Exposing the Fallacies of Security by Obscurity
Full Disclosure

It is unlikely that anyone is ignorant of the concept of full disclosure. While today we often see it applied to cyber security and the like, it dates back to around 1853 with regard to weaknesses in safes and locks. If we dig a little bit, we may even find older references. Having another article talking about full disclosure and trying to convince you that it is a good idea may sound ridiculous, but bear with me. I believe that the early 2017 release of the Shadow Brokers dump has added a twist that was often thought about, but never proven until now, especially in light of the sheer number of recent breaches.

"In information technology and security, 0-day or vulnerabilities that do not have a corresponding patch have always been the monster under our bed."

Full disclosure is the idea that when someone discovers a vulnerability within an application or device or piece of software, they should release the details of said vulnerability to the public. While there are a number of arguments against full disclosure, such as that we cannot fix all of the problems disclosed or that patching is a difficult process in a modern, complex organization, it is still the right path to ensure comprehensive understanding of risk. And to be clear, I actually agree with both of those arguments against full disclosure. I just feel that they are outweighed by the benefits.

First, it is nearly impossible to fix everything that is wrong with our systems and applications. Consider the Equifax breach. Equifax has confirmed that it was compromised from a Struts vulnerability that was released and actively exploited in March 2017. If an organization with the resources of Equifax cannot remediate an actively exploited flaw in 6 months, then how can we expect smaller organizations to do so? Patching everything can become a very complex process, especially with the variety of systems and devices on a modern network, not to mention the rapid adoption of Internet of Things (IoT) and mobile devices that get added into the mix.

But in my opinion, Shadow Brokers, the organization that started releasing exploit and attack tool data leaked from the US National Security Agency (NSA), and the exploits contained within their releases have changed the risk to organizations from unknown vulnerabilities. I say “unknown,” but let us be clear, I mean unknown to the public. In information technology and security, 0-day or vulnerabilities that do not have a corresponding patch have always been the monster under our bed. We know that they exist.

Kevin Johnson, CISSP
Is the chief executive officer of Secure Ideas. He has a long history in the IT field including system administration, network architecture and application development. He has been involved in building incident response and forensic teams, architecting security solutions for large enterprises and penetration testing everything from government agencies to Fortune 100 companies. In addition, Johnson is a faculty member at Institute for Applied Network Security and was an instructor and author for the SANS Institute. In his free time, he enjoys spending time with his family and is an avid Star Wars fan and member of the 501st Legion (Star Wars charity group).
and they can be used against us, but very few people believed that their organization could be impacted by one. (Sidenote: I tried to explain to my daughters when they were young that there is no monster, but they still insisted on monster spray and nightlights. I wonder when companies will do the same with 0-day.) The Shadow Brokers changed this mentality in a big way.

When the Shadow Brokers released the dump, which included red team gems such as EternalBlue (CVE 2017-0144), the attacks and malware that used these exploits spiked. Wannacry, a piece of ransomware that used two of the exploits in the dump, reportedly compromised 240,000 machines on the first day it was released.1 We have also seen a number of other malware outbreaks and samples that use these same reported vulnerabilities.

So why does this change the full disclosure debate? Simple: the government actually is encouraging the development of exploits against vulnerabilities while simultaneously increasing the secrecy around these flaws. The NSA and, presumably, other organizations within the US government and around the world are collecting and developing exploits against popular software. While the White House, under former US President Barack Obama, had stated that the government has a bias toward disclosing vulnerabilities, the exception is when there is a “clear law enforcement or national security use.”2 And by doing this, they are increasing the risk for the rest of us by not having these flaws patched.

Furthermore, the government does not have a strong history of protecting sensitive data. All it takes is looking back at the US Office of Personnel Management (OPM) breach and other similar compromises—not to mention the fact that Shadow Brokers took the exploits out of the NSA. So if the government knows about a vulnerability within popular systems, it is just a matter of time before either a whistleblower or an attacker makes it public.

So how do we prevent this? Simple: full disclosure. If the government or anyone who finds a flaw in software and systems simply notifies the vendor of the issue while letting the public know, we all will be safer. This is due to a number of factors:

- Providing patches or solutions
- Communicating and crowdsourcing patches and solutions
- Individualizing and weighing the need for action

First, the vendor has the information needed to create a patch. They need to know about the flaw to fix it. And by making the flaw public, there is a better chance that the vendor will release solutions and patches. Over the years, there have been tons of examples of companies not fixing issues until there is a high-profile incident around it.

As communication paths increase, we have seen a large uptick in the community discussing these flaws and creating solutions before the vendor.
The next benefit of full disclosure is that the customers and organizations running the systems will know about the flaw and potential solutions faster. As communication paths increase, we have seen a large uptick in the community discussing these flaws and creating solutions before the vendor. When Shadow Brokers released their dump, Twitter and other communication means exploded with people discussing what these tools and exploits meant and how to fix the systems affected. Within hours of the release, there were rules for intrusion detection systems to alert on the attacks and information about what to look for to see if your system was compromised via these tools. This type of team problem solving is not seen without full disclosure.

Finally, full disclosure allows the individual organization to determine where to focus its efforts. How many times do we see a patch get applied because it might fix a security hole? By providing the information, staff can determine if they are going to patch or if some other solution will allow them to protect their systems while maintaining their ability to do their job.

The idea of full disclosure takes all of these benefits and includes the actual flaw information to allow a comprehensive evaluation of the risk and solutions.

All in all, we need full disclosure to ensure that we know why and how our systems are protected.

Endnotes
