CSO

BRICK OF ENLIGHTENMENT
By Dave Lewis

About |
Bringing fire to the village.

NEWS

Mounties join crack down on Russian cyber crime

CSO | Jun 3, 2014 12:52 PM

The Mounties took part in a criminal take down this week that saw a couple of servers seized in Montreal. These systems were being used by criminals, apparently located in Russia, who were running a malware network that was fleecing victims of millions of dollars. A number that has

been kicked around in this case is $100 million although it isn't clear if this is an accurate number or something mired in hyperbole.

From The Globe and Mail:

> *On Friday, the RCMP seized two servers in Montreal in co-ordination with a two-and-a-half-year operation initiated by the U.S. Federal Bureau of Investigation.*
>
> *According to an FBI affidavit filed in Pittsburgh, key servers in the CryptoLocker infrastructure were located in Canada, Ukraine and Kazakhstan.*
>
> *More than 5,000 users were victims in Canada, with potential losses close to $1.5-million, the RCMP said.*

The software in question was called "Gameover Zeus" (GOZ) which made up a large botnet that spanned the globe. The other plus in this take down was that it crippled a piece of software called Cryptolocker. This ransomware that would be delivered via GOZ which would encrypt files on a victim machine and then demand payment to restore the file.

GOZ would primarily be spread via spam email in an attempt to capture individuals banking information as well as that of small to medium sized companies. Another aspect of this software is that it can be used for launching DDoS attacks on targets without the knowledge of the victim. GOZ used an encrypted network, as well as using encryption to foil antivirus solutions, and could distribute file updates to nodes.

This criminal enterprise was allegedly run by one Evgeniy Bogachev who was last known to live in Anapa, Russia. While the authorities in the US may be hoping for some cooperation in bringing Bogachev to justice, I'd be hard pressed to believe that they will get much in the way of traction with the Russians.

While this is a win for the law enforcement crowd, they don't have Bogachev in custody and it is entirely possible that this isn't the end of the story.

(Image used under CC from waferboard)

Dave Lewis — *Global Security Advocate*

Dave has over 15 years industry experience. He has extensive experience in IT operations and management. Currently, Dave is a Global Security Advocate for Akamai Technologies . He is the founder of the security site Liquidmatrix Security Digest and co-host of the Liquidmatrix podcast. Dave also serves on the (ISC)2 Board of Directors. Prior to his current role, Dave worked in the finance, healthcare, entertainment, manufacturing and critical infrastructure verticals. He has worked for a defense contractor as a security consultant to clients such as the FBI, US Navy, Social Security Administration, US Postal Service and the US Department of Defense to name a few. When not at work Dave can be found spending time with his family, playing bass guitar and polishing his âbrick of enlightenmentâ.