International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 4, Issue 3, 2017, PP 10-15
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: http://dx.doi.org/10.20431/2349-4859.0403002
www.arcjournals.org

Cyber Nexus: Challenge to Society

Dr. Vijay Tiwari

Centre for Advance Studies. India

***Corresponding Author: Dr. Vijay Tiwari,** Centre for Advance Studies. India*

Abstract: *Cyberspace is a potent platform for information sharing. However there are security risks for its users. There is a vast variety of cyber vulnerabilities. Compounding the problem further is the fact about delay in detection and reporting of vulnerabilities. This presents an ideal opportunity for "Nexus" among various stake holders whether state sponsored or individuals. This paper analyses types of vulnerabilities, factors that encourage this Cyber Nexus, potency of the threat and countermeasure to ensure safeguard of security interests against such Nexus.*

Keywords: *Cyber risks, unpatched vulnerabilities, cyber space, proxy cyber operations*

1. Introduction

Internet has its origins from USA since 1990. It was regarded as one of the most important tools to share information. It became popular worldwide and people across the world rapidly connected to it. Over a period of time it offered as a platform for secure banking transactions, credit card usage, sharing of information and research through library connectivity and much more. No one may have thought that this virtual space which we now know as cyber space will become a giant monster to hound common man facilities across the world. Cyberspace, which is a platform for information sharing today, presents a wide range of security risks for host of its users whether individuals, semi government institutes or government organizations [1].These threats become more complex when there is a "Nexus" among the nefarious organisations whether state sponsored or non-state actors. In this paper we analyze current threats and their implications to society because of cooperation. We will also try to look deeper in to the aspect whether it will be possible to identify the extant of threat as defining full scope of the cyber threat may not be possible.

2. Enormity of Cyber Risk

Let me commence my analysis by the end state of cyber risk and its impact. Cyber risks may manifest themselves in to cyber-attacks which may include one or more of the following activities:-

(a) Web site defacement be it private or Government.

(b) Interfering with the functioning of service web sites causing disruption. This is popularly known as denial of service attacks.

(c) Injection of malicious worms and viruses that may result in loss/ corruption of crucial data in the machines where they are planted. These worms or viruses may travel over the network and may affect the whole world.

(d) Stealing vital company secrets

(e) Stealing politically sensitive information.

(f) Cyber-attacks may degrade vital networking data that may cripple the network itself.

Large number of Vulnerabilities have been reported and many of them may still be undetected. They are being detected on a daily basis. At times much vulnerability are reported on a single day. These vulnerabilities need to be patched before they could be exploited. It is difficult to assess the damage caused due to their exploitation till safety patches were uploaded.

2.1. Vulnerability

Risks are enormous as vulnerabilities are large and many of them still unknown. Country Report (UK) published

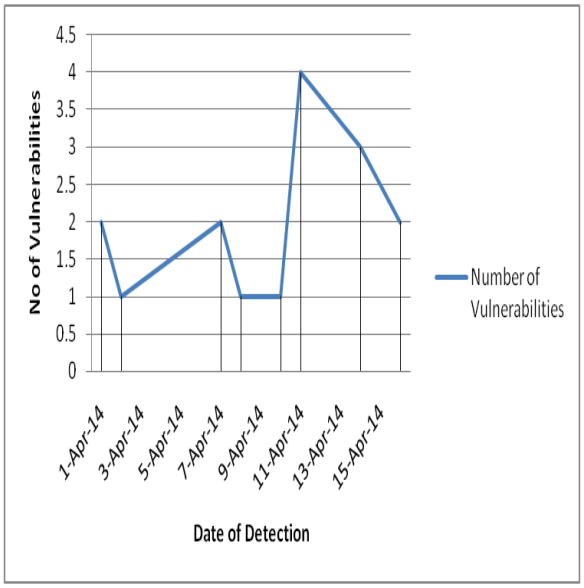

Fig1. *Enormity in Reporting of Vulnerability [1]*

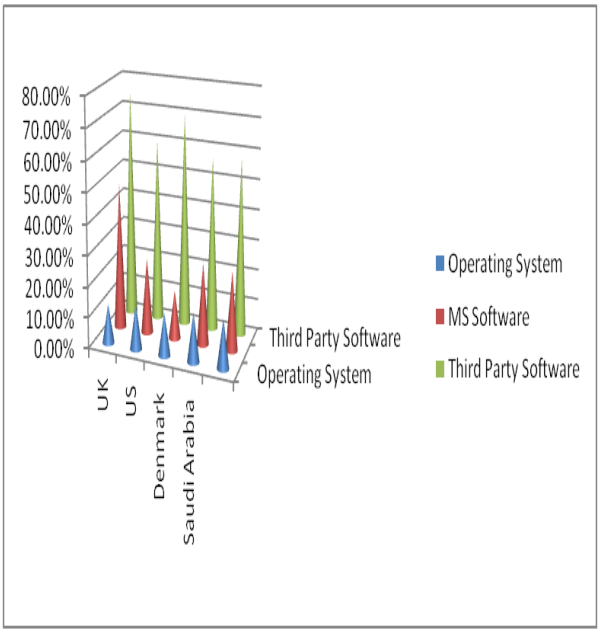

Figure2. *Unpatched Vulnerabilities reported in Secunia Country Report [2]*

by Secunia in fourth quarter of 2013 [2] indicates some of the commonly used software that are vulnerable:

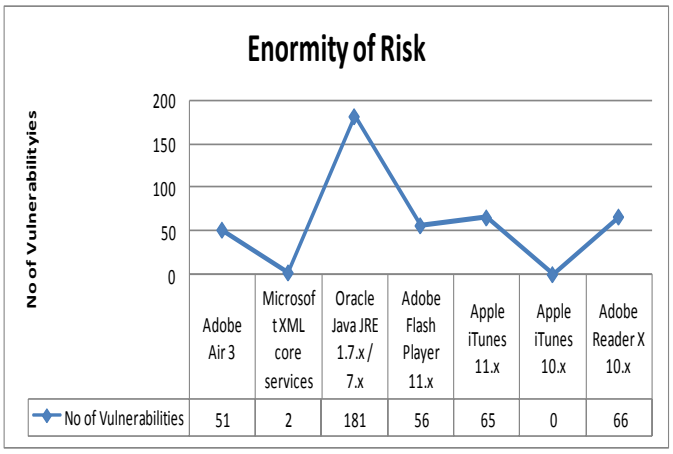

Fig3. *Enormity of Risk among common use software/ package*

2.2. Obsolescent Packages

Software is becoming outdated much faster as user requirements grow. Competition driven market is demanding faster growth and it may sometimes be at a cost of security. Third parties also add lot of vulnerability to any user. End of life programs as on fourth quarter 2013, are listed below [2]:

Table1. *Outdated Vulnerable Software*

Google Chrome 30.x	Microsoft Removal Tool: Blaster/Nachi
Oracle Java JRE 1.6.x / 6.x	Adobe AIR 2.x 15%
Mozilla Firefox 24.x	Adobe Shockwave Player 11.x
Mozilla Firefox 25.x	Skype for Windows 5.x
Google Chrome 29.x	OpenOffice.org 3.x

3. FACTORS THAT ENCOURAGE CYBER NEXUS

3.1. Network Boundaries defy Geographical Boundaries

Cyber-attack may not remain limited to military or any specific private/ governmental organization. The networking boundaries get blurred as there may not be much distinction between private and governmental setup. Cyber space cannot be controlled by any specific organization and hence presents equal opportunities for state and non-state actors.

3.2. Long and Sustained Procedure

Cyber exploitation is a rigorous process which needs to be conducted in a sustained manner. Patience is a virtue in cyberspace. Nexus against a common adversary may therefore lead to tangent results. Geopolitical situations in the world may encourage use of cyber space as a potent weapon of future battle field.

3.3. Technological Advancement

Cyber war gives an edge to technologically advanced country. It also has a lot for the weaker society. Those developed have adequate knowledge to protect themselves however the under-developed may not have much dependency over the networks and hence may not present large vulnerability. The worst affected, in my opinion are the developing countries which are in the process of transforming in to network dependency era. Due to nascent networking and lack of adequate security measures, they present wide vulnerabilities. Technological parity presents an opportunity for Cyber Nexus at organisation or country level.

3.4. Proxy or Shadow Cyber Operations

With more potent international laws and monitoring organisations, it has become increasingly difficult to progress overt cyber operations against the Target Company or country. However, a proxy cyber attack waged from other country can mask the intentions and real beneficiary. Such shadow operations demand well coordinated cyber nexus among various organisations.

3.5. Plurality of Networking Products

Network is an integrated amalgamation of multiple networking devices and processes. Every part must be well understood and its vulnerability known prior to any meaningful exploitation. Various zero day vulnerabilities have been reported in networking tools and operating systems. Cyber nexus, therefore may be a stepping stone to expeditious Cyber operations.

3.6. Broad Based Results and Findings

Cyber operation findings may be of interest to many. At time some organisations/ countries are interested in the outcomes, which may not be intended beneficiaries. Alliance may therefore be a natural strategy which may turn in to nexus depending upon the findings of cyber operations and response there on.

4. UNIQUENESS OF CYBER THREAT

The uniqueness of cyber threat can be gauged from the fact that there are very little ways to distinguish between state and non-state actors. Further complicating matter is the difficulty in

distinguishing between attacks by foreign civilians or groups who are opposed to any nation from within. In 2001, Central Intelligence Agency (CIA) and White House Web sites reported a series of Web site defacement and "denial of service" attacks. It is widely believed that attacks were of Chinese origin [3].It was reported that a group propagated as Internet Black Tigers intruded in to the Sri Lankan Government embassies networks and conducted successful denial of service attack. It is also reported that the Irish Republican Army may have actively considered use of cyber-attack operations against the British [4].

5. WHY CYBER PRESENTS A POTENT THREAT

Almost every person today is linked to computers and networks either directly or indirectly. Through cyber connectivity every connected person can be contacted and manipulated if vulnerabilities exist. Cyber space poses a potent threat as there are vulnerabilities and also there are large numbers of bad actors who are willing to exploit the situation. There are extremely large numbers of vulnerabilities which are categorized in many forms.

5.1. Operating System Vulnerabilities

Whatever be the operating system, vulnerabilities do exist. There are patches provided for the operating system from time to time however there is definite time lag before vulnerability is plugged. Remote exploitation of a **use-after-free** vulnerability in Web Kit, could allow an attacker to execute arbitrary code with the privileges of the current user.

5.2. Utility Software Vulnerabilities

There are large number of popular utilities that have inherent vulnerabilities. These utilities cannot be avoided and hence vulnerabilities are present in the system. iDefense has confirmed the existence of this vulnerability in the following applications that use Webkit [3]:-

- Safari 5.1.2 on Windows XP and OS X Lion
- Safari 5.1.5 on Windows XP and OS X Lion
- Mobile Safari on an iPad 1, iOS 5.0.1
- Chrome 16.0.912.75m on Windows 7

5.3. Multi-Dimensional Issue

The sheer variety of cyber-attacks exposes vulnerabilities of our information networks. This vulnerability is a national security problem. In addition, it may also turn out to be a law enforcement challenge.

5.4. Numerous and Extensive Variety of Targets

Every person and every network can be a target. Every machine could respond to a specific mode of attack. Use of Stuxnet worm against the Iranian nuclear facilities gives a glimpse of cyberspace Targeted attacks.

5.5. Extensive Payloads/Tools for the Cyber Attack

Every day new tools and payloads are generated to exploit the weakness of clients. Viruses, Worms and Trojans are injected regularly through variety of ways to sabotage data integrity and network availability.

5.6. Unclear Responsibility to Address Cyber Threat

There is a large variety of cyber-attack, large number of motives that any attacker may have and numerous means of carrying out the attack. This demands multiple agencies to coordinate their resources and acts together. Vulnerability is, therefore, everybody's problem. The responsibility for defending broadly destructive cyber-attacks remains with multiple agencies.

6. VULNERABILITY DISCLOSURE

There are various ways to discover and report a flaw. Some of the policies are mentioned below:

6.1. Non- Disclosure

Once security vulnerability is discovered in a piece of software, it is not disclosed. The black hat hacker community is reported to Non-disclosure policy [5]. As inherent in the name, it is very difficult to identify the number of vulnerabilities identified but not disclosed. Havana and Röning [6]

have suggested int heir work that up to 17.3% of vulnerability findings are not disclosed. Intent of non-disclosure may mostly be malicious.

6.2. Full Disclosure

Any vulnerability once discovered needs to be fully disclosed to the environment. It must specify; how the vulnerability was found and which all software packages are affected. Full disclosure may also include as how to exploit the weakness and methods of protection. Full disclosure is very helpful for the software developers to introduce protection patches against reported flaws.

6.3. Responsible Disclosure

Responsible disclosure may seem to be a midway between the Non-disclosure and Full disclosure. In this method, vulnerability is reported to the software vendor. It is expected that remedial measures are reported to users within reasonable time. If remedial measures are not reported, full disclosure is resorted to [7].

7. CYBER OPERATIONS AND HIERARCHY SECURITY THREATS

Cyber operation may commence by an innocuous intrusion within a network with a purpose of simply gaining information. Intruder may remain in the system till it is felt that an active role is to be taken and then the process of stealing, altering and sabotaging information may be taken on. Denial of use of network for its integral users is one of the most common activity of any hacker. At times, intruders may have to lie dormant for long time till an opportune moment arrives. Network thus can be crippled by use of viruses and worms specially designed for a purpose.

How to distinguish a cyber-attack from security threat? Very thin line exists between the two actions and it is extremely difficult to quantify or limit information operations. Since the extent of Op is not clear, the response of the target may have wide variation. The first and most important distinction can be guessed from past behaviour of source group in cyberspace. However there cannot be a set behavior pattern for a group. It is likely to be dynamic and impact requirement based. Cyber actors are difficult to categorize and do not follow set definitions. Hence a measured response from target is not feasible and likely to be disproportionate of the threat.

There is no laid down ‘simple hierarchy of threats’. There is always a challenge to ascertain warfare in the cyberspace. There cannot be a set criterion. It is flexible, volatile and case specific. In a similar way, even the response to an intrusion also has to be calibrated to cyber event. Challenge always lies in finding out the exact nature of damage that has been caused and hence it may be speculation which will form the basis of response. What is even more intriguing that results of the response may also take some time to show.

8. COUNTERMEASURES TO CYBER NEXUS

8.1. Own Network Safety

Prevention is the most important countermeasure. Every effort should be made to obviate vulnerability to Cyber attack in the first place. Vulnerability once known must be patched. Patches are being developed at frequent pace and there is likely to be a time lag between knowing the vulnerability and its patching it. Hackers use this window of vulnerability. There are definite instances of exploiting the well known vulnerability as it was not implemented [8].

8.2. State Sponsored Cyber Cooperation

All the government departments need to inter-work for a common cause of cyber security. Government agencies should impress upon both manufacturers and users of computer hardware and software to ensure implementation of security policies more seriously. Manufacturers need to minimise zero day vulnerabilities and make more secure products [9]. At the same time network owners and operators to be more sensitive towards their own cyber security. Government has to ally and collaborate with other friendly governments to ensure collective cyber security.

8.3. Guided Approach Towards Capability Development

As we develop the systems and networking equipment, it is mandatory for them to adaptable to cyber warfare. US developed guidelines known as Defence Lines of Development, popularly known by the acronym TEPID OIL: Training, Equipment, Personnel, Information, Doctrine and concepts, Organization, Infrastructure, and Logistics [10].

8.4. Need for Cyber Doctrine

Cyber space has to be used and sometimes exploited according to some rules. Cyber space may be opaque at times to those who may be watching from outside. However its reach and impact will be far deeper. At national level there must be written rules of engagement which may be in public domain for all concerned to appreciate if nothing else the transparency. It is therefore incumbent on the part of every organization to have stated cyber policy giving out detailed measures to safeguard own networks, identify threats and ensure minimum damage to and early resuscitation of own networks. Countries have developed cyber warfare doctrine and programs keeping in view their technological advancements and capabilities.

8.5. Coordinated Cyber Threat Intelligence Information

Organisations will have to build a cyber threat intelligence capability. This would necessarily mean sharing of information with trusted partners and peers. Information sharing becomes difficult in absence of structured way of representation. Structured Threat Information eXpression (STIX™) is a useful consultative effort for representing structured threat. It is a language that is under development by group of interested parties to support cyber threat management processes in an automated manner.[11] This provides common access mechanism to classify, define and report the cyber threat pattern indicators and manages cyber threat response actions. This language connects cyber observable and indicators of an incident with the procedure, tactics and techniques of threat actors.

9. CONCLUSION

However over a long term manner it would be worth the effort as there are no alternatives. Hence cooperation or the Nexus is the surest way to success. Getting credible deterrence is also very difficult as it is evolving every day and opponent may be a lone hacker to any of the well organized groups acting with state support.

REFERENCES

[1] Paul Cornish, Rex Hughes and David Livingstone, "Cyberspace and the National Security of the United Kingdom: Threats and Responses" available at http://www.chathamhouse. org.uk/research/ security/ papers/view/-/id/726/.

[2] Secunia PSI Country Report - Q4 2013 avilable at http://secunia.com/resources/countryreports/uk/.

[3] iDEFENSE, Inc., white paper, "Inside the China Eagle Hacker Union," April 29, 2002, available at http://www.idefense.com/papers.html.

[4] "Canadian Security Intelligence Service Counter-Terrorism: Backgrounder Series, no. 8" (Canadian Security Intelligence Service, August 9, 2002), available at http://www.csis-scrs.gc.ca/eng/ backgrnd/ back8_e.html.

[5] S. Shepherd, "Vulnerability Disclosure: How do we define Responsible Disclosure?" SANS Institute, http://www.giac.org/practical/GSEC/Stephen_Shepherd_GSEC.pdf, Feb 2003.

[6] T. Havana and J. Röning, "Communication in the Software Vulnerability Reporting Process", MAthesis, University of Jyvaskyla,http://www.ee.oulu.fi/research/ouspg/protos/sota/FIRST2003-communication /paper.pdf, June 2003.

[7] Andrew Cencini, Kevin Yu, Tony Chan, "Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure" , {cencini, tigeru, tonychan} @ u.washington.edu, 07 Dec 2005.

[8] A recent example of this trend involved the SQL Slammer worm. See note 7, above.

[9] Department of Defense Strategy for Operating in Cyberspace, July 2011.

[10] Dorothy E. Denning, "Is Cyber Terror Next?" (New York, NY: Social Science Research Council, November 2001), available at http://www.ssrc.org/sept11/essays/denning.htm.

[11] Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™) by S ean Barnum.

Citation: *Dr Vijay Tiwari (2017). Cyber Nexus: Challenge to Society, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 4(3), pp.10-15, DOI: http://dx.doi.org/10.20431/ 2349-4859.0403002*