# A Case Study on the Spread and Victims of Smart Worms

Mr. Ujwal Babu K*

*Aurora's Technological Research Institute, Hyderabad*

**Abstract**— Security threats caused by worms are increased dramatically. Worms are major security threats to internet. Worms refers to a kind of computer viruses which are actively and widely spread on the internet to infect the computers. Worms spread in a very short span of time and does not give time for any human countermeasures to happen. These cause network traffic which in turn results in the equipment malfunctioning, network crowding etc. Active worms are spread autonomously without the necessary of human interaction. They scan the system, probe them transfer the copy and thus infect the machine. These are detected through anti-virus. Smart worms cause most important security threats to the Internet. These worms develop during their propagation and thus create great challenges to defend against them. In this paper, we look into "Spread and victims of Smart Worms". The Smart Worms are different from traditional worms because of its nature to intelligently manipulate its scan traffic volume over time.

**Index Terms**—Worm, Camouflage worm, Smart Worm.

## 1. INTRODUCTION:

Security in computing is the running issue in current situation. Threats are increased rapidly to disturb the security. Worms are one type of threat to security. Worms are a malicious program code which are, self-propagating and does not require any human interaction by which it infects the hosts. The term "Worm" was coined by John Burner in his novel "The Shockwave Rider". Worms are capable of shackling the working of internet. In order to build better defense systems and enable a good application we study in detail about worms. These worms have known to infect millions of computers and cause heavy damage. In 1988 first worm was discovered which was Morris Worm. Since then it was continued and many worms were find till now like Code Red in 2001, Sapphire in 2003, Zotob in 2005 and so on ....

## 2. RELATED WORK:

2.1 Active Worms: Active worms are those programs which self-propagate across the internet by exploiting security in widely used services. Active worms are used to infect a large number of computers networked together to form botnets. These botnets cause heavy loss of data, Distributed Denial Of Service attack which interrupts the system utilities, access to sensitive information, spread disinformation etc..

## 2.2 Mechanism for Worm Spreading:

Worm propagation can be explained in a clear way as follows. The below is the mechanism of worm propagation. This can be broadly classified into 5 step process illustrated as follows:

2.2.1) Initial Infection: This stage is where it begins with an assumption that system is already infected by the worm and worm is active.

2.2.2) Target Acquisition: For propagation the worm finds additional systems to infect .Worms mainly target systems which are using email addresses, IP addresses etc..

2.2.3) Delivery of Hostile Code: After the system is targeted, it transfers the worm to targeted system for infection. The delivery of code takes place through Email, Web Clients etc.

2.2.4) Execution of Hostile Code: The hostile code which resides in a system is not sufficient for the propagation of worm, the code must be executed and it can be done in many ways through:

- Programming Attacks like Buffer Overflow.
- Clients using emails.
- Automatic execution by target system.

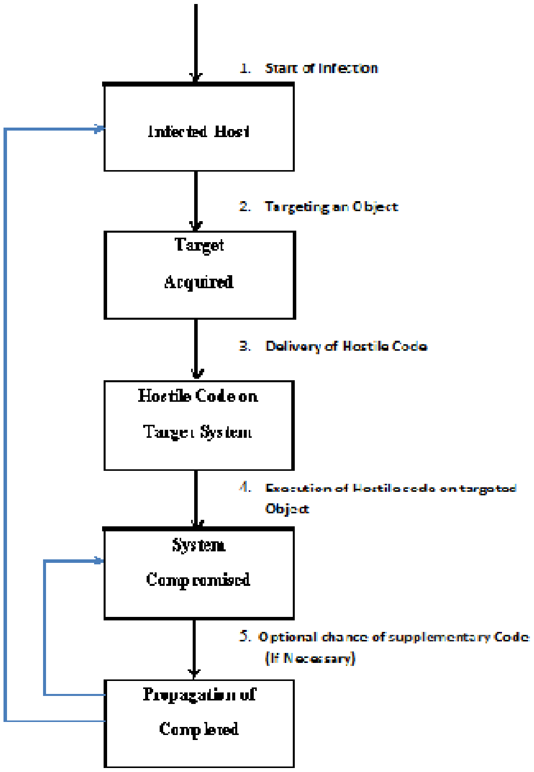
2.2.5) Optional Transfer Of Additional Code : Sometimes the worms does not transfer complete code in the above step if that happens the remaining code will be transferred after the system has been comprised and this can be done through the Network File Systems.

The worm does not need any manual interaction so it just needs to compromise a running program. These running programs are hosted in a server so the worms attack the host machines. When the worms attack the host machines they infect the host machine by modifying the data, terminating the current programs and starting the other programs, installing Trojans, etc.. These worms are faster in action and the defense mechanism should be as faster as them in order to counter it. There has been a substantial damage caused by worms in years and hence efforts are made in developing detection and defense mechanisms against worms.

## 2.3 Detection of worms:

The spread of these worms affect the security in Internet. So, these should be detected early so that threat to the system can be reduced. Various detection techniques are introduced to reduce the loss caused by worms. Many researchers proposed the detection of worm intrusion by tracing connection paths through departments of an organization. So based on this concept Destination Source Correlation (DSC) was developed. This is similar to Moore's distributed "network telescopes".

The detection algorithm described here is a combination of both infection nature of worm and anomaly scan detection mechanism. This approach to some extent effectively detects the fast spreading of worms.


1. Start of Infection
Infected Host
2. Targeting an Object
Target Acquired
3. Delivery of Hostile Code
Hostile Code on Target System
4. Execution of Hostile code on targeted Object
System Compromised
5. Optional chance of supplementary Code (If Necessary)
Propagation of Completed

### 2.4 Destination Source Correlation:

This worm victim detection algorithm is designed by considering the worm infection pattern. Infection patterns of worm are many but in general they follow a common pattern. This algorithm has 2 phases: Finding Infection Pattern and Checking Scan Rate for hosts in first phase.

The general scenario is a sliding window of local network traffic is kept. Two basic items are tracked:

- For each port in traffic we record address of host and scan the source.
- If source scan originates from host that already received scan a worm behavior like infection pattern is observed.

By combining the incoming, outgoing traffic and anomaly scan detection DSC focuses on worm behavior instead not only focusing on symptoms of worms. We consider high rate of outgoing scanning that accompanies a worm which distinguishes authorized from infectious traffic. To identify unusual patterns anomaly detection heuristics are used. These heuristics are not applied to networks with various other infections like behaviors. In such places Chebyshev's inequality is used whether simple heuristic detection can be used or not.

In probability theory, **Chebyshev's inequality** guarantees that in any probability distribution, "nearly all" values are close to the mean — the precise statement being that no more than $1/k^2$ of the distribution's values can be more than $k$ standard deviations away from the mean (or equivalently, at least 1 - $1/k^2$ of the distribution's values are within k standard deviations of the mean). The inequality has great utility because it can be applied to completely arbitrary distributions (unknown except for mean and variance), for example it can be used to prove the weak law of large numbers.

The term *Chebyshev's inequality* may also refer to the **Markov's inequality**, especially in the context of analysis.

Chebyshev's inequality is usually stated for random variables, but can be generalized to a statement about measure spaces.

### 3. LIMITATIONS:

Apart from all these assumptions there are even limitations for DSC in general. Several applications produce infection like traffic and may not have a stable scan rate. The other drawback is DSC cannot be used for multi vector worms. DSC is designed for detection of fast spreading worms and it does not match the perfect algorithm case.

## 4. CONCLUSION:

In this paper we have studied approach for worm spreading and detection mechanisms. We can conclude in this paper that detection algorithms can be used for early detection of worms and for slowing the propagation.

## 5. REFERENCES:

[1] D. Moore, C. Shannon, and J. Brown, “Code-red: a case study on the spread and victims of an internet worm,” in *Proceedings of the 2-th Internet Measurement Workshop (IMW)*, Marseille, France, November 2002.

[2] D. Moore, V. Paxson, and S. Savage, “Inside the slammer worm,” in *IEEE Magazine of Security and Privacy*, July 2003.

[3] CERT, *CERT/CC advisories*, http://www.cert.org/advisories/.

[4] P. R. Roberts, *Zotob Arrest Breaks Credit Card Fraud Ring*, http://www.eweek.com/article2/0,1895,1854162,00.asp.

[5]*W32/MyDoom.B Virus*, http://www.uscert.gov/cas/techalerts/TA028A.html.

[6]*W32.Sircam.Worm@mm*, http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html.

[7]*Worm.ExploreZip*, http://www.symantec.com/avcenter/venc/data/worm.explore.zip.html.

[8] R. Naraine, *Botnet Hunters Search for Command and Control Servers*, http://www.eweek.com/article2/0,1759,1829347,00.asp.

[9] T. Sanders, *Botnet operation controlled 1.5m PCs Largest zombie army ever created*, http://www.vnunet.com/vnunet/news/2144375/
botnet-operation-ruled-million, 2005.

[10] R. Vogt, J. Aycock, and M. Jacobson, “Quorum sensing and selfstopping worms,” in *Proceedings of 5th ACM Workshop on Recurring Malcode (WORM)*, Alexandria VA, October 2007.

[11] S. Staniford, V. Paxson, and N.Weaver, “How to own the internet in your spare time,” in *Proceedings of the 11-th USENIX Security Symposium (SECURITY)*, San Francisco, CA, August 2002.

[12] Z. S. Chen, L.X. Gao, and K. Kwiat, “Modeling the spread of active worms,” in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, San Francisco, CA, March 2003.

[13] M. Garetto, W. B. Gong, and D. Towsley, “Modeling malware spreadin dynamics,” in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, San Francisco, CA, March 2003.

[14] C. C. Zou, W. Gong, and D. Towsley, “Code-red worm propagation modeling and analysis,” in *Proceedings of the 9-th ACM Conference on Computer and Communication Security (CCS)*, Washington DC, November 2002.

[15] Zdnet, *Smart worm lies low to evade detection*,http://news.zdnet.co.uk/internet/security/0,39020375,39160285,00.htm.

[16] J. Ma, G. M. Voelker, and S. Savage, “Self-stopping worms,” in *Proceedings of the ACM Workshop on Rapid Malcode (WORM)*, Washington D.C, November 2005.

[17] Min Gyyng Kang, Juan Caballero, and Dawn Song, “Distributed evasive scan techniques and countermeasuress,” in *Proceedings of International*

*Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, Lucerne, Switzerland, July 2007.

[18] Charles Wright, Scott Coull, and Fabian Monrose, "Traffic morphing: An efficient defense against statistical traffic analysis," in *Proceedings of the 15th IEEE Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Febrary 2008.

[19] C. Zou, W. B. Gong, D. Towsley, and L. X. Gao, "Monitoring and early detection for internet worms," in *Proceedings of the 10-th ACM Conference on Computer and Communication Security (CCS)*, Washington DC, October 2003.

[20] S. Venkataraman, D. Song, P. Gibbons, and A. Blum, "New streaming algorithms for superspreader detection," in *Proceedings of the 12-th IEEE Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Febrary 2005.

[21] J. Wu, S. Vangala, and L. X. Gao, "An effective architecture and algorithm for detecting worms with various scan techniques," in *Proceedings of the 11-th IEEE Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Febrary 2004.

[22] Dshield.org, *Distributed Intrusion Detection System*, http://www.dshield.org/, 2005.

[23] SANS, *Internet Storm Center*, http://isc.sans.org/.

[24] C. C. Zou, W. Gong, and D. Towsley, "Worm propagation modeling and analysis under dynamic quarantine defense," in *Proceedings of the 1-th ACM CCS Workshop on Rapid Malcode (WORM)*, Washington DC, October 2003.

[25] C. C. Zou, D. Towsley, and W. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worm," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 2, pp.105–118, 2007.

[26] C. Zou, Don Towsley, and Weibo Gong, "Email worm modeling and defense," in *Proceedings of the 13-th International Conference on Computer Communications and Networks (ICCCN)*, Chicago, IL, October 2004.

[27] W. Yu, S. Chellappan C. Boyer, and D. Xuan, "Peer-to-peer system based active worm attacks: Modeling and analysis," in *Proceedings of IEEE International Conference on Communication (ICC)*, Seoul, Korea, May 2005.

[28] *Dynamic Graphs of the Nimda Worm*, http://www.caida.org/dynamic/analysis/security/nimda.

[29] S. Staniford, D. Moore, V. Paxson, and N. Weaver, "The top speed of flash worms," in *Proceedings of the 2-th ACM CCS Workshop on Rapid Malcode (WORM)*, Fairfax, VA, October 2004.

[30] Yubin Li, Zesheng Chen, and Chao Chen, "Understanding divide conquer-scanning worms," in *Proceedings of International Performance Computing and Communications Conference (IPCCC)*, Austin, TX, December 2008.

[31] D. Ha and H. Ngo, "On the trade-off between speed and resiliency of flash worms and similar malcodes," in *Proceedings of 5th ACM Workshop on Recurring Malcode (WORM)*, Alexandria VA, October 2007.

[32] Y. Yang, S. Zhu, and G. Cao, "Improving sensor network immunity under worm attacks: A software diversity approach," in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Hong Kong, May 2008.

[33] L. Martignoni D. Bruschi and M. Monga, "Detecting self-mutating malware using control flow graph matching," in *Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Berlin, Germany, 2006 July.

[34] R. Perdisci, O. Kolesnikov, P. Fogla, M. Sharif, and W. Lee, "Polymorphic blending attacks," in *Proceedings of the 15-th USENIX Security Symposium (SECURITY)*, Vancouver, B.C., August 2006.

[35] Linux.com, *Understanding Stealth Scans: Forewarned is Forearmed*, http://security.itworld.com/4363/LWD010321vcontrol3/page1.html.

[36] Solar Designer, *Designing and Attacking Port Scan Detection Tools* http://www.phrack.org/phrack/53/P53-13.

[37] J. Z. Kolter and M. A. Maloof, "Learning to detect malicious executables in the wild," in *Proceedings of the 10th ACM International Conference on Knowledge Discovery and Data Mining (SIGKDD)*, Seattle, WA, August 2004.

[38] X. Wang, W. Yu, A. Champion, X. Fu, and D. Xuan, "Detecting worms via mining dynamic program execution," in *Proceedings of IEEE International Conference on Security and Privacy in Communication Networks (SECURECOMM)*, Nice, France, September 2007.

[39] W. Yu, X. Wang, D. Xuan, and D. Lee, "Effective detection of active worms with varying scan rate," in *Proceedings of IEEE International Conference on Security and Privacy in Communication Networks (SECURECOMM)*, Baltimore, MD, August 2006.

[40] A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distribution," in *Proceedings of ACM SIGCOMM*, Philadelphia, PA, August 2005.

[41] V. Yegneswaran, P. Barford, and D. Plonka, "On the design and utility of internet sinks for network abuse monitoring," in *Proceeding of Symposium on Recent Advances in Intrusion Detection (RAID)*, Pittsburgh, PA, September 2003.

[42] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The internet motion sensor: A distributed blackhole monitoring system," in *Proceedings of the 12-th IEEE Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, February 2005.

[43] D. Moore, "Network telescopes: Observing small or distant security events," in *Invited Presentation at the 11th USENIX Security Symposium (SECURITY)*, San Francisco, CA, August 2002.

[44] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan, "Fast portscan detection using sequential hypothesis testing," in *Proceedings of the 25-th IEEE Symposium on Security and Privacy (S&P)*, Oakland, CA, May 2004.

[45] H. Kim and B. Karp, "Autograph: Toward automated, distributed worm signature detection," in *Proceedings of the 13-th USENIX Security Symposium (SECURITY)*, San Diego, CA, August 2004.

[46] M. Cai, K. Hwang, J. Pan, and C. Papadopoulos, "Wormshield: Fast worm signature generation with distributed fingerprint aggregation," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 2, pp. 88–104, 2007.

[47] R. Dantu, J. W. Cangussu, and S. Patwardhan, "Fast worm containment using feedback control," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 2, pp. 119–136, 2007.

[48] K. Ogata, *MOdern Control Engineering*, Pearson Prentice Hall, 2002.

[49] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study," in *Proceedings of USENIX Workshop on Hot Topics in Understanding Botnets (HotBots)*, Cambridge, MA, April 2007.

[50] P. Wang, S. SParka, and C. Zou, "An advanced hybrid peer-to-peer botnet," in *Proceedings of USENIX Workshop on Hot*

*Topics in Understanding Botnets (HotBots)*, Cambridge, MA, April 2007.

[51] D. J. Daley and J. Gani, *Epidemic Modeling: an Introduction*, Cambridge University Press, 1999.

[52] D. Bruschi, L. Martignoni, and M. Monga, "Detecting self-mutating malware using control flow graph matching," in *Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Berlin, Germany, July 2006.

[53]MetaPHOR, http://securityresponse.symantec.com/avcenter/venc/data/w32.simile.html.

[54] P. Ferrie and P. Sz¨or. Zmist, *Zmist opportunities*, Virus Bullettin, http://www.virusbtn.com.

[55] John Bethencourt, Dawn Song, and Brent Waters, "Analysis-resistant malware," in *Proceedings of the 15th IEEE Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Febrary 2008.

[56] Monirul Sharif, Jonathon Giffin, Wenke Lee, and Andrea Lanzi, "Impeding malware analysis using conditional code obfuscation," in *Proceedings of the 15th IEEE Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Febrary 2008.

[57] Igor V. Popov, Saumya K. Debray, and Gregory R. Andrews, "Binary obfuscation using signals," in *Proceedings of the 17th USENIX Security Symposium (SECURITY)*, San Jose, CA, July 2008.

[58] M. Christodorescu and S. Jha, "Testing malware detectors," in *Proceedings of the 2004 ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*, Boston, MA, July 2004.

[59] X. Wang, W. Yu, X. Fu, D. Xuan, and W. Zhao, "iloc: An invisible localization attack to internet threat monitoring systems," in *Proceedings of the 27th IEEE International Conference on Computer Communications (INFOCOM) Mini-conference*, Phoenix, AZ, April 2008.

[60] J. Bethencourt, J. Frankin, and M. Vernon, "Mapping internet sensors with probe response attacks," in *Proceedings of the 14-th USNIX Security Symposium*, Baltimore, MD, July-August 2005.

[61] Y. Shinoda, K. Ikai, and M. Itoh, "Vulnerabilities of passive internet threat monitors," in *Proceedings of the 14-th USNIX Security Symposium*,

[62] S. Soundararajan and D. L.Wang, "A schema-based model for phonemic restoration," Tech. Report, OSU-CISRC-1/04-TR03, Department of Computer Science and Engineering, The Ohio State University, January 2004.

[63] N. S. Jayant and P. Noll, *Digital Coding of Waveforms*, Prentice-Hall, 1984.

[64] R. E. Yantorno, K. R. Krishnamachari, J. M. Lovekin, D. S. Benincasa, and S. J. Wenndt, "The spectral autocorrelation peak valley ratio (sapvr)- a usable speech measure employed as a co-channel detection system," in *Proceedings of IEEE International Workshop on Intelligent Signal Processing (WISP)*, Budapest, Hungary, May 2001.

[65] S. Theodoridis and K. Koutroumbas, *Pattern Recognition, Second Edition*, Elsevier Science, 2003.

## **Author Biography**:

Mr. K. Ujwal Babu received his Bachelor's Degree in Technology in Computer science and Engineering from Arjun College of Technology and Sciences, JNTU, Hyderabad and Pursuing Masters in Technology in Computer science and Engineering from Aurora's Technological And Research Institute, JNTU, Hyderabad.