Poster: A Ransomware Research Framework

Daniel G. Wolf and Donald L. Goff
Cyber Pack Ventures, Inc.

ABSTRACT

This research develops a series of research frameworks for addressing the problem of ransomware from the perspective of multiple disciplines, begins to develop theories about ransomware, and identifies needs for future research. Approaches include criminal justice, hardware and software technologies, file structures, critical infrastructure impact, an abstract theoretic approach, and money tracking. To date, poster presentations are available and formal articles from each researcher are forthcoming..

1 INTRODUCTION

Ransomware is the malicious software that locks computer files until an extorted fee or ransom is paid for the key to unlock it. This ransom is usually paid in Bit Coin, the “virtual currency” of the Internet, but it may also be paid in actual currency. Extortionists are becoming more sophisticated in their attacks, and their successful attacks are creating disruptive effects on their victims' systems. While these attacks have generally had an impact on individuals or a public or private entity, an attack on critical infrastructure would have the potential to create catastrophic consequences to the general population. A successful ransomware attack may create substantial disruptive effects on victim systems. A ransomware attack on critical infrastructure has major consequences. The availability of both ransomware software and now ransomware-as-a-service means the skill level for entry is low and will likely increase the chance of a significant disruptive event occurring. An actor could use this approach to mask other malicious purpose while providing some level of deniability. That is, the perpetrator may “spoof” the victim, perhaps to trigger a crisis between the alleged perpetrator and the victim. There have been numerous major ransomware attacks against computer systems and data bases which resulted in failures of critical infrastructures including transportation and healthcare. “Wannacry” and “NotPetya” occurred during the period of this research and both showed global impacts. This research approach solicited interest from scholars, policy makers, and corporations and produced seven presentations and posters for presentation in at the Computational Cybersecurity in Compromised Environments (C3E) Workshop and publication. The seven researchers showed a wide range of approaches to the problem. Their backgrounds included computer scientists, operations engineers, and behaviorists from both academia and industry. Research synopses: Dusko Pavlovic (University of Hawai'i) “RansomAIR filled with Clouds”. A ransomware attack is transactional between attacker and victim, but it can be defeated by cloud storage. Coding, not cryptography, provides sufficient protection since crypto systems have an insecure transmission rate. Coding can speed up the process. In this model, a Sudoku grid is used as the code basis. David Maimon (University of Maryland, College Park) “An Evidence-Based Ecological Approach for Disrupting Ransomware Spread”. A ransomware model should account for key junctures which may be effective in influencing attackers' and victims' decision-making processes: These junctions are the ransomware initiators - ransomware affiliates junction, the online offenders-victims junction, and the online offenders-money launderers' junction. An evidence-based ecological perspective provides an ideal framework for conceptualizing ransomware because it stresses moving beyond decision makers' political, financial, social background and personal experience to a model in which policy decisions are made based on scientific findings. Peter Chin (Boston University) “Ransomware Classification RNN”. This project applied Recurrent Neural Network (RNN) on ransomware detection. The ransomware and benign executables were put in a virtual machine. Cuckoo Sandbox was used to analyze the behaviors of them in the virtual computer. Then, the behavior report which records the actions and their corresponding times were translated into the inputs for RNN. This neural network was able to detect ransomware based on its behaviors. RNN can be trained on a server and then deployed to a PC. The trained RNN will just analyze the behavior of the program, so even if it is not up-to-date, it still has the ability to find the newest ransomware while keeping a lower false positive rate. The computer finds ransomware without communicating without interacting with database with machine learning. Van Parunak (ABC Research, Inc.) “Ransomware Analysis as Dialog for Attribution and Reconnaissance (RADAR)”. This study applies a novel Ransomware Analysis as Dialog for Attribution and Reconnaissance (RADAR) model to find commonalities between attacks in terms of linguistics, grammar and sequence of actions. Using this methodology, we analyzed case studies form seven attacks. Findings had a high degree of correlation. David Nicol (University of Illinois Urbana-Champaign) “The Threat of Ransomware in Energy Delivery Systems”. Energy delivery systems are different from enterprise networks, and

HoTSoS '18, April 10–11, 2018, Raleigh, NC, USA

ACM ISBN 978-1-4503-6455-3/18/04…$15.00
https://doi.org/10.1145/3190619.3190634

the differences work to our advantage. Ransomware has already appeared at power utilities, but only on the business side of the enterprise. The big issues in energy delivery systems are the consequences of physical damage and harm to humans resulting from loss of control, situational awareness, operational service and administrative support service. Our approach to the problem is to use known best practices to develop a "cut-out" between inbound documents/code and transfer/viewing by users such as, mimecast, "Targeted Threat Protection-Attach Protect," and "Sandboxie." Applications such as Sophos and Carbon Block Cb can be used to White list outbound connections. Rigorous and enforced limitations on connecting to OT devices are needed, plus good computer hygiene and known technologies can lengthen the attack chain required to place ransomware inside of an industrial control system. Marco Carvalho "An Approach to Ransomware Effects Mitigation". Our approach includes on-the-fly backup of user files, file access monitoring and interception, file system file driver, and risk-based online backup. Backup is initiated when the risk level is above a certain threshold based on a risk level assessment done by monitoring user and system activity. System files are not considered for backup since they can be recovered from installation media. Enable backups when matching certain criteria – process id/name, files, directories, connected hosts. Network-based monitoring and non-intrusive scanning capabilities can be placed within enterprise gateways to scan and filter ingress traffic and are used in conjunction with anti-spam and email filtering software. There can still be adverse consequences, however. David Burke (Galois, Inc.) "Understanding the Ransomware Landscape through System Dynamics Models". This research program comprises a look from computer science, economics, counterintelligence, and futurist perspectives. Ransomware is now a business and has good perceived value-- victims are confident that paying the ransom will unlock data and there is a low cost of entry for entrepreneurs. There are multiple sources for ransomware software. System Dynamics models consist of stocks and flows. For the attacker, the challenge is to determine the probability of payment by the victim. This creates challenges in modeling: it is tempting to add more detail and precision, but overly detailed models are harder to grasp. There is tension between fidelity and understanding. Additional challenges include the use of modeling qualitative vs. quantitative results and the need for sensitivity analysis. Future work Future research into ransomware should address a continuation of studying ransomware case studies to gain more insight into patterns, relevant data collection, systems dynamics modelling, and finding methods to disrupt the ransomware ecosystem. An open question for future work is "Where's the sweet spot for ruggedized authentication and provenance of digital artifacts?" Rigorous experimentation to evaluate the performance and overheads induced by the proposed defense, develop more advanced behavior models for risk assessment and defense activation are needed. We should design interfaces to enable user feedback to the operation of systems and develop a deployable package for end-user installation of defense capability.

REFERENCES

1. Kohlbrenner, Anne, Araujo, Frederico, Taylor, Teryl, Stoecklin, Marc Ph.. 2017. POSTER: Hidden in Plain Sight: A Filesystem for Data Integrity and Confidentiality. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. :2523–2525.
2. Chen, Zhi-Guo, Kang, Ho-Seok, Yin, Shang-Nan, Kim, Sung-Ryul. 2017. Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph. Proceedings of the International Conference on Research in Adaptive and Convergent Systems. :196–201.
3. Lee, Jeonghwan, Lee, Jinwoo, Hong, Jiman. 2017. How to Make Efficient Decoy Files for Ransomware Detection? Proceedings of the International Conference on Research in Adaptive and Convergent Systems. :208–212.
4. Dion, Yap L., Joshua, Abigail A., Brohi, Sarfraz N.. 2017. Negation of Ransomware via Gamification and Enforcement of Standards. Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence. :203–208.
5. Pradhan, A., Marimuthu, K., Niranchana, R., Vijayakumar, P.. 2017. Secure Protocol for Subscriber Identity Module. 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM). :358–362.
6. Yin, H. Sun, Vatrapu, R.. 2017. A First Estimation of the Proportion of Cybercriminal Entities in the Bitcoin Ecosystem Using Supervised Machine Learning. 2017 IEEE International Conference on Big Data (Big Data). :3690–3699.
7. Zimba, A., Wang, Z., Chen, H.. 2017. Reasoning Crypto Ransomware Infection Vectors with Bayesian Networks. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). :149–151.
8. Gonzalez, D., Hayajneh, T.. 2017. Detection and Prevention of Crypto-Ransomware. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). :472–478.
9. Chen, Q., Bridges, R. A.. 2017. Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). :454–460.
10. Subedi, K. P., Budhathoki, D. R., Chen, B., Dasgupta, D.. 2017. RDS3: Ransomware Defense Strategy by Using Stealthily Spare Space. 2017 IEEE Symposium Series on Computational Intelligence (SSCI). :1–8.
11. Yalew, S. Demesie, Maguire, G. Q., Haridi, S., Correia, M.. 2017. Hail to the Thief: Protecting data from mobile ransomware with ransomsafedroid. 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). :1–8.
12. the ARM TrustZone extension and running in the secure world. It does backup of files
13. Kuzuno, H., Karam, C.. 2017. Blockchain explorer: An analytical process and investigation environment for bitcoin. 2017 APWG Symposium on Electronic Crime Research (eCrime). :9–16.
14. Han, Jordan W., Hoe, Ong J., Wing, Joseph S., Brohi, Sarfraz N.. 2017. A Conceptual Security Approach with Awareness Strategy and Implementation Policy to Eliminate Ransomware. Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence. :222–226.
15. Bhattacharya, S., Kumar, C. R. S.. 2017. Ransomware: The CryptoVirus Subverting Cloud Security. 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET). :1–6.
16. Nicholas, Charles. 2017. Document Engineering Issues in Malware Analysis. Proceedings of the 2017 ACM Symposium on Document Engineering. :3–3.
17. Zahra, A., Shah, M. A.. 2017. IoT based ransomware growth rate evaluation and detection using command and control blacklisting. 2017 23rd International Conference on Automation and Computing (ICAC). :1–6.
18. Shao, S., Tunc, C., Satam, P., Hariri, S.. 2017. Real-Time IRC Threat Detection Framework. 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W). :318–323.
19. Huang, Jian, Xu, Jun, Xing, Xinyu, Liu, Peng, Qureshi, Moinuddin K.. 2017. FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. :2231–2244.
20. Kolodenker, Eugene, Koch, William, Stringhini, Gianluca, Egele, Manuel. 2017. PayBreak: Defense Against Cryptographic Ransomware. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. :599–611.
21. Cabaj, K., Mazurczyk, W.. 2016. Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall. IEEE Network. 30:14–20. 4 pages.