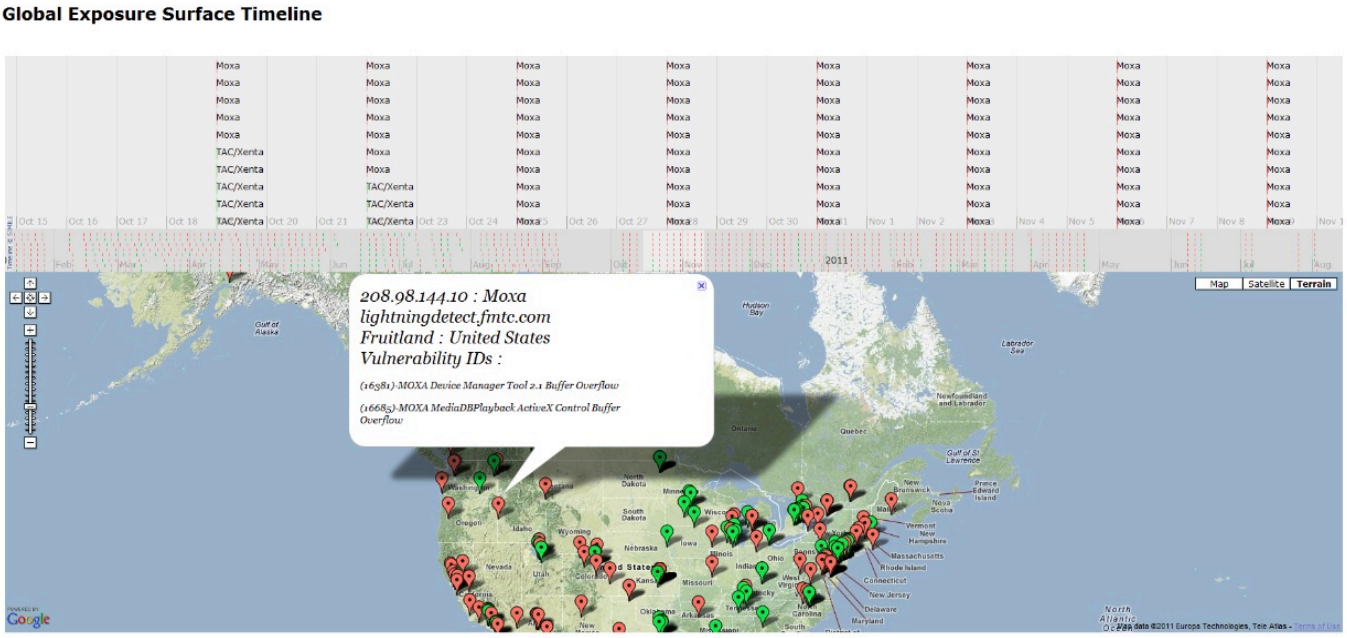
10K Reasons to Worry About Critical Infrastructure

A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public internet, including water and sewage plants, and found that many could be open to easy hack attacks, due to lax security practices.



Screenshot showing an industrial control system in Idaho that's connected to the internet. The red tag indicates there are known vulnerabilities for the device that might be exploitable. Two known vulnerabilities are listed at the bottom of the text bubble.

Infrastructure software vendors and critical infrastructure owners have long maintained that industrial control systems (ICSes) — even if rife with security vulnerabilities — are not at risk of penetration by outsiders because they’re “air-gapped” from the internet — that is, they’re not online.

But Eireann Leverett, a computer science doctoral student at Cambridge University, has developed a tool that matches information about ICSes that are connected to the internet with information about known vulnerabilities to show how easy it could be for an attacker to locate and target an industrial control system.

“Vendors say they don’t need to do security testing because the systems are never connected to the internet; it’s a very dangerous claim,” Leverett said last week at the S4 conference, which focuses on the security of Supervisory Control and Data

Acquisition systems (SCADA) that are used for everything from controlling critical functions at power plants and water treatment facilities to operating the assembly lines at food processing and automobile assembly plants.

“Vendors expect systems to be on segregated networks — they comfort themselves with this. They say in their documentation to not put it on an open network. On the other side, asset owners swear that they are not connected,” Leverett said. But how do they know?

To debunk the myth that industrial control systems are never connected to the internet, Leverett used the SHODAN search engine developed by John Matherly, which allows users to find internet-connected devices using simple search terms. He then matched that data to information from vulnerability databases to find known security holes and exploits that could be used to hijack the systems or crash them. He used Timemap to chart the information on Google maps, along with red markers noting brand devices that are known to have security holes in them. He described his methodology in a paper (.pdf) about the project.

Leverett found 10,358 devices connected through a search of two years worth of data in the SHODAN database. He was unable to determine, through his limited research, how many of the devices uncovered were actually working systems – as opposed to demo systems or honeypots – nor was he able to determine in all cases whether the systems were critical infrastructure systems installed at power plants and other significant facilities or simply ICSes that controlled things like high school lighting systems or the heat and air conditioning system in office buildings.

But Leverett said a few of the systems he investigated did actually belong to water facilities in Ireland and sewage facilities in California.

He also found that only 17 percent of the systems he found online asked him for authorization to connect, suggesting that administrators either weren’t aware that their systems were online or had simply failed to install secure gateways to keep out intruders.

To avoid obtaining unauthorized access to the systems, Leverett didn’t try to connect to the systems himself but passed the information to the Department of Homeland Security last September, which took on the task of notifying the owners of systems, where they could be identified, or their ISPs. In the case of systems based overseas, DHS worked with some dozens of CERTs (Computer Emergency Response Teams) in those countries to notify ISPs and device owners.

Leverett’s tool shows how easy it is for a dedicated attacker or just a recreational hacker to find vulnerable targets online to sabotage.

He told conference attendees that he worked on the tool full time for three months and part time for an another three months, noting that if “a student can put this together, surely a nation state can do it.”

A conference attendee who works for Schweitzer, a maker of industrial control

systems, called the tool “extremely valuable” and said his company had notified customers whose systems were found online.

“At least one customer told us ‘We didn’t even know it was attached’,” he said.

Leverett is not the first to use SHODAN to uncover ICSes connected to the internet. Last February, independent security researcher Ruben Santamarta used SHODAN to identify online remote access links to SCADA systems at multiple utility companies. But Leverett is the first to show how easy it would be for attackers to automate device location information with vulnerability and exploit data.

Leverett used 33 queries to find the devices online, using the names of popular industrial control systems such as “SoftPLC,” a control system used primarily in Eastern Europe, and “Simatic S7,” a system made by Siemens that was targeted last year by the Stuxnet worm in an attack aimed at sabotaging Iran’s uranium enrichment program.

Using banner information that is broadcast by each connected system – such as the date and timezone, which can help place a machine geographically, as well as the type and version of servers and devices being used – Leverett searched databases for information about patched and unpatched vulnerabilities (including a list of new vulnerabilities that a group of researchers exposed in six industrial control systems at the S4 conference) as well as known exploits to attack those systems. Then he plugged the data into his visualization tool. Without trying to access the ICSes, Leverett was unable to determine if the devices that were found are patched, and therefore not vulnerable to the existing exploits, or if they are protected by intrusion prevention systems.

www.wired.com [1]

Posted by Janine E. Mooney, Editor

January 24, 2012

Source URL (retrieved on *03/10/2014 - 4:28am*):
http://www.wirelessdesignmag.com/news/2012/01/10k-reasons-worry-about-critical-infrastructure

Links:
[1] http://www.wired.com