Avum Cyber Security Approach: Prevention, Detection, and Threat Removal

Jerry Hill, *Senior Science Advisor, Avum, Inc.*

Abstract—If you believe that your system has not been intruded upon and your private information, including classified information, compromised, you could be right. It is equally likely that you are wrong. Unless steps outlined in this paper have been implemented, the latter is a distinct possibility.

1 Background

AVUM, Inc. has been active in Cyber Security on our own behalf and that of our commercial and DoD customers for several years. Thus our customers' application domains present a logical path for us in expanding research already begun in developing a Cyber Security application to detect and prevent Cyber intrusion into target systems. This document provides an overview for our plan to develop techniques and tools to run in a Virtual Machine (VM) environment that would analyze all applications prior to their being allowed to run in operational computer systems.

2 Problem

Intrusive software proliferation is increasingly sophisticated. Intrusive for purposes of this paper is divided into malicious software, commonly referred to as "malware," and "spyware," the intent of which is to surreptitiously copy private information from the host system being invaded. For purposes of this paper malware and spyware, are considered separately because of their differing objectives.

Malware's intent is to cause harm to computer systems, or to various levels of computer controlled infrastructure, such as reservoirs, petroleum refineries, and manufacturing facilities, such as our automobile plants, and food processing plants. Our national power grid would fall into this category.

Spyware, on the other hand, does no immediate harm to the host system and consists of a program, or programs, designed to mine data that can be used for financial gain at the owner's expense, or to compromise company confidential information, or classified government information, which could be used to undermine a company's business model, or in the extreme, compromise national security.

While we are aware that such intrusive software's objective is to steal personal, private, or classified data or inflict harm on the host system in which it has intruded, or the network over which it communicates, we are also aware that the host itself could possibly have been procured with the malware or spyware, which could have, been unknowingly installed by the system owner or owner's representative.

Increasingly complex computer systems provide a rich environment for malware attacks, or a malware host that surreptitiously gleans proprietary information from unwary applications. The larger and more complex a system, the more difficult malware detection or convincing proof of its absence - becomes. The threat of malware/spyware attacks, therefore, presents an unavoidable computer security risk, making protection from, and/or detection of the presence of malicious code critical to systems operating on, and transmitting and storing proprietary or classified information.

3 Solution

Of course it would be the ultimate achievement to prevent malware intrusion into the system in the first place; therefore our approach is to achieve that goal. Our plan is to intercept software prior to its being loaded into the target system; including complex systems with numerous disparate applications within the secure network infrastructure and servers. We have developed a prototype system and are pursuing research leading to a yet more robust solution that can combat the increasingly intelligent malware threats. Our goal is to develop a malware detection system dynamic enough to match that malware sophistication by employing an application called Java Pathfinder (JPF) to analyze applications for malicious or spyware attributes in a virtual environment prior to their being loaded into the target system (See attribution approach, below). Every possible path would be analyzed in the virtual environment, with the composite results being assessed against properties that we would expect to find only in malicious or spy software.

This analysis would further result in identification of new properties to expand the existing malware properties list to be used in future path analysis. We will present more research on JPF's capabilities as a malware detection tool as we continue our investigation of alternative VM Cyber Security implementations.

We employ attribution, which closely parallels our Intelligent Agent Framework (refer to IA Malware Detection and Response). Attribution uses sensors to locate the origin of Cyber attacks (now thousands per hour). Attribution is necessary for defensive and preemptive protective measures.

Listed on the following page are some key attribution concepts and known security threats which we address in developing our VM detection approach. Also listed are key governmental agencies of special interest to us, since they and we are concerned with the same threats. Thus these organizations are of interest.

• *J. Hill is responsible for Avum's Program Execution and Life-Cycle Engineering. E-mail: jhill@avum.com*

Manuscript created May 12, 2013.

Attribution Concepts

Agent.btz

Sometimes referred to as AWF (or Agent. AWF), Agent.btz is a malicious Trojan Downloader affecting the Microsoft Windows Operating System. It is considered to be obsolete, but provided the basis for follow-on more sophisticated malware, thus we cannot ignore it.

Struxnet (worm)[1]

Stuxnet epitomizes a worldwide cyber threat to infrastructures and industrialized processes. Hackers are copycatting Stuxnet (targets industries, including power plants and grids). An understanding of Stuxnet provides insight into what might be expected from this quarter.

Primary Threats

1) Cyber espionage, 2) Cyber theft of intellectual property, 3) Cyber destruction (still on the horizon, but we include this one in our approach, as if it is already a threat).

Critical Targets

U.S. electrical grid, financial system, which have already been penetrated. Reservoirs, sea ports, airports, railway terminals, and population centers are all potential targets.

China

Considered as being the first nation to mount cyber attacks on a broad scale. China is not openly hostile, but is a major Cyber Security threat for stealing proprietary and classified information.

United States Central Command (Centcom) Role

A theater-level Unified Combatant Command of the U.S. Department of Defense. CENTCOM area of responsibility includes the Middle East, North Africa, and Central Asia, with combat roles in Iraq and Afghanistan, and support roles in Kuwait, Bahrain, Qatar, the United Arab Emirates, Oman, Pakistan, and central Asia.

Cyber Command

Headed by Gen. Keith Alexander, who also heads NSA (as of this writing on 1/5/2013), and who led building of "robust and layered defenses" against Cyber attack, said it is time to give up on piecemeal measures (e.g., firewalls) and re-engineer the worldwide cyber system to be more innately secure. While Cyber Command is currently tasking contractors to upgrade Cyber Security, no standards[2] are in force to manage and control and help integrate and direct the activities of those contractors. We see this as a possible role for Avum.

Global Awareness

Our stress must expand to incorporate regional and global surveillance and a variety of platforms, including high altitude airships.

Networking and Collaboration

A team approach is required to best provide countermeasures. Key players thus include Government entities including: Department of Homeland Security (DHS) (In addition to CIA, FBI, NSA, NRO, and NIS, in support of the Warfighters, see Figure 1 below). This collaboration includes the National Institute of Standards (NIS) and Warfighters, Academia leaders, e.g., MIT, Purdue, and Carnegie Mellon University, Industry leaders that include Aerospace companies such as Northrop Grumman, Lockheed-Martin, and Boeing.

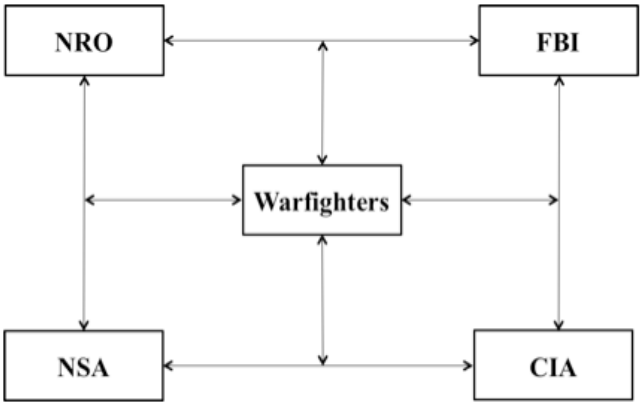

Fig. 1: Detecting Broad Cyber Invasion Through Collaboration

A government program called EINSTEIN (or Einstein) provides a good example of networking and collaboration between security agencies. Einstein was developed to provide situational awareness by sharing of data between governmental security organizations. This program was initiated in 2002 and has been incrementally upgraded to the present. Through this collaboration, security agencies can more quickly identify cyber intrusion and determine if it is localized or a broad attack against other security agencies[3].

Deterrence Through Denial

While always remaining diligent in identifying malware that may have penetrated our systems, we direct our primary focus on stopping penetration in the first place, by executing detection procedures in a VM environment and ensuring awareness of the big picture awareness to include:

- **New Sensors** – Stay aware of new sensors to keep reconnaissance and countermeasures current with emerging technology.
- **Software Signatures and Intelligence Systems**[4] – If we are finding signatures it means our systems have been penetrated, thus the need for detection procedures to run in a virtual environment on all applications prior to their being loaded on the physical host.
- **Countermeasures to Include Preemptive Challenges** – According to some Cyber officials, we should be prepared to employ kinetic weapons to counter or preempt Cyber assaults on national security networks. The danger here is that an accomplished hacker might point us to an innocent

1. http://www.totallyintegratedautomation.com/2011/04/defending-against-industrial-malware/
2. http://en.wikipedia.org/wiki/Cyberwarfare_in_the_United_States
3. https://www.dhs.gov/cybersecurity-and-privacy
4. Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security - Stephen G. Batsell, Nageswara S. Rao, Mallikarjun Shankar

source, which we subsequently neutralize, placing us in an untenable geopolitical situation, including armed conflict.
- **Threat Sources** – So far the assumption is that the threat seems to be from individual hackers vs. hostile nation states, but this may be a dangerous assumption since individual hackers will have a market for their information. That market may include hostile nations who may in turn use the information thus attained for directing kinetic weapons against our national resources.

We keep in mind this list of attributions when integrating security measures into our systems. But we must also assume that a malware developer might anticipate any given approach, and take their own countermeasures; thus we would expect a comprehensive plan to include counter-countermeasures.

For example, if an application to be loaded on the target system contained dead code, we recognize that the path analyzer would not find it, but the only way malicious software could reach the dead code to fulfill its malicious intent, would be to modify itself during execution to provide a path to that code. Therefore, self-modifying code becomes part of the path analysis, and thus a property.

Once having found the path to the dead code, it would be included in the path analysis. Thus self-modifying code and dead code represent two properties in our original properties list. Our initial research, currently in progress, is to determine as many of these properties as possible to be applied in a virtual environment. Through the analysis of a large number of applications, the virtual system would "learn" an extensible number of characteristics of malware, using that information to dynamically expand the properties list, with a corresponding increase in the malware detection rate.

Since current firewalls are notoriously ineffective and are routinely being defeated by malware developers, current malware detection focuses on catching malware in the act after it has already invaded the target system. Unfortunately, no matter how good detection is, once the malware is running on the target platform the risk is significant, with the potential for damage then being measured in seconds, if not milliseconds. This underlines the importance of malware and spyware detection running on all applications on a VM prior to their being loaded into the operational host.

Our investigation finds that even the best of the malware detection applications advertise detection only minutes after initial intrusion, but a lag of even seconds could be too late to stop the transfer of critical information to external hostile destinations, or significant damage to owner applications and databases. Thus the best malware protection would be to not allow the malware into the owner platform in the first place, but this level of security is not currently being provided industry-wide to an extent that would provide a comfortable level of confidence in Information Assurance (IA) in typical system environments.

The current approach is shackled with severe limitations. Techniques now being employed, of which we are aware, are largely based on the assumption that malware invasion is inevitable, with detection being in the host system as soon as possible on day one of the intrusion, followed by quarantine and elimination of the threat. Detection techniques that are signature-based, anomaly-based, or that provide detection based on behavior are run on the application only after it is running in the system. Running JPF or a similar VM detection system has the potential to significantly reduce or eliminate this problem.

The two most common forms of malware/spyware detection, as of the writing of this paper, are signature-based and anomaly-based detection, which require pre-knowledge of the malware, and are only initiated after the malware has invaded a target system. With no pre-knowledge, malware can go undetected for days, if not weeks or months, inflicting significant damage and distribution of security-sensitive, if not highly classified information to the malware/spyware source. This has, in fact, happened, though how prevalent these invasions are is an open question.

The limitations of current methods of malware detection on the host computer, at best, briefly allow access to databases and applications, and at worst can allow spyware to execute for months without detection. Thus, we treat allowing malware access to the host system as being unacceptable. The basic premise of our developing plan is that malware must be detected and eliminated prior to intrusion.

We will intensify our investigation into malicious software detection, starting with the currently understood malware obfuscation and signature-based properties, progressing to development of predictive capabilities to recognize obfuscation metamorphoses of existing malware, and potential new malware, which may, or may not be related to known malware patterns or their metamorphic progeny.

We are looking at going a step (or several steps) beyond signature/anomaly-based detection. For example, we could use the data gained from successful intrusions or those captured in virtual machines to produce histograms mapping to source and destination points to reveal potential self-propagating malware intrusion[5]. This example is one of several paths we are exploring, as Avums investigation continues.

The initial analysis and discovery phases will provide properties to be applied during application path analysis in the VM environment, the current plan being JPF, which we are continuing to research.

Based on the foregoing, we currently envision a virtual system to detect recognizable system execution that would signal unusual activity attributable to the presence of malware. With malware being detected, the system administrator would be given an alarm, so that action could be taken to extract as much information as possible about the malware then remove and isolate it from the system for further study.

Though we would make every effort to detect malware in the virtual environment, post-intrusion detection still has significant value in detecting malware making it through the virtual system. We would facilitate information exchange between the virtual system and the imbedded malware detection applications to ensure the latest properties are available to both.

Our plan requires an initial list of properties, which will be established to provide a baseline for our pre-intrusion malware protection. This properties list will originally be based on known properties that can be gleaned from current desktop and laptop systems, and various mobile platforms, such as those in the Android-based mobile application, Nokia's Symbian, Apple's iOS, Microsoft's Windows Phone 7, RIM's BlackBerry OS, and embedded Linux distributions such as Maemo and MeeGo marketplaces. To ignore these mobile applications would be to deny the rapidly accelerating forward momentum

5. Self-Propagating Malware Detection using Information-Theoretic Tools, Syed Khayam & Hayder Radha, Mich State University

of technology.

Such an approach is necessary to place us one step ahead, rather than one step behind the creators and maintainers of malicious/spyware software. We would cooperate in a network of users of these systems to share information on malware to help them and us to predict malware prior to its arrival on any system, whether desktop or mobile.

IA Malware Detection and Response

Avum views this challenge as being one of advancing the state-of-the-art in malware detection, rather than improving detection by observing syntactic patterns or anomalous behavior, both of which are subject to time lags or unacceptable uncertainty in detection results. As demonstrated in this paper, we are already researching the potential of developing a semantics-based detection framework that recognizes malicious code through studying the semantics, rather than the signature of a malicious program. That is, by monitoring behavior of known malware, we believe we can establish a pattern of behavior that must break with the system architecture it was meant to invade and compromise.

With success of our Virtual Machine malicious software detection, we believe that both government and corporate entities can significantly exceed goals and meet future goals in a timelier manner. Further, we believe that as our malware detection technique matures through "learning" from malware inspection by applying comprehensive program path analysis, we can eventually get malware intrusion down to zero. This would be achieved through adaptation of our IA Framework to rapidly sort through extraneous information to zero in on that information which is directly relevant to pending intrusion, including that for mobile application.

Our VM analysis is application naïve, so it will provide malware detection as a front end to any system based on those specific properties. Therefore any system, stationary or mobile, requiring Cybersecurity should benefit from our VM malware detection.

4 Conclusion

The DoD has already experienced breeches in Cyber Security (see endnote). And it is possible that we may have already experienced cyber attacks on our electrical grid[6], as represented by widespread power outages in the northeast and southeast, recalling these incidents over the last few years, with one being as recently as 2012. However, we are not currently, as of the date of this paper, privy to any information that would substantiate that possibility, or that there was any evidence to that effect. Still it would be good to be on guard for activities that might be attributable to such attacks on our infrastructure.

Acknowledgments

We acknowledge our governmental security agencies: NSA, CIA, FBI, DHS, NRO, and DoD. They work on our behalf, while fielding criticism without complaint. These are in addition to our academic institutions and industry. Thank you.

6. http://www.nap.edu/openbook.php?record_id=12050&page=117

References

[1] The Department of Homeland Security. *Cyber Security.* 2013. <https://www.dhs.gov/topic/cybersecurity>
[2] Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack, Board on Energy and Environmental Systems, Division on Engineering and Physical Sciences. *Terrorism and the Electric Power Delivery System*. The National Academic Press. 2012.
[3] The Economist. *Cyber War: The Worm Turns.* December 4, 2008. <http://www.economist.com/node/12725712>
[4] Wikipedia.org. *Struxnet*. 2013. <http://en.wikipedia.org/wiki/Struxnet>

Endnote

A case in point; the August 2010 Cyber Attack on DoD cited in this paper:

In an article from EWeek dated August 25, 2010, a Defense Department official discusses the details of a formerly classified cyber-attack on the U.S. military. This is given to show that cyber attacks can even occur on what are considered to be our most secure systems, and that more research needs to be done in order to further eliminate these risks. The article reads as follows:

> "A senior Pentagon official has revealed details of a previously-classified malware attack he declared the most significant breach of U.S. military computers ever. In an article for Foreign Affairs, Deputy Defense Secretary William J. Lynn III writes that in 2008, a flash drive believed to have been infected by a foreign intelligence agency uploaded malicious code onto a network run by the militarys Central Command..."(Read more on *EWeek.com*).

Jerry Hill Mr. Hill, as Senior Science Advisor for Avum, Inc., brings to the company his 40 years of experience in computer system architecture, design, and process-driven system development. He has worked in the capacity of System Architect, and Project Manager in the development of science-based, computer systems for NASA/JPL, Air Force, Navy, and Army contracts. He has proposed solutions for and won at least two contracts with each of these NASA and DoD clients. Mr. Hill is currently focusing on the acquisition of new business for the company, in interoperable Web-based applications, in which they excel.