This third in a series of four articles by Kathleen E. Hayman, Michael Miora, CISSP-ISSMP, FBCI and Allen P. Forbes presents discusses the environment or climate affecting the activities of cyber pirates and privateers.

One of the interesting differences in recent years is the rise of targeted attacks, in which specific organizations are being attacked using malware of different kinds. Mikko Hypoonen, Chief Research Officer of F-Secure, has a useful nine-minute lecture on the topic on YouTube that provides an excellent introduction to the problem.<http://www.youtube.com/watch?v=nFw9ZH0y0V3c>

This article looks at targeted attacks in India, China, the Pacific Rim and Oceania.

India

Corporations and financial institutions operating in India pose a serious cyber security threat since many multinational corporations outsource functions such as technical support and customer services to India. This outsourcing makes India an ideal location for learning vulnerabilities specific to a target and for collecting personally identifiable information (PII) and other information that could be used to conduct spear phishing<http://www.fbi.gov/page2/april09/spearphishing_040109.html> and other attacks.

In India in particular, the insider threat is significant due to the close-knit nature of Indian operations. If employees are not sufficiently vetted prior to hire, an entire insider organization could, in theory, penetrate outsourced operations. According to a July 2009 report from the UK National Endowment for Science, Technology and the Arts (NESTA), “…the biggest incentive to work in a call centre [in India] is to be able to hack the bank accounts and illegally withdraw millions from bank customers.”<http://www.nesta.org.uk/assets/Uploads/pdf/Research-Report/cybercrime-report-NESTA.pdf>

The national Indian government is highly motivated to protect and cultivate its online industry. For example, many major city police departments have cyber crime investigative elements. There are also national initiatives and legislation aimed at reducing cyber crime.<url>

China

China is thoroughly permeated with technology,<url> with a government that does not always distinguish between legitimate and illicit business practices.<url> China is a highly potent and dangerous environment for cybercrime whose tentacles have worldwide reach.<url>

According to a team of Canadian researchers,<http://www.f-secure.com/weblog/archives/ghostnet.pdf> a Chinese network, apparently sanctioned by the Chinese government, “…controls approximately 1,200 infected computers internationally,
including such ‘high-value targets’ as Indonesia's Ministry of Foreign Affairs and the Indian Embassy in Kuwait, as well as a dozen computers in Canada.”

This network, known as GhostNet, is believed by the Canadian team to be controlled by the Chinese government for intelligence purposes. The Chinese government has denied these allegations.

However, if this and other reports are accurate, there is little reason to expect sufficient Chinese law enforcement support for private cyber security when the government engages in illegal activity itself.

Many of the computers infected by GhostNet were Windows-based. The main tool employed by GhostNet was identified by only 11 out of 34 virus scanners the Canadian team used. The team strongly recommended switching to an open-source system, such as Linux, to reduce the likelihood of targeting and penetration. The main tool GhostNet used was a Chinese-designed Trojan horse software program known as Ghost Rat commonly available on the Internet.

According to one team member:

“What GhostNet reveals...is that a large swath of high impact political and economic targets can indeed be compromised, including ministries of foreign affairs, embassies, and international organizations. Many of these organizations were compromised for many months, without their knowledge, and the attackers had potential access to all sorts of sensitive documents, and even had the ability to eavesdrop on classified meetings through the activation of web cameras and listening devices. Although most governments have invested heavily in secure methods of communication, many have not. This is particularly the case in the developing world where information security is often a distant priority next to other goals, such as the elimination of poverty or even simply access to information.”

Pacific Rim/Oceania

Australia and other South Pacific nations appear to be actively grappling with cyber security. According to MIS Asia, a significant proportion of cyber attacks in Australia are actually based in Japan, due to good connectivity between the two countries. According to Philippines Department of Justice Assistant Secretary Geronimo Sy, 70-80% of complaints concerning online activity in the Philippines were incidents of “character assassination.”

South Korea has recently attempted to gain more control over Internet use within its borders. A blogger with the pseudonym of Minerva who predicted the collapse of Lehman Brothers and the sharp decline in South Korea's currency was arrested for promoting economic instability. Although Minerva was acquitted, the South Korean government has continued to closely monitor online economic activity and commentary.

South Korea continues its “real name” system, which requires users to provide their government ID number in order to post online, and a law was proposed in February as a result of the Minerva case to hold those who post anti-government rhetoric online liable for prosecution. [MK]
comments: the notion that suppressing free speech is a useful tool in the fight against cybercrime is problematic.]

South Korea is taking extreme measures to regulate Internet use without hindering private business. However, the cyber crime threat remains real for South Korea. In July 2009, a botnet was used for a distributed denial of service (DDOS) attack on US government agencies, media outlets, and South Korean financial institutions. The attack was unusual in a number of ways, one of which was the fact that the botnet was restricted to 180,000 computers, nearly all located in South Korea. The botnet was unusually small, and appears to have been designed specifically for the attack.<http://www.computingsa.co.za/article.aspx?id=1048560>

Africa

Africa is expected to continue and perhaps increase its involvement in cyber crime. Nigeria continues to be a common source country. New fiber optic cables installed earlier this year to increase connectivity in East and Southern Africa. Concerns regarding the targeting of local networks are commonly expressed. However, the possibilities run both ways, and local Nigerians are regularly recruited into aiding cyber crime.<http://www.businessdailyafrica.com/Company%20Industry/-/539550/651592/-/u787jtz/-/

South Africa displays traits that the BRIC (Brazil, Russia, India, and China) countries possess such as what Misha Glenny in McMafia <http://www.amazon.com/McMafia-Journey-Through-Criminal-Underworld/dp/B002RAR108> describes as “steep levels of poverty and unemployment; a high standard of basic education for a majority of the population; and a strong presence of more traditional organized crime forms;” it may yet become another Pirates’ Cove.

At present, however, South Africa is still in the throes of establishing cybercrime laws.<http://www.iol.co.za/index.php?set_id=1&click_id=15&art_id=vn20060711041205244C326588>

South Africa does not yet compete economically with the BRIC nations. Its standards of education were damaged by apartheid policies, from which the country is still struggling to recover.<http://www.southafrica.info/about/education/mediocrity.htm> One of the studies that may shed light on the current computer crime situation in South Africa is being conducted by three members of the University of Cape Town; it will be interesting to see what they publish.<http://mybroadband.co.za/vb/showthread.php?t=183195>

In the last of these four articles, the authors examine issues of defense against cyber pirates such as passive defenses, such as firewalls, anti-malware and other conventional defenses, and active defenses such as counter attacks.

* * *

The authors welcome comment from the wide variety of people who will be offended by the generalizations about crime in specific regions of the world published in these articles. Ripostes containing references to published studies are particularly welcome.

* * *

ABOUT THE AUTHORS

Kathleen Hayman is an analyst with the US Department of Justice, and she has been a consultant with Certico Corporation<http://www.certicoglobal.com> for three years. She can be reached at Kathleen.Hayman@gmail.com.
Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute (<http://www.thebci.org/>)(FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation, (<http://www.contingenz.com>) a specialty consulting firm and the developers of IMCD Business Backup. (<http://www.contingenz.com/IMCD>) He can be reached via email at mmiora@contingenz.com or mmiora@miora.com.

Allen Forbes is currently the President of Certico Corporation (<http://www.certicoglobal.com>) serving large critical infrastructure providers in all matters concerning security. A 28-year veteran in the US Marine Corps and currently a member of the US Marine Corps Reserve, Forbes has served in a number of senior logistics, operations, intelligence, and security positions in both the government and private industry. He can be reached at aforbes@certicoglobal.com.

M. E. Kabay, PhD, CISSP-ISSMP (<mailto:mekabay@gmail.com>) specializes in security and operations management consulting services. CV online. (<http://www.mekabay.com/cv/>)

Copyright © 2009 Kathleen E. Hayman, Michael Miora, Allen P. Forbes & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.