



September 1, 2011

## Breaking the Next Case

By Deb Radcliff

<http://www.scmagazineus.com/breaking-the-next-case/printarticle/209773/>

**Ever-evolving strategies and technologies are just some of the issues facing today's cybercrime investigator, reports [Deb Radcliff](#).**

An email snagged by the FireEye inline sandbox was destined for an employee working on a sensitive R&D project. The message contained detailed information about the employee and past projects he worked on with another colleague, from whom the mail portended to come.



"The email was convincing enough to make even the most discriminating employee click the link," says Mark Leary (*left*), CISO of TASC, a professional services company servicing U.S. intelligence, defense and other agencies of high interest to foreign governments, terrorists and hacktivists. "When we investigated further, we realized the spear phisher got the information over LinkedIn."

While nothing got through to the employee and no harm was done, what keeps Leary up at night is knowing that adversaries intent on espionage against his government clients are always out there – in large numbers. These attackers are funded and organized, and often are beyond the reach of the law while continually advancing their intrusion and evasion technologies.

"What we're looking at is the blurring of cybercrime, cyberespionage and cyberwarfare," says Ronald Deibert, director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs at the University of Toronto. "These activities have exploded, and criminals still have relative impunity from investigations because so many of these attacks are launched from outside the country."

The majority of the latest cyberthreats are highly automated programs looking for low-hanging fruit on which to install botware and trojans, says David Koretz, president and CEO of Mykonos. The good news,

he adds, is that law enforcement and service providers are getting proficient at investigating this type of attack.

However, more advanced threats, like those observed in Mykonos deception traps used to protect websites, are much harder to investigate, particularly in cases of state-sponsored cyberterrorism and sophisticated organized crime.

Koretz is referring to so-called APTs (advanced persistent threats), which, over periods of time, manage to get inside systems and remain hidden to siphon money and valuable financial data and intellectual property.



Chris Novak (*left*), managing principal for the investigative response unit at Verizon Business, says that while the term “APT” is being overused by victim organizations, today’s attacks are more often seeking intellectual property to sell to well-financed buyers.

“We had one case where a phone was actually brought into a store for repair before that model had even been released on the market,” says Novak. “This was reported to the phone manufacturer and when we investigated, the network activity led to a contractor’s PC.”

While there have been a growing number of arrests and prosecutions in cases of international cybercrime, there’s still a need for more global cooperation, says Richard Bejtlich, CSO of Mandiant and VP of the network intelligence firm’s Computer Incident Response Team.

The volume of evidence produced by so many of today’s different types of crime, along with the growing attack surfaces from which to gather evidence, are causing backlogs in investigations while highlighting the need for new standardized tools to support new forms of investigations.

For example, Jim Christy, retired special agent and director of Future Exploration for the Department of Defense Cybercrime Center, points to mobile phones, e-readers, iPads/notebooks, smartphones and backup media devices – all of which have different operating systems, and versions that call for specialized evidence recovery tools.

While there are solutions available for different phones and storage devices, standardization of how these platforms collect and store data for imaging and searching would greatly help investigators, Christy (*right*) says.

Then there’s investigating in the cloud. For example, how does one search someone’s mail when they keep it in the Gmail or Yahoo cloud, asks Duncan Monkhouse, international president for the High Tech Crime Investigative Association.



“The cloud cases are there,” says Monkhouse. “How the evidence is gathered, verified and used to prove culpability are all different in the cloud.”

He describes one case that involved DropBox, Microsoft instant messenger, Gmail and Yahoo accounts all in the cloud. After initial imaging of the suspect’s computer memory, investigators searched through the browser history to find these accounts and their login names and passwords.

Then they used another mobile application to download the contents of these web accounts to a folder on an evidentiary backup disk and copied that to another disk for searching. This folder was imaged to create a working copy for analysis.

So despite the medium in which the data is stored, the initial steps of evidentiary gathering – preserving and imaging the evidence – still applies, says Kimberly Peretti (*right*), director of PricewaterhouseCooper’s forensic technologies practice and former prosecutor for the U.S. Department of Justice.



“Investigations are becoming more difficult, but there are also new sources of information and evidence trails left behind,” says Peretti, who calls this time period the “era of cybercrime.”

For example, at least one new type of threat – hacktivism – is actually leaving evidence trails that are leading to arrests and prosecutions. Collectives, such as Anonymous and LulzSec, post data they’ve taken from government, commerce and gaming sites, and when they talk about their exploits on blogs and Twitter, they’re leaving clues behind that can be followed and linked together, Peretti says.

As new bad actors and attack surfaces enter the cybercrime scene, there has also emerged a demand for skills that exceeds supply. Mandiant’s case-load is growing significantly every year, which is causing backloads of from two weeks to two months, even though the company says it is continuously training and hiring.

The U.S. Department of Defense Cybercrime Center is also experiencing exponential growth of investigations – as well as volume of data to be processed, says Christy.

To develop new talent and tools, Christy’s agency sponsors an annual “Digital Forensics Challenge,” which drew participation from more than 920 teams this year who presented at the DoD’s annual Cybercrime Conference in January.

“In today’s investigations, almost every case has a cyber element,” Christy says. “For that, we’re going to need an educated workforce – and more tools.”