2018 TAG CYBER SECURITY ANNUAL

VOLUME 2

INTERVIEWS WITH CYBER LUMINARIES

Expert Advisory Research

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber

September 2018

TAG cyber

Security Outside the Firewall

Cyber security intelligence and response automation against external web, social and mobile threats have become critical controls in most enterprises.

Lou Manousos, CEO of RiskIQ

If there is one constant in cyber security, it is that nothing is constant. In the wake of business digital transformation, threat actors are impacting operations, customer trust, and brands through web, mobile, and social attack vectors. It is simply more convenient for hackers to exploit a business' online presence and exposures in an organization's attack surface. This offers accessible and lucrative targets to commit acts of fraud, misuse, and malicious activity, often duping users to gain access credentials, sensitive and financial information, and system control. Security teams must re-assess their security posture and apply resources, intelligence and controls to mitigate external threats and adversaries. Lou Manousos, CEO of RiskIQ, is an expert in this area, and he spent some time with us to discuss trends in digital threat management and the provision of advanced internet intelligence and response capabilities to support enterprise customers.

EA: What exactly is digital threat management?
LM: Organizations have embraced online mechanisms to enhance product stickiness, customer engagement, and their online ecosystem. Threat actors seize the digital opportunity as well; external threat actors now account for 70% of enterprise data breaches as per the latest Verizon data breach report. Phishing, malvertising, ransomware, rogue mobile apps, web site and app exploits, brand abuse, and fake social posts are all examples of threats that originate outside the firewall. Digital threat management extends visibility and control for organizations across external web, mobile, and social digital channels, and brings that into the fold of security operations. This is more than just threat intelligence data feeds, it is about enabling SOC, red, and blue team resources to gain the insight and automation necessary to efficiently execute tasks that identify, preempt and remediate digital security issues that directly affect their business.

EA: Why have so many CISOs not fully addressed digital risks regarding Internet-facing assets such as domains and broader phishing threats?
LM: Adversaries no longer must attack firewalls or maneuver laterally between systems to impact the IT organization and damage business. They can more easily phish with a fake email or online advertisement and website, exploit a susceptible web app or form, create a fake mobile app, or even target a weak affiliate site to feed malware. From our business perspective, most companies only know a small fraction of their Internet-facing assets that can affect their business, and many exposed and exploited assets were outside the purview of IT – and that is what has left companies and CISOs exposed. The sheer volume and respective dynamics associated with all the external assets connected to a business, from company sites and apps to those by service providers, affiliates and adversaries, has outpaced conventional defenses. The general presumption is that current controls, such as those provided by vulnerability scanners, pen testing, next-generation firewalls, and endpoint security will suffice, but *they don't*. For example, relying on point-in-time discovery against only known assets is a false sense of security in the digital world, and reliance solely on reputation services and endpoint updates does not address targeted attacks that are custom and zero-day. The key is intelligence and automation to close gaps in digital defense and to enable CISOs to align with business initiatives while mitigating risks.

EA: How does your team go about collecting and disseminating intelligence on external threats?
LM: We've taken on the investment, technology, and expertise to build out a substantial Internet reconnaissance system comprised of global proxy network, collectors, and scanning technologies to capture data in a variety of ways. We actively scan the entire IPv4 range as virtual users representing different browsers, regions and networks. We collect passive DNS and WHOIS information and more. We actively monitor thousands of mobile app stores and millions of apps. And we have relationships with seven of the leading social networks to actively track posting details. All this data is stored and curated in an elastic warehouse where we apply analytics in the form of correlation models, pattern matching algorithms, data science and research. While the data can be consumed as feeds for some organizations, we have three popular products delivered as SaaS web applications that leverage this data. Our Digital Footprint tool enterprises to understand, monitor, and remediate exposures in their digital attack surface and track their risk rating. Our External Threats tool allows the SOC to identify digital attacks, to triage the issue, and automate response. And our popular PassiveTotal tool enables incident responders and researchers to investigate external threats, adversaries and exploits.

EA: What sort of mitigations can be performed when an organization is under attack?
LM: Certainly, after you identify an external threat, you want your SOC and other security team members to be able to make informed decisions and act. In many cases, our correlation models unearth external threats as they are being weaponized – allowing the defense to preempt attacks. We have automated mitigation tasks across digital channels, and offer an extensive API set for interoperability with custom and popular security systems. For digital threats, including targeted attacks which utilize newly identified phishing and malicious sites, we can update blacklists for blocking within Firewalls and

web filtering tools. We can enrich threat data into SIEMs. And we can send our external asset discovery data into GRC and VA tools. In addition, the RiskIQ platform can dynamically submit phishing, scams and other malicious URLs directly to Google Safe Browsing and Microsoft SmartScreen to block these URLs within 95% of web browsers in a matter of minutes. For digital threats where the organization has little to no direct, immediate control over an external asset, our platform offers automated takedown workflow, and monitoring. This would cover such digital threats as domain, mobile, social, and brand abuses, where it requires contacting an entity for dispute and corrective actions, including their support infrastructure, such as registrars and hosting providers.

EA: Any advice for organizations in this area to get started? Can small companies afford to purchase digital threat management?
LM: Small to medium enterprises can and should perform an assessment of risk with regards to their potential exposure to digital threats. We have packaged our products to even accommodate organizations with limited means and resources. In fact, RiskIQ has a Community Edition of our tools that gives entry level access to our information and tools at no cost. This is for our PassiveTotal threat investigation tool and our Digital Footprint attack surface inventory tool. Also, many managed security service providers are offering a variety of digital threat management within their service portfolio. This would allow small companies to extend their digital defense capabilities.

Design – TAG Cyber LLC
Finance – M&T Bank
Promotion – TAG Cyber LLC
Facilities – WeWork, Fulton Street Station, New York City
Administration – navitend
Research – Liam Baglivo, Matt Amoroso, Miles McDonald
Lead Author – Dr. Edward G. Amoroso

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the author of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2018 TAG Cyber Security Annual volumes. The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.