THE GLOBE AND MAIL

TRACKING KOOBFACE

Meet Koobface, Facebook's evil doppelgänger

RON DEIBERT AND RAFAL ROHOZINSKI
Special to Globe and Mail Update
Published Friday, Nov. 12, 2010 12:27PM EST
Last updated Friday, Nov. 19, 2010 11:52AM EST

There is an episode of Star Trek in which Captain Kirk and Spock are confronted by their evil doppelgängers who are identical in every way except for their more nefarious, diabolical character.

The social networking community Facebook has just such an evil doppelgänger – and it is called Koobface.

Cybercrime thrives not just because of ingenuity and lawlessness, but because of social media opportunities. Koobface (an anagram of Facebook) succeeds by mimicking normal social networking behaviour. It is like a digital amoeba, living parasitically on our sharing habits. It leverages the most successful of all age-old criminal techniques – our readiness to extend trust – with our eagerness to click on links. We have become conditioned into a world of intense social interaction. We click on website addresses and documents like mice clicking on pellet dispensers. And it is that conditioned tendency that Koobface exploits with precision.

We undertook this investigation as a continuation of our work on cyber espionage that began with Tracking Ghostnet and Shadows in the Cloud. In both cases, we found that the attackers' systems were built upon off-the-shelf crimeware code and tradecraft, readily obtained and applied either by state-based actors or commissioned from criminals all too ready to serve as privateers to sell their wares to the highest bidder.

We were intrigued: if the criminal merchants of code were ready to engage in the high-end of the exploitation market – breaking into government systems to obtain sensitive documents – then what was going on in the streets, and the myriad globalized pathways of cyberspace that now connect more than two-thirds of humanity?

As with those earlier cases, our lead technical researcher Nart Villeneuve was able to take advantage of mistakes made on the part of the attackers to secure their own infrastructure; our access was almost comprehensive, allowing us insight into their inner workings for a period of months.
What we found with Koobface gave us pause: clearly cybercrime is profitable, but equally clearly, there is little incentive or even basis for our existing institutions of policing to do much about it.
The entrée point for Koobface is almost irresistible: a link sent from a fake "friend" prompting a visit to a video site that purportedly reveals the recipient captured naked from a hidden web cam. Who wouldn't follow that link? But for the hapless recipient, that one click leads down a Kafka-esque rabbit hole of

viruses and trojan horses, and straight into the tentacles of the Koobface network.

The mechanisms put in place by Koobface operators to generate revenue walk a very fine line, and are at times so subtle that it is difficult, if not impossible to identify who, if anyone, is actually a victim. Although our investigation determined the Koobface gang drew revenues of more than $2-million a year, the combined earnings were derived from thousands of individual micro-transactions on the order of a fraction of a penny each, spread across victims in dozens of national jurisdictions. Each commandeered computer that clicked on an online ad or downloaded a fake anti-virus package generated a cut for the gang. So meticulous were the attackers that they created an automatic text message alert to themselves each day summing up their spoils.

Without a victim, particularly a complainant, it is almost impossible for a police force to justify the resources to investigate a case like Koobface. Police officers ask: what's the crime? Prosecutors ask: what or whom am I supposed to prosecute? In the case of Koobface, it is almost as if the system were purposefully designed to fall between the cracks of both questions.

Even more debilitating is the international character of Koobface. Cybercrime networks succeed by hiding locally while leveraging a global infrastructure. Electrons may move at speed of light, but legal systems move at the speed of bureaucratic institutions, especially across national borders. Living in St. Petersburg, Russia, the Koobface gang might as well be living on Mars, so poorly developed are the mechanisms of international law enforcement co-operation.

Although we turned over the entire Koobface database we acquired as evidence to Canadian law enforcement, including evidence identifying the individuals behind it, we were not surprised that there has been no arrest or prosecution, for the reasons listed above.

We also worked with the broader security community who had studied Koobface to notify the hosting companies and service providers upon which Koobface had built its malignant enterprise: some 500,000 fraudulent Google blogger and Gmail accounts, and 20,000 Facebook accounts. The action to disable these accounts will temporarily bring the network to its knees, but not terminate it. Koobface will surely live to see another day as long as the individuals behind it roam free.

Some may argue Koobface earned its operators a few million dollars on a nearly victimless crime. Is that really something that warrants concerted international policing and attention? Maybe not. But here it is important to understand the broader ecosystem of which Koobface is just one small example. A recent study by Bell Canada suggested that $100-billion out of $174-billion of revenue transiting Canada's telecommunications infrastructure is “at risk.” The same operator measured over 80,000 “zero day” attacks per day targeting computers on its network – meaning, attacks that are so new the security companies have yet to register them. These are staggering figures, which if translated into physical terms – bank robberies and break-ins – would be prompting politicians into immediate action.

There is another element of Koobface that should give us even more pause. The Koobface gang had a certain charm and ethical restraint. They communicated with security researchers about their intents and their desire not to do major harm. They limited their crimes to petty fraud, albeit massive in scale and scope. But the scary part is that they could have easily done otherwise.

Thousands of compromised computers networked together with an invisible tether controlled by a few individuals can be employed to extract pennies from unsuspecting victims, as it was with Koobface, or sensitive national security documents from government agencies, as it was with Ghostnet and Shadows. It can be used to direct computers to click on fake advertisements for Viagara, or marshal them together to attack a meddlesome human rights website, as it is with increasing frequency from Iran and Kazakhstan to Burma and Vietnam.

Criminal networks such as these are growing as fast as the social networking platforms upon which they parasitically feed. Koobface is just one example of an entire ecosystem that threatens to put at risk the very entity on which it depends – a free and open cyberspace. How to clean up and control it, without undermining the positive characteristics of social networking we have all come to enjoy, is one of the major challenges of global security policy today.

Ron Deibert is Director of the Canada Centre for Global Security Studies and Citizen Lab, Munk School of Global Affairs, University of Toronto. Rafal Rohozinski is CEO of the SecDev Group and Psiphon Inc, and Senior Fellow, Munk School of Global Affairs, University of Toronto. Together they are the principal investigators of the Information Warfare Monitor.