

Q&A: Cyberintelligence

Avivah Litan

Cyberintelligence enables enterprises and government agencies to detect many types of threats and thwart their ensuing damage. Cyberintelligence extends an enterprise's security "radar" outside the perimeter of its own organization, highlighting threats that otherwise likely would not be seen.

STRATEGIC PLANNING ASSUMPTION

Adoption of cyberintelligence services by government security agencies could catapult this market to well more than \$100 million in revenue by 2011. During the next five years, Gartner expects increasing recognition of the need to extend the security net outside of the enterprise, and use of cyberintelligence services will be considered a much more common practice for enterprise-class organizations than they are today.

ANALYSIS

Cyberintelligence is a continually evolving Web-based intelligence service that has its roots in anti-phishing and brand-monitoring services. For the past five years, most of these services helped enterprises detect phishing attacks before or soon after they were launched against their customers, or they protected enterprise brands by searching for and stopping abuses of trademarks, counterfeit activity, loss of intellectual property, copyright and other brand infringements (see "Toolkit: A Checklist for Brand-Protection and Anti-Phishing Controls," "Brand-Monitoring and Anti-Phishing Vendors," "Evaluating Brand-Monitoring and Anti-phishing Services" and "Brand-Monitoring and Anti-phishing Services Intersect Several Security Markets"). Many more use cases for cyberintelligence have since emerged, and the services are now being used to detect and thwart many more types of threats outside the virtual and physical borders of an organization. Some of these newer use cases include detecting homeland security threats, monitoring suspicious employee activities outside of work and protecting company executives from would-be wrongdoers such as kidnappers. Technologies used in cyberintelligence primarily consist of crawling and searching the Web so that desired information can be found, and monitoring peer-to-peer (P2P) file traffic on public networks for specific keywords or phrases.

Despite the usefulness of cyberintelligence in promoting security outside an enterprise's organizational boundaries, and in detecting threats that cannot be seen inside the enterprise, the cyberintelligence market, now worth less than \$50 million in annual revenue, has been relatively slow to take off — most probably because most enterprises don't begin to fathom its usefulness until after they are hit by an attack that could have been previously spotted on the Internet and, therefore, stopped before any damage was done. At less than \$150,000 a year (for most small-to-midsize implementations), these services can be a bargain if the threats and potential damage unearthed by them are addressed in a timely and responsive fashion. Most organizations, however, are not staffed adequately to deal with externally uncovered threats, and have little mind share left over after they tend to security functions that guard information and assets inside their organizational boundaries.

Still, Gartner believes the cyberintelligence market will grow at double-digit rates during the next five years, largely because of a reported \$17 billion budgeted to be spent during the next five years on U.S. cybersecurity as the U.S. Homeland Security agencies dole out new contracts for President Obama's cybersecurity operation. Cyberintelligence will have a role in defending the U.S. against cyberthreats and cyberattacks launched from unfriendly parties — often in foreign countries such as China and Russia — that threaten U.S. national infrastructure and military installations. Already, one large defense firm, QinteiQ, a London-based research and defense contractor firm with a separate U.S. division and about \$3 billion in revenue, acquired a small cyberintelligence services firm, Cyveillance, for \$40 million with a possible additional \$40 million in earn-outs. Cyberintelligence services can be particularly helpful in spotting leaked or stolen secret information, which, when in the possession of the "wrong hands," can lead to serious national security threats.

Question: What is cyberintelligence?

Answer: Cyberintelligence has several meanings and components:

- Cyberintelligence services search the Internet on behalf of institutional, corporate, and individual paying clients searching for evidence of a threat or potential attack against them and helping them take action to protect themselves.
- Cyberintelligence gathers and analyzes information transmitted and/or stored on the World Wide Web.
- Cyberintelligence uses a diverse set of technologies to make sense out of vast amounts of information, including automated threat detection and heuristic analytics.

Question: What are the best practices in cyberintelligence technology and services?

Answer: Suppliers of cyberintelligence technology and services should have:

- Broad and deep search and detection capabilities.
- Ability to scour the hidden corners of the Internet that are not visible to public search engines, such as Google. This is important because data can be hidden from Web crawlers or simply hidden behind Completely Automated Public Turing tests to tell Computers and Humans Apart (CAPTCHAs) or passwords.
- Ability to perform contextual cross-analysis of URLs embedded in various sources such as spam e-mail.
- Multilingual capabilities (threats come in all languages).
- Access to multiple sources for information. For example, information can be found from or on Web crawling, spam filtering, message boards, Internet Relay Chats (IRCs), public forums, auction sites, botnet command and control servers, stolen data drop points, Internet advertising, and public peer-to-peer file-sharing networks.
- Timely and effective incident response capabilities. This means the vendor should be able to perform takedown services, which refers to taking down the Web server used to launch an attack or offense. The time required to take down a site is a key performance measure, because the longer the offending site is up, the more damage it can cause. Often, it is very problematic to take a site down because it may be located in a foreign country, at an uncooperative ISP, in a remote unmanned location or on a server in a decentralized botnet army. Still, most attacks can be taken down within four hours.
- Data dilution capabilities, which means that the cyberintelligence service creates sessions that look like real victims falling for an attack. However, it is, instead, feeding the perpetrators bogus data — such as invalid user IDs and passwords. In these instances, care must be taken to not exacerbate the criminals' malicious activity, which could potentially worsen if they believe they are in a temporary cyberwar with a data dilution service.
- A broad line of services where multiple use cases can be supported. These can range from detecting and preventing intellectual property theft, financially motivated attacks, threats to health and safety of employees, etc.

- A strong analytical team.

While machine-based searching and analysis is essential to finding the bad "needles in the haystack," a good cyberintelligence service still requires human analysis and judgment of the results that are unearthed by the systems. This requires that the cyberintelligence service employ a team that is well versed in research and analytical skills.

Question: What does industry momentum and demand look like for cyberintelligence services?

Answer: Despite more than five years since these services launched, the vendors serving this market still only earn less than \$50 million in annual revenue. That is largely because clients are most likely to contract for such a service only after experiencing a destructive incident, such as:

- A phishing attack
- Lost sales and damaged reputation, for example due to counterfeit sales using a company's good name and brand

Most enterprises are so focused on securing their systems and processes within their organizational perimeters that they don't think about all the threats that exist outside their perimeters.

Threats are increasing quickly, and potentially exponentially, as virtual enterprise boundaries expand with Web 2.0 and as employees use social networks like Facebook and Twitter, along with music and file sharing from their corporate PCs.

Question: What are some of the use cases for cyberintelligence?

Answer: Some use cases are:

- Anti-phishing services — consisting of detecting phishing attacks and taking them down — are the oldest use case for cyberintelligence services, and have been around for more than five years. Still, some aspects of phishing attacks are still on the rise (see "The War on Phishing Is Far From Over"). More than 5 million U.S. consumers lost money to phishing attacks during the 12 months ending in September 2008, a 39.8% increase over the number of victims a year earlier.
- Counterfeit detection and takedown. The sale of counterfeit merchandise across the globe is especially prevalent in the retail and pharmaceutical industries. Some of these cases can be life-threatening — for example, dangers are high when counterfeit drugs are sold that don't deliver the medical treatment required and expected. Other dangers have unfolded — for example, when counterfeit baby formula tainted with lead paint was sold using known brand names, or when fake diabetes test strips were inserted into boxes with real ones and then sold as a package to unsuspecting customers.
- Executive protection, such as threats against CEOs. There have been several cases of disgruntled, laid-off employees who have stalked their former CEOs and their families, figuring out, for example, the CEO's and his/her family's habits. This included their recreational activities (such as what time the wife goes to gym or when the family goes on vacation), and noting where, when, and how their children go to school. They then use this information to launch threats against the family in exchange for ransom, or even have engaged in petty crimes such as throwing rocks at the windows of a CEO's home, if the CEO and his family are on vacation and not resident therein.

- Detecting enterprise IT security failures (weaknesses). There are many examples of sensitive corporate IT security information being inadvertently shared with malicious users on the Internet.
- Detecting theft or abuse of intellectual property, for example:
 - Documentation marked proprietary for internal use only that presents lists of people's names, Social Security numbers, salaries, etc.
 - Formulas, patented designs, processes, and other R&D material that is improperly disseminated (shared) on the Internet or available through P2P shared directories.
 - Business plans, merger and acquisition (M&A) agreements, pricing, or confidential customer information that mistakenly got out of the confines of the corporate network.
- Detecting stolen customer data being posted for sale on underground forums by former employees. Laid-off employees selling stolen customer data have been seen boasting about their credentials — for example, being a former chief information security officer (CISO) or Microsoft-certified developer — to gain credibility with underground forums where they sell their data.

Question: What should enterprises look for in a cyberintelligence solution and service provider?

Answer: Solutions and service providers should:

- Have expert detection capabilities.
- Be able to identify attacks before they launch or do damage.
- Search the "hidden" Web and leverage multiple sources.
- Have fast takedown services. Lost time means lost money.
- Possess analysis and forensic capabilities.
- Be a "trained" machine.
- Have trained people to operate the system.
- Have reporting and notification services.
- Be capable of prioritizing alerts/incidents and workflow/routing.
- Be capable of providing diligent, upfront preparatory work undertaken by the service provider as well as the enterprise client to identify threats, threat severity levels, workflow of threats to the responsible personnel, response strategies, etc. Without these preparatory steps, the information uncovered by the cyberintelligence service will fall through the cracks, thwarting threat prevention efforts.
- Be capable of after-the-fact reporting.
- Provide postincident information so that enterprise staff can learn from the incidents and stop them from happening again.
- Provide 24/7 operations and support, because that's how the threats and attacks work.

- Have the staffing available to work closely with the enterprise to continuously fine-tune detection and reporting to reflect evolving requirements.
- Be considered a broad and deep cyberintelligence solution.

Enterprises should look for a solution that does not just focus on phishing or brand protection, because one type of attack can morph into another. A cyberintelligence service that can catch this transformation is preferable.

Question: What do user enterprises need to do to make cyberintelligence services useful to them?

Answer: Pinpoint the business problem you are attempting to solve before engaging a cyberintelligence service.

Make sure you define clear business ownership and ensure you have requisite staff resources for dealing with information unearthed by these services, so that it is used to take action against offensive activities. Otherwise, cyberintelligence services may be a wasted investment.

Demand and analyze after-the-incident reporting from service providers to help defend your enterprise from similar attacks in the future.

Question: Which vendors provide cyberintelligence services, and how much do they cost?

Answer: There are several cyberintelligence services vendors that come from various different pedigrees with many technical competencies in common, such as takedown services, heuristic analysis and extensive search capabilities. While the technology is becoming somewhat commoditized, each vendor typically has its own service differentiators and challenges. Representative vendors include Branddimensions, Cyveillance (recently acquired by QinetiQ), MarkMonitor, New Momentum, RSA, the Security Division of EMC, and S21sec. Tiversa also participates in the cyberintelligence field; however, its core technology differs in that it is the only one that specializes in and performs P2P file transfer monitoring over public networks.

Vendors usually charge between \$12,000 and \$100,000 per year per module. Subscription fees also depend on the number of languages supported, level of customer service, and number of brands and domains monitored. Setup costs and professional services are extra.

RECOMMENDED READING

"The War on Phishing Is Far From Over"

"Toolkit: A Checklist for Brand-Protection and Anti-Phishing Controls"

"Brand-Monitoring and Anti-Phishing Vendors"

"Evaluating Brand-Monitoring and Anti-phishing Services"

"Brand-Monitoring and Anti-phishing Services Intersect Several Security Markets"

"QinetiQ/Cyveillance Deal Will Boost Cyberintelligence Market"

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509