Concealed Internet traffic and exfiltration: The insider threat and resolution

Thomas B. Martin
Holy Family University
Forensics Inc.

Stephen Leibholz
Forensics Inc.

ABSTRACT

This paper summarizes the problems of concealed Internet traffic, and data exfiltration resulting from penetrations, or by ostensibly vetted personnel, via an Internet link, particularly exploiting vulnerabilities introduced by IPv6. Less than 1% of organizations are running IPv6 on their boundary protection devices[4]. As a result they are vulnerable to a new type of attack; IPv6 tunneled over IPv4 networks.

Much of the attention in organizations is focused on preventing attacks from the outside. However, once penetrated, the same resources are not committed to prevent unwanted data exfiltration. Several recommendations are presented to protect an organization from these threats.

Keywords: Data exfiltration, hidden Internet messages. deep packet inspection, IPv6, biometrics, MAC address, encryption, GPS, NAT.

INTRODUCTION

Cyber warfare is gaining increasing awareness as incident after incident has occurred. It is very difficult to protect an enterprise from being penetrated by malware that can wreck havoc within an organization. The problem of cyber espionage, particularly involving insiders, however, has not received the same notoriety since many enterprises are unaware that it has occurred.

Similar to cyber warfare, the problem of data exfiltration resulting from cyber espionage and the use of Internet connectivity is a growing problem. This paper will present several methods to prevent or reduce unwanted data exfiltration through network channels.

The recent depletion of IPv4 addresses has generated new issues with the onset of IPv6. New security issues must be countered with new solutions. China has become the leader in IPv6 technology, impressing the world with the biggest IPv6 network at the 2008 Olympics. The world's most populous country with the largest number of citizens connected to the Internet, has approximately 9% of IPv4 addresses compared to 41% for the United States.[1] IPv6 solves the problems associated with shortages of IPv4 addresses, but provides new opportunities for espionage.

DEPENDENCE ON DATA

As product manufacturing markets have contracted in the US, knowledge-based industries have continued to grow. Virtually all of this knowledge is contained in enterprise databases, the value of which is inestimable. We have begun the era of yottabytes, barely taking note of terabytes, petabytes and exabytes on our swift journey to an all-digital-data world.

For countries/enterprises/individuals antagonistic to the US, it is easier to steal data—particularly by rogue insiders— than to develop technology. These assets are worth protecting.

DATA EXFILTRATION

Data exfiltration can occur many ways [2]; this paper only addresses exfiltration through network channels. An enterprise cannot control the types of attacks that may be waged on the intrusion side of the network. This is not the case for exfiltration, an enterprise may use any methods to prevent unwanted outbound network communications. Some useful tools and policies are listed below. Particular emphasis is given to application layer attacks, which require new strategies to defend organizations.

IPv6

The current version of the Internet, IPv4 was depleted of addresses on February 3, 2011 [3]. The shortage of addresses has led to the introduction of IPv6 which has 128-bit (16-byte) source and destination IP addresses. Many organizations do not see a reason to convert to IPv6, and believe they are not running IPv6. Whether an organization knows it or not, any laptop/PC running Vista or Windows 7 incurs a vulnerability from which attacks can come that will be invisible to IPv4 networks [4].

World IPv6 day occurred on June 8, 2011, with the participation of most major ISPs. IPv6 traffic still accounts for less than 1% of Internet traffic [5]. Because of security vulnerabilities, it is imperative that an organization quickly convert all network edge devices to IPv6 capability.

Deep Packet Inspection

A very powerful and controversial tool is deep packet inspection. Basically, this is simply examining the payload of every packet for message content. Normally, only the headers are examined in networks today.

Since the Internet today uses IPv4 for 99% of the traffic, it will be a slow migration to IPv6. Three transition strategies are being employed: header translation, dual stack and tunneling of IPv6 inside IPv4 [6]. Tunneling is the most precarious method for today's IPv4 networks. The IPv6 packet is included inside the message field of an IPv4 packet. The contents of the IPv6 packet will not be noticed by an IPv4 firewall or intrusion detection system. Hidden IPv6 traffic running across an organization's network can wreak havoc, allow malware to enter the network, and be the basis for a denial of service attack [6]. The only defense against such attacks is deep packet inspection (DPI).

The widespread use of DPI is inevitable. There is no other defense against application layer attacks. However, this certainty of DPI inevitability has been challenged by the ACLU [7]. The age-old privacy versus security debate will continue into the indefinite future. The first few security breaches caused by tunneled IPv6 inside an IPv4 packet have occurred, and many more are certain to come in the near future. These events will be stimuli to organizations to defend against such attacks.

It is important to differentiate between DPI as employed by organizations for protection against attacks and data exfiltration, and DPI as employed by ISPs. There is a legitimate concern for misuse of the results of DPI by ISPs. This topic is not addressed in this paper, but an elegant solution to this problem is contained in "Cyber War" by Clarke and Knake [8].

Biometrics

Biometric identification can be made a requirement for every employee in an organization. A multiplicity of biometric signatures are possible: fingerprint, voice print, iris scan, facial recognition, IR scan, etc. Access to an organization-provided device and the organization's intranet should only be allowed for personnel with a biometric signature(s) on file. Sign on procedures can require a produced biometric at the time of the opening of a session. For example, in order to open a session, the user could be required to repeat several random words displayed to the employee. Voice ID would then permit/deny the sign on. Web cams together with facial recognition can also ensure that the employee is present during the session.

Global Positioning System

Every device supplied by an organization, be it laptops, desktops, or mobile devices should contain an activated GPS monitoring capability. Since each device must be used only by the appropriate individual signed in with proper biometric, the location of every employee is known at time of sign in. As mentioned above, web cams can ensure through facial recognition that the individual remains at the device during a session.

Encryption

Encryption should be used for all communications within and outside of the premises. Similarly, all databases must be encrypted. AES is the recommended method of encryption over DES [9].

Network Address Translation (NAT)

It has been speculated that, with the advent of IPv6, NAT will no longer be required. Although it is true that IPv6 will make possible networks of direct communications between a virtually limitless number of addresses, there are other reasons to retain NAT within organizations. Security is the foremost reason; not communicating information about the addresses of internal devices still trumps any other consideration.

Traffic Analysis

A history of traffic must be maintained for each employee. This history must include addresses sent to, amount of data sent, and history of responses from destination sites.

INTEGRATED APPROACH TO DATA EXFILTRATION PROBLEM

Policy Statement

The major points in a statement to employees of an organization should consist of clearly defined Internet use policies. Key to this policy is the right of the organization to monitor all activities on Internet usage. Only organization-supplied devices should be allowed to connect to the organization's intranet. Each of these devices must be equipped with a biometric signature sign-in procedure and active GPS location. A database will be maintained associating each employee with the MAC address of all organization-supplied devices, current GPS location of each, and biometric signature of each employee. No employee should be permitted to allow another person to use their devices after sign-in. This can be checked by an active webcam facial recognition feature running continuously.

Protecting the Enterprise

At the egress point in an organization, the technologies described above can ascertain answers to the following questions:

- Who sent this packet? – Biometric signature
  - The biometric information should be removed by the boundary device(s) before sending to the outside world
- What device was used to send this packet? – MAC address
- Where was the device? – GPS location
- What was the content of the payload in the packet? – Deep packet inspection
- Was this packet addressed to a site that has been addressed before? – Traffic analysis and maintenance of traffic history for each employee.

- Is all the data consistent with known information? – Enterprise security devices.

CONCLUSIONS

All possible technologies must be used to protect organizations from security breaches. Cyber War is a reality today and will continue for the foreseeable future. The problem of unwanted data exfiltration is far easier to solve than the problem of preventing unwanted penetrations. Most enterprises have concentrated on preventing unwanted intrusions. In addition, deployment of IPv6 in boundary protection devices has not kept up with the impending rapid conversion to an all IPv6-based Internet.

Three important conclusions are presented in this paper:

1. IPv6 must be operating at all network boundary devices.
2. Deep packet inspection must be used for both inbound and outbound traffic.
3. Biometrics, encryption, traffic analysis and history, NAT, GPS location, MAC addresses, must all be used to protect an organization against unwanted data exfiltration.

The techniques and solutions presented in this paper should significantly improve security of an organization and would make it very difficult for an employee to avoid being caught through forensics analysis, should an unwanted data exfiltration occur from an internal source.

This paper is intended as a wake-up call for organizations to recognize the threats and aggressively respond to exfiltration vulnerabilities. They can be prevented.

REFERENCES

Andrew S. Tanenbaum, David J. Wetherall, “Computer Networks”, Prentice Hall, 2011

Annarita Giani, Vincent Berk and George Cybenko, "Data Exfiltration and Covert Channels", Proceedings of the SPIE Vol. 6201, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IV Orlando, Florida, April 2006 http://www.icann.org/en/news/releases/release-03feb11-en.pdf

Barb Feige, Caroline Fedrickson, Jay Stanley, and James Thomas Tucker, Comments of the ACLU before the FCC Hearing on Broadband and the Digital Future, July 21, 2008

C. E. Caicedo, J. B. D. Joshi, and S. R. Tuladhar, “IPv6 Security Challenges”, Computer, IEEE Computer Society, volume 42, issue 2, 2009, pp. 36-42

https://www.arin.net/knowledge/about_resources/ceo_letter.pdf

http://www.bgexpert.com/addressespercountry.php

Richard A. Clarke and Robert K. Knake, “Cyber War”, Harper Collins, 2010, pp. 161-166

Thomas B. Martin, “IPv6 and Deep Packet Inspection”, Journal of Technology Research, Volume 3, Academic and Business Research Institute, April 2011