TECHNICAL FORMATS AND LAWS ARE NOT THE BARRIERS TO IMPROVED ATTACK DATA SHARING

Patrick Cain
Resident Research Fellow, APWG (apwg.org)
President, The Cooper-Cain Group, Inc. USA (coopercain.com)

This short statement is submitted in response to a call for papers for The Coordinating Attack Response at Internet Scale (CARIS) workshop, sponsored by the Internet Architecture Board (IAB) and the Internet Society (ISOC), on Friday, June 19th in Berlin.

Introduction

The APWG has been using a special block list to gather, analyze, and share URLs used in phishing since 2003. The block list varies from 10,000 to 160,000 entries before the entries time-out after 72 hours. In the past few years, the APWG has explored and started collecting and sharing other types of data—some more sensitive, some less timely—with varying success. The issues that we have encountered have been surprising to the APWG technocrats as well as the policy community since the issues are very different from the public's expectations.

The Perceptions and Some Definitions:

Although many will allege that misaligned technical standards or formats are the leading barrier to improved cybercrime data exchange and attack mitigation efforts, the APWG has found other nontechnical issues still impede optimal efficiency. The nontechnical issues, described below, are misunderstood and generating enough concern to cause many parties to refuse to assist in identification and mitigation efforts completely.

Although this workshop lumps all "Internet Scale" attacks together, there are different attach classes that require vastly differing responses. One large class is the "defend" class that includes traditional wide-scale denial of service (DOS) attacks where response speed is important and the critical responders are mainly Internet Service Providers (ISPs) as the attack targets cannot defend themselves. When the attack is over, things may return to normal. Another class is the "respond" class, where a new vulnerability is widely and quickly exploited. Here, targets may actually be able to respond on their own to defend themselves, but the speed of response is still important. At the conclusion of the attack, the target may be in much worse shape than they were before the attack. The third class is the "inquisition" class, where the attack happens over a long period of time; is targeted at a specific software or hardware application; the target only knows of the attack after it succeeds; and the intended post-attack effect is to prosecute the attacker. Each of these classes requires different coordination, data sharing, and investigative parties; they should not be treated as one homogenous group.

The Challenges

There are actually two purposes behind sharing attack information: 1) the common defense of the sharing group, and 2) group collaboration for a specific end-action such as arrest, deterrence, or defamation. The impediments for common defence appear to be centered around a few areas, some technical some political:

1. Lack of common understanding of different types of "Internet data"

When one mentions "data sharing," many people immediately think of Internet search histories and react accordingly. Common definitions, a means to delineate data by type, and the ability to exchange motivations are required for understanding what data are being exchanged, under what kinds of circumstances, and for what processing purposes. This is a formidable barrier to data exchange, particularly internationally.

2. The goal is to have organizations share data between members

Some government-based organizations seem to think members send data “to them” instead of to other members “via them.” As an example, infected system notifications only go to the owner of the infected system, not to a sharing group to be used to block incoming connections to their networks.

3. Lack of common data-marking standards

Reporting, exchanging, and accepting large amounts of data requires a robust means to mark data submitted to the sharing center in order to guide how to re-share or otherwise redistribute the data. Data provided by a member organization is *belongs* to that member and they should have a mechanism to control where that data goes. Using “simplified” marking schemes may allow for easier understanding but fails to allay concerns about sensitive data being mishandled.

4. FOIA act exemptions

One daunting challenge to disclosing vulnerability or attacker information to other parties is providing sufficient information to the vulnerable or attacked party to allow them to provide corrective actions. At times “sufficient information” may include collection or method information that the discloser would not like to be made public lest disclosure compromise the collection or detection method. In the interest of submitting that information to the attacked party, the disclosed may use the services of a government-sponsored or -operated ISAC or CERT. There is widespread belief that information submitted to government-sponsored entities may incur FOIA-type issues. For example, alleging an entity is party to an attack may cause that (allegedly annoyed) party to request information so that they may harass the reporting party. Not all submitted data should be FOIA-exempt, but some method for marking data/requesting privacy is needed. Whether this is accomplished with submitter identification removed from submissions to government-sponsored ISACs or a non-government aligned third party that only reports anonymized data is an implementation detail. In many cases, this is crime data and should have all the rights and benefits afforded that data type in the non-computer world.

5. Liability restrictions

The likelihood of inducing errors into the data stream increases as the speed of information sharing increases. Errors happen. Mechanisms should be developed that allow for robust information sharing with limited liability for inadvertent errors.

6. Data shared in common defense should not be silently shared with others

Many times, a reporting party may have details of a successful cyber-crime against another entity and uses a CERT or ISAC to quickly notify the affected entity. There is a strong concern that a government-operated CERT or aligned entity may—with good intentions—forward the received data to a law enforcement or regulatory agency that creates additional unintended consequences on both the reporter and affected parties. For example, the ISAC receives a report that a regulated entity’s system is acting compromised. The reporting party has no trusted contact at that entity. The ISAC notifies the impacted entity but may also notify a member of a law enforcement agency (LEA). The LEA may contact the entity to collect details of the compromise, setting in motion a series of panicked internal investigations and possibly regulatory filings before the entity can evaluate, much less confirm the issue or reply back to the ISAC identifying a false positive. The goal of an ISAC or CERT should be to receive anomalous activity reports to forward to the affected party, not to act as a collection point for other agencies.

Conclusion

Although the challenges seem daunting, addressing them - even in a slow but steady fashion - should increase the trust amongst the necessary parties to actually share more attack data and foster better communication and cooperation among responding parties. We are optimistic it will happen.