Decision Sciences Institute
Global Malware Attacks: Does Cultural Factors Explain the Growth?

Anita Britton
Virginia State University
Email: abritton@vsu.edu

Aurelia Nicholas-Donald, PhD
Virginia State University
Email: adonald@vsu.edu

ABSTRACT

Empirical evidence from the World Economic Forum along with the country's gross development product and Hofstede Cultural Dimensions plays a role in predicting the nations that are more likely to deliver malware attacks. The number of malware attacks executed vary greatly from nation to nation. The findings indicate that malware attacks executed significantly correlates with GDP. After controlling for economics, national culture dimensions plays a significant role in the level of malware attacks. The results have implications for multi-national firms and cultural researchers.

KEYWORDS: Malware, Security, Hofstede, Cultural Dimensions,

INTRODUCTION

Security threats have become a key issue for industry and government entities today. The growth of the security threats has made it difficult for countries to retain control of all aspects of technology and the Internet. One popular and very dangerous threat is malware. Malware is often understood to be a catch all term for threats such as computer viruses, spyware, adware, and other software installed without a user's consent (Tian, Islam, Batten, and Versteeg, 2010; Stallings, Wardman, Warner, and Thapaliya, 2012; Mohata, Dakhane, and Pardhi, 2013).
The increasing variety of threats and the aggressiveness of attacks have made protecting information a complex task for businesses (Knapp, Marshall, Rainer and Morrow, 2006). The literature offers few explanations for the global growth in malware attacks. A recent study by International Data Corporation and National Singapore University (2014) expected that the annual cost of malware would be over $491 billion a year (Robinson 2014). Consumers are likely to spend 1.2 billion hours dealing with the after effects of malware. In a high technology society, understanding the factors that lead to malware growth is important. This study proposes that culture is one of the factors that have an impact on malware growth.
Prior research has also focused on the effects that culture has on decision-making (Vitell, Nwachukwu and Barnes, 1993; Briley, Morris, and Simonson, 2000; Lowry, Zhang, Zhou, and

Fu, 2010; Peterson, Miranda, Smith and Haskell, 2003) indicated that culture plays a significant role in decision-making. (Tung and Quaddus 2002) extended researched further and determined that culture plays a role in the type of technologies used to support decision-making. The literature also suggests that culture is one among a number of national-level factors associated with the rate of IT adoption (Krumbholz, Galliers, Coulianos, and Maiden, 2000) and implementation (Robey and Rodriguez-Diaz, 1989).

The purpose of this study is to examine the relationship between culture and the malware attacks a country sends. To study the relationship other factors must be explored for this study we use Gross Domestic Product (GDP). The next section reviews prior literature on the suggested factors. Section 3 discusses the hypotheses and explains the methodology. The last sections include the results and the discussion. The paper concludes by wrapping up the research and providing insight for future research.

LITERATURE REVIEW

Malware

Ho and Heng (2009) labeled malware as an increasing threat to the world. Malicious software was once referred to as a computer virus before Yisrael Radai coin the term malware, in 1990 (Elisan, 2012). Identifying locations of malicious software include an executable file, malicious structural features, decryption code, and cryptographic functions. Detecting a malicious structural feature embroils comparing a known malicious structural feature to one or more instructions of the executable file. Another identifying feature of a malicious structural feature is by examining graphically and statistically comparing windows of bytes or instructions in a section of the executable file. Cryptography is an indicator of malicious software. (Schmid, Weber, Haddox-Schatz and Geyer 2010). Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. (Santos, Penya, Devesa, and Bringas, 2009). The first category of malware propagation concerns parasitic software fragments that attach themselves to some existing executable content. The malicious intent describes the ability of malware and shows the opportunity of the software to act against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, as for example Regin, or it may cause harm, often as sabotage as for example, Stuxnet, or to extort payment, as for example, CryptoLocker. (Stallings et al., 2012; Mohata et al., 2013)

Cultural Factors

Because culture plays a significant role in decision-making (Peterson et al., 2003) we believe that culture should play a role in explaining why specific countries execute malware attacks more than other factors. For this study, we use Hofstede cultural dimensions.

Hofstede

Hofstede and Hofstede (2001) characterized countries using four dimensions. In the following section, we describe the four dimensions and explain their importance. In the past, studies have demonstrated how culture can promote or shape technology use. Culture does not exclusively determine technology use. Hofstede poses that the use of technology is similar to other social practices. Using Hofstede's perspective, we will predict how culture is likely to influence the level of malware attacks a nation receives (Hofstede and Hofstede 2001). Below we examine each dimension.

HYPOTHESIS

Individualism / Collectivism

On the individualist side, we find cultures in which the ties between individuals are loose: everyone looks after him/herself and his/her immediate family. On the collectivist side we find cultures in which people from birth onwards are integrated into strong, cohesive in-groups, often extended families (with uncles, aunts and grandparents) that continue protecting them in exchange for unquestioning loyalty, and oppose other in groups. (Hofstede, 1998) Individualistic traits, such as self-reliance and assertiveness, are valued over collectivistic traits, such as dependability and generosity. Individualistic cultures frown upon power differences between individuals and value direct communication to avoid misunderstandings.

High individualism countries (for example Australia, France, Canada and Denmark) tend to be early adopters of technology (Bagchi, Hart, and Peterson 2004). Bagchi et al.(2004) also posed that countries with high individualism have more purchasing power and remain cognizant of technological developments. From this, we derive the following hypothesis, countries high in individualism will execute more malware attacks.

$\boldsymbol{H_1}$: *More malware-executed attacks are from nations with high individualism.*

Power Distance

Hofstede's Power distance Index measures the extent to which the less powerful members of organizations and institutions (like the family) accept and expect that power be distributed unequally (Hofstede and Hofstede, 2001). Bochner and Hesketh (1994) posed that countries with high power distance (for example, Japan, Italy, and Argentina) were more task oriented. For this reason, we believe countries high in power distance will execute more malware attacks.

$\boldsymbol{H_2}$: *More malware-executed attacks are from nations with higher power distance.*

Masculinity/Femininity

Masculinity versus its opposite, femininity refers to the distribution of roles between the genders, which is another fundamental issue for any society. The IBM studies revealed that a woman's values differ less among societies than men's values; men's values from one country to another contain a dimension from very assertive and competitive, and maximally different from women's values on the one side, to modest, caring, and similar to women's values on the other. Masculine refers to the assertive pole and the modest, caring pole, 'feminine'. The women in feminine countries have the same modest, caring values as the men; in the masculine countries, they are somewhat assertive and competitive, but not as much as the men are, so that these countries show a gap between men's values and women's values. (Hofstede, 1998)

$\boldsymbol{H_3}$: *More malware-executed attacks are from nations with higher masculinity.*

Uncertainty Avoidance

Uncertainty avoidance deals with a society's tolerance for uncertainty and ambiguity; it ultimately refers to man's search for Truth. It indicates to what extent a culture programs its members to feel either uncomfortable or comfortable in unstructured situations. Unstructured

situations are novel, unknown, surprising, and different from usual. Uncertainty avoiding cultures try to minimize the possibility of such situations by strict laws and rules, safety and security measures, and on the philosophical and religious level by a belief in absolute Truth; 'there can only be one Truth and we have it'. (Hofstede and Hofstede, 2001)

$\boldsymbol{H_4}$: *More malware-executed attacks are from nations with higher uncertainty avoidance.*

Economic Factor (GDP)

Lelarge and Bolot (2009) and Hofmeyr, Moore, Forrest, Edwards, and Stelle, (2013) researched the importance of protecting yourself from the effects of malware. Another study, Guerra (2009), reviews the effects economics has on malware, in particular cybercrime. An earlier study, (Anderson, Bohme, Clayton, and Moore, 2009) introduced the thought of a relationship between economics and cybercrime. We use Gross Domestic Product (GDP) to examine the relationship between economics and malware in specific.

$\boldsymbol{H_5}$: *Malware attacks are greater in nations with lower Gross Domestic Product.*

METHODOLOGY

DATA

The variables used to predict national differences in the security infrastructure were Hofstede four cultural dimensions and GDP per capita. They served as the independent variables and the country's level of security infrastructure served as the dependent variable.

RESULTS

Table 1: Correlation Table

	Hofstede uncertainty avoidance	*Hofstede masculinity*	*Hofstede individualism*	*Hofstede power distance*	*GDP (Billions) 2016*	*Malware host*
Hofstede uncertainty avoidance	1					
Hofstede masculinity	0.3349183	1				
Hofstede individualism	-0.1103542	0.1201556	1			
Hofstede power distance	-0.0546616	-0.192584	-0.600572476	1		
GDP (Billions) 2016	-0.186309	0.187406	0.188559238	0.036042	1	
Malware host	-0.1511574	0.000644	0.339714756	-0.11125	0.838507	1

The results show that a correlation exists, however the strongest correlation exist between GDP and the country executing the malware.

To predict the number of malware attacks executed based on culture and GDP a multiple linear regression was calculated. A significant regression equation was found ($F(5, 15) = 12.69$, $P < 0.000$ with an R^2 of .809.

The results predicted malware hosts is equal to -1428542+1439.532 (GDP) + 47339.03 (Uncertainty Avoidance) – 59777.6 (Masculinity) + 41984.04 (Individualism) – 29334.1 (power distance). Both GDP and Culture were significant predictors of malware hosts.

Regression

Regression Statistics	
Multiple R	0.899381
R Square	0.808886
Adjusted R Square	0.745181
Standard Error	3616718
Observations	21

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	5	8.3E+14	1.66E+14	12.69744	6E-05
Residual	15	1.96E+14	1.31E+13		
Total	20	1.03E+15			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	-1428542	5259506	-0.27161	0.789623	-1.3E+07	9781830	-1.3E+07	9781830
Hofstede uncertainty avoidance	47339.03	43357.68	1.091826	0.292137	-45075.7	139753.7	-45075.7	139753.7
Hofstede masculinity	-59777.6	42646.87	-1.40169	0.181361	-150677	31122.06	-150677	31122.06
Hofstede individualism	41984.04	38779.27	1.082641	0.296065	-40672	124640.1	-40672	124640.1
Hofstede power distance	-29334.1	48078.06	-0.61014	0.550904	-131810	73141.82	-131810	73141.82
GDP (Billions) 2016	1439.532	199.5284	7.214671	3E-06	1014.247	1864.817	1014.247	1864.817

CONCLUSION

This preliminary study provides empirical results on the factors that lead to a stronger information systems infrastructure. Most studies examine IT adoption. This study examined the existence of information systems infrastructure. In the past ten years Malware attacks has increased more than 50%. One solution is to build sound infrastructure to reduce the number of malware attacks.

The study employs empirical data for 10 nations for generalization. The study found that GDP was the only factor that made a significant statistical contribution to computer information systems infrastructure.

REFERENCES

Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2009). Security economics and European policy. In *Managing information risk and the economics of security* (pp. 55-80). Springer US.

Bagchi, K., Hart, P., & Peterson, M. F. (2004). National culture and information technology product adoption. *Journal of Global Information Technology Management*, *7*(4), 29-46.

Bochner, S., & Hesketh, B. (1994). Power distance, individualism/collectivism, and job-related attitudes in a culturally diverse work group. *Journal of cross-cultural psychology*, *25*(2), 233-257.

Briley, D. A., Morris, M. W., & Simonson, I. (2000). Reasons as carriers of culture: Dynamic versus dispositional models of cultural influence on decision making. *Journal of consumer research*, *27*(2), 157-178.

Elisan, C. C. (2012). Malware, Rootkits & Botnets A Beginner's Guide. McGraw Hill Professional.

Guerra, P. (2009). How economics and information security affects cyber crime and what it means in the context of a global recession. *BlackHat USA 2009, Turbo Talk Whitepaper*..

Ho, Y. L., & Heng, S. H. (2009, December). Mobile and ubiquitous malware. In *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia* (pp. 559-563). ACM..

Hofmeyr, S., Moore, T., Forrest, S., Edwards, B., & Stelle, G. (2013). Modeling internet-scale policies for cleaning up malware. In *Economics of Information Security and Privacy III* (pp. 149-170). Springer New York.

Hofstede, G. (1998). Identifying organizational subcultures: An empirical approach. *Journal of management studies*, *35*(1), 1-12.

Hofstede, G. H., & Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Sage.

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Morrow, D. W. (2006). The top information security issues facing organizations: What can government do to help? *Network security*, *1*, 327.

Krumbholz, M. A., Galliers, J., Coulianos, N., & Maiden, N. A. M. (2000). Implementing enterprise resource planning packages in different corporate and national cultures. *Journal of Information Technology*, *15*(4), 267-279.

Lelarge, M., & Bolot, J. (2009, April). Economic incentives to increase security in the internet: The case for insurance. In *INFOCOM 2009, IEEE* (pp. 1494-1502). IEEE.

Lowry, P. B., Zhang, D., Zhou, L., & Fu, X. (2010). Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. *Information Systems Journal*, *20*(3), 297-315.

Mohata, V. B., Dakhane, D. M., & Pardhi, R. L. (2013). Mobile Malware Detection Techniques. *International Journal of Computer Science & Engineering Technology (IJCSET)*, *4*(04), 2229-3345.

Peterson, M. F., Miranda, S. M., Smith, P. B., & Haskell, V. M. (2003). The sociocultural contexts of decision-making in organizations.

Robey, D., & Rodriguez-Diaz, A. (1989). The organizational and cultural context of systems implementation: Case experience from Latin America. *Information & Management*, *17*(4), 229-239.

Robinson, T. (2014). Breaches, malware to cost $491 billion in 2014, study says. *Accessed June 5*, 2014.

Santos, I., Penya, Y. K., Devesa, J., & Bringas, P. G. (2009). N-grams-based File Signatures for Malware Detection. *ICEIS (2)*, *9*, 317-320.

Schmid, M. N., Weber, M., Haddox-Schatz, M., & Geyer, D. (2010). *U.S. Patent No. 7,644,441*. Washington, DC: U.S. Patent and Trademark Office.

Stallings, T., Wardman, B., Warner, G., & Thapaliya, S. (2012). WHOIS selling all the pills. *International Journal of Forensic Computer Science*.

Tian, R., Islam, R., Batten, L., & Versteeg, S. (2010, October). Differentiating malware from cleanware using behavioral analysis. In *Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on* (pp. 23-30). IEEE.

Tung, L. L., & Quaddus, M. A. (2002). Cultural differences explaining the differences in results in GSS: implications for the next decade. *Decision Support Systems*, *33*(2), 177-199.

Vitell, S. J., Nwachukwu, S. L., & Barnes, J. H. (1993). The effects of culture on ethical decision-making: An application of Hofstede's typology. *Journal of Business Ethics*, *12*(10), 753-760.