APPLIED RESEARCH

Introduction

The APWG is honored to provide information related to international cooperation and prevention of cybercrime to the 7th session of Intergovernmental Expert Group. The APWG, founded in 2003, operates a large international e-crime data clearinghouse that mediates the exchange of machine-event data related to cybercrimes between private sector stakeholders and public sector law enforcement. These days, that clearinghouse's progeny delivers upwards of more than one billion data elements per month in answer to data requests by APWG members.

In this missive, APWG's tenders its observations in its nearly two-decade history of developing policies and data instrumentation for the global, programmatic suppression of common cybercrimes - and makes recommendations for globalized suppression of cybercrime. Over the last 17 years, APWG has witnessed criminals, as well as investigators, responders, and nation state policies evolve in their respective roles and enterprises in cyberspace. Criminals continue to thrive in - and redefine - the cyberattack landscape. Meanwhile, the global response to mitigate threats, and to identify, apprehend and prosecute cybercriminals, lags behind.

Public sector law enforcement officials have recognized that one of the best practices to mitigate e-crime is though robust programmatic sharing of intelligence on criminal infrastructure: Information sharing has for decades been a vibrant, committed, and growing trust-based collaboration between nation states and private organizations. Those organizations recognize that law enforcement organizations cannot collect, process and share such data alone: they rely heavily on the private sector for data and analytic tools.

The recently evolving data protection and accessibility landscapes, however, have adversely and profoundly affected information exchanges among parties committed to mitigate cyberattacks and cybercrimes.

APPLIED RESEARCH

Cybercrime is continually evolving as criminals race to find new victims - and investigators and educators develop novel ways to prevent victimization. As an example, ransomware attacks used to just encrypt a victim's hard disk drive and try to derive payment to allow decryption. Today, ransomware has evolved to both encrypt the local media and copy the victim's data to a remote site. The criminal offers to help you decrypt your data for a small fee, and - for a much larger fee - "promises" to not publicly release your data.

Crypto-currency use in payment systems also adds new challenges to traditional money-laundering and follow-the-money investigations. These new tactics require new techniques to educate users. APWG and Washington-based research partner NCSA specifically designed and deployed its STOP. THINK. CONNECT. Campaign in 2010 (adopted by the United States and 22 other nations to date) to be extensible in order to map its messaging assets to all of the cybercrime threat models citizens may confront over the years, for instance, in recognition of the dynamic nature of cybercrime.

It is the ever-evolving and ever more frequently mutating surface of the cyber threatscape that moves APWG to make the following recommendations, revisiting - and expanding - on some of the discussion this institution offered in it its Commentary for the Sixth Session of the Intergovernmental Expert Group on Cybercrime <https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments6th_IEG_Cybercrime_Compilation_comments_Observers.pdf> As follows:

Data Handling Authority for Machine Event Data for Private Sector Interveners

Studies have consistently shown that more than 95 percent of internet-based crime is detected and initially investigated not by the public sector bodies, but by private organizations, government funded research projects and commercial concerns, including: the APWG (an anti-cybercrime clearinghouse that mediate exchanges of phishing attack data and data related to abuses of cryptocurrency exchanges); CAIDA (the Center for Applied Internet Data Analysis); Cambridge Cybercrime Center at Cambridge University; commercial reputation data service operators such as Spamhaus and SURBL; and commercial security services providers.

When cybercrime data processing is placed into the same category as third-party commercial tracking or personalization services, private-sector cybercrime "first" responders, forensic analysts, and criminal investigators are subject to the same rules as marketing and tracking organizations. Ironically, the very parties who historically work to mitigate cybercrime also work to identify and prevent abuses of special data are encumbered by the same rules and regulations as the commercial enterprises that regulations and directives are attempting to constrain through law.

The language and interpretation of GDPR are an important and enduring case in point. Law enforcement organizations are afforded access to WHOIS registrant contact data related to registration of domain names. There must be some granularity in assignment of access to this essential forensic data and categories of authorized access must be built unambiguously into the law. Private actors working in the interest of public safety are feeding public-sector law enforcement with the data (and actionable interpretations thereof) to protect the public. These cybercrime responders and forensic artisans must have a different classification than marketing and tracking enterprises. Private sector investigations in the interest of public safety merit the same access as public sector investigations.

The GDPR offers clarification and guidance exclusively for law enforcement operations and in so doing discounts the communities of cyber investigators and first responders who programmatically exchange data that are used to neutralize cybercrime events before they become damaging to people and enterprises. These communities also provide data, services, and tools that law enforcement and departments of justice worldwide rely upon to identify, apprehend and prosecute cyber attackers and criminals.

A Universal Nomenclature for Cybercrime Data

The larger community of stake-holding interveners needs to develop a common definition for data that require special handling or treatment. New regulations or directives often have different - or new - definitions for data items that the regulators deem private, sensitive, or otherwise objectionable to allow to be exchanged. For example, the definition of personally identifiable information (PII) varies among EU regulation and many other states. A universally recognized definition for special data can remove the impediments and impedances associated with identifying, for example, what special data can be shared, how, and for how long and thus allow investigators and law enforcers in multiple states to access these data more efficiently - dramatically improving e-crime mitigation, investigation, victim reduction, and perpetrator apprehension.

National and Transborder Cybersecurity Awareness Campaigns

Cybercrime has no season. It is a 24/7 attack on all IT users everywhere all the time and requires citizens to be alert to existing cybercrime models - and the newest techniques being employed by cybergangs. For that reason, APWG has promoted its own STOP. THINK. CONNECT. Cybersecurity awareness campaign and assisted in its launch in 23 nations. Member nations of multi-laterals as we as all intergovernmental organizations should find ways to support these kinds of campaigns to reduce citizen victimization programmatically through awareness and education.

Machine Event Data vs. Personally Identifiable Information

The kind of data that cybercrime responders and forensic artisans routinely seek and exchange are, for example, the logs of a web, application or cloud server, or compromised systems. The log files are a great resource in identifying the criminal activities. For example, the data that APWG archives on its eCrime eXchange system for its members identifies systems and behavior observed at those systems that is associated with fraudulent or criminal enterprise and the network locations of the systems without obtaining or revealing PII. [SEE: Figure 1] APWG eCX data archive is one example of many forms of unenriched, network event and machine event data that are used to identify fraud or criminal enterprises.

Investigators and public-sector law enforcement have or can (legally and formally) request access to other data such as WHOIS records or billing statements to identify the actors.

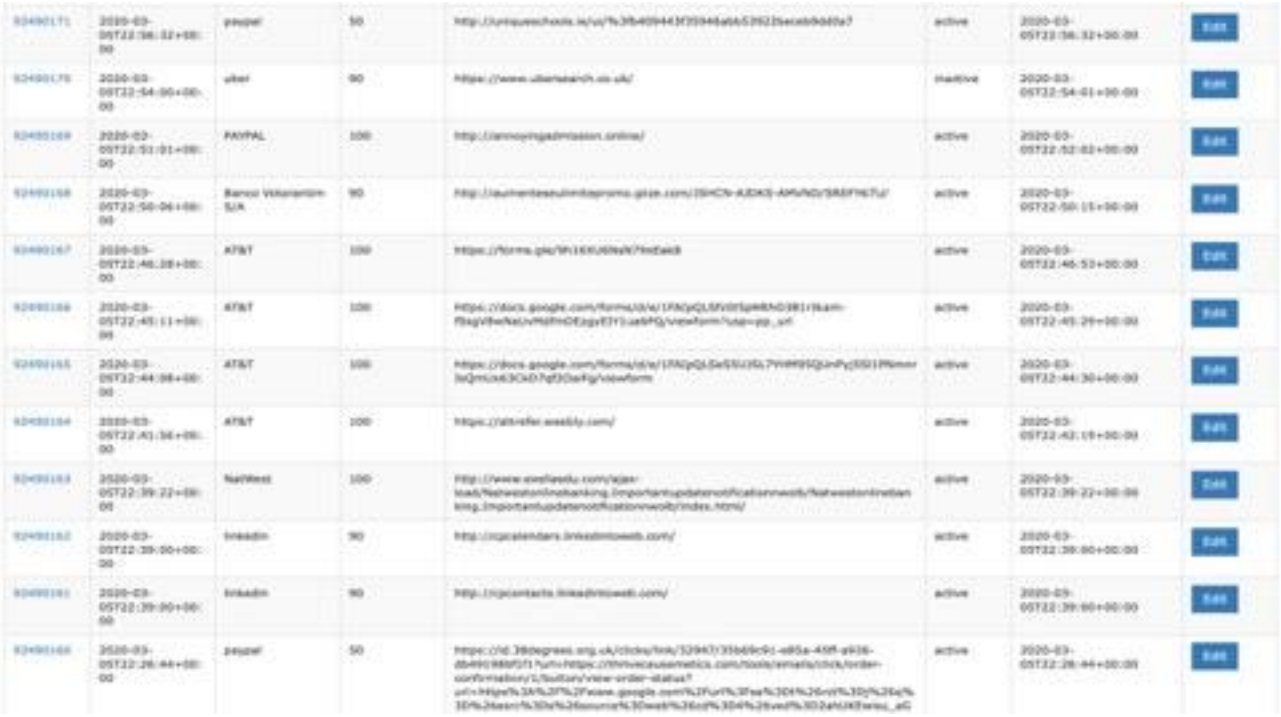

Figure 1: Data table of phishing URL reports in CSV format from APWG eCrime eXchanage, March 5, 2020.

APWG and its data-exchange correspondents see the policy utility of the term *machine event data*, a term that we recommend to all policy development agencies and authorities use to describe automatically generated technical background data that can be shared and correlated instantaneously through computer programs.

Machine event data is automatically generated by networked computers as incidental data required for workaday maintenance and troubleshooting – as well as by security systems (such as intrusion detection or firewall devices) when they discover malicious activity. APWG asks that the International Expert Group consider whether or not a consent option is required - or should be required - for this type of event data.

Policies and definitions in law and regulations that would clearly and unambiguously distinguish machine event data from PII could more precisely frame discussions around privacy and associated law and regulation and align them with operational realities. Legislation and regulation should be, at a minimum, evidence based. It the absence of non-ambiguous language distinguishing machine events from PII that prevents the resolution of conflicts between privacy laws and counter-cybercrime efforts by both private and public sectors. Many initiatives to preserve the rights and freedoms of citizens – and subsequent misapplication – can and do demonstrably cause more harm than good for want of clarity and mutual understanding of workaday realities.

Automated Data Exchanges for Programmatic Security Schemes

Much of the data exchange required to respond persistently and effectively to cybercrime is embedded in security software products developed by industry and installed on computing devices. These software tools are fueled by continually refreshed databases to safeguard users' devices and personal data from new threats as they emerge.

Embedded data exchange routines are a key component of computer security software. Computer security software companies programmatically exchange copies of malware with each other that is routinely recovered from customer machines operated by individuals, as well as networked computers managed by commercial enterprises, to update security software products with the latest data that maximizes those tools efficiency in protecting their users from the very latest threats.

As well, these companies and cybercrime investigators also subscribe to commercial and NGO-managed services and government-sponsored resources that supply such data as malware samples (and abstractions of them expressed as digital fingerprints for quick identification of known malevolent code), attack information, operational data related to cybercrime schemes and events and the network numbers of Internet Protocol (IP) addresses that have been associated with cybercrime and other malevolent or antisocial behavior.

In conclusion, APWG has identified these policy dimensions in which private sector enterprises can be more efficiently utilized in the protection of citizens and the promotion of justice as enforced by public sector agencies and law enforcement. A much more powerful and unified global response to the growing cybercrime threat is at hand if the stake holding communities, including policy makers at the head of the table, can resolve some fundamental conflicts in the engagement of data that is essential for the programmatic and maximally efficient suppression of predictable, everyday cybercrimes. Those key issues include: the establishment of a common nomenclature for cybercrime data; data handling authority for machine event data for private sector intervenors; and the legal disambiguation of PII and machine event data.

The directors of the APWG and trustees of the APWG.EU in Spain have at hand a large community of experts and researchers from every stake-holding sector and libraries of relevant research that can be put to the task of resolving the policy and operational collisions that allow cybercrime to grow unchecked today. In that pursuit, do know that APWG and APWG.EU and all of their formidable resources and networks are at the committee's disposal.

Patrick Cain,

APWG Resident Research Fellow

Peter Cassidy,

APWG Secretary General and Director

CEO, STOP. THINK. CONNECT. Messaging Convention