Conquering the cyber attacks: analysis and protecting the enterprise resources

Article *in* International Journal of Business Continuity and Risk Management · January 2016

DOI: 10.1504/IJBCRM.2016.10002275

2 authors:

Ahmed Y. Mahfouz
Prairie View A&M University
23 PUBLICATIONS **155** CITATIONS
SEE PROFILE

Emmanuel U Opara
Prairie View A&M University
31 PUBLICATIONS **90** CITATIONS
SEE PROFILE

Conquering the Cyber Attacks: Analysis and Protecting the Enterprise Resources

Emmanuel U Opara
College of Business
Prairie View A&M University
Prairie View, Texas 77446
(Corresponding author: Emmanuel U Opara)
(Email: euopara@pvamu.edu)

Ahmed Y. Mahfouz
College of Business
Prairie View A&M University
Prairie View, Texas 77446
aymahfouz@pvamu.edu

Abstract

Security breaches of all kinds are growing in complexity, sophistication, and impact. Hacktivists are bypassing conventional security deployments at will by breaching network systems. Security professional have invested billions of dollar into conventional defenses. Yet attacker are compromising networks at an alarming manner. Regardless of what vendor or combination of typical defense-in-depth tools an organization deployed, attackers are bypassing these with ease. This study will analyses these development and develop awareness among security practitioners so that that they can be prepared to defend their enterprise system.

Keyword: Hacking, Exploit, Vulnerabilities, Cyber security, Malwares

Introduction

The quest for online presence have reignited everything from banking to healthcare to education to entertainment. The global network has altered countless industries, nation states and every aspect of civilization. Cyber criminals have evolved. Opportunist hackers of the past are now replaced by targeted well-funded cyber-crime rings. These criminals are penetrating network platforms causing damages and hijacking corporate intellectual properties. Study has shown that cyber-attacks are growing at an exponential rate and solutions have not been found to mitigate the problems [1,18].

Criminals such as Anonymous, frequently attack enterprise systems in the name of social causes by envisaging strategies to cause significant financial and reputational damage to a targeted organization [22].

Layered security defenses have failed because today's security architecture are based on a signature approach. Anomalies baseline detective tools are not up to speed or are not in existence in most of the organizations.

Recent, sophisticated attacks have often been called shell shock, zero-day and Advanced Persistent Threats, terms that are sometimes derided, but has attained widespread adoption within the security environment. These attacks as they are called, have unique and significant qualities that make them more difficult to defend [4]. These are a few examples of the threats anomalies that catch organizations by surprise. Other attacks include one of the most predominant malware attack, named "Gh0st RAT", whose source code is dated back to 2001. This sophisticated malware nicknamed Gh0st RAT (Remote Access Terminal) is a Trojan "Remote Access Tool" used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth. When injected into a platform, it has capabilities of creating havoc such as taking full control of the remote screen on the infected bot, providing real time as well as offline keystroke logging and providing live feed of webcam, microphone of infected host. Other potential problems include downloading remote binaries on the infected remote host, and taking control of remote shutdown and reboot of host. Furthermore the "Gh0st RAT" malware has the capability of disabling infected computer remote pointer and keyboard input, entering into shell of remote infected host with full control, providing a list of all the active processes and clearing all existing SQL Server Data Tools [SSDT] of all existing hooks [6].

Nation state have been using some sophisticated cyber espionage tool as a spy campaign against international targets since 2007. An example is the "Regin" which is a back door-type Trojan whose structure displayed a degree of technical competence and sophistication. Nation state use this as a top-tier espionage tool that enables stealthy surveillance. It is a multi-staged, modular threat, meaning that it has a number of components, each depending others, to perform attack operations. These types of threats are very uncommon and can be compared to the Stuxnet/Duqu family of malware because they do not seem to share any common code with other threats. These families of advanced tools in which "Regin" belong, have been used in spying operations against governments, infrastructure operators, businesses, researchers, and private individuals. "Regin" as the name is called, is structured in such a manner that its perfect fit for persistent, long term surveillance operations against targets [4,5,6].

Another dangerous malware is the Stuxnet Worm that targets industrial control systems that are used to monitor and control large scale industrial facilities like power plants, dams, waste processing systems and similar operations. This worm allows attackers to take control of these systems without the operators knowing [24].

The fact remains that businesses regardless of size or the industry, are subject of becoming victims of cybercrime. The reason is because known malware is prevalent and perceptible, but they are not innocuous. Legacy systems do not have proper or updated security mechanisms in place and as such have backdoors that are not protected or even identified as existing. Other concerns include third-party applications that are outdated and vulnerabilities that are not patched.

As study [18] had indicated, most of the data breaches start with simple malware infestation. These malware, if not detected and mitigated, could weaken security apparatus of the network thereby exposing the organization to threats that could be damaging. These damages could include extensive loss of valuable financial, personal data and intellectual intelligence.

This study will identify why attackers are bypassing conventional security deployments almost at will, and breaching network infrastructures. The result will show a startling indictment of conventional security architecture and address why cyber security had slipped through all layers of organization's defense-I depth deployment.

Literature Review

Study had shown that since 2013, global organizations of all sectors and sizes have grappled with a new wave of distributed denial of service attacks that at best have been a nuisance, at worst have served as distractions so cyber-criminals could commit fraud. However it concluded that DDoS defenses have improved, but the attacks continue to evolve in scale and sophistication [16].

Another study [27], indicated that the data leaked from the Ashley Madison breach reportedly include details of more than 30 million customers, including some who used email addresses tied to corporate accounts - ranging from Shell to Starbucks to Wells Fargo - as well as official government and military accounts in the United States, Canada, the United Kingdom and beyond.

[4], 2014, in their study on a malware, nicknamed "**Regin** described it as an "extremely complex piece of software that can be customized with a wide range of different capabilities that can be deployed depending on the target." This malware is a back door-type Trojan whose structure displays a degree of technical competence that is rarely seen, indicating that a nation state is behind it.

Another study found that in 2013, "Regin" malware infected the nation states of Russia, Saudi Arabia, Mexico, Ireland, India, Afghanistan, Iran, Belgium, Austria and Pakistan however, no confirmed infection report were noted in the United States and United Kingdom [5,10].

[2,3,7,8,13,] among others found that Department of Home Land Security [DHS] revealed that 5 percent of the cybersecurity incidents its Industrial Control Systems Cyber Emergency Response Team responded to in fiscal year 2014 were tied to weak authentication. However, four percent were tied to abuse of access authority and control. National Institute of Standards and Technology (NIST) noted that the guide, Identity and Access Management for Electric Utilities, could help energy companies reduce their risk by indicating how they can control access to facilities and devices from a single console.

According to report in [15], a recent hacking study indicating the vulnerability of American government organizations to hacking by foreign government-baked hackers was in evidence again when, a few days ago, it was revealed that Russian government hackers, using spear-phishing attacks, breached Joint Staff e-mail system. The breach caused about 4,000 civilian and military employees to lose access to their e-mail while the system was cleaned"

In another study, [14,16] recorded flaws in vehicle security, which allowed hackers to hack a car, remotely activating its windscreen wipers, applying its brakes, and even disabling them – and do all this by using simple text messages. The vulnerability was found in small black dongles which are connected to the vehicles' diagnostic ports. The dongles are used by insurance companies and fleet operators and are plugged into the car's onboard diagnostics port (OBD-II).

A recent study found that Russian government-backed hackers have managed to hack the Pentagon's unclassified e-mail server used by the office of the Joint Chiefs, Military officials. The level of the sophistication of the attack shows that it has been conducted by hackers with the resources typically available only to nation states [17, 19, 20, 23].

Early studies as reported by [9, 11, 12], noted that phishing, malware, and zero-days give information security experts the most headache. Also that network access control [NAC] remains the top technology for reducing a network's attack surface.

Methodology

To examine the issues regarding threats of cyber-security on enterprise networks and resources, a questionnaire was designed and distributed to IT security professionals and academics at a technology trade professional conference, USENIX Security '15 conference in Washington, DC.

The survey participants are IT professionals and academics. The practitioners work in or administer computer systems and handle many aspects of technology, including network security, with extensive years of experience, including network administrators, security consultants, and senior executives at their respective firms. These firms represent both mid-size and enterprise, large organizations. The academics conduct research in and publish information systems research.

The sample of completed responses is 145. This survey should represent a random sample, and be representative of the IT professionals and researchers in the field. The survey with a total of 11 questions, used Likert scales ranging from 1 ("mostly concerned") to 5 ("do not know") on rating questions regarding security threats, and categorical or yes/no questions for gender and IT position rank. The purpose of the questionnaire was to gauge the concerns of IT professionals and researchers on security issues at their organizations.

Data Analysis and Results

The present study analyzes the responses from participants based on their gender and rank in the organization (i.e. 2 predictor variables, analyzed separately), regarding what they deem as security threats, specifically on phishing (including spear phishing), malware (viruses, worms, and Trojan

horses), zero-day attacks, denial of service/distributed denial of service (DDos), and advanced persistent threats (APTs), i.e. 5 criterion variables, analyzed separately. A total of 10 hypotheses are analyzed. Independent samples t tests are used for data analysis using SAS 9.40 PROC TTEST. The pooled *t* test was used since the folded *F* test for testing equality of variances in any given pair of samples was not significant, and hence the variances are statistically equivalent or similar for any given pair of samples.

Gender was examined since the males in the sample outnumbered the females considerably, 2 to 1, and consequently it was important to test for gender effects bias. Males constituted 100 of the sample; and females, 45. The first five hypotheses deal with gender. Males were coded as 1; females, 2.

H_0: There is no difference between male and female perspectives regarding security threats of *phishing* attempts on their organization.

H_1: There is a difference between male and female perspectives regarding security threats of *phishing* attempts on their organization.

There is no significant difference in male vs. female perspectives regarding the security threat of *phishing* attempts; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 1), $t_{143} = 0.65$, $p = 0.52$, at the 0.05 level of significance. The means for both groups are very close, $M = 1.39$ for males, $SD = 0.49$, on a scale of 1 ("mostly concerned") to 5 ("do not know") regarding their organization's concern for this type of cyber threat; $M = 1.33$, $SD = 0.48$, females.

Table 1. Results of the t Test Between Gender and Phishing

Variable: Phishing				
Gender	N	Mean	Std Dev	Std Err
1	100	1.39	0.4902	0.049
2	45	1.3333	0.4767	0.0711
Diff (1-2)		0.0567	0.4861	0.0873
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	0.65	0.5171
Satterthwaite	Unequal	87.071	0.66	0.5133

The second hypothesis tests whether males and females have differences in perspective regarding *their company's concern for malware, as a cyber-threat against their organization*.

H_0: There is no difference between male and female perspectives regarding security threats of *malware* attempts on their organization.

H_1: There is a difference between male and female perspectives regarding security threats of *malware* attempts on their organization.

There is no significant difference in male vs. female perspectives regarding the security threat of *malware* attempts; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 1), $t_{143} = -0.30$, $p = 0.77$, at the 0.05 level of significance. The means for both groups are very close, $M = 1.33$ for males, $SD = 0.47$, on a scale of 1 ("mostly concerned") to 5 ("do not know") regarding their organization's concern for this type of cyber threat; $M = 1.36$, $SD = 0.48$, females.

Table 2. Results of the t Test Between Gender and Malware

Variable: Malware				
Gender	N	Mean	Std Dev	Std Err
1	100	1.33	0.4726	0.0473
2	45	1.3556	0.4841	0.0722
Diff (1-2)		-0.0256	0.4762	0.0855
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	-0.3	0.7654
Satterthwaite	Unequal	83.044	-0.3	0.7678

The third hypothesis tests whether males and females have differences in perspective regarding *their company's concern for zero-day attacks, as a cyber-threat against their organization*.

H_0: There is no difference between male and female perspectives regarding security threats of *zero-day* attacks on their organization.

H_1: There is a difference between male and female perspectives regarding security threats of *zero-day* attacks on their organization.

There is no significant difference in male vs. female perspectives regarding the security threat of *zero-day* attacks; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 1), $t_{143} = -0.28$, $p = 0.78$, at the 0.05 level of significance. The means for both groups are very close, $M = 1.178$ for males, $SD = 0.39$, on a scale of 1 ("mostly concerned") to 5 ("do not know") regarding their organization's concern for this type of cyber threat; $M = 1.2$, $SD = 0.40$, females.

Table 3. Results of the t Test Between Gender and Zero-Day Attacks

Variable: ZeroDay				
Gender	N	Mean	Std Dev	Std Err
1	100	1.18	0.3861	0.0386
2	45	1.2	0.4045	0.0603
Diff (1-2)		-0.02	0.3919	0.0703
Method	Variances	DF	t Value	Pr > |t|

Pooled	Equal	143	-0.28	0.7766
Satterthwaite	Unequal	81.395	-0.28	0.7807

The fourth hypothesis tests whether males and females have differences in perspective regarding *their company's concern for DDos attacks, as a cyber-threat against their organization*.

H_0: There is no difference between male and female perspectives regarding security threats of *DDos* attacks on their organization.

H_1: There is a difference between male and female perspectives regarding security threats of *DDos* attacks on their organization.

There is no significant difference in male vs. female perspectives regarding the security threat of *DDos* attacks; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 1), $t_{143} = 0.32$, $p = 0.75$, at the 0.05 level of significance. The means for both groups are very close, $M = 1.27$ for males, $SD = 0.45$, on a scale of 1 ("mostly concerned") to 5 ("do not know") regarding their organization's concern for this type of cyber threat; $M = 1.24$, $SD = 0.43$, females.

Table 4. Results of the t Test Between Gender and DDos Attacks

Variable: DDos				
Gender	N	Mean	Std Dev	Std Err
1	100	1.27	0.4462	0.0446
2	45	1.2444	0.4346	0.0648
Diff (1-2)		0.0256	0.4427	0.0795
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	0.32	0.7482
Satterthwaite	Unequal	86.944	0.32	0.7461

The fifth hypothesis tests whether males and females have differences in perspective regarding *their company's concern for APTs, as a cyber-threat against their organization*.

H_0: There is no difference between male and female perspectives regarding security threats of *APTs* on their organization.

H_1: There is a difference between male and female perspectives regarding security threats of *APTs* on their organization.

There is no significant difference in male vs. female perspectives regarding the security threat of *APTs*; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 2), $t_{143} = 0.32$, $p = -0.41$, at the 0.05 level of significance. The means for both groups are very close, $M = 2.20$ for males, $SD = 0.85$, on a scale

of 1 (“mostly concerned”) to 5 (“do not know”) regarding their organization’s concern for this type of cyber threat; $M = 2.27$, $SD = 1.03$, females. It is noteworthy to mention that both the means and standard deviations for both groups regarding APTs are higher in comparison with the other four cyber threats values. Of all the five threats, it seems both high and low-level IT personnel view APTs as the least threatening in comparison to phishing attempts, malware, zero-day attacks, and DDos, based on mean values of the responses.

Table 5. Results of the t Test Between Gender and APTs

Variable: APTs				
Gender	N	Mean	Std Dev	Std Err
1	100	2.2	0.8528	0.0853
2	45	2.2667	1.0313	0.1537
Diff (1-2)		-0.0667	0.9115	0.1636
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	-0.41	0.6843
Satterthwaite	Unequal	72.204	-0.38	0.7057

The following five hypotheses tested the perspective of an IT personnel in terms of his or her rank in an organization (e.g. executive vs. non-executive) and the organization’s concern regarding the cyber threats of phishing attempts, zero-day attacks, malware, DDos, and APTs. Executives/Senior IT Administrators were coded as 1; lower-level IT personnel, 2. There were 86 Executives/Senior IT Administrators out of 145 in the sample; the remaining 59 respondents were lower-level IT personnel.

The sixth hypothesis tests whether top Executives/Senior IT Administrators vs. lower-level IT personnel have differences in perspective regarding *their company’s concern for phishing attempts, as a cyber-threat against their organization*.

H_0: There is no difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *phishing* attempts on their organization.

H_1: There is a difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *phishing* attempts on their organization.

There is no significant difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding the security threat of *phishing* attempts; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 1), $t_{143} = 1.04$, $p = 0.30$, at the 0.05 level of significance. The means for both groups are very close, $M = 1.41$ for Executives/Senior IT Administrators, $SD = 0.49$, on a scale of 1 (“mostly concerned”) to 5 (“do not know”) regarding their organization’s concern for this type of cyber threat; $M = 1.32$, $SD = 0.47$, lower-level IT personnel.

Table 6. Results of the t Test Between IT Rank and Phishing Attempts

Variable: Phishing				
ExcAdmin	N	Mean	Std Dev	Std Err
1	86	1.407	0.4942	0.0533
2	59	1.322	0.4713	0.0614
Diff (1-2)		0.0849	0.485	0.082
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	1.04	0.3019
Satterthwaite	Unequal	128.58	1.05	0.2979

The seventh hypothesis tests whether top Executives/Senior IT Administrators vs. lower-level IT personnel have differences in perspective regarding *their company's concern for malware attacks, as a cyber-threat against their organization*.

H_0: There is no difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *malware* attacks on their organization.

H_1: There is a difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *malware* attacks on their organization.

There is a significant difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding the security threat of *malware* attacks; hence both groups view it differently as a threat, $t_{143} = -2.19$, $p = 0.03$, at the 0.05 level of significance. The means for both groups are the following: $M = 1.27$ for Executives/Senior IT Administrators, $SD = 0.45$, on a scale of 1 ("mostly concerned") to 5 ("do not know") regarding their organization's concern for this type of cyber threat; $M = 1.44$, $SD = 0.50$, lower-level IT personnel. This reflects that the strategic vision regarding malware threats differs from the tactical and/or operational levels of an organization. The lower-level IT personnel may encounter such attacks on a regular basis, while top executives may not experience such daily occurrences of threat. Being on the front-lines would create a different perspective for the lower-level IT personnel.

Table 7. Results of the t Test Between IT Rank and Malware Attacks

Variable: Malware				
ExcAdmin	N	Mean	Std Dev	Std Err
1	86	1.2674	0.4452	0.048

2	59	1.4407	0.5007	0.0652
Diff (1-2)		-0.1732	0.4685	0.0792
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	-2.19	0.0304
Satterthwaite	Unequal	114.91	-2.14	0.0345

The eighth hypothesis tests whether top Executives/Senior IT Administrators vs. lower-level IT personnel have differences in perspective regarding *their company's concern for zero-day attacks, as a cyber-threat against their organization*.

H_0: There is no difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *zero-day* attacks on their organization.

H_1: There is a difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *zero-day* attacks on their organization.

There is no significant difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding the security threat of *zero-day attacks*; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 1), $t_{143} = 1.30$, $p = 0.20$, at the 0.05 level of significance. The means for both groups are very close, $M = 1.22$ for Executives/Senior IT Administrators, $SD = 0.42$, on a scale of 1 ("mostly concerned") to 5 ("do not know") regarding their organization's concern for this type of cyber threat; $M = 1.14$, $SD = 0.35$, lower-level IT personnel.

Table 8. Results of the t Test Between IT Rank and Zero-Day Attacks

Variable: ZeroDay				
ExcAdmin	N	Mean	Std Dev	Std Err
1	86	1.2209	0.4173	0.045
2	59	1.1356	0.3453	0.045
Diff (1-2)		0.0853	0.3897	0.0659
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	1.3	0.1973
Satterthwaite	Unequal	137.95	1.34	0.1819

The ninth hypothesis tests whether top Executives/Senior IT Administrators vs. lower-level IT personnel have differences in perspective regarding *their company's concern for DDos attacks, as a cyber-threat against their organization*.

H_0: There is no difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *DDos* attacks on their organization.

H_1: There is a difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *DDos* attacks on their organization.

There is no significant difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding the security threat of *DDos attacks*; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 1), $t_{143} = 0.18$, $p = 0.86$, at the 0.05 level of significance. The means for both groups are very close, $M = 1.27$ for Executives/Senior IT Administrators, $SD = 0.45$, on a scale of 1 ("mostly concerned") to 5 ("do not know") regarding their organization's concern for this type of cyber threat; $M = 1.25$, $SD = 0.44$, lower-level IT personnel.

Table 9. Results of the t Test Between IT Rank and DDos Attacks

Variable: DDos				
ExcAdmin	N	Mean	Std Dev	Std Err
1	86	1.2674	0.4452	0.048
2	59	1.2542	0.4392	0.0572
Diff (1-2)		0.0132	0.4428	0.0749
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	0.18	0.8602
Satterthwaite	Unequal	125.91	0.18	0.8599

The tenth hypothesis tests whether top Executives/Senior IT Administrators vs. lower-level IT personnel have differences in perspective regarding *their company's concern for APTs, as a cyber-threat against their organization*.

H_0: There is no difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *APTs* on their organization.

H_1: There is a difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding security threats of *APTs* on their organization.

There is no significant difference in perspective between Executives/Senior IT Administrators and lower-level IT personnel regarding the security threat of *APTs*; hence both groups view it equally as a threat given the values of their respective means (on a scale of 1 to 5, whereby the means are closer to 2), $t_{143} = 0.56$, $p = 0.58$, at the 0.05 level of significance. The means for both groups are very close, $M = 2.26$ for Executives/Senior IT Administrators, $SD = 0.92$, on a scale of 1 ("mostly concerned") to 5 ("do not know") regarding their organization's concern for this type of cyber threat; $M = 2.17$, $SD = 0.89$, lower-level IT personnel. It is noteworthy to mention that both the

means and standard deviations for both groups regarding APTs are higher in comparison with the other four cyber threats values. Of all the five threats, it seems both high and low-level IT personnel view APTs as the least threatening in comparison to phishing attempts, malware, zero-day attacks, and DDos, based on the values of the means of the responses.

Table 10. Results of the t Test Between IT Rank and APTs

Variable: APTs				
ExcAdmin	N	Mean	Std Dev	Std Err
1	86	2.2558	0.9227	0.0995
2	59	2.1695	0.8935	0.1163
Diff (1-2)		0.0863	0.911	0.154
Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	143	0.56	0.576
Satterthwaite	Unequal	127.39	0.56	0.5738

Summary of the Hypotheses

Ten hypotheses were tested to see if there was a significant effect among pairs of samples. Five involved gender and each of the threat of phishing, malware, ZeroDays attacks, DDos, and Advanced Persistent Threats [APTs], separately. The remaining five examined the Information Technology IT] role of Executives/Senior IT Administrators regarding the same aforementioned threats in comparison with the perspectives of lower level IT staff and professionals. In nine hypotheses, both females and males, and high and low level personnel did not differ significantly in their perspectives regarding any of the five cyber threats; hence, they agree on the concerns for such threats, given the values of the means of their responses. It is noteworthy to mention that both the means and standard deviations for both groups regarding APTs are higher in comparison with the other four cyber threats values. Of all the five threats, it seems both high and low-level IT personnel view APTs as the least threatening in comparison to phishing attempts, malware, zero-day attacks, and DDos.

Only in one hypothesis, whereby the IT role showed a significant difference in perspective regarding malware, i.e. Executives/Senior IT Administrators had a different concern regarding the threat of malware on their organization, in comparison with lower IT personnel. This means a different view strategically vs. tactically/operationally when it comes to how malware impacts an organization.

Overall Conclusion

Our study revealed that knowledge is power since awareness of specific circumstances that give rise to vulnerabilities allow security practitioners to address the root causes of a given breach. Most of these survey participants feel that their systems are somewhat secured, however vigorous secure development practices should be adhered to prevent compromised exploits from becoming a disaster. The study also revealed that security professionals should move away from passive, poorly integrated defenses that provide a fragmented view of threats to a dynamic approach that can identify the anomalies from those malware families that are difficult to detect.

Our literature reviews also found that the threats from sophisticated malware continue to rise as attacks on organizations such as "Target' and "Home Depot" highlighted the risk associated from network and point of sales operations. This study uncovered ongoing developments, increasing sophistication and divergent code base on malware deliverables. Majority of IT staff in the study agree that security teams can no longer afford to passively wait for attacks to occur. Instead they need to implement a dynamic adaptive defense approach that actively search and eliminate new and unseen exploits such as the Zero-day, Shellshock, Frame-sniffing, Game-over, Zeus, Gepaw, Heap-spray, Money-Pack, Advanced Persistent Threats [APTs], before they become a problem.

Some of the malware identified in this study are centered on high-profile incidents as Heartbleed and Shellshock attacks, that could lead software developers and architects to tackle security issues more effectively, especially those in foundational or legacy codes.

A multi-layered approach is necessary in order to deploy effective controls. By approaching security breaches with a focus on privileged identity management, data security, access governance, and advanced authentication procedures, organizations can protect their most critical resources from potential hacktivists.

Organizations that success in reducing the chances of a security breach should think beyond the direct cost savings of lost data, fines and lawsuits, instead should focus on an integrated architecture that enables big picture cyber vigilance.

Implication for practitioners

As our study has illustrated, much of the conversation on cyber security has focused on rising assault volume and increased attack sophistication. Identifying these does help raise awareness to the problem however it does not disclose the totality and implications of a breach. Any unmitigated attack could costs an organization approximately $40,000 per hour. The effects of the implications could be lost business opportunities which could include loss of clients, data theft, litigations and loss of intellectual property.

Challenges

The key to as an effective cyber defense is early detection since this will avert the worst effect a breach will have on an organization. In the past, conventional signature-based defenses have

been the problem. This is true because anti-detection techniques, such as code-morphing and binary packing, can create a bombardment of exclusive binary samples from the same malware family and be more problematic to a network.

Appendix. Questionnaire of the Study

1=Mostly concerned
2= Moderately concern
3= Hard to Decide
4= Not concerned
5= Do not know

1 **Select Gender Male = 1; Female = 2**

2 **Are you an Executive or a Senior IT Administrator?**

3 How secured do you think your company network is?

4 How strongly do you agree to the effectiveness of the Network Security Systems of your organization?

5 Do you agree that investment in Intrusion Detection Systems [IDS] in 2015-2016 that would increase with private software companies and system integrators will provide the best systems solutions to thwart network attacks?

6 **On a scale of 1 [least] to 5 [most], rate your company's concern for each of the following types of cyberthreats targeting your organization?**

Phishing / spear—phishing attacks

Malware [virus, warms, Trojans]

Zero-day attacks [against publicly unknown]

Web application attacks [buffer overflows, XML,SQL injections]

Denial of service [Dos] / distributed denial of service

Advanced persistent threats [APTs] targeted attacks - rats etc.

SSL-encrypted threats

Mobile device malware [smartphones, tablets]

7 On a scale of 1[least] to 5 [most], rate the groups that pose the greatest network security threat to your organization.

Hackers

Current and former Employees

Foreign Nation-States. Examples: China, Russia, North Korea

Software Analysis

8 On a scale of 1[least] to 5 [most], rate the following proactive activities and techniques that your organization uses to counter Advanced Persistent Threats [APT], Shell Shock, Zero-Day threats

Malware [virus, warms, Trojans]

Intrusion Detection Systems

[a] Signature Base

[b[Anomalies Base

Rogue Device Scanning

Analysis of IP Traffic [including masking and subnetting

Deep Packets inspection

9 On a scale of 1[least] to 5 [most], rate the following Zero-Day Exploits that hit your company in the past 12 months.

Java attacks

Water Hole attacks

Operating Systems attack

Internal Explorere Zero-Day attack

10 How effective is your organization's intrusion detection systems to detect and protect against today's cyber threats?

11	How dedicated is your organization in investing on advanced security technologies like next generation firewalls, SIEM ETC?

References

[1] Anderson, Kerry A.; "A Case for a Partnership between Information Security and Records Information Management," *ISACA Journal*, vol. 2, 2012, www.isaca.org/archives

[2] Rapid7 Report (2012): "Data Breaches in the Government Sector." Rapid7. September 6, 2012. http://www.rapid7.com.

[3] Steinbart, Paul John; Robyn L. Raschke; Graham Gal; William N. Dilla; "Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions," forthcoming in the *Journal of Information Systems*, 2013.

[4] Kaspersky lab Report [2014], The Rein Platform Nation-State Ownage of GSM Networks, Version 1.0 24 November 2014

[5] http://www.mcafee.com/in/resources/white-papers/foundstone/wp-know-your-digital-enemy.pdf

[6] http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf

[7] Goldman, C. FreeWave Technologies. www.elp.com/articles/powergrid_international/print/volume-17/, 2012.

[8] Baldor, Lolita C. (2013), ""US Ready to Strike Back against China Cyberattacks," Yahoo News, 19 February 2013, http://news.yahoo.com/us-ready-strike-back-against-china-cyberattacks-225730552--finance.html.

[9] Ashford, Warwick; (2013), "Why Has DLP Never Taken Off?," *Computer Weekly*, 22 January 2013, www.computerweekly.com/news/2240176414/Why-has-DLP-never-taken-off.

[10] Forrester Research, Inc. "Kill Your Data To Protect It From Cybercriminals. July 12, 2012

[11] Gross, Michael Joseph; "A Declaration of Cyber-War," *Vanity Fair*, April 2011, www.vanityfair.com/culture/features/2011/04/stuxnet-201104

[12] Macaulay, Tyson; Bryan Singer; *Cybersecurity for Industrial Control Systems SCADA, DCS, PLC, HMI, and SIS*, CRC Press, USA, 2012

[13] World Economic Forum, Partnering for Cyber Resilience (PCR), 2014, www.weforum.org/issues/partnering-cyber-resilience-pcr

[14] Verizon, *2014 Data Breach Investigations Report*, 2014, www.verizonenterprise.com/DBIR/

[15] Secunia, Vulnerability Review, 2014, http://secunia.com/vulnerability-review/vulnerability_update_all.html

[16] Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020," Newsroom, 12 December 2013, www.gartner.com/newsroom/id/2636073

[17] Gartner, "Gartner Says the Internet of Things Will Transform the Data Center," Newsroom, 19 March 2014, www.gartner.com/newsroom/id/2684616

[18] Freescale, *What the Internet of Things (IoT) Needs to Become a Reality*, white paper, May 2014, www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf

[21] Hardgrave, Bill; "RFID Adoption Is on Target," *RFID Journal*, 5 January 2015, www.rfidjournal.com/articales/view?12575

[19] Intel, *Developing Solutions for Internet of Things*, white paper, 2014, www.intel.in/content/dam/www/public/us/en/documents/white-papers/developing-solutions-for-iot.pdf

[20] NCC Group, *Security of Things: An Implementer's Guide to Cyber-Security for Internet of Things Devices and Beyond*, 2014, https://www.nccgroup.com/en/learning-and-research-centre/white-papers/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/

[21] D. E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," New York Times, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obamaordered-wave-of-cyberattacks-against-iran.html [cited 15.11.2012]

[22] [Olson2012] We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency, Little, Brown and Company (June 5, 2012), ISBN 978-0316213547

[23] Eds. Jari Rantapelkonen & Mirva Salminen, "The Fog of Cyber Defense" National Defense University/Department of Leadership and Military Pedagogy. Juvenes Print OY 2013.

[24] David Albright, Paul Brannan, and Christina Walrond. Stuxnet malware and natanz: Update of isis december 22, 2010 report. Technical report, World Wide Web, http://isis-online. org/uploads/isis-reports/documents/stuxnet_update_15%Feb2011.pdf, February 2011.

[25] Mark Clayton. Stuxnet cyberweapon looks to be one on a production line, researchers say. Technical report, World Wide Web, ttp://www.csmonitor.com/USA/2012/0106/ Stuxnet-cyberweapon-looks-to-be-%one-on-a-production-line-researchers-say, January 2012.

[26] Contributors. Stuxnet. Technical report,WorldWideWeb, http://en.wikipedia.org/wiki/Stuxnet.

[27] Krebson Securty –In depth Security News and Investigation. July 15, 2015.