Being Dr Evil for a Moment

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

Friend and colleague Prof Ric Steinberger < http://www.linkedin.com/pub/ric-steinberger/15/677/106 > wrote the following thoughtful essay in one of his email messages and has granted permission to post it here. Everything below is Ric's own work with minor edits from Mich.

* * *

Most people who work in information security are accustomed to thinking defensively: How can I prevent "bad things" from happening that would damage computers or networks, or allow unauthorized people to view/alter confidential information? We seldom are in a position to think offensively: How would I attack or damage an opponent's systems or gain access to information the opponent doesn't want me to see?

Edward Snowden's recent releases – mostly through Glenn Greenwald of *The Guardian* < http://www.theguardian.com/world/nsa > – make it clear that the NSA is very much playing offense – trying really hard to obtain copies of every bit of digital information that US citizens (and those of many other nations) have created. As documented in extensive references by the Electronic Frontier Foundation < https://www.eff.org/nsa-spying >, the NSA gets copies of all phone calls (metadata, and probably call content), emails, files in the cloud, communications on social networks like Facebook, copies of physical letter envelopes. Several large US based companies have been corralled into this effort, named Prism: Yahoo, Microsoft, Apple, Google, AOL, Facebook, Twitter, Paltalk, perhaps more that have not been revealed so far.

But what does the NSA not have access to unless the FBI physically plants some kind of device or software bug on their targets' computers and networks? [Note that the NSA targets are all US citizens plus many in other nations.] As far as we know, the NSA cannot do direct searches or copies of individuals' computer systems, home or business networks. Why not? Because in many cases, users may create this data without its ever being transmitted over the Internet. Could the NSA break into specific systems physically and/or electronically? Of course. But that requires time, manpower, money and in theory, a warrant issued by a judge. Therefore imagine plotters in different locations collaborating by creating local information, copying it to USB thumb drives and mailing them to each other. Do we really imagine that the NSA has not considered this?

So, if I were director of strategy at the NSA, I would want unfettered, universal access to that "last mile," the final refuge of Americans' digital privacy: files stored on their personal computers, including smart phones. The question is: How do I get it? I can't have the FBI break into every house and business in the country, at least not yet. But what if I could install spyware and/or botnet clients on every major operating system? OK, how do I do that? There are a couple approaches, each with advantages and disadvantages. I could try to bully Microsoft, Google, Apple and some Linux vendors into installing the spyware/botnet software via patches. Most of these companies are already part of Prism, so in theory, I could just extend the "Prism walls." But what if that's just too obvious? What if the Prism companies successfully push

back, or tie me down for years with legal challenges?

So I move to plan B: I approach the major US anti-malware companies, like Symantec, McAfee, ESET, more. Anti-malware software is installed on almost every home and work PC/Mac computer. I get National Security Letters and force these companies into the Prism program. Then I require them to add a high quality (think Stuxnet) spyware/botnet client that is capable of reporting on and even sending copies of every file a user possesses or reads via Web access. If, or when, I'm found out, I can always insist that this is totally for national security, to help catch terrorists, and that citizens with nothing to hide have no reason to worry. Isn't that what the East Germans and the Nazis said? [Note that savvy tech users who monitor their outgoing connections should be able to spot something odd going on, and even block it. That situation could require more collaboration with Symantec, McAfee – require them to allow the NSA to access users' systems from Symantec, and McAfee IP addresses.]

What if there's too much pushback on plan B? I can try plan C: Go directly to the major chip companies. That would be Intel, AMD, the ARM companies and any vendor who makes CPU chips for mobile devices. Force them into Prism if they're US companies. If they're not, then put pressure on US mobile phone vendors and carriers to only use CPUs from Prism companies. If I can insert the microcode I want directly into these CPUs, then I own the devices that use them. Doesn't matter what operating system or encryption strategy is used: I get access to whatever files and plain text I want. And it's all for free: I don't even have to pay for network access.

And if plan C doesn't work? Remember that I'm Dr Evil. I have an almost unlimited budget and can operate in near complete secrecy - as long as no more Ed Snowdens show up. So I can always think of more nefarious ways to defeat encryption by finding the money, staff and friendly FISA Court judges to help me succeed. Remember: My goal is to be able to intercept and examine the communications of any network user anywhere on earth. That means you, your family, doctors, lawyers, judges, Congress people, senior executives, Presidents. Don't even think about reducing my budget or imposing oversight because I know all your secrets and can easily blackmail you.

Ok, let's turn off Dr Evil. As far as I know, the anti-malware and CPU companies are not in the Prism program. But it could happen.... unless we show a lot more resistance than we have been.

[MK adds: Bruce Schneier addressed the issue of cooperation between companies and the NSA in a series of postings in the August 15, 2013 *Crypto-Gram* < https://www.schneier.com/crypto-gram-1308.html#1 >]

* * *

Ric Steinberger< http://about.me/ricsteinberger > is President of Mobile App Research Group < https://angel.co/mobile-app-research-group > and has been teaching in the Norwich University Master of Science in Information Security & Assurance program < http://infoassurance.norwich.edu/ > since 2006.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >