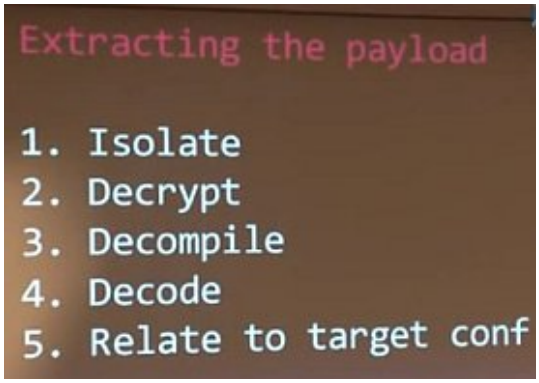
NSA AND COMPROMISED ENCRYPTION: THE SWORD CUTS BOTH WAYS



[Snapshot, Ralph Langner presentation re: Stuxnet, outlining payload extraction (c. 2012 via YouTube)]

If you want fresh and weedy perspectives you won't find in corporate-owned media, please donate!

A friendly handshake is offered;
Names are swapped after entry;
The entrant delivers a present;
The present is unboxed with a secret key…

And * BOOM *

Payload delivered.

This is cyber weapon Stuxnet's operations sequence. At two points in the sequence its identity is masked – at the initial step, when identity is faked by a certificate, and at the third step, when the contents are revealed as something other than expected.

The toxic payload is encrypted and cannot be read until after the handshake, the name swap, and then decrypted when already deep inside the computer.

In the wake of the co-reported story on the National Security Agency's efforts to crack computer and network encryption systems, the NSA claims they are only doing what they must to protect the country from terrorists, criminals, and cyber attacks generated by individuals, groups, and nation-state actors.

Defense, though, is but one side of the NSA's sword; it has two lethal edges.

While use of encryption tools may prevent unauthorized access to communications, or allow malicious code to be blocked, the same tools can be used to obstruct legitimate users or shut down entire communications systems.

Encryption APIs (ex: Microsoft CryptoAPI embedded in Windows operating systems) are often used by higher level applications – for example, a random number generator within the API used to create unique keys for access can also be used to create random names or select random event outcomes like a roll of the dice.

In Stuxnet alone we have evidence of encryption-decryption used as cyber warfare, the application planned/written/supported in some way by our own government. This use was Pandora's Box opened without real forethought to the long-term repercussions, including unintended consequences.

We know with certainty that the repercussions weren't fully considered, given the idiocy with which members of Congress have bewailed leaks about Stuxnet, in spite of the fact the weapon uncloaked itself and pointed fingers in doing so.

One of the unconsidered/ignored/unintended consequences of using weaponry requiring encryption-decryption is that the blade can cut in the other direction.

Imagine someone within the intelligence community "detonating" a cyber weapon built in the very same fashion as Stuxnet.

A knock at the door with a handshake;
Door open, package shoved in, treated as expected goods;
Encrypted content decrypted.

And then every single desktop computer, laptop, netbook, tablet, and smartphone relying on the same standardized, industry-wide encryption tools "detonates," obstructing all useful information activities from personal and business work to telecommunications.

At least one other cyber weapon built with a similar profile as Stuxnet, but with the ability to profile systems and report "home" – has already gathered a snapshot of the computing environment and may have left behind content earmarking systems as friendly/not-friendly.

Metadata collected continuously by the NSA informs them through network analysis exactly which systems – whether computers, servers, or smartphones – are the most important nodes on any monitored network to which cyber weapons should be pushed in order to disperse clones of defensive/offensive cyber weapons most efficiently for maximum effective contagion.

The NSA will tell you that these kinds of tools are critical to protecting the country and its interests, but without any real oversight, created in the dark by entities who may have additional or different agendas than our own, and accessible by administrators who may be compromised, the sword they wield can deliver a mortal wound – to us.

Like the Clinton Administration's Clipper Chip, the assault on encryption represents an end-run around adequate debate by well-informed representatives and the public as to whether the use of cyber weapons requiring compromised encryption systems is appropriate, let alone whether this double-edged sword should be contained in a way that it cannot be used inappropriately against citizens.

Congress has deliberated about the development and implementation of an internet kill switch,

the use of which may or may not be legal under the Communications Act of 1934; each time the public has been enraged about the possibility that the government would have the ability to shut down communications altogether.

But NSA's mucking about with encryption systems offers the opportunity to surreptitiously build a kill switch on any and all systems containing compromised encryption – and with NSA's influence, the standards to which both computers, phones, and encryption systems are built ensure that nearly any and all devices, attached to a network or USB-enabled can be shut down once a cyber weapon has been deployed.

In other words, the NSA has likely built internet kill switch capability – and any debate in Congress against such capability has been futile.

How will the NSA defend this? Will it merely issue another terse statement like this one offered Friday:

> "It should hardly be surprising that our intelligence agencies seek ways to counteract our adversaries' use of encryption. Throughout history, nations have used encryption to protect their secrets, and today, terrorists, cybercriminals, human traffickers and others also use code to hide their activities. Our intelligence community would not be doing its job if we did not try to counter that.
> While the specifics of how our intelligence agencies carry out this cryptanalytic mission have been kept secret, the fact that NSA's mission includes deciphering enciphered communications is not a secret, and is not news. Indeed, NSA's public website states that its mission includes leading "the U.S. Government in cryptology … in order to gain a decision advantage for the Nation and our allies."
> The stories published yesterday,

> however, reveal specific and classified details about how we conduct this critical intelligence activity. Anything that yesterday's disclosures add to the ongoing public debate is outweighed by the road map they give to our adversaries about the specific techniques we are using to try to intercept their communications in our attempts to keep America and our allies safe and to provide our leaders with the information they need to make difficult and critical national security decisions."

In other words, to do its job the NSA must have a sword that can kill both its targets and those it is supposed to protect – just shut up about that sword hanging by a thread over your head, already. It's not for you. Really.