Enterprise wages a new war against hackers

Rory Crump

Big U.S. companies tired of being hacked are striking back in a vigilante effort to stop cyber criminals and Internet espionage. Angry and frustrated over continued security breaches, enterprise security teams are taking justice into their own hands after hitting dead ends with both law enforcement and legal action. Called an “active defense” or “strike-back,” these counterattacks target perpetrators with like-minded methods ranging from strategic deception to hacking back. Beating hackers at their own game raises legal questions and creates an operational risk experts think aren’t worth the hassle. Do businesses at the epicenter of free enterprise tighten the perimeter and hope for the best, or fight back with reformed hackers armed with similar skills and an honest paycheck.

Symantec calculated cyber crimes cost the world $114 billion each year. The same 2011 study indicated total cyber-crime losses exceed costs associated with the global black market in marijuana, cocaine and heroin combined. The Department of Defense claims to be hit with approximately six million “threatening probes” each day. Meanwhile, enterprise is trying to reduce network costs, and offload data to cloud providers and put the security onus on them.

Security veterans suggest enterprise should choose passive measures for battling malicious hacks that compromise sensitive data, sabotage trust and drain IT budgets. DOD and the NSA have been wrestling with the same notion for years, and private security firms intimate the same well-funded organizations threatening national security are bleeding into the private sector, launching more sophisticated attacks and harboring darker motives. And U.S. industry makes a great mark. Not just because of market cap or western bravado, but because we have a heavily wired economy – connected, bloated and vulnerable.

A prime target is the oil and gas industry, pumping out critical resources through valuable infrastructures. And financial services companies count time with security threats. Tech trade secrets and research are always hot commodities. And with a recent LinkedIn attack outing over six million encrypted passwords, hackers are exposing business social networks, too. Suddenly – as high-value targets – government and business appear one and the same.

Stakes are higher, attacks are increasing, and corporate hackers wear many faces and employ many schemes to bring down networks, gather competitive intelligence, or simply steal intellectual property. Hackers are cross-pollinating techniques and ideologies. It’s dangerous out there, and enterprise wants to counterpunch attackers with a back hack. But first they have to find them.

Eastern Europe is well documented as the land of loose regulations and organized cyber crime. China specializes in big network attacks, and big time denials. Cyberespionage in China seems to be more of a cultural phenomenon, a patriotic endeavor benefiting the entire nation. The Washington Post just reported the U.S. and Israel masterminded the Flame virus aimed at Iran’s nuclear initiative. And Anonymous – the mercurial hacker movement of international descent – boosted HBGary’s network in 2011 and published its e-mail database, a humiliating gaffe for a company in business to battle both cyberespionage and cyberterrorism.

This global boiler room full of designer skills, moving targets and varied interests has created an epidemic, and forced U.S. companies to find alternative solutions to network security.

A cottage industry of startups wants to meet the business demand for more offensive tactics, claiming traditional antivirus software is no match for today's stealthy, more malicious hacker. CrowdStrike and Trail of Bits help locate attackers and build defense strategies around measurable data plucked from lab-rat analysis. Incident response is one service – a post-mortem dissection of a hacked network intended to uncover both the root cause and attribution. Digital forensics is common in law enforcement and civil litigation, but more suited in this case for a cursory investigation. But when guarding against a future attack, an adversarial assessment would be recommended. Or documentation of known industry threats culled from known hacker tools and techniques.

This more targeted approach is really preventive maintenance for leaky networks. And a concept straight out of Sun Tzu's "Art of War." On the surface, the premise is consultative and in the spirit of due diligence: identify threats, evaluate risk, and deliver actionable metrics that patch holes before an attack. However, the rest is up to the hiring company – the one screaming for vengeance.

Reuters cited, based on insight from notable security gurus, three options enterprise is contemplating or enforcing to defend against network raiders. A notorious move is setting up digital decoys - or honeypots - that invite thieves to snoop around worthless data in an unpatched, bogus network. The second trick turns stolen documents into "beacons" that may reveal a hacker's location and identity. Beacons are designed to signal an intrusion, and theoretically expose vulnerabilities in a hacker's rig.

The last – and most controversial – is a preemptive strike, or hacking back. Although bold and seemingly just, both security and legal experts warn this more aggressive tactic could violate the Computer Fraud and Abuse Act and open the kimono to a host of other problems, including counterattacks and collateral damage. Especially if the target is not an Internet swindler, but a network assassin employed by a nation state with a political agenda and bad intentions.

Reuters also reported companies are hiring "contractors" to do the work. Imagine what those resumes look like. It shows they mean business.

With shareholders to please and mouths to feed, what is a corporate entity suffering a string of break-ins supposed to do. Confuse them a little, launch a few digital spies, or pick a cyber war. Don't call the government. They are stuck in a deeper cyber matrix, defending attacks against critical agencies while raising their own offensive. Plus government, in many cases, plays by different rules. At best the outcome for enterprise is a zero-sum game. At worst a full-scale cyber attack from seasoned hackers could behead a Fortune 500 company.

Enterprise is sick of the abuse, and wants to take the fight to the less-ethical hackers attacking networks at will, and with little consequence. Blame passwords, budgets, discovery, vendor gaps, lack of education, or even internal negligence. Some government and industry experts even view the current situation as hopeless.

The merits and morals behind hacking are immaterial to balance sheets, and it doesn't matter what hat a hacker wears, or where the hack came from. Company heads are finding the threat is always imminent, and may test – or escalate - hacking back as a weapon of last resort. Or, network performance and asset protection becomes more about risk management and less about security.