KEY PERSONNEL ONLINE FOOTPRINTING SERVICE
PROFESSIONAL SERVICES

The perennial weak point in any security system is the human element. Key personnel are constant targets of hackers because of their financial transaction authority, network privileges, access to sensitive business information, or their figurehead status. Key personnel can include senior executives, board members, and others in positions of financial, technological, or informational privilege.

Organizations face attacks from adversaries with a wide range of agendas and capabilities:

- Fraudsters seeking financial gain
- International organized crime and ransomware gangs
- Nation states conducting espionage
- Competitors performing business intelligence
- Hacktivists doxxing executives and defacing websites
- Disgruntled elements such as extremists or former employees

BlueVoyant investigative experts are ready to perform an open-source, dark web, and social media investigation in order to provide a footprint of your organization's key personnel to mitigate potential vulnerabilities presented by online exposure.

BUSINESS EMAIL COMPROMISE (BEC) MITIGATION

In a BEC attack, cybercriminals target personnel with access to your organization's funds and deceive them into making wire transfers to bank accounts that appear to belong to business partners, but are actually fraudulent and controlled by criminals.

The most successful BEC attacks typically occur by phishing key personnel and gaining control of their email inbox. The sophistication of these attacks has reached a zenith in recent years. The FBI warns that BEC attacks are now "carried out by transnational criminal organizations that employ lawyers, linguists, hackers, and social engineers." [1]

SHORING UP THE BEACH HEAD

Reducing the possibility of social engineering attacks also mitigates against the introduction of malware into your organization's network. If a key individual is spearphished or tricked into opening a malicious document, attackers can gain access to sensitive data by installing information stealing malware or disable your organization by dropping ransomware on the network.

AUDITING SOCIAL MEDIA PRESENCE

Your organization's most empowered individuals have personal lives. And just like everyone else, they can sometimes have accounts that unwittingly share more information than is appropriate or secure enough relative to their duties. BlueVoyant investigative analysts will identify all of the social media accounts associated with a key individual and scan for insufficient privacy standards, inappropriate postings, or disclosures that can form the basis for an effective social engineering attack.

PERSONAL SAFETY ASSESSMENT

Executives can be the target of disgruntled elements, ranging from activists to potentially violent extremists. BlueVoyant analysts have insight into these potentially violent communities hosted on the surface web and in the dark web. If your organization's personnel are mentioned in threat actor chatter in the context of a dangerous conversation, we can alert you to the threat in order to take appropriate precautions.

This is particularly important in the context of travel to major events or can be used for extra security during a Public Relations response.

[1] *https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise*

KEY PERSONNEL ONLINE FOOTPRINTING SERVICE
PROFESSIONAL SERVICES

SUMMARY

INVESTIGATION ELEMENTS

BlueVoyant employs expert Open Source and Dark Web Intelligence Analysts who leverage cutting-edge investigative expertise.

Additionally, BlueVoyant has access to a range of state of the art investigative resources to provide our clients with unparalleled insight into the online footprint of your organization's key personnel.

A Key Personnel Online Footprinting Report comprises the following:

- Comprehensive Open-Source (OSINT) survey of the key individual's online presence;
- Comprehensive Dark Web investigation and analysis;
- Social media footprinting and analysis;
- Assessment of leaked Personally Identifiable Information (PII);
- Compromised credentials and email account breach investigation.

PROACTIVE SECURITY BENEFITS:

- Mitigate spearphishing and other social engineering attacks to prevent business email compromise and malware infection;
- Identify "doxxes" of key personnel by hacktivists, extremists, or other disgruntled elements;
- Physical security preparation before major events such as international conferences, business summits, extended vacations, and PR campaigns;
- Audit and reduce a key personnel's online exposure;
- Audit and respond to key personnel's account exposure;
- Identify and mitigate password reuse or insufficient password practices.

BLUEVOYANT PROFESSIONAL SERVICES

BlueVoyant combines proven front line experience responding to advanced cyber threats with expertise in building world class defensive cybersecurity programs to stop threat actors in their tracks.

Our team's knowledge of attacker methodologies matched with our access to the latest threat intelligence enables us to fully prevent, assess, respond, and remediate your cybersecurity events.

BlueVoyant is armed with decades of real world cyber investigative experience within every major industry.

Whether you are dealing with insider threats, a ransomware infection, business email compromise, or a complete malware based network compromise, BlueVoyant has the tools and experience to make sure your organization is able to eliminate the threat and ensure protection of your brand, reputation, and assets.

CONTACT US

Have you experienced a breach event and need assistance? Please contact the BlueVoyant Incident Response team at incident@bluevoyant.com.