SCIENCE INQUEST
Excellent in sharing scientific knowledge

Open Access
Research Article

Volume 1 Issue 1 *Journal of Forensic and Crime Investigation*

Network Platforms, Advanced Persistence Threat – The Changing Patterns of Cyber-Attacks

Opara EU*, Mahfouz AY and Holloway RR

College of Business, Prairie View A&M University, Prairie View, Texas, USA

***Corresponding Author:** Opara EU, College of Business, Prairie View A&M University, Prairie View, Texas, USA, E-mail: euopara@pvamu.edu

Citation: Opara EU, Mahfouz AY, Holloway RR (2017) Network Platforms, Advanced Persistence Threat – The Changing Patterns of Cyber-Attacks. J Forensic crime investi 1(1): 104

Received: June 13, 2017; **Published:** September 28, 2017

Abstract

Enterprise systems are constantly being attacked by cyber criminals in an escalating manner and this threat has continued to grow. The problem remains that mitigation tools are not adequate to keep attackers at bay. This study will outline signature and non-signature oriented threats on computers and network and will recommend ways enterprise systems can prevent and secure organizational network.

Keywords: *Forensic; Hacking; Exploit; Vulnerabilities; Cyber security and Malware*

Introduction

In 2017, Cyber-attacks are projected to get worst. Online crimes and economic espionage are expected to cost the global economy more than $750 billion annually. This problem is escalating exponentially at an alarming rate. Several high-profile breaches over the past years have resulted in millions of dollars in lost revenue, exposed risk and exploits, governmental sanctions, and loss of public confidence in the breached organizations. Non signature oriented threats such as Shell Shock, Advanced Persistent threats [APTs], Zero-Day, top the list of major concerns to industry security professionals [1].

According to a study by Price Waterhouse in 2015, more than 40% of security breaches resulted in over 60% increase in theft of intellectual property [2].

Security professional are constantly fighting some of the most potent weapons used by advanced threat actors which include, Zero-day, APT Tactis, Zeus Trojan [Zbot], Stuxnet, Malicious Computer Worm, Duqu, Flame, RATs [Remote Access Trojan], GhOst RAT, and Shell Shock also known as Bash door. Others, include Ransom-ware, Threat kits, Malware, Spear-phishing, Rombertik, CrypotLOcker, CryptonWall, Armored, Sparse-infector, Multi-partite, Macro, Polymorphic, FakeAV, MacDefender, W32/Netshy-P, the Sobig virus, Mimail, Bagle, Regin etc. [3].

Some of these threats are examples of anomalies that are very difficult to detect by the signature detection tools. The problem behind these anomalies is that there is no patch mechanism that the breached organizations may apply to prevent systems and network from becoming victims in real-time [4].

"Regin" spyware has been problematic to organizations since 2008. Hackers use "Regin' as an intelligence gathering and continuous monitoring system to exploit organizations. This bug is used to attack individuals, small businesses, private companies, governmental entities, research institutions, telecommunication companies etc. [5].

As this study will show, the cyber-world is witnessing an amazing time in history because of the advancement in technology, the internet of things [IoTs], and the proliferation of inter-connected peripheries. These advancements have exposed networked organizations to unexpected vulnerabilities. The sad phenomenon is that the industry is slow to managing these developments while the attack vectors gets complex and difficult to manage.

Open Systems Interconnection Model OSI TCP/IP Stacks

Most of the security vulnerably found in networking systems happen at the application layer of the OSI model or

TCP-IP stacks. Exploits at these layers include malicious code objects, found in signature and signature-less oriented configurations.

At the presentation layer, the problematic security concern is encryption because this layer is responsible for making encryption and decryption of data transmitted over the network.

At the session layer, a known exploit malicious tactic that cyber actors use to take advantage of security vulnerabilities is session hijacking. These actors exploit this layer because most unencrypted application traffic authentication, happen at the beginning of a communications sequence. Cyber actors might use a hijacking attack to disable the entire enterprise network.

At the transportation layer, a hacker could attack the network using the SYN-Flood attack mechanism. This exploit takes advantage of weaknesses in the way some operating systems handle TCP's three-way handshaking process.

In the Network layer, cyber actors can manipulate datagram fragments so that one of these two conditions will happen: two fragments overlap or two adjacent fragments will not meet, thereby compromising the network.

The datalink and the physical layers are subject to threats that do not affect other layers. However, if a hacker has control to these layers, the hacker could use a hardware or software packet sniffer to monitor traffic and do havoc to the entire network.

Enterprise systems that collect and stores sensitive data are vulnerable to cybercrime and are at risk for a data breach. This study will highlights the reasons why effective cybersecurity is complex to deliver and further illustrate that the security defenses of organizations are eroding the traditional and legacy perimeters which are creating more motivation for threat actors. The study will conclude with effective ways to mitigate these problems.

Literature Review

Reports from Krebson Security (2015), Villeneuve (2015), among others, showed that a large DDoS attack was carried out using a botnet of zombie 25,000 CCTV cameras against a jewelry shop website [6,7]. This attack exposed the dangers of keeping IoT devices connected to the Internet while remaining unsecured. This study concludes by summarizing that securing the network is critical to both the physical and network components in the TCP/IP suite or OSI stacks.

In another study by Lolita (2013), and Warwick (2013), it was found that the attack on Target was from external cyber-actors [8,9]. The study revealed that the attackers were able to gain access using stolen credentials from a third-party HVAC vendor. The criminals gained elevated privileges and hacked the Ariba/BMC accounts. They deployed memory scrapers on Point of Sale [POS] systems and extracted customers' credit card data. As a result, Target suffered a market loss of over $5 billion dollars and were fined over one billion dollars for the breach.

Smith (2014), and Lawrence (2014) found evidence that cybercrime and economic espionage cost the global economy more than $450 billion dollars annually [10,11]. Their studies summarized by equating cybercrimes to the negative economic impact of global drug trafficking.

In other studies by Rantapelkonen., *et al*. (2013), and the Gartner report (2013), it was reviled that Edward Snowden breach on NSA started with his gaining privileged access to a constrained set of networks [12,13]. He escalated this privilege and was able to steal both usernames and passwords login credentials as well as SSH access keys from dozens of his colleagues. This resulted to the compromise of United States of America confidential documents and data thefts.

According to a Pricewaterhouse Coopers study, in 2015, 38% more security incidents were detected than in 2014. The study concluded by showing a 56% increase in theft of intellectual property [2].

Reports from NCC Group, Security of Things (2014), Intel Development Solutions for IOTs (2014), Secunia (2014), Verizon (2014), among others found evidence that "Regin" bug, the advanced hacking spyware, has been stealing Russian, Saudi and Irish state secrets for several years [14-18]. According to the study, this bug has the capability of stealing passwords, capture screenshots and restore deleted files in order to cause havoc to an organization. Their studies conclude by summarizing that "Regin" may be a case of "false flagging" in which a nation target exploits to avoid being detected. Regin is said to be a low-key spyware that is used to hack networks for extended time period before any detections are possible.

Berthiaume (2015), and Carter (2015) in their reports on CareFirst Blue Cross BlueShield breach, found evidence that hackers gained access to a database that members use to get access to the company's website and web services [19,20]. The breach resulted in 1.1 million members having their names, birth dates, email addresses and subscriber information compromised.

Nichols (2015), and Perlroth (2015), in their study found evidence that the Russian and Chinese governments are likely behind widespread cyber espionage that has hit targets in the US and elsewhere. Their reports conclude that the effort to hack into US defense contractors, Eastern European governments and European security organizations were probably sponsored by the Russian government.

A recent study found that Russia was behind the recent intrusion into a key, unclassified e-mail server used by the office of the Joint Chiefs of the United States military. The study concludes that the attack had a sophistication that indicated it was state sponsored and that the likely culprits are Russia and China [21,22].

A study by Krebs on Security (2015), found that Ashley Madison made headline after a hacking group, penetrated its servers and published the information of over 37 million users online [6]. The hackers leaked maps of sensitive information that comprised of internal company servers, employee network account information, company bank account data and salary information.

Methodology

To investigate pertinent cyber-security challenges on enterprise networks and resources, a questionnaire was given out to technology professionals and researchers in the field of cyber-security at a Network Security 2015 conference in Las Vegas, Nevada. The objective of the survey was to ascertain the challenges and issues facing both technology professionals and researchers regarding cyber-security threats at their respective organizations.

The survey respondents represent technology professionals in the cyber-security industry, as well as governmental and university researchers. The sample pool includes practitioners in the field, with varying years of experience and rank from top executives, senior systems administrators to lower-level IT staff, who administer and maintain their information systems and handle network security in their respective organizations. These organizations span mid-size to Fortune 500 companies. On the other hand, the researchers in the sample conduct and publish cyber-security research for federal agencies and universities in higher education.

The sample size was 242 completed responses, representing a random sample of technology professionals and researchers. There were 15 items in the questionnaire, with Likert scales whose anchors ranged from 1 to 5, "strongly disagree" to "strongly agree," respectively. The respondents' items on gender and IT high level job ranking had categorical choices, respectively: 1 (male) and 2 (female); 1 (yes) and 2 (no). There were 165 male and 77 female respondents, representing 68.2% and 31.8% of the sample, respectively. 131 of the sample subjects reported their IT rank as Executive or a Senior IT Administrator, while 111 reported the rank as a lower-level IT employee, representing 54.1% and 45.9% of the sample, respectively.

Data Analysis and Results

The present study examined the data of questionnaire respondents investigating the effects of the independent variables (gender, IT rank of the respondents, respondent's perceived sense of network security within his or her organization, and respondent's view regarding his or her organization's level of investment in intrusion detection systems (IDS), on 10 dependent variables (Zero-day, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks) to better understand cyber-security threats and challenges within organizations. (One independent variable Network Effectiveness was dropped since it had positive correlation with two other independent variables, Network Security (r = 0.73) and Investment in IDS (r = 0.73).

Independent Variables	
Gender	Gender? Male = 1; Female = 2
IT_Rank	Are you an Executive or a Senior IT Administrator? Yes = 1; No = 2
NetSec	How secure do you think your company's network is?
*NetEffev**	*How strongly do you agree to the effectiveness of the Network Security Systems of your organization?*
InvstIDS	Do you agree that your company should investment more money in Intrusion Detection Systems (IDS) in 2015-2016?

Dependent Variables	
ZeroDay	Zero-day attacks
DDoS	Denial-of-service (DoS)/distributed denial of service (DDos)
APTs	Advanced persistent threats (APTs), targeted attacks – RATs, etc.
SesnHijk	Session Hijacking attacks
FormatStn	Format string attacks
IP_Spoof	IP address spoofing attacks
IPS	Intrusion Protective Systems (IPS). Intrusion Detection Systems (IDS), Signatures/Abnormal event detection and prevention techniques
NetTech	Network Technologies (firewalls, routers, switches, etc.)
OS	Operating Systems attacks
IE_Zero	Internal Explorer Zero-Day attacks

Table 1: Independent and Dependent Variables in the Present Study
*NetEffev was dropped due to its high correlation with NetSec (r = 0.73) and InvstIDS (r = 0.73)

Please see Table 1 for a list of the variables, and Table 2 for descriptive statistics regarding the dependent variables. The data was analyzed using multivariate analysis of variance (MANOVA) followed by separate univariate tests using analysis of variance (ANOVA), using SAS 9.40. The level of significance was at .05.

Variable	N	Mean	Std Dev	Min	Max
ZeroDay	242	4.07	0.586	3.00	5.00
DDoS	242	4.17	0.644	3.00	5.00
APTs	242	4.07	0.601	3.00	5.00
SesnHijk	242	4.19	0.613	3.00	5.00
FormtStn	242	4.08	0.589	3.00	5.00
IP_Spoof	242	4.19	0.631	3.00	5.00
IPS	242	4.39	0.568	3.00	5.00
NetTech	242	3.95	0.578	2.00	5.00
OS	242	4.01	0.618	3.00	5.00
IE_Zero	242	3.98	0.656	2.00	5.00

Table 2: Descriptive Statistics of the Dependent Variables

Gender Effects

Before investigating the results of the variables in the survey, it was pertinent to examine any gender effects, given the disproportionate male representation. The sample (N = 242) was 165 male and 77 female, with males accounting for 68.2% of the sample size.

H_1: Males and females differ on their perspectives regarding cyber-security threats and challenges within their organizations, in the form of Zero-day, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks.

MANOVA results showed there was no significant multivariate effect for Gender, Wilks' lambda = 0.96, F (10, 231) = 0.85, p = 0.58. Hence, there were no gender effects at the 0.05 level of significance. Both males and females view the 10 cyber-security attacks similarly and do not differ in their perspectives regarding such threats.

Statistic	Value	F Value	Num DF	Den DF	Pr > F
Wilks' Lambda	0.962	0.85	10	231	0.5834
Pillai's Trace	0.035	0.85	10	231	0.5834
Hotelling-Lawley Trace	0.037	0.85	10	231	0.5834
Roy's Greatest Root	0.037	0.85	10	231	0.5834

MANOVA Test Criteria and Exact F Statistics for the Hypothesis of No Overall Gender Effect
H = Type III SSCP Matrix for Gender
E = Error SSCP Matrix
S=1 M=4 N=114.5
Table 3: Results of the Overall Multivariate Effect of Gender

Multivariate Results: Interaction and Main Effects

Given there were no gender effects, we proceeded to examine the MANOVA results for the overall effects of all 3

independent variables (IT rank of the respondents, respondents' perceived sense of network security within their organization, and respondents' views regarding their organization's level of investment in intrusion detection systems (IDS) on all 10 independent variables (Zero-day, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks).

First, interactions effects among the independent variables were examined using MANOVA. If there were no interaction effects among the independent variables, then we can proceed to investigate the main effects of each independent variable.

H_2: There are significant interaction effects among all pairs of and all three of the independent variables combined (respondents' IT rank, perceived sense of network security, and views regarding their organization's level of investment in IDS) regarding cyber-security threats within their organization in the form of Zero-day, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks.

There was statistically significant interaction effects among all pairs of and all 3 of the independent variables combined at the 05 level of significance with the following MANOVA results:

- IT_Rank*NetSec, Wilks' lambda = 0.00, F(18, 432) = infinity, $p < 0.0001$
- IT_Rank*InvstIDS, Wilks' lambda = 0.00, F(36, 811) = infinity, $p < 0.0001$
- NetSec*InvstIDS, Wilks' lambda = 0.00, F(27, 631) = infinity, $p < 0.0001$
- IT_Rank*NetSec*InvstIDS, Wilks' lambda = 0.00, F(2, 223) = infinity, $p < 0.0001$

Given there were interaction effects, the following hypotheses of the main effects cannot be examined:

H_3: There is a difference between Executive/Senior IT Administrators and lower-level IT professionals in their views regarding cyber-security threats within their organizations in the form of Zero-day, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks.

H_4: There is a difference in perceived sense of network security regarding cyber-security threats in an organization in the form of Zero-day, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks.

H_5: There is a difference in views regarding an organization's level of investment in IDS regarding cyber-security threats in the form of Zero-day, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks.

The results of these 3 hypotheses were actually significant, but these main effects cannot be interpreted given the interaction effects were significant.

Univariate ANOVA Results

The MANOVA results showed significant interaction effects among the independent variables, and hence the main effects of each independent variable could not be examined. However, separate univariate ANOVAs were conducted to further understand the effects of the three independent variables (IT rank, network security, investment level in IDS) on each of the 10 dependent variables separately (Zero-day attacks, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks).

H_6: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding Zero-day attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on Zero-day attacks at the 0.05 level, F(17, 224) = infinity, $p < 0.0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	82.66	4.86	Infty	<0.0001
Error	224	0.00	0.00		
Corrected Total	241	82.66			

Table 4: ANOVA Results for the Dependent Variable: Zero-Day Attacks

H_7: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding DDoS attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on DDos attacks at the 0.05 level, $F(17, 224) = 20.39$, $p < 0.0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	60.78	3.56	20.39	<.0001
Error	224	39.28	0.18		
Corrected Total	241	100.05			

Table 5: ANOVA Results for the Dependent Variable: DDoS Attacks

H_8: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding APT attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on APT attacks at the 0.05 level, $F(17, 224) = 64.0$, $p < 0.0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	72.10	4.24	64.00	<.0001
Error	224	14.84	0.07		
Corrected Total	241	86.94			

Table 6: ANOVA Results for the Dependent Variable: APTs

H_9: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding Session Hijacking attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on Session Hijacking attacks at the 0.05 level, $F(17, 224) = 28.49$, $p < 0.0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	61.97	3.65	28.49	<.0001
Error	224	28.66	0.13		
Corrected Total	241	90.63			

Table 7: ANOVA Results for the Dependent Variable: Session Hijacking Attacks

H_{10}: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding Format String attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on Format String attacks at the 0.05 level, $F(17, 224) = 1244.0$, $p < 0.0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	82.63	4.86	1244.36	<.0001
Error	224	0.88	0.004		
Corrected Total	241	83.51			

Table 8: ANOVA Results for the Dependent Variable: Format String Attacks

H_{11}: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding IP Address Spoofing attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on IP Address Spooking attacks at the 0.05 level, $F(17, 224) = 25.72$, $p < 0.0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	63.39	3.73	25.72	<.0001
Error	224	32.48	0.15		
Corrected Total	241	95.87			

Table 9: ANOVA Results for the Dependent Variable: IP Address Spoofing Attacks

H_{12}: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding IPS attacks.

There was a statistically non-significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on IPS attacks at the 0.05 level, $F(17, 224) = 1.56$, $p < 0.0762$. IPS encompasses intrusion protective systems (IPS), intrusion detection systems (IDS), and signatures and/or abnormal event detection and prevention methods.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	8.23	0.48	1.56	0.0762
Error	224	69.48	0.31		
Corrected Total	241	77.71			

Table 10: ANOVA Results for the Dependent Variable: IPS

H_{13}: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding Network Technologies attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on Network Technologies attacks at the 0.05 level, $F(17, 224) = 14.60$, $p < 0.0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	42.32	2.49	14.60	<.0001
Error	224	38.19	0.17		
Corrected Total	241	80.50			

Table 11: ANOVA Results for the Dependent Variable: Network Technologies Attacks

H_{14}: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding OS attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on OS attacks at the 0.05 level, $F(17, 224) = 19.30$, $p < 0.0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	54.67	3.22	19.30	<.0001
Error	224	37.32	0.17		
Corrected Total	241	91.98			

Table 12: ANOVA Results for the Dependent Variable: OS Attacks

H_{15}: Respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization differ regarding IE Zero-day attacks.

There was a statistically significant effect of respondents' IT rank, their perceived sense of network security, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization on IE Zero-day attacks at the .05 level, $F(17, 224) = 17.36$, $p < .0001$. There was no need to run ANOVA comparison contrasts for IT rank given the levels for IT rank are only binary: Executive/Senior IT Administrator vs. lower-level IT employee.

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	17	59.04	3.47	17.36	<.0001
Error	224	44.82	0.20		
Corrected Total	241	103.85			

Table 13: ANOVA Results for the Dependent Variable: IE Zero-Day Attacks

Summary of the Hypotheses

A total of 15 hypotheses were tested to better understand the impact of cyber-security threats within organizations as reported in a questionnaire by IT industry professionals and researchers. First, there were no gender effects between male and female technology professionals and researchers, so they do not differ in their perspectives regarding security threats within their organizations. Second, given there were interaction effects among the 3 independent variables (respondents' IT rank as Executive/Senior IT Administrator vs. lower-level IT staff, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS), it was not possible to examine the main effects of the 3 independent variables on the 10 dependent variables (Zero-day attacks, DDoS, APTs, Session Hijacking, Format String, IP Address Spoofing, IPS, Network Technologies, OS, and IE Zero-day attacks). Separate univariate ANOVAs were run to better understand the effects of the independent variables on each dependent variable separately. See Tables 14 and 15, showing a summary of the results at the 0.05 level of significance.

Independent Variables	Hypothesis	p-value	Significant?
Gender	1	p = 0.5834	No
Main Effects			
IT_Rank	3	p < 0.0001	Yes
NetSec	4	p < 0.0001	Yes
InvstID S	5	p < 0.0001	Yes
Interaction Effects			
IT_Rank*NetSec	2	p < 0.0001	Yes
IT_Rank*InvstIDS	2	p < 0.0001	Yes
NetSec*InvstIDS	2	p < 0.0001	Yes
IT_Rank*NetSec*InvstIDS	2	p < 0.0001	Yes

Table 14: Summary of the Hypotheses Based on MANOVA

Running univariate ANOVAs showed that the 3 independent variables did have a significant effect on each of the 10 dependent variables separately, except for IPS (H12). The IPS variable includes intrusion protective systems

(IPS), intrusion detection systems (IDS), and signatures/abnormal event detection and prevention techniques. Hence, respondents' IT rank, their perceived sense of network security within their organization, and their views regarding their organization's level of investment in IDS regarding cyber-security threats within their organization do not differ regarding IPS attacks. The nonsignificant result may be due to respondents' hesitation towards these tools, since some of them may interfere with legitimate business traffic on the organization's network.

Dependent Variables	Hypothesis	p-value	Significant?
Zero-day attacks	6	$p < .0001$	Yes
DDos	7	$p < .0001$	Yes
APTs	8	$p < .0001$	Yes
Session hijacking attacks	9	$p < .0001$	Yes
Format string attacks	10	$p < .0001$	Yes
IP Address Spoofing attacks	11	$p < .0001$	Yes
IPS – intrusion protective systems	12	$p = .0762$	No
Network technologies	13	$p < .0001$	Yes
Operating system attacks	14	$p < .0001$	Yes
IE Zero-day attacks	15	$p < .0001$	Yes

Table 15: Summary of the Hypotheses Based on Univariate ANOVAs

Conclusion

Our study revealed that knowledge is power since awareness of specific circumstances that give rise to vulnerabilities allows security practitioners to address the root causes of a given breach. Most of the survey participants feel that their systems are somewhat secured. However, vigorous secure development practices should be adhered to, 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-based malware deliverables. Majority of the 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 searches and eliminates new and unseen exploits such as the Zero-day, Shellshock, Frame-sniffing, Game-over, Zeus, Gepaw, Heap-spray, Money-Pack, and 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 help 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 are active in reducing the chances of a security breach, should think beyond the direct cost savings of lost data, fines and lawsuits, and instead should focus on an integrated architecture that enables a big picture cyber vigilance.

Lesson Learned

Security teams have to adopt breakthroughs as part of a continuous monitoring strategy. They should understand their network. Team members should be trained to remain alert for any suspicious activity on the network in real-time. These experts should not only monitor inbound communications but should be watchful of all the security updates as a general best practice.

DNS query logging should always be enabled so that the system will be able to detect hostname lookup for known malicious C2 domains. In order to disclose and communicate data breaches in a timely manner, network systems should be configured to detect random string entropy such as unknown certificates, file names etc.

Security administrators should never store clear-text sensitive data in the server in source code mode. They should always rotate their API tokens and service credentials intermittently. Software developer should be properly trained about securing coding practices.

Enterprise system's should not just rely on perimeter security alone but should implement a threat intelligence platform which will be able to recognize potential malware activities from multiple threat intelligence sources and mitigate as needed. Security administrators should encrypt data-at rest and ensure that the encryption keys, network access control and identity management mechanism are activated to ensure data is secure.

References

1. Vaughan-Nichols SJ (2015) Securing the Internet: Let's encrypt to release first security certificates September 7.

2. Report on 2015 inspection of Pricewaterhouse Coopers LLP - PCAOB (2016).

3. CyberSource (2015) 15th Annual online fraud report: Online payment fraud trends, merchant practices and benchmarks. San Francisco, CA: Visa-CyberSource.

4. Perlroth N (2015) IRS breach demonstrates the need to guard personal data, The New York Times B2.

5. Zetter K (2015) Attackers stole certificate from Foxconn to hack Kaspersky with Duqu 2.0. Security.

6. Krebs B (2015) Krebson Security: In depth security news and investigation.

7. Villeneuve N (2015) TeslsaCrypt: Following the money trail and learning the human costs of ransomware.

8. Baldor LC (2013) US ready to strike back against China cyberattacks, Yahoo News, 2013.

9. Ashford W (2013) "Why has DLP never taken off?" Computer Weekly.

10. Smith A (2014) Newly discovered sophisticated malware has been spying on omputers for six years. Newsweek.

11. Lawrence D (2014) Spy vs spy: The US government designed and funds the best defense against its own surveillance. Bloomberg Businessweek 42-47.

12. Gartner Rantapelkonen J, Salminen Mirva (2013) The fog of cyber defense. National Defense University/Department of Leadership and Military Pedagogy.

13. Gartner (2013) Gartner says the Internet of things installed base will grow to 26 billion units by 2020. Newsroom.

14. NCC Group (2014) Security of things: An implementer's guide to cyber-security for Internet of things devices and beyond.

15. Intel (2014) Developing solutions for Internet of things.

16. Secunia vulnerability review 2014 (2014).

17. Verizon 2014 data breach investigations report (2014).

18. World economic forum, partnering for cyber resilience (PCR) (2014).

19. Berthiaume D (2015) Amazon shuts digital wallet, Chain Store Age.

20. Carter M (2015) Mobile wallets are not convenient enough for consumers. Payments Source.

21. Kaspersky Lab Report (2014) The Rein platform nation-state own age of GSM networks (Version 1.0.).

22. Gartner (2014) Gartner says the Internet of things will transform the data center. Newsroom.