Towards Protection, Detection, and Recovery from Windows-based Crypto Ransomware

Ahsan Ayub

Ph.D. Student and Graduate Research Assistant

Tennessee Tech University

Cybersecurity Education, Research and Outreach Center (CEROC)

Pre-Proposal Research Presentation

Tuesday, April 14, 2020

What is Ransomware?

- A type of malware that takes over the system by affecting the victim machine via email, remote desktop protocol, software vulnerability, etc.
- Mainly two kinds of ransomware –
  - Locker Ransomware
  - Crypto Ransomware

Ransomware - An Ever Growing Menace (1/2)

- Fastest growing cybercrime
- From 2017 (US$ 533m) to 2018 (US$ 646m), ransomware attack has increased by 21% in the U.S. [a]
- Global ransomware damage predicted US$ 20b in 2021. [b]
- A business will fall victim to a ransomware attack in every 11 seconds by 2021. [b]
- On average, a ransomware attack lasts for 7 days 8 hrs [c]
  - Causing extensive financial and reputational damage

[a] The Cost of Cybercrime by Accenture Security, published in 2019.
[b] 2019 Official Annual Cybercrime Report by Herjavec Group.
[c] Coveware's q1 ransomware marketplace report, published in 2019.

Ransomware - An Ever Growing Menace (2/2)

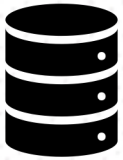
Year	New Families
2016	247
2017	327
2018	222
2019 (Jan – Apr)	40

Source: "Narrowed Sights, Bigger Payoffs: Ransomware In 2019 - Security News - Trend Micro USA". 2020. TrendMicro.Com. Accessed April 6 2020 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

Cryptographic Scheme Used in Ransomware

- Symmetric Encryption
  - AES is, for example, used for fast encryption of File System
- Asymmetric Encryption
  - RSA key pair is, for example, used for comparatively slower encryption of File System
- Hybrid Encryption Kolodenker et al. [2017]
  - Modern day ransomware authors use this scheme
  - Use of both asymmetric and symmetric encryption

Hybrid Encryption



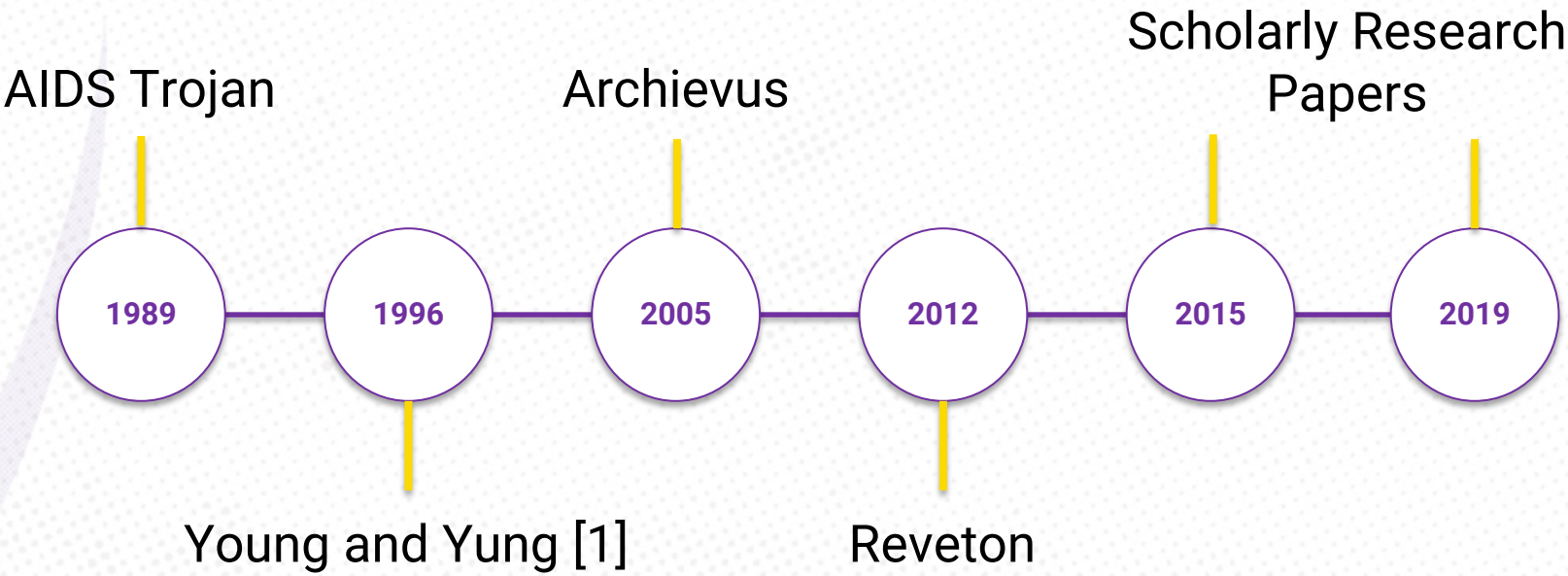
C&C Server

Victim Machine

RSA Key Pair

Session Key

Historical Timeline



Preliminaries

- Methodologies for the prototype
  - I/O Request Packet (IRP) Logs: Default mechanism for requesting I/O operation
  - System calls: Request of service(s) from the kernel of the operating system it is executed on
  - File change: Computation of change of file w/ hash values
  - Decoy files: Honey files w/ user agreement
- Desired performance metrices
  - Data / File recovery and key recovery
  - Real-time detection
  - Isolating damage or terminate the malicious process

State-of-the-Art Research (1/6)

Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks

Amin Kharraz[1], William Robertson[1],
Davide Balzarotti[3], Leyla Bilge[4], and Engin Kirda[1,2]

[1] Northeastern University, Boston, USA
[2] Lastline Labs, Santa Barbara, California, USA
[3] Institut Eurecom, Sophia Antipolis, France
[4] Symantec Research Labs, Sophia Antipolis, France

Venue: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, **2015**.

State-of-the-Art Research (2/6)

- Explained how the core parts of ransomware engineered
  - Encryption mechanism
  - Deletion mechanism
  - Locking mechanism
- Proposed a general methodology to detect ransomware attacks w/o making any assumptions on how it affects user's file system
  - API Call Monitoring
  - Monitoring File System Activity
  - Using Decoy Resources

State-of-the-Art Research (3/6)

UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware

Amin Kharraz
Northeastern University
mkharraz@ccs.neu.edu

Sajjad Arshad
Northeastern University
arshad@ccs.neu.edu

Collin Mulliner
Northeastern University
collin@mulliner.org

William Robertson
Northeastern University
wkr@ccs.neu.edu

Engin Kirda
Northeastern University
ek@ccs.neu.edu

Venue: 25th USENIX Security Symposium, **2016**.

State-of-the-Art Research (4/6)

ShieldFS: A Self-healing, Ransomware-aware Filesystem

Andrea Continella
andrea.continella@polimi.it

Alessandro Guagnelli
alessandro.guagnelli@polimi.it

Giovanni Zingaro
giovanni.zingaro@polimi.it

Giulio De Pasquale
giulio.depasquale@polimi.it

Alessandro Barenghi
alessandro.barenghi@polimi.it

Stefano Zanero
stefano.zanero@polimi.it

Federico Maggi
federico.maggi@polimi.it

DEIB, Politecnico di Milano, Milan, Italy

Venue: ACSAC (Annual Computer Security Applications Conference), **2016**.

State-of-the-Art Research (5/6)

Redemption: Real-time Protection Against Ransomware at End-Hosts

Amin Kharraz[1] and Engin Kirda[1]
{mkharraz,ek}@ccs.neu.edu

Northeastern University, Boston, USA

Venue: RAID (International Symposium on Research in Attacks, Intrusions, and Defenses), **2017**.

State-of-the-Art Research (6/6)

RWGuard: A Real-Time Detection System Against Cryptographic Ransomware

Shagufta Mehnaz(✉), Anand Mudgerikar, and Elisa Bertino

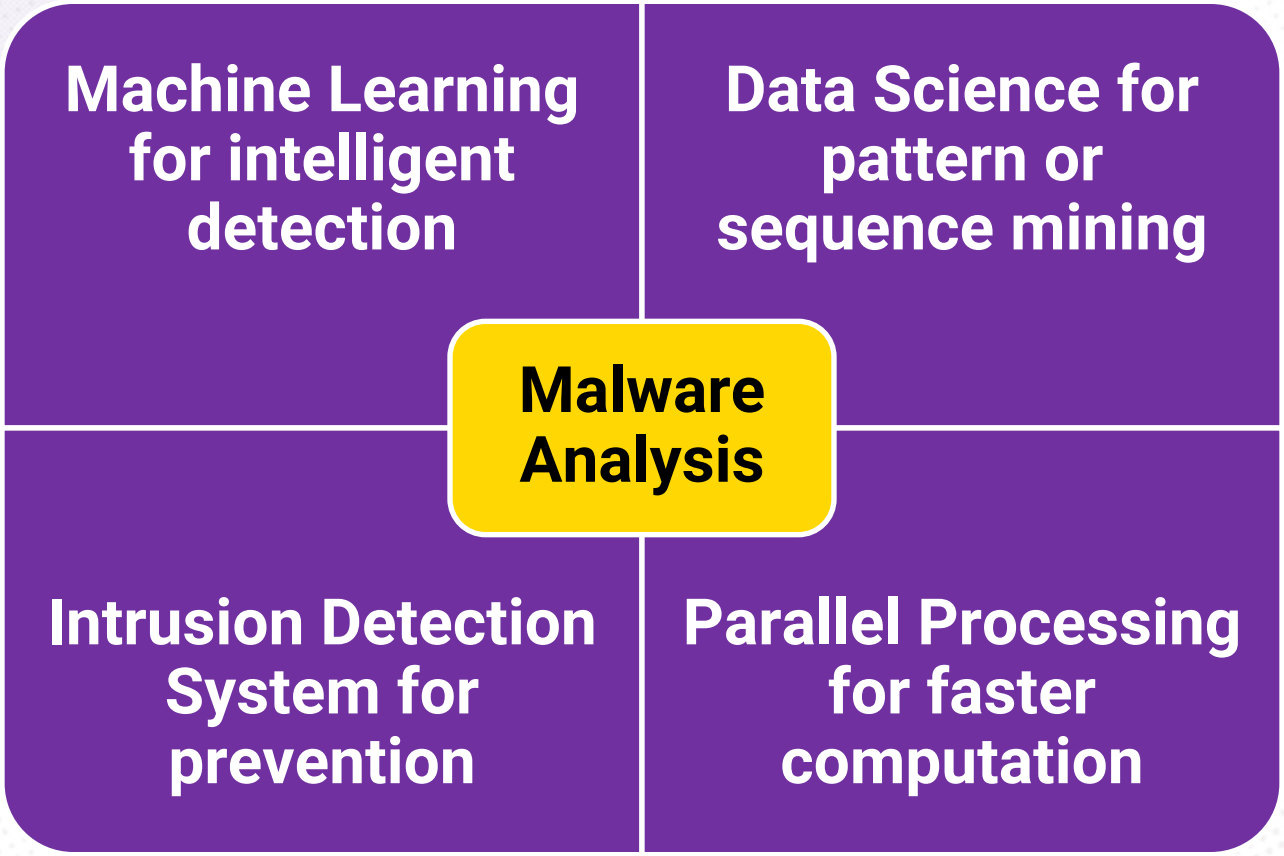
Purdue University, West Lafayette, IN, USA
{smehnaz,amudgeri,bertino}@purdue.edu

Venue: RAID (International Symposium on Research in Attacks, Intrusions, and Defenses), **2018**.

State-of-the-Art Research: Comparison

Prototype	IRP Logs	Sys Calls	File Change	Decoy Files	ML	File Rec	Key Rec	Real Det.	Isolatn	Data Sci.
RWGuard [2]										
Redemption [3]										
FlashGuard [4]										
PayBreak [5]										
CryptoDrop [6]										
EledeRan [7]										
Unveil [8]										
SheildFS [9]										

Focus of Research



Static Malware Analysis for Ransomware

- Limited work in this space for ransomware detection
- Analyze meta-data of the Portable Executable (PE) file of ransomware w/o executing it
  - Opcode sequence
  - Control flow graph
  - Function call graph
  - Machine activity
- Statistical / Characteristics analysis of the debugged code
  - # of jumps, # of bytes, etc.
- Natural language processing (NLP) based detection scheme

Dynamic Malware Analysis for Ransomware

- I/O Request Packet (IRP) logs mining
  - Extract useful pieces of information
  - Find sequence mining and automate the process
- Analysis of Command and Control (C&C) server communication for network isolation
  - Combat ransomware w/ Network-based Intrusion Detection System (NIDS)
- Machine / Deep learning based detection schemes
  - Time interval analysis for early detection

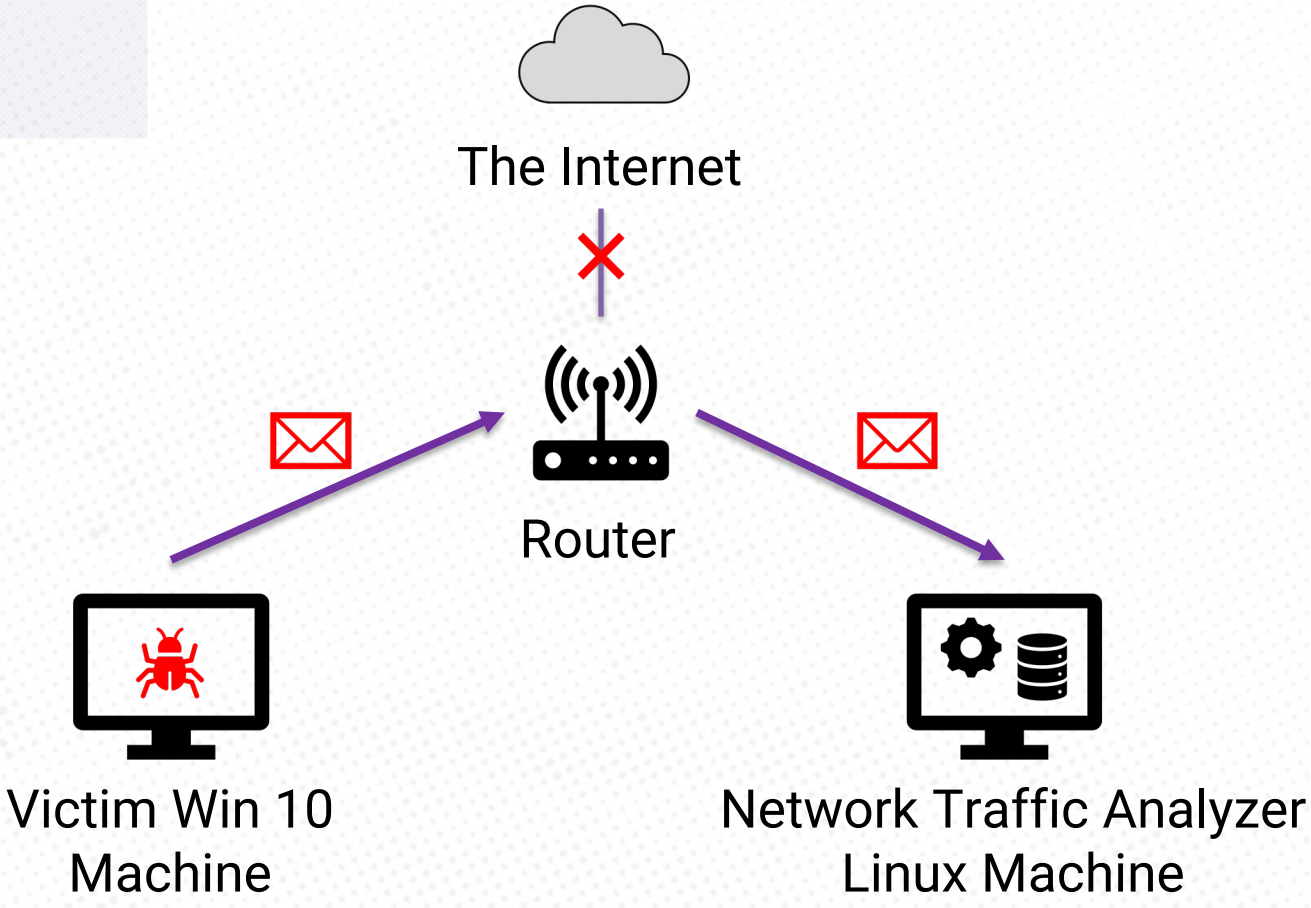
IRP Logs Mining for Ransomware Detection

- Goal: Detecting early sign of ransomware infection by performing post-analysis of affected system
- Twofold phases in this research project
  - Understanding the affected system through 386 ransomware samples' datasets
  - Applying acquired knowledge from the affected system to detect early ransomware behavior
- Mentor: Dr. Andrea Continella (Post-Doc, UCSB)
- Status: Work on progress; planning to submit in SecureComm 2020

Binary Analysis for Ransomware Detection

- Goal: Could we come up with a statistical set of attributes from the meta-data of the ransomware PE files to perform an efficient and unbiased detection?
- We have thus far parsed through approx. 450 ransomware samples to extract PE headers, along with other relevant piece of information.
- Mentor: Dr. Stacy Prowell (ORNL)
- Status: Work on progress

Monitor Network Logs for Ransomware Analysis



RWArmor: What is Our Plan?

- Devise an effective ransomware-aware solution based on the following attributes –
  - (Full) File recovery
  - Early detection
  - Taking back control of the affected system
  - Optimized solution: Less memory and computation overhead
    - Parallel computation
    - Kernel-level driver-based utility program
- Address “The Five Function” (NIST)
  - Identify, Protect, Detect, Respond, and Recover

Summary

- Performed a detailed literature study to find research gaps in ransomware detection and create a bridge between academic and industry research
- Isolated promising avenues to do research on to make our study unique and impactful
- Designed the path towards the completion of Ph.D. program w/ goals and milestones along the way
- Mentored by the domain expert in every research project

Aside from this Research Track

- **M. A. Ayub**, W. A. Johnson, D. A. Talbert, and A. Siraj, "Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning," IEEE 2020 52nd Annual Conference on Information Sciences and Systems (CISS).
- **M. A. Ayub**, Z. A. Onik, and S. Smith, "Parallelized RSA Algorithm: An Analysis with Performance Evaluation using OpenMP Library in High Performance Computing Environment," 2019 22nd International Conference of Computer and Information Technology (ICCIT), 18-20 December, 2019.
- **M. A. Ayub**, S. Smith, and A. Siraj, "A Protocol Independent Approach in Network Covert Channel Detection," 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, 2019, pp. 165-170.
- [Journal Review] **M. A. Ayub**, S. M. Smith, A. Siraj, and P. J. Tinker, "Towards Domain Generating Algorithm based Malicious Domains Detection."

Program of Study: Direct Ph.D. (1/2)

Courses: 10 / 43
Research: 0 / 30

[3cr] CSC 5200 Computer Networks
[3cr] CSC 5570 IT Security
[3cr] CSC 6903 ScTp: Research Probs in Nat Info Security
[1cr] CSC 6910 Computer Science Seminar

Courses: 19 / 43
Research: 0 / 30

[3cr] CSC 5575 Info Assurance & Cryptography
[3cr] CSC 6230 Machine Learning
[3cr] CSC 6740 Parallel/Distributed Algorithm

Courses: 25 / 43
Research: 3 / 30

[3cr] CSC 6575 Internet Security
[3cr] ECE 7970 Sel. Top: Machine Learning in Cybersecurity
[3cr] CSC 7990 Research and Dissertation

Courses: 31 / 43
Research: 6 / 30

[3cr] CSC 6220 Data Mining
[3cr] CSC 6580 Advanced Reverse Engineering
[3cr] CSC 7990 Research and Dissertation

Program of Study: Direct Ph.D. (2/2)

Courses: 37 / 43
Research: 9 / 30

Fall 2020

46 Cr

[3cr] CSC 6903 Advanced Topics: Secure SW Dev
[3cr] CSC 7210 Anomaly/Intrusion Detection Sys
[3cr] CSC 7990 Research and Dissertation

[3cr] CSC 7240 Intelligent Info System
[3cr] CSC 7575 Security Topics in Smart Grid
[3cr] CSC 7990 Research and Dissertation

Spring 2021

Courses: 43 / 43
Research: 12 / 30

55 Cr

Courses: 43 / 43
Research: 21 / 30

Fall 2021

[9cr] CSC 7990 Research and Dissertation

64 Cr

[9cr] CSC 7990 Research and Dissertation

Spring 2022

Courses: 43 / 43
Research: 30 / 30

73 Cr

References (1/2)

1. Adam Young and Moti Yung. Cryptovirology: Extortion-based security threats and countermeasures. In Proceedings 1996 IEEE Symposium on Security and Privacy, pages 129–140. IEEE, 1996.
2. Shagufta Mehnaz, Anand Mudgerikar, and Elisa Bertino. Rwguard: A real-time detection system against cryptographic ransomware. In International Symposium on Research in Attacks, Intrusions, and Defenses, pages 114–136. Springer, 2018.
3. Amin Kharraz and Engin Kirda. Redemption: Real-time protection against ransomware at end-hosts. In International Symposium on Research in Attacks, Intrusions, and Defenses, pages 98–119. Springer, 2017.
4. Jian Huang, Jun Xu, Xinyu Xing, Peng Liu, and Moinuddin K Qureshi. Flashguard: Leveraging intrinsic flash properties to defend against encryption ransomware. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pages 2231– 2244. ACM, 2017.
5. Eugene Kolodenker, William Koch, Gianluca Stringhini, and Manuel Egele. Paybreak: defense against cryptographic ransomware. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pages 599–611. ACM, 2017.
6. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin RB Butler. Cryptolock (and drop it): stopping ransomware attacks on user data. In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), pages 303–312. IEEE, 2016.
7. Daniele Sgandurra, Luis Muñoz-González, Rabih Mohsen, and Emil C Lupu. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. arXiv preprint arXiv:1609.03020, 2016.

References (2/2)

8. Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda. UNVEIL: A large-scale, automated approach to detecting ransomware. In 25th USENIXg Security Symposium (USENIX Security 16), pages 757–772, 2016.
9. Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, and Federico Maggi. Shieldfs: a self-healing, ransomware-aware filesystem. In Proceedings of the 32nd Annual Conference on Computer Security Applications, pages 336–347. ACM, 2016.

Inspiration Note

To succeed you have to produce the absolute best stuff you're capable of producing—a task that requires depth.

— Quoted from the book
Deep Work by Cal Newport

THANK YOU!

Happy to take any questions you may have…

https://www.tntech.edu/ceroc | @TechCEROC | ceroc@tntech.edu