (468)

468 items total

Tracking (468) Network (137) Paths Machines Autoruns Diagram

Scan Request(s) sent.

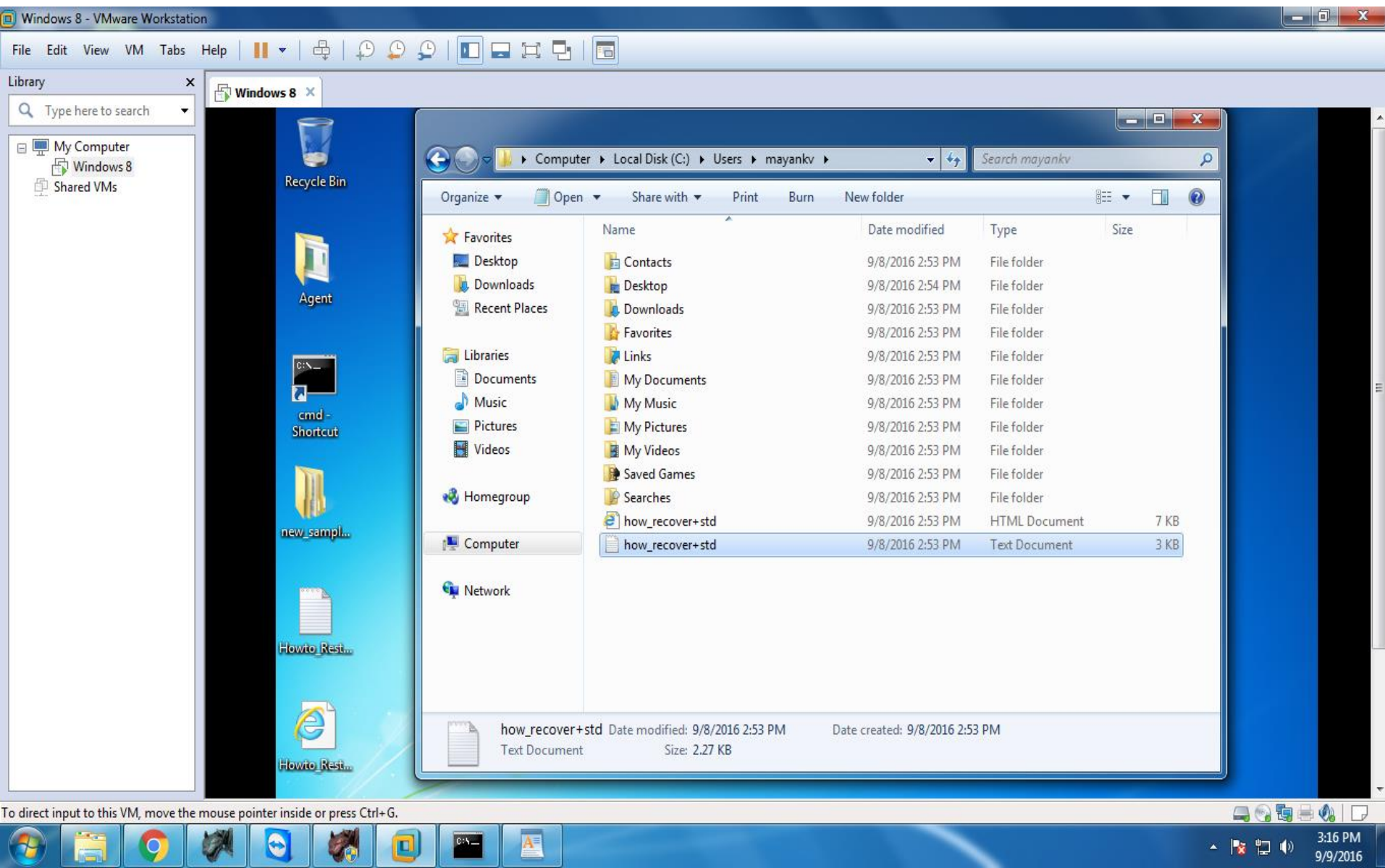
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

RSA ECAT: Version 4.1.2.0

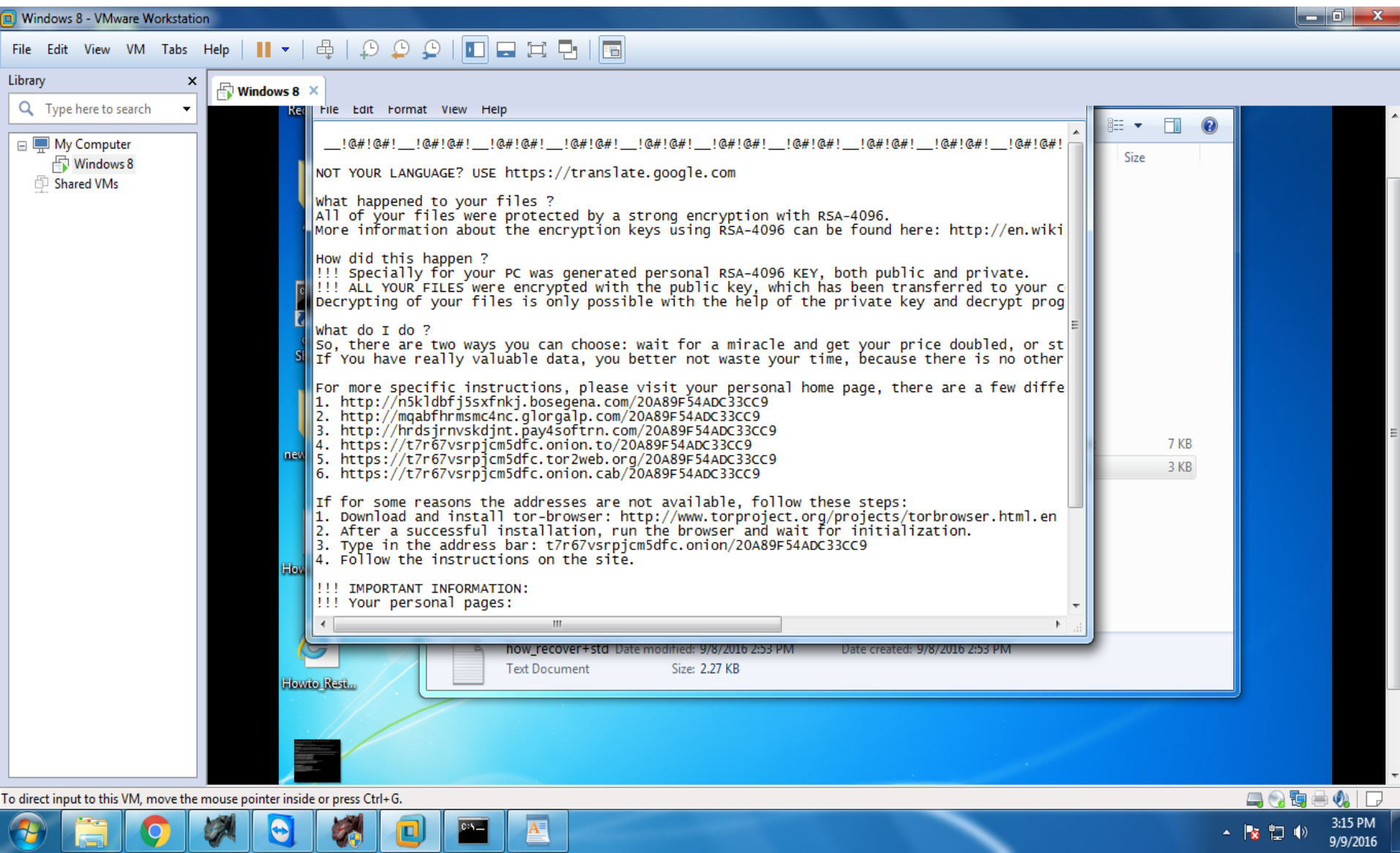
UserName=IIIITD\mayankv, Host=., Instance=, Database=ECAT\$PRIMARY, Build=1301990, Version=4.1.2, Schema=29, Number of Servers=1

3:16 PM 9/9/2016

Drive containing new file named as 'how_recover+std', created by ransomware with information of encryption and ransom to be paid



File named 'how_recover+std', created by ransomware with information of encryption and ransom to be paid



Accuracy comparison of Classifiers

Algorithm	Number of Correctly Classified Samples	Number of Misclassified Samples	Accuracy
Complex Tree	165	5	97.1%
QDA	141	29	82.9%
LDA	119	51	70.0%
SVM	99	71	58.2%
KNN	84	86	49.4%

Conclusion

- Analysed 848 ransomware samples using Cuckoo sandbox
- Identified 45 IOCs & 11 most important IOCs for 7 ransomware families
- Accuracy comparison of 5 classifiers used for classification, Complex Tree giving best results of 97.1%

Future Work

- Automation of the analysis phase
- Covering all the ransomware families

References

- [1] <https://cuckoosandbox.org/>
- [2] <https://antivirusinsider.com/bitdefender-free-anti-ransomware-tool-review/>
- [3] <https://www.foolishit.com/cryptoprevent-malware-prevention/technical-information/>
- [4] <https://www.bleepingcomputer.com/forums/t/572146/cryptomonitor-stop-all-known-crypto-ransomware-before-it-encrypts-your-data/>
- [5] <https://www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf>
- [6] http://dl.surfright.nl/hmp-command-line_reference-1_6.pdf
- [7] Ahmadian, Mohammad Mehdi, Hamid Reza Shahriari, and Seyed Mohammad Ghaffarian. "Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares." Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on.IEEE, 2015.

References

- [8] Bhardwaj, Akashdeep, et al. "Ransomware Digital Extortion: A Rising New Age Threat." Indian Journal of Science and Technology 9 (2016): 14.
- [9] Bitdefender Ransomware detection and prevention tools detailed study: <https://antivirusinsider.com/bitdefender-free-anti-ransomware-tool-review/>, accessed on: 21st April, 2017.
- [10] Cabaj, Krzysztof, MarcinGregorczyk, and WojciechMazurczyk. "Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics." arXiv preprint arXiv:1611.08294 (2016).
- [11] Chandramohan, Mahinthan, HeeBengKuan Tan, and LwinKhinShar. "Scalable malware clustering through coarse-grained behaviormodeling." Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering.ACM, 2012.

References

- [12] Dr.XinLuo and Dr.Qinyu Liao: Awareness Education as the Key to Ransomware Prevention
- [13] Kevin Liao, Ziming Zhao, Adam Doupe, and GailJoonAhn: Behind Closed Doors: Measurement and Analysis of CryptoLocker Ransoms in Bitcoin
- [14] Kharraz, Amin, et al. "UNVEIL: A Large-Scale, Automated Approach t Detecting Ransomware." 25th USENIX Security Symposium (USENIX Security 16).USENIX Association, 2016.
- [15] Nari, Saeed, and Ali A. Ghorbani. "Automated malware classification based on network behavior." Computing, Networking and Communications (ICNC), 2013 International Conference on.IEEE, 2013.
- [16] Sgandurra, Daniele, et al. "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection." arXiv preprint arXiv:1609.03020 (2016).
- [17] Tianda Yang, Yu Yang, Kai Qian, Dan Chia-Tien Lo, Ying Qian, Lixin Tao: Automated Detection and Analysis for AndroidRansomware



Thank You