SHARING THREAT INTELLIGENCE TO MITIGATE CYBER ATTACKS

Cyber adversaries tend to use the same or similar infrastructure across multiple targets. Hence, an early warning system that enables threat-intelligence sharing between trusted partners could give potential victims the chance to put preventive counter measures in place. Real-time threat-intelligence sharing among trusted partners was the concept behind a Catalyst demonstration showcased at TM Forum's Management World in May. Its ground-breaking work has just been followed up in Phase II, by popular demand.

TM Forum's Security Management Program began working on cyber threat intelligence (CTI) in January 2013. Over the past 10 months it has attracted a huge amount of interest, greatly helped by the highly successful Catalyst project demonstration, *Sharing threat intelligence to mitigate cyber attacks,* which took place at TM Forum Management World in May 2013.

CTI sharing allows organizations to identify more threats, find them sooner, take action against them and reduce the costs – financial and otherwise – of being victims. As this process is repeated over time, organizations' knowledge bases expand, meaning they are better placed to keep pace with evolving tactics of adversaries.

Crowd-sourcing is the key to security

To these ends, the Catalyst project team created an architecture[1] and white paper[2] about why 'crowd sourcing' for intelligence is needed and then set about putting together a demonstration to pull it all together. The team leveraged mature technologies and standards and proved just how a trusted group can be brought together – quickly – in the form of the Catalyst's champions, vendors and supporters for everyone's benefit (see panel at right).

While technologists tend to focus on that aspect, this team invested considerable effort in understanding the business proposition of CTI. They took processes associated with distributed denial of service attacks (DDoS), mobile malware and malicious URLs (big data feed) with use cases across four personas: IT operations, security operations, threat analysts, and security executives. They also developed a CTI Sharing Calculator to understand return on investment.

The calculator enables organizations to input their own processes and determine savings resulting from information gleaned from the community. This community could include other staff in any organization, peers, supply chain and other business partners, or the crowd. It takes into consideration measurements like estimating the time needed to understand the threat both with and without CTI sharing to calculate a value and understand the efficiencies gained.

This calculator provides a quantitative linkage between technology teams and what CxO level executives need to understand the value of CTI to the business.

Secondly, the calculator includes a section for estimating the cost of an intrusion. It leverages data provided by RSA from

WHO DID WHAT IN THIS CATALYST PROJECT?

Champions: AT&T, DSTL (U.K. MOD), Orange, Telecom New Zealand and Telstra

Vendor Participants: cVIdya Networks, Edge Technologies, EMC/RSA, Microsoft, Symantec and ThreatConnect

Supporters: Bell Canada, Birmingham City University, MITRE and the Security Fabric Alliance

its own 2011 intrusion along with a *2010 Annual Cost of Data Breach* study from Symantec[3] to allow organizations to put a cost to an intrusion, both as a percentage of revenue and the number-of-records-compromised perspective.

The calculator is easy to use, and can be used by any organization regardless of size or industry.

Combining collaboration with automation

Leigh Reichel, Chief Financial Officer, Cyber Squared, had a hand in developing the CTI Calculator. He stated, "Bottom line [is] combining cyber threat intelligence with collaboration and automation platforms allows the trained cyber analyst to find more threats faster, and has substantial impact on both operational costs and revenue."

The live demonstration of the second phase of this Catalyst project was due to start almost as soon as we went to press, at TM Forum's Digital Disruption 2013 event in San Jose, California. Please contact Christy Coffey, ccoffey@tmforum.org, for more information or to get involved in the next phases of this important work.

Phase II expanded the scope of threats shared in the APT, mobile malware and DDoS areas. It aimed to harden interfaces, add dashboards for visualization and, importantly, show how responses to newly shared threat intelligence can be automated.

Participants included AT&T, Bell Canada, Birmingham City University, cVidya Networks, Edge Technologies, EMC/RSA, Microsoft, MITRE, Orange, Security Fabric Alliance, Symantec, Telecom New Zealand, Telstra, ThreatConnect (a division of Cyber Squared), and the U.K. MOD's Defence Science and Technology Laboratory (DSTL).

Visit the TM Forum's Cyber Security downloads page at: www.tmforum.org/cybersecuritydownloads.

[1]You can download our Threat-intelligence Sharing Guidebook with the architecture in it from the TM Forum's Cyber Security download center here: http://www.tmforum.org/cybersecuritydownloads.
[2]www.tmforum.org/threatintelsharewhpaper
[3] www.symantec.com/en/uk/about/news/release/article.jsp?prid=20120320_11

CATALYST PROGRAM: TM FORUM'S INNOVATION ACCELERATOR

What? The Catalyst program is the TM Forum's innovative approach to rapidly launching and creating leading-edge solutions.
Based on the most pressing requirements of end users such as service providers, MSOs, defense agencies, enterprise IT departments and others, teams of end users, system integrators and suppliers collaborate on a solution that culminates in a series of live demonstrations at TM Forum's major events.

These demonstrations both leverage and enhance TM Forum best practices and standards, including Frameworx (see page 43). The results are fed back into the TM Forum for use by the industry at large. Besides serving as a proving ground, Catalysts also enable end users to gain real-world insight to help guide strategic investment decisions.

Who? Participants can come from just about anywhere – from service and solution providers across communications, healthcare, utilities, financial services, cable and the digital services' spectrum. Each project has end-user champions such as service providers, MSOs, defense agencies and enterprise IT departments, including international banks, utilities companies and research universities.

Participants range from large suppliers to system integrators to start-up software companies. Anyone, business or technical, who is interested in discovering, addressing and solving critical industry issues is welcome to join in.

Why? Catalyst projects are a highly cost-effective and rapid ways to carry out collaborative research and development, using TM Forum best practices and standards and continually yield high quality results. Long-standing, close business relationships grow from trust and knowledge gained during project lifecycle.

For more information about the Catalyst program, please go to www.tmforum.org/catalystprogram and/or contact Megan Lunde, Catalyst Program Manager, TM Forum via mlunde@tmforum.org.