Malware Prognosis: How to Do Malware Research in Medical Domain

Sai R. Gouravajhala, Amir Rahmati, Peter Honeyman, Kevin Fu
University of Michigan

Abstract

Malware in the medical domain presents serious ramifications for patient safety. Previous work in this field has either focused on individual devices or used network traces to examine malware infection in medical networks. In this work, we evaluate the benefits and shortcomings of each approach and examine the characteristics that make or break them. Based on these characteristics, we present three recommendations that can benefit future research: (1) Network data gathered must either be targeted or be longitudinal in nature to be valuable; (2) Effective network administration plays an important role in mitigating the incidence of medical device malware; and, (3) Device level investigation is important for discovering vulnerabilities that can impact malware infectability.

1 Goal & Presentation Format

The goal of this presentation is to spark a lively discussion on how to conduct effective malware research in the medical domain. We will survey two general (and complementary) approaches that researchers use to tackle this problem. Based on the results seen with these approaches, we propose a set of recommendations that can enhance the efficacy of research in the medical domain.

We will use all 20 minutes to sustain a lively discussion. A potential breakdown is: 12-minute talk with 8 minutes for Q&A and discussion.

2 Malware in Medical Domain

Malware in the medical domain presents serious ramifications for patient safety [10, 9]. Indeed, in June 2013, the FDA issued a safety bulletin urging manufacturers and hospitals to incorporate cybersecurity measures into their devices and networks [5]. To this end, there are two general (and complementary) approaches for conducting malware research in the medical domain, each with its own challenges.

Bottom-up. In this approach, one starts at the the medical device level and moves up, thereby generalizing vulnerabilities to a whole class of devices. For instance, a report filed in the FDA's MAUDE database details software vulnerabilities found in the firmware of an automated external defibrillator. These vulnerabilities could lead to arbitrary code execution, as well as provide a pathway for malware infections [2]. It has been shown that numerous medical devices in hospitals can be compromised with relatively little effort [11]. Clark et al. show the ease with which a particular model of a pharmaceutical compounder can be infected with numerous run-of-the-mill malware samples [4]. The device-level perspective can lead to fruitful discoveries, though it is usually on a per-device basis. There also exist challenges: it is difficult to acquire medical devices for testing purposes, as there are regulatory and cost roadblocks involved.

Top-down. In the top-down approach, one starts at the network perspective and moves down, thereby finding patterns and insights on malware infections. Gouravajhala et al. captured NetFlow data from the University of Michigan Health System (UMHS) transit points for a 24-hour period. Using this data and a reputation-based blacklist, they tried different heuristics to find anomalous end system behavior that could suggest malware infection [6]. Though they did not find any malware infected end systems in UMHS, they did find candidates that warrant further attention. The top-down approach's clear advantage is its holistic nature: data for every networked device is seen. However, the main challenge is that getting the data is hard. Hospitals are generally hesitant to placing network taps on mission-critical networks, as there are privacy-concerns. Hospitals also place medical devices behind virtual local area networks (VLANs), firewalls, access control lists (ACLs), and isolated networks, so some data may not even be seen at routers in higher-levels.

It is interesting to note, however, that the use of these policies is not a panacea for the preclusion of malware infections. For instance, misconfigured ACLs can accidentally give Internal access to devices. Compromised USB flash drives can be plugged into medical devices that are behind the isolated network, thus circumventing the air gap. Indeed, there exist instances where machines behind isolated local area networks were infected with Conficker [8]. In the same vein, Kramer et al. [7] state that, between January 2009 and December 2011, the Department of Veterans Affairs (VA) database had 142 separate instances of malware infections that affected 207 medical devices; yet, as Clark et al. [4] point out, the IT department at the VA regularly uses ACLs and VLANs to separate medical devices from the rest of the network.

3 Recommendations

From the previous work in this sphere, we learned several lessons on how to conduct effective research on malware detection in medical devices. We distill these lessons into three recommendations:

1. **Network traces need to either be targeted to specific events or be longitudinal in nature.**

   All major findings coming from medical networks research have either targeted specific events (e.g., Confliker worm [8]) or have been the result of a longitudinal study (e.g., 2009-2012 Veterans Affair report [7]). On the other hand, the use of short term traces, such as seen in [6] on the other hand, has shown to yield little results. Using only 24 hour of traces, researchers were unable to see any activity from some of the online medical devices at all. Future research on medical networks should consider these results when considering the timing and scope of data collection.

2. **Effective network administration is a potent means of limiting both the number and scope of malware incidents.**

   Outbreaks can, and do, happen, but effective IT policies can ameliorate both damage and disruption time. In case of the Conficker worm in UMHS, heavy use of VLANs and ACLs significantly limited the infection. In the Radiology department, the infection was limited to only two devices [1].

   This might also suggest that looking into smaller hospital networks, which do not possess an around-the-clock and dedicated IT support team, might prove more fruitful for finding malware in medical networks.

3. **Looking for vulnerabilities at the device level is both fruitful and important for understanding how easily systems can become infected, either accidentally or intentionally.**

   Previous device-level research has generally been successful in finding vulnerabilities in medical devices (e.g., [4, 11]). Starting with an individual device can potentially reap rewards, as we can extend any software or implementation vulnerabilities to all units of that device. With mounting evidence, we can more easily engage medical device manufacturers in constructive conversations to fix these vulnerabilities and help nullify the resistance some manufacturers have to patching their products [3]. Moreover, by learning about a vulnerability, we can better judge how a device will react to malware infections, so we can invest resources into better protecting those devices at the network administration level.

References

[1] Personal communication, dale fay, umhs radiology department.

[2] Maude adverse event report: Cardiac sciencepowerheart aed g3 plus, 06 2011.

[3] BAXA CORPORATION. Preventing cyber attacks. `https://btsp.baxa.com/Sales%20Portal/ExactaMix/Preventing%20Cyber%20Attacks.pdf`, Loaded Oct. 2012.

[4] CLARK, S. S., RANSFORD, B., RAHMATI, A., GUINEAU, S., SORBER, J., XU, W., AND FU, K. WattsUpDoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices. In *USENIX Workshop on Health Information Technologies* (Aug. 2013).

[5] FDA, U. Fda safety communication: Cybersecurity for medical devices and hospital networks (june 13, 2013).

[6] GOURAVAJHALA, S. R., RAHMATI, A., CHAVIS, E., KUNE, D. F., HONEYMAN, P., BAILEY, M., AND FU, K. Stigmalware: Investigating the prevalence of malware in the clinical domain. In *Poster and Short Talk session of 35rd Annual IEEE Symposium on Security and Privacy* (San Jose, CA, May 2014).

[7] KRAMER, D. B., BAKER, M., RANSFORD, B., MOLINA-MARKHAM, A., STEWART, Q., FU, K., AND REYNOLDS, M. R. Security and privacy qualities of medical devices: An analysis of fda postmarket surveillance. *PloS one 7*, 7 (2012), e40200.

[8] MILLS, E. Conficker infected critical hospital equipment, expert says. *CNET* (April 2009).

[9] TALBOT, D. Computer viruses are ”rampant” on medical devices in hospitals. *MIT Technology Review* (October 2012).

[10] THREATS, I. U. S. Increase in cybercrimes against the healthcare sector.

[11] ZETTER, K. Its insanely easy to hack hospital equipment, Apr. 2014.