Why CyberCrime Remains a Growing Business: And How to Stop It

By Derek Manky

http://www.forbes.com/sites/ciocentral/2013/02/01/why-cybercrime-remains-big-business-and-how-to-stop-it/

Cybercrime is big business. And it's growing in scope and impact.

But what may not be obvious to the casual observer is that cybercrime is growing in its reach and sophistication because of two key factors: the consumerization of crimeware and the adoption of time-tested business processes to enhance the profitability of crime syndicates worldwide.

Given the widespread availability of millions of variations of malware, botnets, phishing exploits, and the like, today's cybercriminal does not need to possess deep technical skills - to the contrary. Malicious software code is as easy to get your hands on as virtually any downloadable app.

The disturbing trend in cybercrime is the "enterprise-class" approach crime syndicates take to grow their businesses. Today's syndicates employ hierarchies of participants with roles that mirror the executive suite, middle management and the rank and file. The executive suite oversees strategy and operations that initiate nefarious acts. Recruiters identify "infantry" that carry out large-scale attack schemes on a permanent hire or outsource (affiliate) basis. They also create and had-out malware and mold reward programs to pay affiliates once successful attacks are carried out.

Understanding "Crime-as-a-Service"

Given the ubiquitous adoption of cloud computing, social networking, BYOD and mobile communications, cybercriminals now have unprecedented reach across and into more organizations, databases, desktops and mobile devices than ever before. Infrastructure advances and the enormous number of avenues for attack are giving cybercriminals a smorgasbord of attack vectors to choose from.

To capitalize on these opportunities, cybercrime syndicates use recruiters to attract new "talent" via fully realized web portals, many of which protect themselves with disclaimers like, "We do not allow spam or other illicit methods for machine infection." This is a method of passing off legal responsibility to the hired "infantry" while providing the necessary malware needed to execute a full-fledged infection campaign.

Fanning the Flames

The drivers of these constantly evolving tools are extensive R&D organizations that create custom-order code to produce private botnets, fake antivirus software and deployment systems. In turn, these are typically carried out for premeditated, targeted attacks – known as Advanced Persistent Threats, or APTs.

Another key contributor to the expanding influence of cybercrime is the hosting provider. Simply put, affiliates need somewhere to store attack content ranging from exploit code, malware and stolen data. Taking a page out of Wall Street, crime syndicates are engaging in mergers and acquisitions to grow their botnets through the use of another organization's botnet. A recent example is Zeus & Spyware. Zeus, circa 2007, peaked in 2010 as the most prolific banking crime kit around. The crimeware kit would create new versions of powerful malware which had the capability to steal banking credentials, as well as hijack and manipulate secure online banking sessions. A rival botnet known as SpyEye emerged in 2010 and tried to take over what was clearly a successful market. The competition hurt profits for both, so in late 2010, the two authors merged source code, retied Zeus support and passed the torch to SpyEye.

And with creative profit-sharing flair, crime syndicates are continuing to grow sophisticated pay per click/install/purchase affiliate programs to reward up and coming cybercriminal affiliates on a performance-based scale.

How to Stop It

Given this grim outlook, what successes are turning the tide? Several large-scale botnet takedowns showcase the advantages of working groups and task forces.

In January of this year, the large Eastern European botnet Virut was taken down with the help of local CERT teams and partners. This particular botnet had control of closed to 900,000 unique IP addresses in Poland alone and is thought to be the fifth most widespread threat in 2012. Virut was a widespread threat as early as 2008, as it had a unique hybrid capability that allowed it to spread through other botnets. In essence, it was using the competition to amplify its success. Since Virut code was complex and could embed itself in other infections, detection and takedown was difficult over a five-year run.

Regrettably, these "stops" are a drop in the bucket. Kelihos, for example, came back in another form after being stopped. While the dismantlement of a botnet's command and control center is optimal, another preventive strategy to clamping down on crimeware is to vet domain registrations to avoid the creation of these domains. A good case in point is the Conficker Working Group that helped filter out domains before they could be registered to prevent the spread of that particular botnet.

But the best approach to effectively fight cybercrime requires global participation. We need an international body that can mediate disputes and dispatch resources to

share information about cybercrime trends. A central reporting and information sharing channel between the private and public sectors is also needed. The best example of this kind of information sharing thus far is FIRST (Forum of Incident Response and Security Teams), circa 1990. When it comes to law enforcement, varying jurisdictions and laws complicate the prosecution of cybercriminals. FIRST helps address this problem through collaboration.

Unfortunately, many attacks are handled outside this forum and ad-hoc crime-fighting groups seem to pop up like a game of whack-a-mole. It is apparent that the best way to take a chunk out of cybercrime is attacking its Achilles heel: going after the cash flow itself. The best targets would be affiliate programs, the cash cows that pay out commission and rewards to hired affiliates ("infantry") who carry out malicious attacks. If the well dries up, so will the rest of the food chain.

So where does this leave us? Practically speaking, the most effective way to secure a business from crimeware is from the inside out. Organizations need to take matters into their own hands to proactively prevent the spread of crimeware among its employees, partners and customers.

What this amounts to is a highly layered security strategy consisting of vital elements that include intrusion prevention, botnet and application control, Web filtering, antispam, and antivirus. Companies must engage in regular accounting of digital assets and assessment of potential security flaws. Organizations must aggressively educate users about security best practices while implementing enforceable mechanisms for security policy violations. They must also implement an incident response plan – "what happens if?" It is imperative for companies to work together with security experts in this highly dynamic threat landscape.

Through collaborative global efforts and organizational commitment to deploying aggressive multi-layered security policies, the cybercrime epidemic can eventually be contained.