How 'Zero Days' is a cybersecurity canary in a coal mine

Jul 19, 2016 Save This ()

Courtney Gabrielson
Nonmember Contributor (/about/person/0011a00000DlK6nAAF)

It's been said that truth is often stranger than fiction, and documentary "Zero Days" proves that old adage to be true. In this case, it's a truth that security and privacy pros may want to heed - but more on that in a bit.

Helmed by acclaimed filmmaker Alex Gibney (http://www.imdb.com/name/nm0316795/), "Zero Days" covers the U.S. and Israeli-hatched supervirus – informally known as "Stuxnet (https://iapp.org/news/a/state-of-siege-infrastructure-and-industrial-security-and-privacy-on-the-iot/)" – created to hamstring the Iranian nuclear program in 2009. But that's starting the story at the end. The film begins by unwrapping the tale halfway through: when the powerful virus of unknown origin began infecting computers over the globe and sending cyberspace less-than-comfortably close to the brink of a meltdown.

At the time, the operation was shrouded in mystery. It took the work of Kaspersky Lab anti-virus technicians and a collection of intelligence leaks to expose the culprits and their motives, which are as multilayered as a slice of baklava.

Indeed, the film is perhaps best understood like that famous Greek dessert: multi-layered, slick, and delicious. The elements surrounding the story at hand are numerous, spanning years of religious enmity, political upheaval, presidential administrations, and the ethics that surround war in a not-so-physical plane: cyberspace. Then there are the storytellers: former governmental officials from across the globe, representatives from the IT world and Iran, and the symbolic "whistleblower," the movie's only significant female representation (hmm) which really isn't a woman at all.

Making all these dynamics harmonize is no easy task, but Gibney does so with ease. The far-reaching subject matter is approachable yet challenging, and he lays the various foundations that make the pieces of the dizzyingly large puzzle come together like a slowly tightening noose. At one point, one of the technologists that worked to decode Stuxnet quipped that the story he was a part of felt like something straight out of Hollywood. He's right.

A particular source of consternation for those interviewed is the intangibility of the virus and the space it occupies.

If it's hard to regulate a threat you cannot see, it's equally difficult as a filmmaker to translate that threat from a jumble of facts into something viscerally unsettling. While one can certainly understand the power of technology to destroy a reputation, there's something terrible about the aforementioned whistleblower, her visage distorted and pixelated to conceal her identity, tirelessly morphing under the audience's watchful eye as she tells her story of

another. Then, Gibney often brings the viewers “into” the code with visuals that seem otherworldly in their seamlessness. It’s numbers and letters crackle with the warning sound of a rattlesnake, silently hissing, alive. We are in the presence of a latent yet powerful danger, the “magic words” that can protect or destroy us.

That’s the power of the film: what it doesn’t say. It doesn’t pretend to have the answers, nor do its subjects. While nearly all the interviewees express a need for regulation, no one seems to present a solution.

Except, perhaps, the need for dialogue. Since the Stuxnet virus, neither the U.S. nor Israeli government has admitted to their involvement in the attack, and issues of cyberwarfare and defense are still very hush-hush. “This stuff is hideously over classified,” said former CIA and National Security Agency Director General Michael Hayden. “And it gets in the way of a mature, public discussion as to what it is we as a democracy want our nation to be doing up here in the cyberdomain.”

“Zero Days” is sure to spark that conversation. It’s enormously watchable and profoundly disturbing. It forces the viewer to internalize the headlines. Essentially, it makes lofty ideas and legislative buzzwords very real and very approachable, enough to get your mom, friend or colleague to engage and discuss the new and untamed frontier that is cyberspace.

For privacy and security pros, “Zero Days” serves as a sort of canary in the coal mine. As various past-and-present American government officials call for discussion, they’re also encouraging legislators to dive headlong into building both a legal and ethical framework surrounding cyberwarfare and defense, much like politicians did in the halcyon days of the nuclear arms race. After all, the technology that built Stuxnet is now available for other nations to copy and deploy. And it appears that's exactly what's happening.

Symantec security researcher Liam O'Murchu, who was one of the first researchers to study Stuxnet, recently told CSM Passcode (http://www.csmonitor.com/World/Passcode/Security-culture/2016/0718/Stuxnet-ushered-in-era-of-government-hacking-say-experts), "When we first started looking at Stuxent, we had, maybe, one or two attacks we believed were nation-state related. Now, we're looking at over 100 campaigns from all over the world." And though such attacks may be aimed at critical infrastructure, who's to say organizations, both public and private and all the personal data contained within, won't be collateral damage to such cyber warfare? If it's true that Sony Pictures was a victim of North Korea and the Office of Personnel Management a victim of China, who's to say we won't start seeing many more such invasions?

“Yes, it may be hard, and [building guidelines for cyberwarfare] may take 20 or 30 years, but it’ll never happen unless you get serious about it,” one former American official said during "Zero Days."

“Getting serious” could mean a host of different things for different groups. There has been no shortage of calls for a public- and private-sector threat data sharing exchange and for laws to mandate such exchanges, but many companies are wary of sharing data with the government and other competing businesses. So as we continue to depend upon a rapidly growing internet of things, and as nation-states grow more determined to build cyber weapons, "getting serious" about cybersecurity grows more stark.

Will it take an international agreement as extensive as the Nuclear Non-Proliferation Treaty (https://en.wikipedia.org/wiki/Treaty_on_the_Non-Proliferation_of_Nuclear_Weapons)? Maybe so. In the meantime, let's hope the canary keeps breathing.

Top image from "Zero Days" trailer (https://www.youtube.com/watch?v=Lq11OUKSDnU)

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200