6man Working Group
Internet-Draft
Intended status: Informational
Expires: December 1, 2012

T. Macaulay
2Keys Security Solutions
D. McMahon
Bell Canada
E. Doron
Radware
P. Jungck
Cloudshield

May 30, 2012

Internet reputation intelligence: Problem Statement
draft-macaulay-6man-reputation-intelligence-00

Abstract

This draft represent the initial public discussion of the value of proactive, reputation intelligence on the Internet and some of the challenges associated with these services that may be partially addressed through novel use of IPv6 features and functions.

This document is intended to outline the concept of Internet reputation intelligence, the benefits it brings to network elements and endpoints. This draft also addresses the challenges associated with legacy security systems based on threat-signatures, and some of the current weaknesses of reputation management systems.

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 1, 2012.

Table of Contents

1. Introduction

Threats on the public Internet in forms such as malware (malicious software) and phishing have reached new levels of efficiency and effectiveness, where vulnerabilities are routinely discovered and exploited faster than vendors can release patches. Similarly, the time between system penetration (when the attack succeeds), and exploitation (when the asset is utilized in a manner unauthorized by the owner) can be very small.

This situation is creating a major burden for risk managers. On the business side, increased vulnerabilities and associated system exploitations lead to increased regulation and legislative sanctions. On the technical side, ever more security tools, products and vendors are required to keep even basic IT services "reasonably" secure, raising overall costs and complexity.

Security resources inside organizations are frequently overworked, and are often limited to reactive measures. Enterprises are looking towards a variety of service-providers (carriers, ISPs, managed security service providers - MSSPs) to provide them with proactive capabilities. Some service providers now create and maintain reputation information, and use existing trusted, business relationships with organizations to deliver this intelligence through novel a variety of means; the challenge becomes the effective and efficient delivery of this intelligence.

IPv6 may offer some useful abilities to deliver reputational information in-band, in near-real-time, through the use of features such as the flow label or headers extensions. IPv6 headers may be formatted with reputation scores such that network elements or end-points could read the reputations and apply organizational security policy on inbound or outbound packets and flows.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in .

3. Background

Internet based threats in the form of malware and the agents that control this software (organized crime, spies, hacktivists) have surpassed the abilities of signature-based security systems to remain up to date and provide timely mitigations. Whether they be: on the

enterprise perimeter in elements such as firewalls and proxies, in elements such as Intrusion Detection Services (IDS) within the organizational network, at the endpoint points in the form of anti-virus or host-IDS, or as managed services in the form of anti-virus/ spam "in the cloud", a signature-based system needs supplementary support from reputation-based systems.

Signature-based security systems all rely upon malware being detected, isolated, dissected, and templated into unique hash-identifiers or regular expression filters, which are then distributed far and wide as information-bases containing hundreds of thousands if not millions of malware "signatures". In order to utilize these signature bases, perimeter, network or end-point security elements must typically assemble data payloads and hash the contents looking for matches with the signature base. Some security systems try to enhance or supplement signature-based approach with heuristic-based analysis, looking for patterns in network traffic or packet contents as indicators of malware or malicious activity. Signature-based systems are highly effective for known malware, but they don’t know what they don’t know. Meanwhile, heuristic based systems make intelligence guesses, but are subject to desensitizing false-positives. All these systems represent resource-intensive infrastructure and administration.

The sensitivity of IP networks continues to grow as a new generation of "smart" devices is enabled with Internet Protocol. These devices include those using both fixed line and wireless networks for remote operation and networking highly dispersed devices. The range of these devices makes this situation new and exceptional in a security context: control devices and sensors represent the interface between the logic world of networks and software applications, and the physical world where affects are kinetic in nature. This diverse collections of IP-based assets is coming to be known as the Internet of Things (IOT). In response to the accelerating threats and elevating consequences associated with incidents, the security vendor community and various non-profit entities have developed products and services integrated with forms of reputation intelligence. This intelligence enables proactive security controls to supplement signature-based and heuristic systems, and better protect logical systems.

Reputation intelligence typically consists of IP addresses and domains (associated with IP addresses through DNS), which have been observed engaged in either attack or victim-behaviours such as: inappropriate messaging and traffic volumes, suspicious domain name management, Botnet command-and-control traffic, attempts to send or relay malware and other indicators of either malicious intent or compromise.[REF 2] IP addresses may also end up on a security

reputation list if they are identified as compromised through vendor-specific signature-based processes. The proactive element of the reputation intelligence lies in the ability for hosts to be forewarned of the reputation of addresses on the Internet. The overall effect is a new layer of security which can be applied within, on, or beyond the organizational perimeter. For instance, security managers could configure perimeter access control services to escalate authentication based on reputation, or instruct upstream service providers or carriers to not route packets below a certain reputation to organizational gateways.

Security reputation intelligence can be derived from a multiple sources. It can come from security vendors or other analytics organizations who trace active malware attack-vectors and publish them to open and closed subscriber-lists. Another reputation source is security or network-management infrastructure within a carrier or service provider network, or vendor security products located on customer premises. In these instances reputation may be learnt through analytics aggregated on ambiguous data from many devices after attacks.

At this time, security reputation intelligence from closed and open sources is typically made available to perimeter and end-point products through both standards-based and proprietary queries to on-line information bases. In many cases, this reputation intelligence is distributed over the open Internet and relies on subscriber "pull" requests for batched downloads of large or incremental info-bases, or individual queries on source IPs attempting to connect to a given host. [REF 3]

This system of using proactive, security reputation intelligence has many benefits, specifically:

1. provides an additional layer of security based on empirical observations otherwise beyond the visibility of most organizations
2. is proactive in natures, allowing threats to be managed at the network level before the payload is delivered at the application level
3. facilitates the conservation of application-layer security and associated resource (processing, storage, licensing, administration, power)
4. is flexible, and can be applied at different locations in the subscriber infrastructure, from upstream of the perimeter to deep in the internal network
5. is applicable to a variety of different communications elements and end-points, from organizational messaging infrastructure to remote, embedded sensors and controllers

Conversely, proactive, reputation intelligence has current challenges. Specifically:

1. the "pull" distribution model is subject to direct attack/denial of service at Internet distribution points
2. is often proprietary to vendor products and not interoperable, requiring independent administration of elements
3. can create network-layer processing overhead on communications elements and endpoints
4. introduces flow latency while reputation queries are sent, received and processed
5. introduces intelligence latency as reputation lists will be inevitably cached and periodically refreshed by subscribers

3.1. Use cases

The following are example use-cases for a security controls based upon proactive reputation intelligence systems.

Cloud-based (Upstream) Use-case: Traffic to a user (a subscriber) of reputation intelligence is routed through a proxy-type device off premises (in the service-provider "cloud") configured to compare source IPs of flows to the reputation intelligence. The proxy-type device applies a policy established by the subscriber. For instance, according to reputation score, drop the packets, quarantine the packet for more inspection, issue alarms, or pass the packets and associated flows to escalated-authentication systems, or do nothing.

Perimeter-based (subscriber-premises) Use-case: Security elements on the subscriber perimeter or within the DMZ such as firewalls, IDS, proxies, DNS, SMTP server and other assets are enabled to compare source IPs of flows to reputation intelligence. The security element applies a policy established by the subscriber according to the reputation score. For instance, drop the packets, quarantine the packet for more inspection, issue alarms, or pass the packets and associated flows to escalated-authentication systems, or do nothing.

Internal network (subscriber-premises) Use-case: The objective is to detect outbound communications to sites with a degraded reputation, potentially indicating that the internal device has been compromised. Security elements inside the subscriber enterprise such as zone-firewalls, routers, IDS, proxies, DNS, SMTP servers and other assets are enabled to compare destination IPs of flows to reputation intelligence. For instance, a vulnerable internal device is attempting to download a botnet malware payload from a known malware drop-site domain (IE, malware.example.com); in response, the internal security element may drop the packets, quarantine the packet for more inspection, or issue alarms.

End-point Use-case: Subscriber end-points, such as desktops, servers, phones, physical security (door strikes, cameras), automation and control devices, environmental sensors and other elements are enabled with reputation intelligence. These elements compare source or destination IPs of flows to reputation intelligence. The subscriber end-point applies a policy established by the subscriber according to reputation score and possibly differentiated by the type of end-point. Given that end-points may be very simple or low-power devices, using the appropriate intelligence delivery systems may make the policy-enforcement options comparably simple; for instance, drop the packets.

Coarse-grade refinement: Organizations which possess independent reputation capabilities may choose to also procure upstream or cloud-based reputation services, which are used as adjuncts. For instance, an organization operating a global network for internal communications supporting thousands of servers and desktops will have access to an internal reputation and intelligence base with unique reputational insights. Such organizations may wish to receive reputation intelligence from a third party to support further processing on the perimeter, the internal network and/or end-points.

4. Security Considerations

The creation of a reputation intelligence is complex, and requires the ability to collect large volumes of ambiguous network, sensor and end-point system information. This information must then be normalized, aggregated, weighted and correlated using sophisticated intelligence algorithms. The first task of collecting information is hard, but already accomplished by many carriers, service providers and vendors as part of existing operations. It is the development and application of intelligence algorithms to the large, ambiguous data sets that creates reputation intelligence and adds novel and unique value, and a proactive security potential.

Reputation intelligence algorithms are necessarily used by all suppliers of reputation information to create some sort of relative score or degree of positive or negative reputation. Frequently, reputation algorithms are unpublished. As a result, the quality of the intelligence can be difficult to assess and compare. For instance, the following elements could be considered as functions within a reputation algorithm that may influence the accuracy of the intelligence:

- A function to account for large Internet portals with many, independent URLs with good reputations, but also some proportion of dangerous (bad reputation) URLs sharing the same IP address

- o A function to account for the distance in time between the last observed suspicious or illicit behavior and the present
- o A function to account for the reputations of adjacent IP addresses or domains
- o A function to account for the original, per-processed source of the intelligence (open source, closed source, domain of control, uncontrolled domain)
- o A function to account for the volume or velocity of suspicious or illicit behavior (IE. High spam rate or low n' slow data exfiltration)
- o A function to account for the duration of suspicious or illicit behaviour (IE. Sustained spam or infrequent beaconing)
- o A function to account for lifetime of domain to source IP associations (IE. Newly minted domain names or previously un-observed/un-assigned addresses
- o A function to account for the proportion of traffic from this source which is benign versus demonstrably illicit
- o A function to account of the nature of the suspicious or illicit behavior (automated port scanning versus malware-drop)
- o other?

Even given the assumption that reputation algorithms among suppliers of reputation intelligence are somehow comparable, the issue of common scales effects interoperation and security management. For instance, reputation scores can be expressed in many manners:

- o As a positive or negative score above or below a benign score or a score for which no reputation information is available
- o A negative score relative to a completely trusted class of IP
- o A positive score relative to the least trusted IP addresses
- o as a quantitative metric
- o as a qualitative metric

Some reputation systems will start with un-processed activity logs under the direct control of the intelligence supplier but also logs submitted from a variety of sources. The degree to which the input sources of intelligence are controlled has a baring on the potential resistance of the intelligence to poisoning (injected with mis-information to ruin good reputations and make bad reputations appear better). For instance, a (presumably open-source) volunteer-maintained form of reputation intelligence may be more prone to poisoning than a carefully authenticated, closed-source of reputation intelligence. Similarly, reputation intelligence derived from sources physically outside the domain of control of the service provider is more susceptible to poisoning than intelligence from sources that control physically and logically control the log and data sources.

Finally, under certain circumstances the management or application of

reputation intelligence may come with some form of legal or regulatory burden. As a result, the calculation of reputation intelligence may need to be distinct from the delivery of reputation intelligence and yet again from the enforcement, in order to mitigate legal or regulatory risks.

5. Acknowledgements

The authors wish to acknowledge the guidance and support of Michael Richardson.

6. References

6.1. Normative References

[REF1] Bradner, S., Ed., "The Internet Standards Process - Revision 3", October 1996.

6.2. Informative References

[REF2] Macaulay, T., Ed., "Upstream Intelligence: anatomy, architecture, case studies and use-cases.", Information Assurance Newsletter, DOD , Aug to Feburary 2010 to 2011.

[REF3] Wikipedia, W., "Reputation Black List (RBLS)", May 2012.

Authors' Addresses

Tyson Macaulay
2Keys Security Solutions
1550 Laperriere Ave - Suite 202
Ottawa, Ontario
Canada

Email: tmacaulay@2keys.ca

David McMahon
Bell Canada
160 Elgin Street - Floor 5
Ottawa, Ontario
Canada

Email: dave.mcmahon@bell.ca

Ehud Doron
Radware

Email: ehudd@Radware.com

Peder Jungck
Cloudshield

Email: peder@cloudshield.com

Full Copyright Statement

Intellectual Property