

---

# Detecting advanced cyber intrusions & cyber-based economic espionage

## Advisory services

### Forensic services

#### A proactive breach indicator assessment

There is one common denominator in all cybercrime investigations: digital evidence was present in the environment long before the victim organization became aware. In our experience, advanced transnational criminal enterprises often maintain remote access to the target environment for 6-18 months before being detected. For state-sponsored cyber intrusions, unfettered access lingers on for years and sometimes is never detected. Further, detection usually does not involve in-house technology, processes, or people. Rather, detection comes in the form of a tip from domestic law enforcement, a customer, a business partner, or some other third party.

When foreign governments, organized crime, or a corrupt competitor targets an organization, the techniques employed to compromise the network and steal sensitive data are well-planned and methodical. Foreign governments in particular are very patient and invest heavily in the research and development of custom malicious code and sneaky data exfiltration techniques. The purpose of today's advanced cyber threats is two-fold: steal the target data and maintain access to the environment for as long as possible. Although this was always the purpose of foreign governments, it has become the mantra of the other cyber threat groups as well. What is particularly clever about these advanced cyber attackers is their ability to quickly understand the victim environment once they achieve network penetration and then use authorized access credentials, network protocols, and programs to deepen their infiltration and hide in plain sight. If discovered, they simply unleash custom developed malicious code to remain under the cyber security radar.

Signature-based and rule-based detection and prevention technology, like anti-virus, firewalls, and IDS/IPS is no match for malicious software (malware) developed by patient, highly motivated, and well-funded adversaries. These technologies will only detect/prevent what is known thus rendering them ineffective against advanced cyber threats. Also, a methodology of the state-sponsored threats is to reduce their file system footprint and primarily operate within live memory. Then, they use counter-forensic utilities to wipe files created by the attacker, and ensure that remote access is maintained by employing a persistent technique that will survive a reboot or even a re-image.

Today's cyber-based economic espionage committed by advanced cyber threat groups is not solely focused on user-created files stored on hard drives and shared drives. The email content of key personnel has become a primary target as this information provides near real-time intelligence of business dealings. **Our recent investigative experience has determined that some cyber threat groups are specifically stealing the email of those people involved in business deals outside of the United States.** Such an email theft campaign is not confined to the organization involved in the merger or acquisition: **Outside counsel of those organizations also becomes a target.** Again, using the same stealthy techniques to compromise the law firm's network, steal data and email, and establish a long-term foothold.

#### What to do?

How can an organization determine if its environment has fallen victim to an advanced and persistent cyber intrusion that is currently evading detection by in-house technology, processes, and people? Using real lessons learned from the forensic investigation of such cyber incidents in a reactive capacity for our clients, PwC offers an innovative Breach Indicator (BI) Assessment which can include all or some of the following:

**Log BI assessment:** PwC works with client personnel to gather logs from a variety of systems and technologies then PwC practitioners review these data sets for specific indicators relevant to the advanced techniques unveiled from our Incident Response engagements. On the surface, this evidence often appears as legitimate system and user behaviors. PwC produces a report of findings and recommendations.

---

# Detecting advanced cyber intrusions & cyber-based economic espionage

## Advisory services

### Forensic services

#### A proactive breach indicator assessment

##### What to do?

**Host-based BI assessment:** Leveraging the technology of a PwC Joint Business Relationship, we deploy this technology within our client's environment and scan the entire enterprise or a subset of systems for BIs. This assessment **identifies suspicious activity within live memory** on the endpoint systems under assessment. BIs are triaged for relevance and PwC produces a report of findings and recommendations. We can also deliver- this solution as an ongoing **Managed Service which scans hosts weekly** from our forensic lab and we provide a weekly report of findings.

**Network-based BI assessment:** Leveraging the experience of a PwC Joint Business Relationship which has helped government agencies detect advanced cyber intrusions, we collect network traffic for an agreed-upon period of time then analyze that traffic in a lab for BIs, such as inbound traffic from hostile hosts on the internet, exfiltration of data, and unusual system-to-system connections within our client's environment. PwC produces a report of findings and recommendations.

#### Disrupt the spread of compromise, revenue loss, and lurking legal/regulatory/reputational risks

Is your environment compromised? Are data and/or email being pushed out of your environment? Our proactive services help clients understand if they are compromised but do not know it. The right type of BI Assessment, or combination thereof, is a factor of our clients business, its industry, its areas of operation, and its business partners and contractors, and of course budget. We welcome the opportunity to discuss the right approach that meets your needs.

Leveraging our reactive cybercrime investigative lessons enables you to improve your cyber security posture and reduce a myriad of risks in creative and innovative ways. PwC's cybercrime services can be engaged to assess an organization's cyber space for indications of malicious activity that is not being detected by in-house technology and people. Conducted under the privilege of a legal risk assessment, the findings of our proactive cybercrime assessments are protected and can be quickly used to neutralize an in-progress attack or reduce the risks associated with a successful compromise.

For more information, please contact

#### Dave Burg

(703) 918 1067

david.b.burg@us.pwc.com

---

#### Shane Sims

(703) 918 6219

shane.sims@us.pwc.com

---

#### Ed Gibson

(703) 918 3550

ed.gibson@us.pwc.com

---

#### Kimberly Peretti

(703) 918-1500

kimberly.k.peretti@us.pwc.com

---