In trying to further the sharing of time-critical electronic crime (eCrime) information, the APWG, in partnership with other information gathering organizations, has developed and promoted extensions to standardized data sharing formats such as the IETF's Incident Object Document Exchange Format (IODEF). The APWG has also been developing the technology, as well as procedural and content-based rules, for sharing data on phishing, network attacks, and other eCrime events.

Successful eCrime event data sharing requires that those three pillars—standards-based technology, operational procedures, and content rules—are thought-out and tested. Historically, event sharing regimes get stuck by trying to develop the operational procedures well before the other two pillars have been constructed. The APWG has found that piloting the technology and content-rules simultaneously has significantly aided in the development of the operation procedure pillar. To continue that development and to assure that the technology stays aligned with the operational procedures, the APWG is launching a table-top exercise to further refine the data models and to validate certain operational assumptions.

The expectation is that additional technology requirements and missing data content will be identified by performing some eCrime-event data exchanges using near-real data by parties that normally use or consume that type of information. Additionally, actual data exchanges will help to refine the operational, policy, and procedural issues that appear whenever a data exchange question arises.

THE TABLE-TOP DATA EXCHANGE EVENT

With implementations of the IETF's IODEF Standard (RFC5070) continuing and the standardization of the APWG's phishing extensions to it, it is time to validate assumptions made during their development. The APWG proposes to plan and operate a table-top exercise to: refine the actionable data elements collected on specific types of eCrime; precisely define how those elements are exchanged; and thereafter to act as an aid to further develop the operational data sharing policies and procedures necessary for those exchanges. The goal is to recreate how actual network or eCrime event data is (or would be) shared amongst the initial reporting party, subsequent investigators, and responsible entities for action.

This table-top 'event' will ask participants to put near-real data into a suitable format and then forward that data to another investigating or executing party. The second investigator may enter more data, remove or desensitize portions of the received data, perform corrective action, or just pass the data to another responsible party for further action.

To garner wider participation and to meet the primary goals, the actual 'table-top' exercise may involve a virtual entity such as a common website, or it may be operated from multiple locations. As the exercise is designed to capture and share relevant information, showing the data in an acceptable format and having it transferred in as close to actual environments as possible are extremely relevant goals. As described below, the exercise is designed to validate some primary objectives, although validating additional assumptions would be beneficial.

THE PILOT EXERCISE OBJECTIVE

The primary objective of the exercise is to confirm that the data exchange format and content rules are sufficient for an event reporting party ('originator') to supply another party/investigator with enough actionable data about an event such that the second investigator can investigate the event without further communication between the parties. Historically, notifying another party of an event required a number of communicating round-trips to identify the **actual time and Time Zone** of an event; to request additional event data; or to understand what was being reported. This part of the exercise should determine whether a single communication suffices between the two parties if a suitable data format — and accompanying rules for mandatory content—is used to report the incident. A basic exercise with paper-based forms will also be available, but the intent is to use a web-based form to capture the event information in an IETF IODEF XML structure. The web-based exercise will transfer data between parties via simple email.

SECONDARY GOALS

There are a number of less critical but still important assumptions to validate in this exercise, summarized below in three groupings.

Require specific information in reports

The first group consists of exercises to determine if reporting parties can be persuaded, either technologically or via process, to supply complete sets of event data. Many times a reporting party may omit a critical piece of data like the time zone of the event or the offending IP Address.

Additionally, do the current standard reporting formats capture the information for a complete and actionable report? The exercises should note any shortcomings of the required data sets.

Internationally agreed upon eCrime definitions

Are there consistent definitions for the types of eCrime used in the exercises that would allow investigators in multiple countries to implicitly understand and react to them? The exercises may help refine these definitions.

Enhanced multilingual capabilities

Can the reporting format be used to support multilingual reports? (i.e., if a reporter uses their local language to describe the eCrime, can a receiving party use translation tools to understand the reporters' description and take appropriate action?) In the past, many eCrime reporters have submitted reports in English, which is not their native tongue. Trying to convey highly-technical eCrime jargon in a non-native language is a challenge in the best of circumstances. Using language tags in tools to mark data allows reporters to use their native tongue to describe the event and supports the ability for receiving parties to perform local translations to their native tongue, hopefully cutting down on miscommunication and misunderstanding that should allow for faster reporting.

Can capturing, reporting, and sharing event data workable when computerized.

Another assumption is that entering and sharing eCrime data can benefit from using web forms and computer automation to perform data validation and processing. Portions of the exercises should validate or void this assumption.

ECRIME DATA EXCHANGE SCENARIOS

The actual exercise will be a series of event reporting and exchanging activities to quantify meeting the objectives and goals. The activities will start with an overly simple exercise to verify the system's stability and the readiness of the participants, then moves to more complex scenarios with less defined data. Participants may offer other scenarios to improve the usefulness of the event. The exercises may change during the event based upon feedback from the participants.

Exercise 1: Establishing a Baseline

Goal: Get participants up to speed; check system stability and common terminology.

eCrime: Report a phishing or other fraudulent URL to the APWG, an ICANN registrar, or CERT.

Exercise 2: A Real, but Simple eCrime Report

Goal: Convey actual data to a responding party to either add investigative data or to take immediate action.

eCrime: Report a "botnet command and control" server's IP Address to the relevant ISP or CERT for blocking.

Exercise 3: Insert additional data into an eCrime report and forward to another party

Goal: Verify that a receiving party can insert additional information into an existing eCrime report and forward it to another for successful understanding.

eCrime: Initial reporter will identify web sites with malicious software; other reporters will add additional web sites and forward the updated report to others.

Exercise 4: An everyday, illegal content, eCrime

Goal: Notify appropriate party in another country of illegal content. (Content will be selected by reporting participant.) This should test the ability to identify enough data to another party for further investigation.

eCrime: Distribution of illegal content over bullet-proof hosting service. Hosting is either using fastflux DNS and proxied or on a Peer2Peer network.

Exercise 5: A complicated PII data discovery eCrime

Goal: Notify multiple appropriate parties in different country of apparently compromised or stolen credentials. Test the ability to send recovered sensitive data and investigative data to multiple parties.

eCrime: A trove of account data was discovered on a server in country I, targeting victims in countries P and B, and discovered in country F. The recovered data is an obvious privacy violation, contains banking credentials of individual and corporate accounts, and was discovered by the investigator through a normal route such as sloppy criminal web configurations.

Exercise 6: Evolving eCrime Reporting

Goal: Do the current data formats support new or evolving eCrime?

eCrime: Participants will suggest currently evolving eCrime types such as cyber bullying, malicious advertisements, or other participant-requested eCrime and then attempt to report it via the current formats and techniques.

ADDITIONAL INFORMATION OR TO PARTICIPATE

More information, copies of the standards and assorted tools are available at the APWG website, http://www.antiphishing.org/iodefFormat.html.

For participation details, to receive additional information, or to suggest evolving eCrime types, please contact:

Patrick Cain
Resident Research Fellow
APWG
pcain@antiphishing.org

Peter Cassidy
Secretary General
APWG
pcassidy@antiphishing.org