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

By:
Mayank Verma
9915314019

Advisors:
- Ms. Anuradha Gupta
- Mr. Ponnurangam Kumaragura

Ransomware

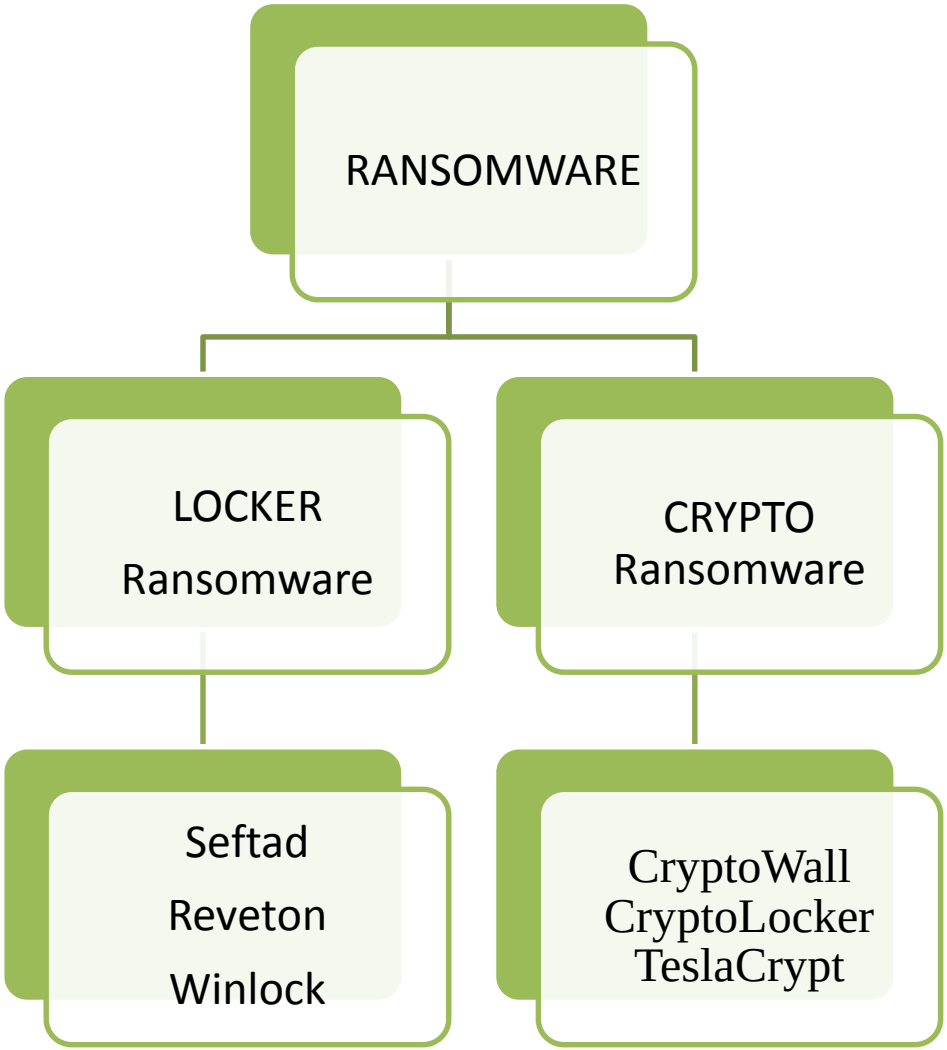
Hijack User System

Ransomware malware

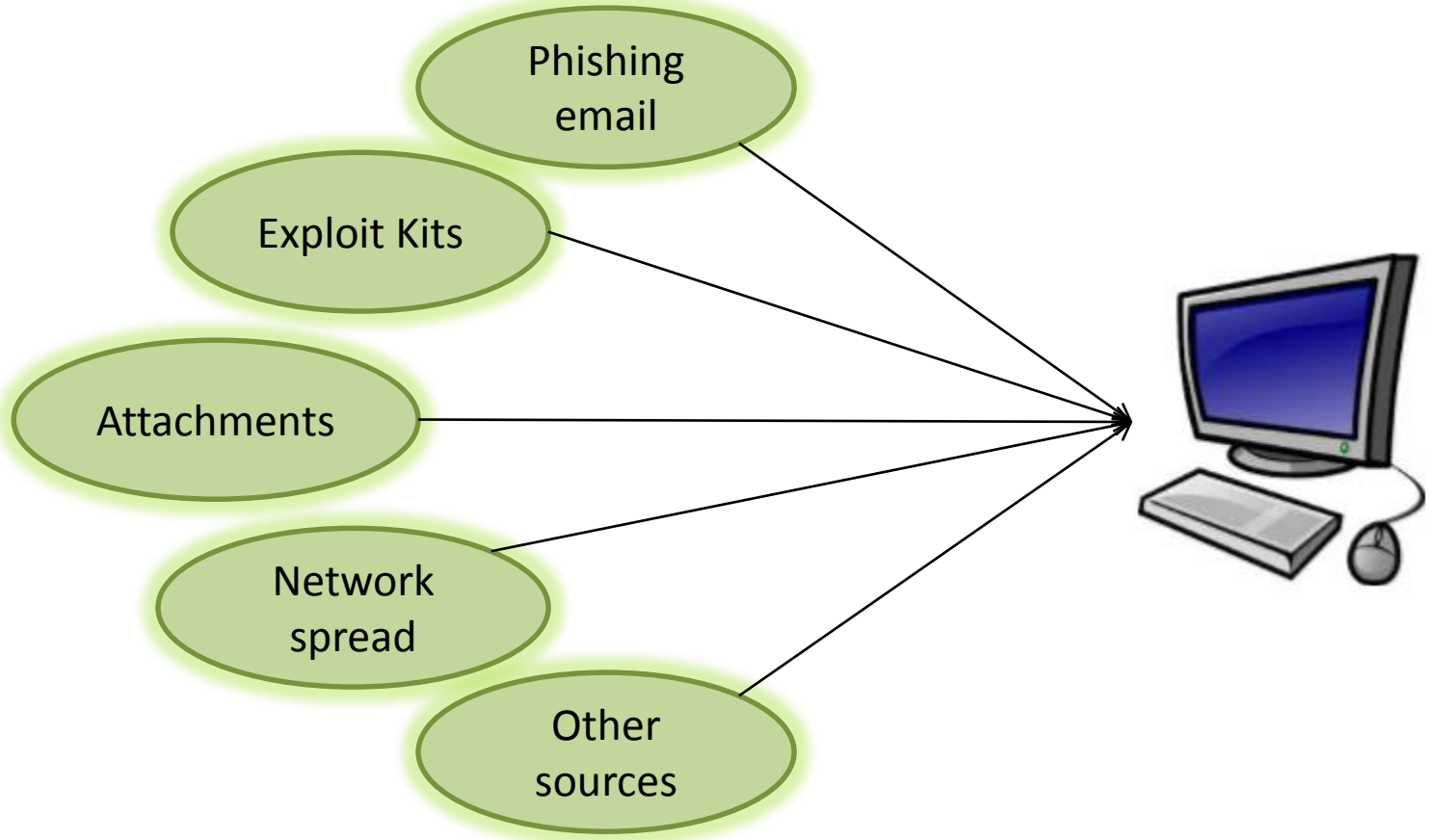
Encrypts files or Locks system

Demand Payment

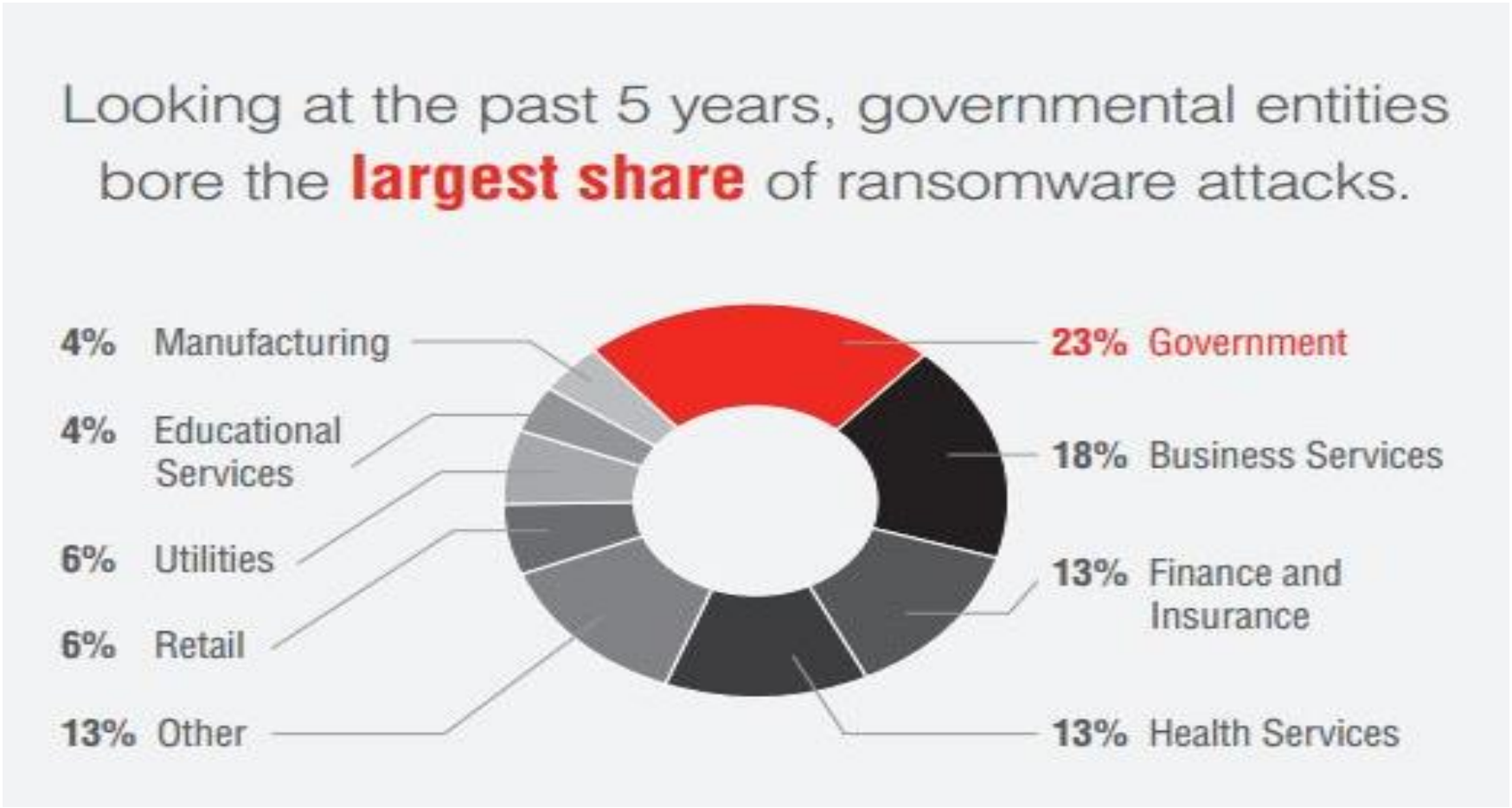
Types of Ransomware



Propagation



Affected Areas



http://www.riskmanagementmonitor.com/ransomware-threats-jump-300/

Motivation

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

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

BBC BBC iD News Sport Weather Shop Earth Travel

NEWS

Home Video World Asia UK Business Tech Science Magazine Entertainm

Technology

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

15 May 2017 | Technology

Share

Problem Statement

To Identify Indicator of Compromises (IOCs) for ransomware

Classification of unknown ransomware samples using machine learning classifiers

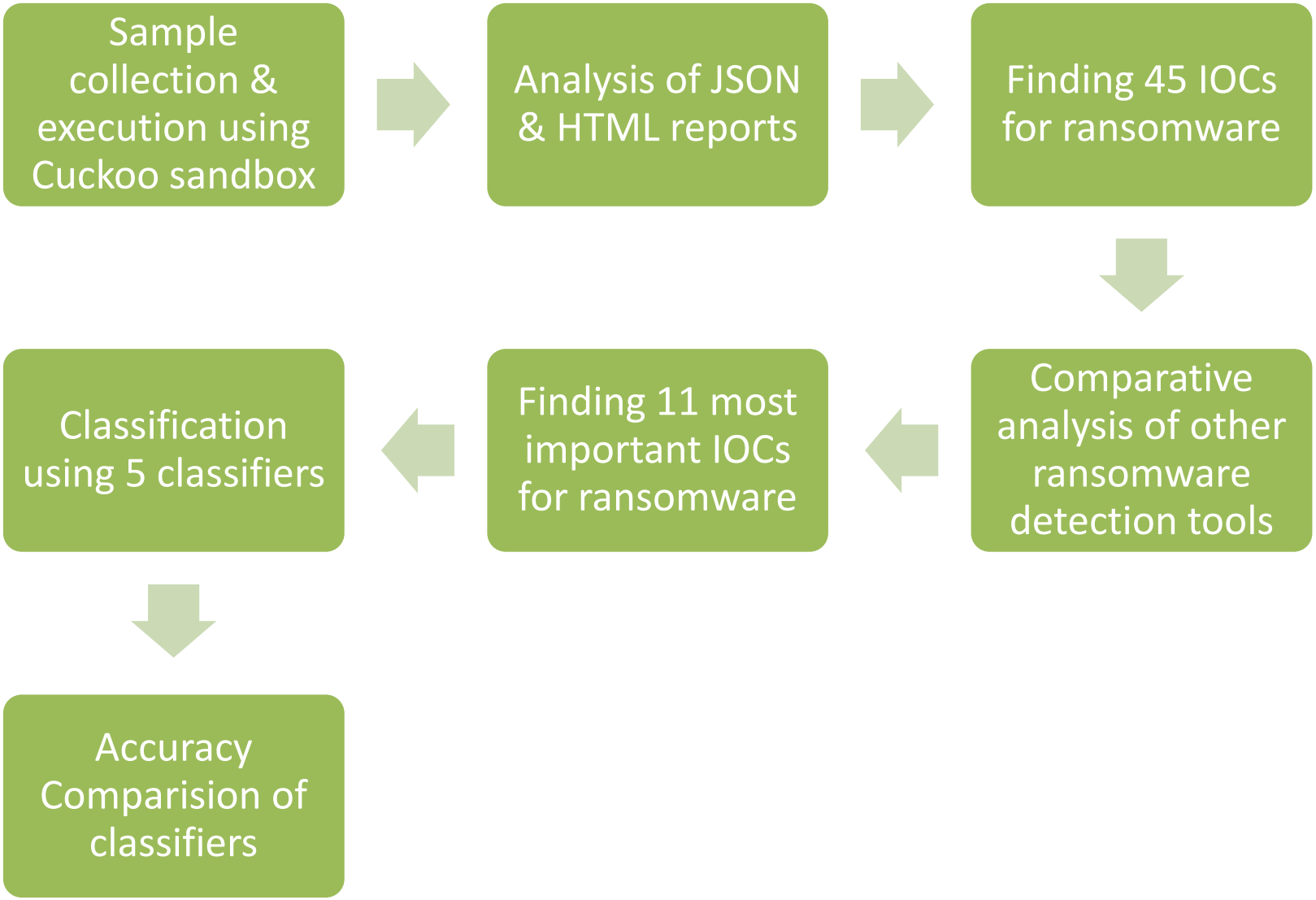
Related Work

Static & Dynamic	Network	Others
• 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	• 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	• 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	Similar work	Similar Work
• Interactions between malware and sensitive system resources • File, Registry, Process, Network • Prototype based clustering technique is used for malware clustering	• For all malwares • Based on Network realted features • IP Address, Port number, & dependencies between network activities • Modelled as Graph • WEKA tool used for malware classification into their respective families.	• Ransomware & goodware • 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


Sample collection & execution using Cuckoo sandbox
Analysis of JSON & HTML reports
Finding 45 IOCs for ransomware
Comparative analysis of other ransomware detection tools
Finding 11 most important IOCs for ransomware
Classification using 5 classifiers
Accuracy Comparision of classifiers

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

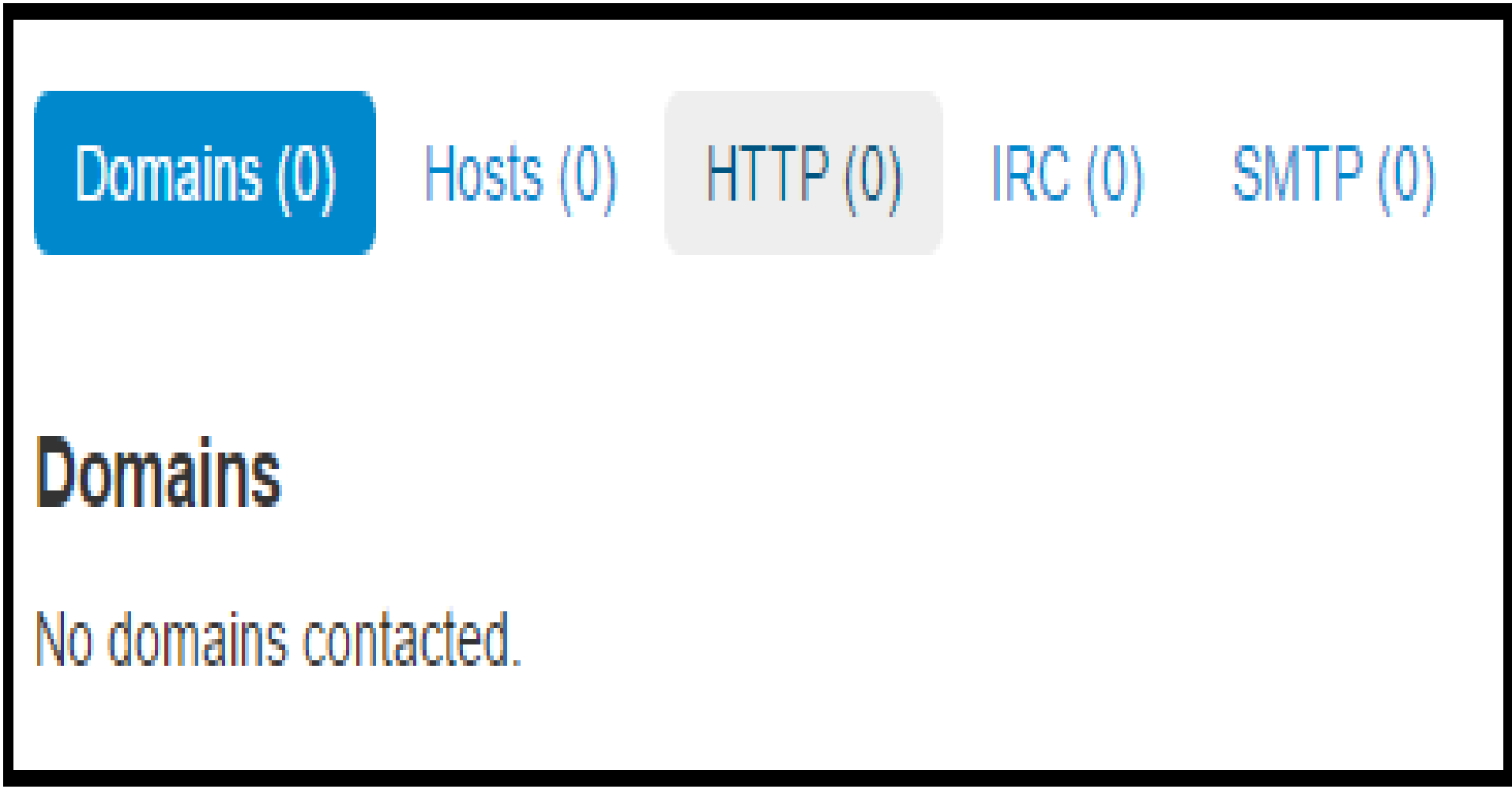
Results and Observations

Observation for winlocker ransomware

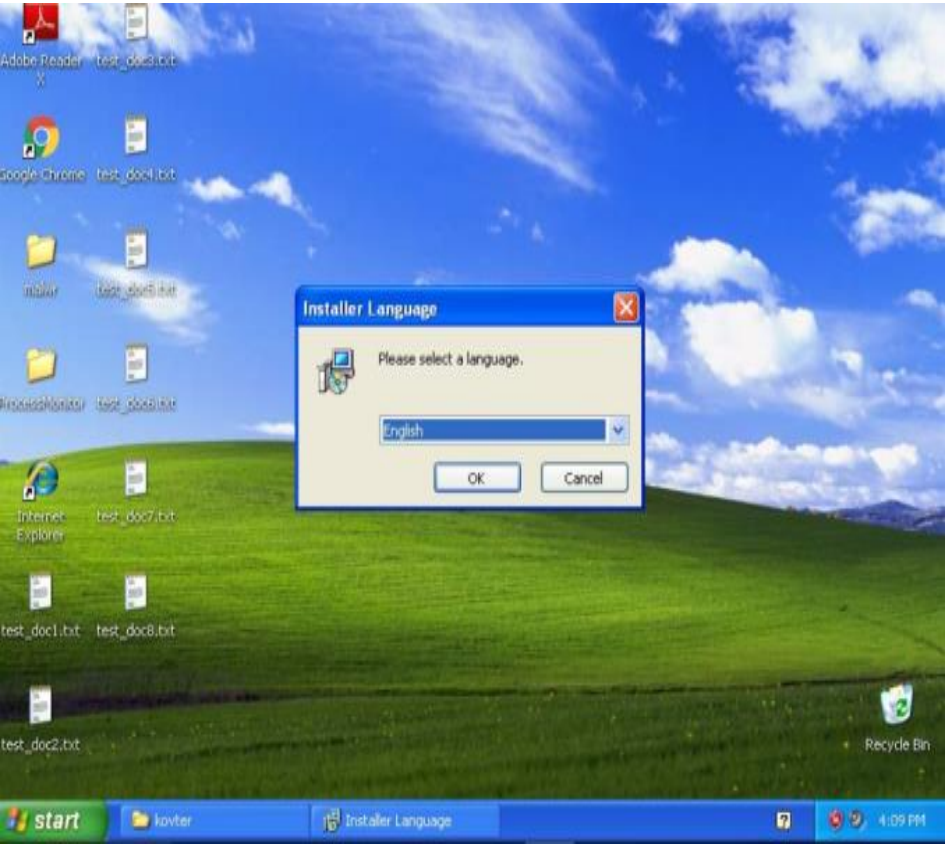
Desktop snapshot before ransomware execution

Desktop snapshot after ransomware execution with no applications available

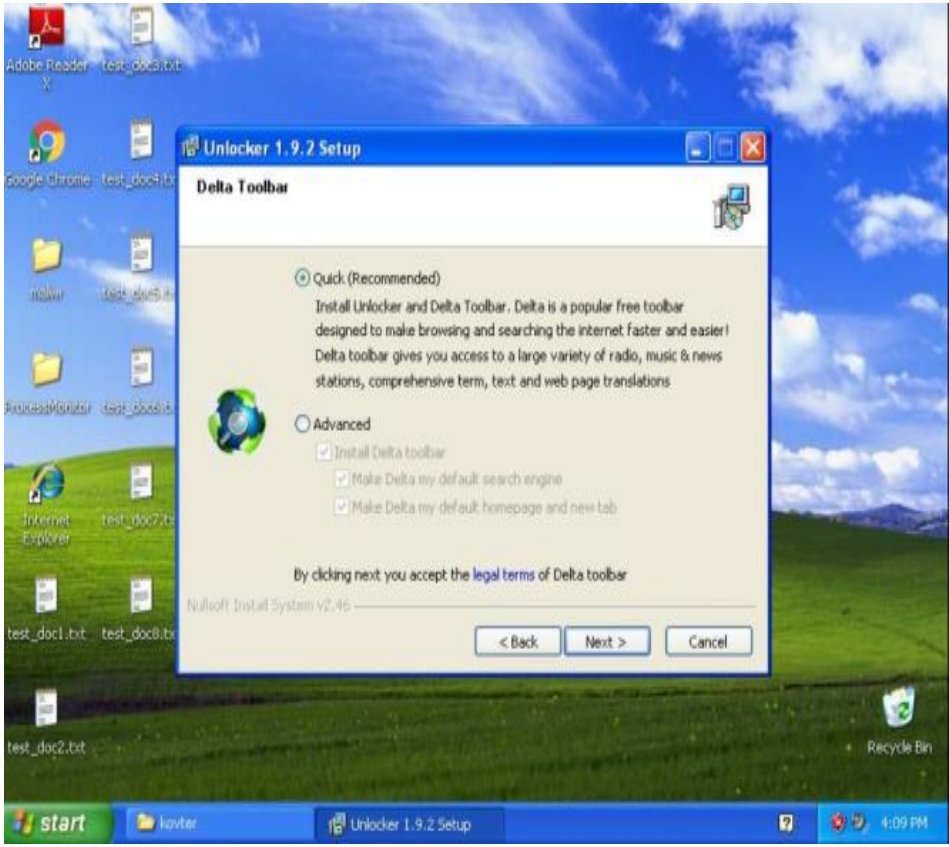
Snapshot of cuckoo sandbox HTML report for winlocker ransomware, showing no network related behaviour



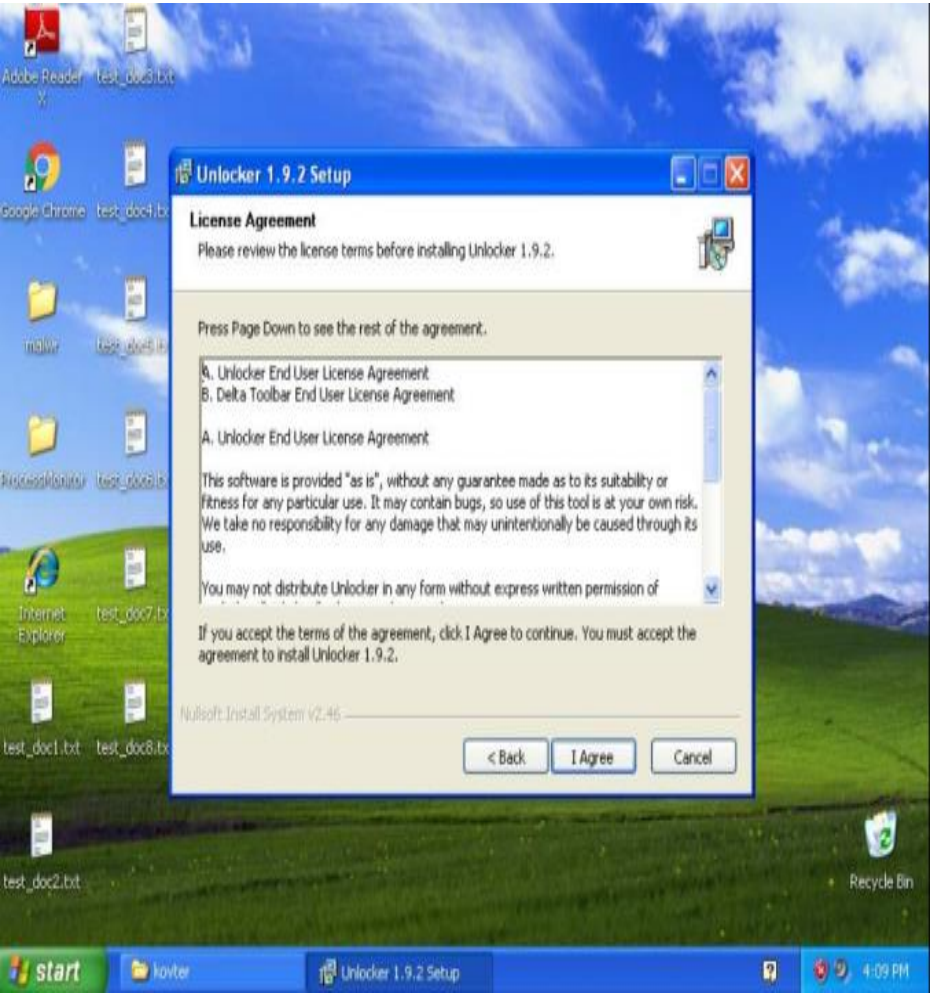
Observation for crypto ransomware, Installing Unlocker for files deletion



Desktop snapshot after crypto ransomware execution, showing language selection



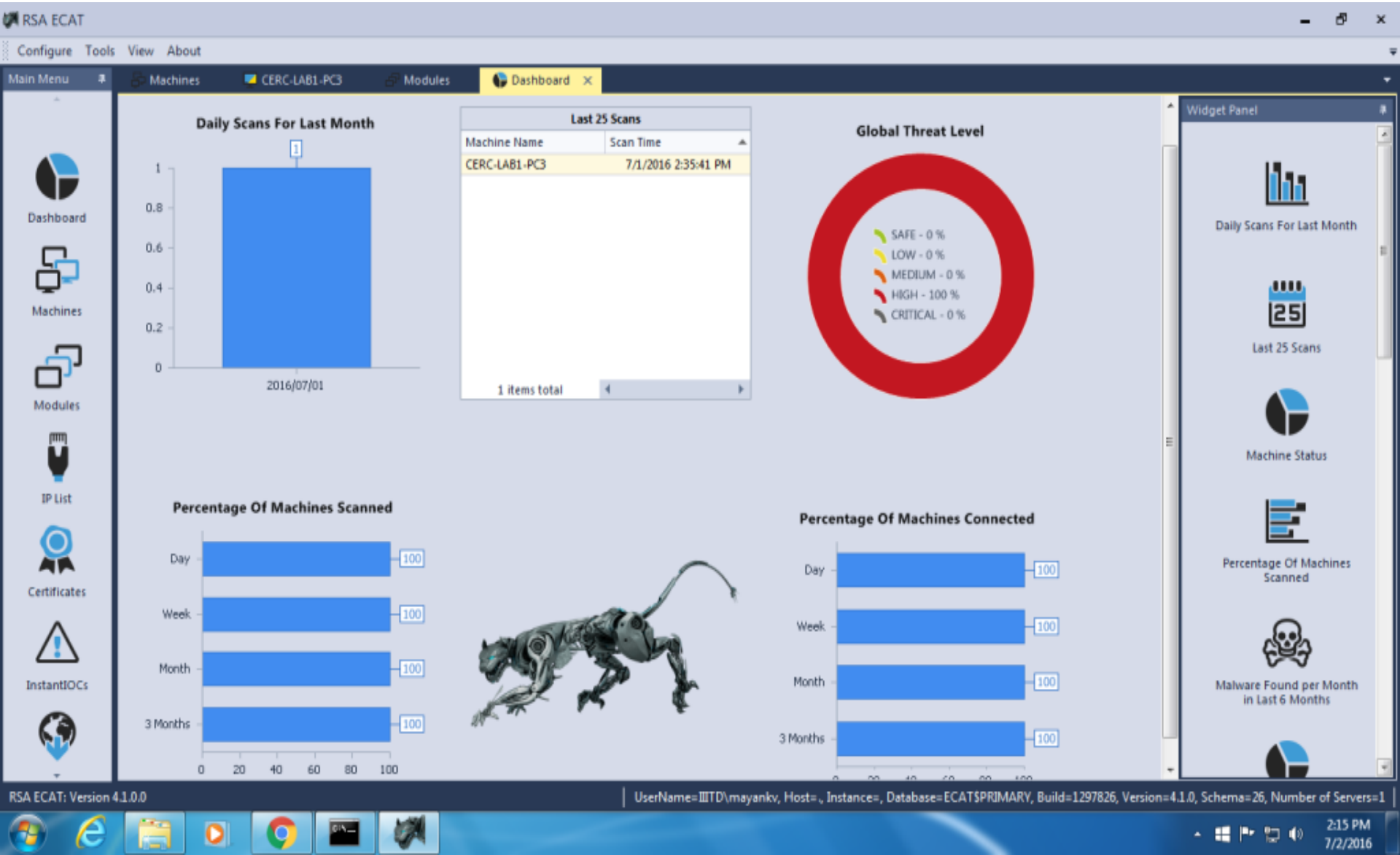
Desktop snapshot after crypto ransomware execution, showing quick installation feature selecion for unlocker installation



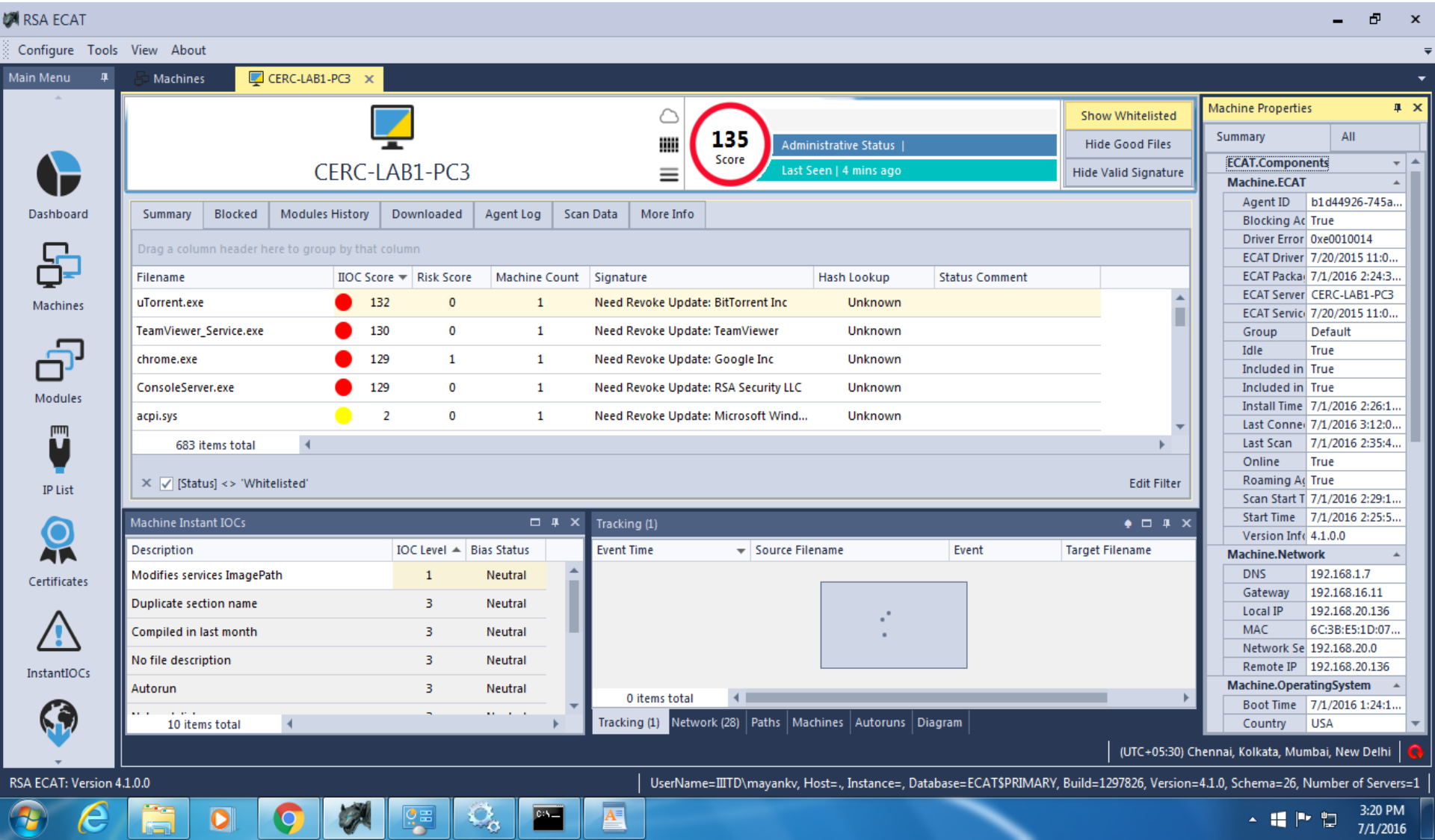
Desktop snapshot after crypto ransomware execution, showing ransomware agreement to all the terms and conditions as a legitimate user

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

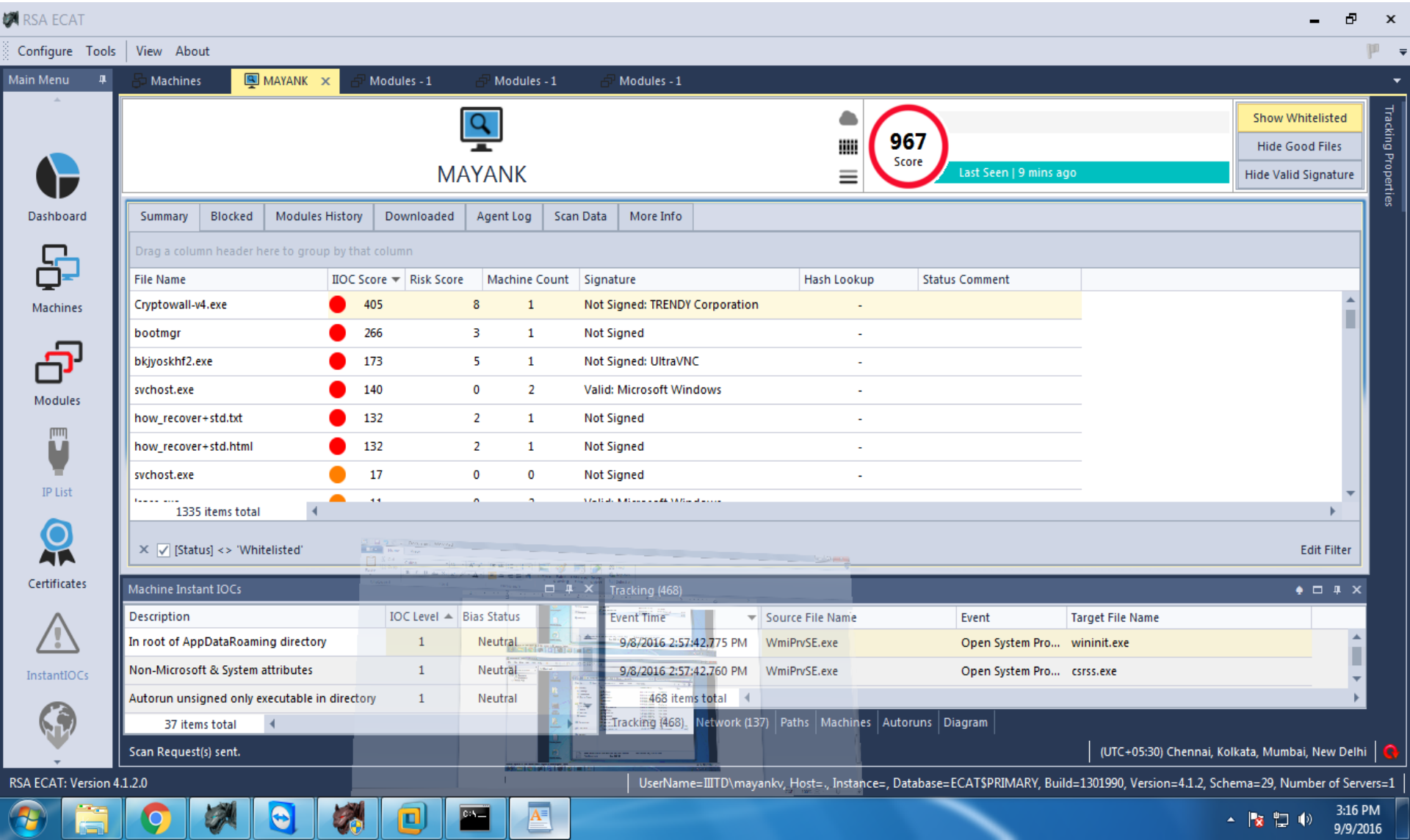
Installed malware detection tool showing global threat level



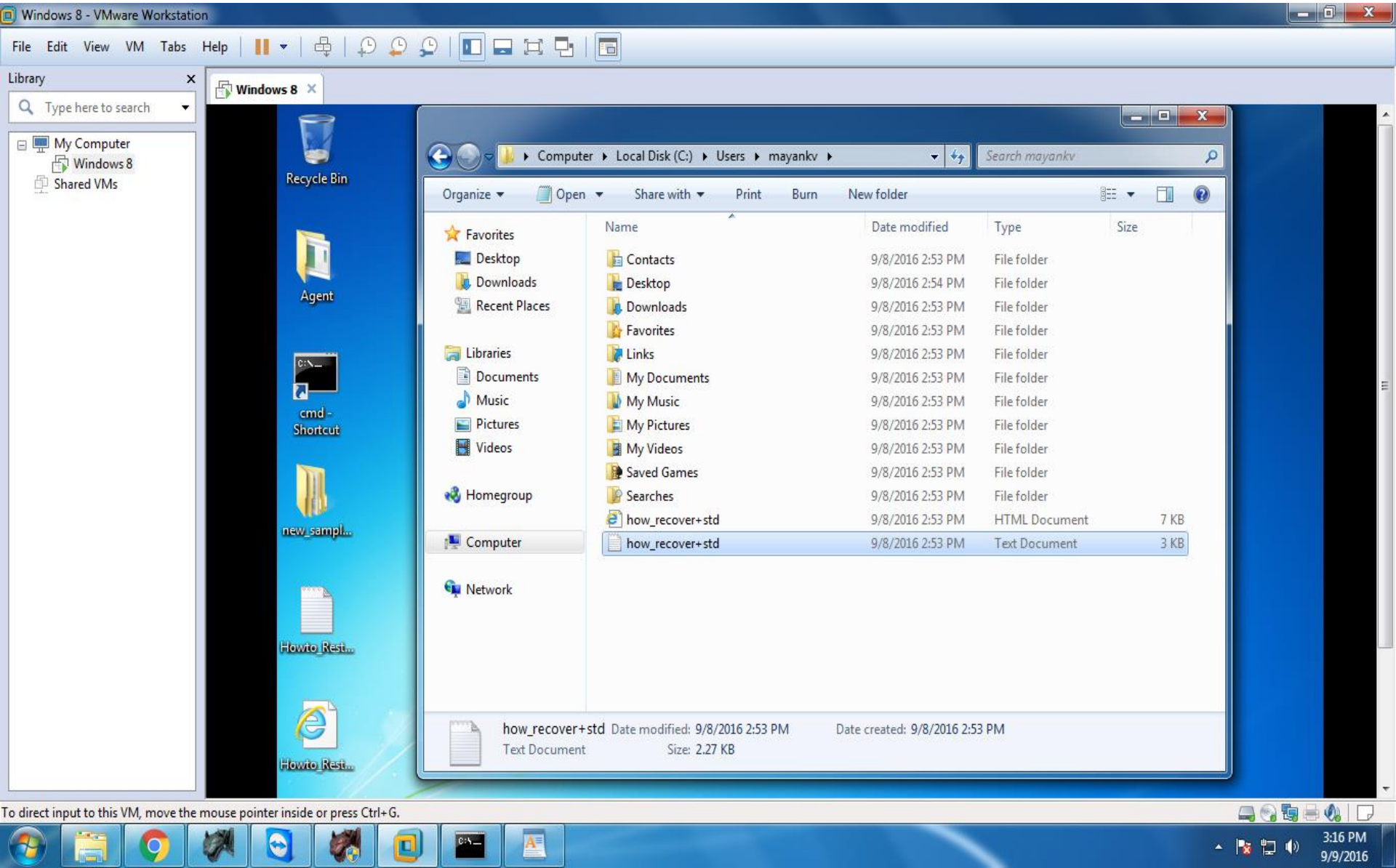
Malware detection tool showing global threat level before ransomware execution



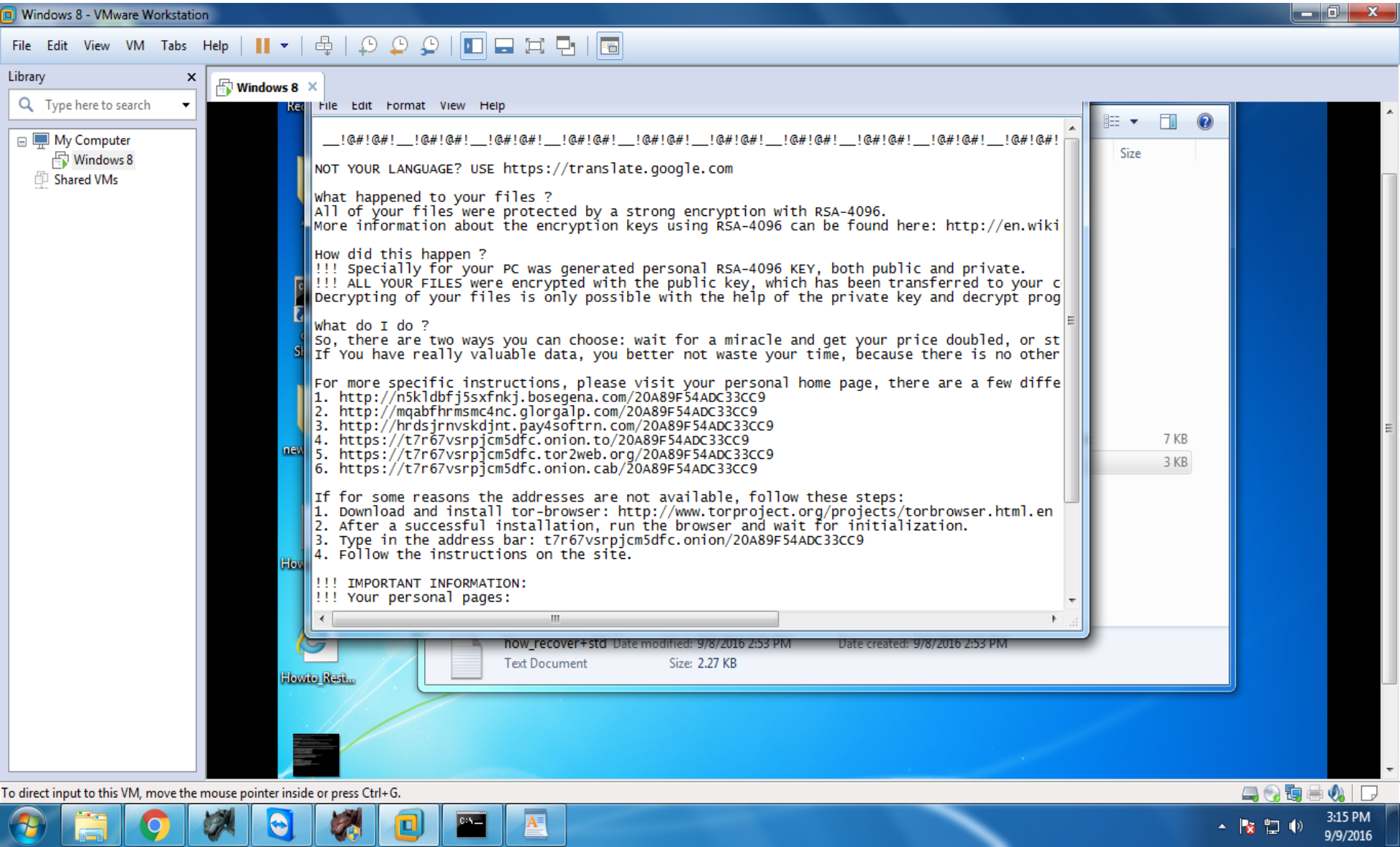
Malware detection tool showing global threat level after cryptowall ransomware execution



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 comparision 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


JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY
jiit
विद्या तत्व ज्योतिसमः

Thank You