silo
By Authentic8

EXPERT Q&A

Social Media Monitoring and Dark Web Investigations

Authentic8's National Security Engagement Lead and former CISO at the White House Matt Ashburn sat down with Forrester's Brian Kime to discuss cyber investigations, where they lead and their importance to private and public sector organizations. The two hosted a webinar featuring Kime, and continued the conversation in the following Q&A.

Kime is a Forrester senior analyst covering cyber threat intelligence, vulnerability risk management and industrial control system security. In this role, he helps organizations identify, assess, and prioritize cyber and physical threats; prepare for emerging attack vectors; and reduce cyber risk in enterprise IT and operational technology (OT) environments.

Social Media Monitoring

Ashburn: *We see social media sites and applications as rich resources for gathering information related to our investigations but are concerned we'll put ourselves and/or the company at risk. How should we get started? Do you have any "do's and don'ts" when it comes to social media?*

Kime: Your organization and your high-profile employees are more vulnerable than ever, which is why you need to integrate social media monitoring into your security strategy immediately. Here are a few recommendations for firms to manage social media risks.

- **Develop a framework and assess your social risk posture**
  Identify your most valuable social points of presence, actors and assets, and consider the consequences for your organization if those high-value accounts were compromised or impersonated. To determine value, consider the business influence and brand influence of those accounts as well as the data and people they are associated with.
- **Include social media in your security audits and threat intelligence**
  How people use and interact on social media continues to evolve rapidly, as do the tactics cybercriminals wield to exploit it. Cyber threat intelligence services can help track the methods the adversarial groups are using against organizations like yours. As the threat landscape evolves and new threats and use cases emerge, be sure to review your social media security posture with regular audits and vulnerability assessments.
- **Make social media risk training and awareness an annual imperative for all employees**
  Encourage your employees to verify that new social media connections are who they say they are by connecting over email, instant messaging or phone. Create training modules on how to identify email phishing and suspicious social media activity. Identify your most at-risk and valuable employees, such as IT system and domain administrators, high-profile executives, employees in finance or R&D, etc., and set stricter policies and technical oversight controls for them.

- **Consider limiting messaging features in social media**
  You may want to limit messaging features to only those who use it to speak on the company's behalf. And review your marketing team's security practices to ensure they don't share access credentials for your brands' social accounts; require that they access accounts through a social media management solution and reduce reliance on static passwords by requiring two-factor authentication (2FA). You should also actively monitor and protect your high-profile accounts for suspicious behavior and establish a process to monitor and submit takedown requests for fraudulent social accounts misusing your brand names and logos.

Dark Web Investigations

Ashburn: *Is tracking activities on the dark web really a need for corporations? Seems more applicable to government- and law enforcement-type investigations.*

Kime: Absolutely yes. While the dark web is primarily used by hackers for hire (either independent or state sponsored) who are trying to make a profit by selling stolen data, tracking the dark web can still be very valuable. For one, tracking the dark web helps corporations identify if their own data is for sale which might be indicative of a data breach or malicious insider activity. While you should still block access to the Tor browser and block Tor traffic at the firewall for all employees, enabling a small group of users with dark web access will provide additional insight about potential data breaches against other malicious activities targeted against your firm.

Proactive Threat Intelligence Gathering

Ashburn: *How do I convince upper management that we need to allocate resources to do more proactive threat intelligence gathering vs. just reacting after the fact all the time?*

Kime: Intelligence helps decision makers reduce risk and uncertainty. Boards of directors are concerned with managing reputational and regulatory risks to preserve stockholder value. Therefore, intelligence should always lean towards being proactive by assessing the organization's threats' intent and capability to breach or attack the organization. More tactical and operational benefits to threat intelligence include:

- Reducing adversary dwell time and mean time to recover by providing intelligence to the incident response team
- Improving the signal-to-noise ratio of the security operations center by providing more complete, accurate, relevant and timely information on new and emerging threat activity
- Driving threat hunting via robust assessments and models of an organization's threats; via threat hunting, the security team is able to build new, more relevant detections and improve alerting
- Designing and deploying security controls relevant to the organization's threat landscape

Managed Attribution vs. Incognito Mode

Ashburn: *How useful/important is actively managing attribution versus, say, being very cautious and making sure to use incognito mode in my browser?*

Kime: Users tend to think 'incognito mode' or 'private browsing' conceals their activity from all snooping, when the reality is those privacy modes do not prevent websites, ISPs, your employer or school from logging your activities, tracking your presence and attributing your browsing to your organization. For any user who conducts sensitive research or intelligence collection outside the corporate network, it is vital that we covertly access those hostile resources so that we do not give away our presence or intelligence requirements to our adversaries. By actively managing our own attribution (vice attributing cyberthreat activities to criminals or state organizations) we preserve our operational security and reduce the likelihood and consequences of a threat detecting our research or our intelligence collection.

The more organizations know about their adversaries, the better they are equipped to prevent attacks, identify fraud, and find weaknesses in their security posture. Researchers use all available tools to gather intelligence on suspected attackers, follow up on threats, and track down perpetrators. To protect threat hunters and their missions, organizations need to implement specialized strategies, policies and controls; and arm their researchers with tools and frameworks that can prevent accidental exposure to malware, mask their location and identity, and conceal the true intent of their investigation.