Study finds Chinese Hardware Powers U.S. Voting Machine

December 16, 2019 12:37 by Paul Roberts

A new study by the firm Interos found that many hardware components in a popular touchscreen voting machine used in the U.S. originate in China or Russia.

Efforts by the federal government and campaigns to keep state sponsored hackers from Russia and China out of U.S. elections may have overlooked a one major source of vulnerability: the hardware and software 'guts' of voting machines.

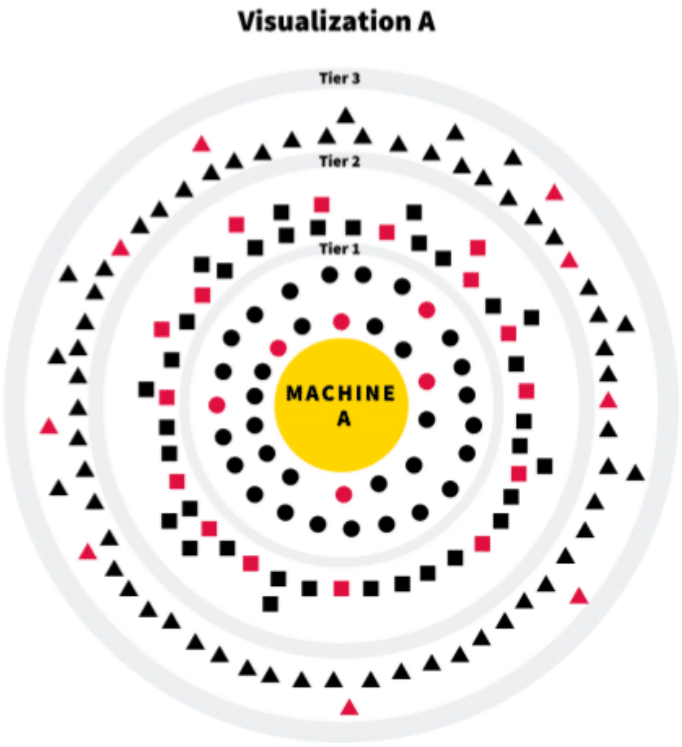
A study by the security firm **Interos** has found that one fifth (20%) of the hardware and software components in a popular voting machine came from suppliers in China. Furthermore, close to two-thirds (59%) of components in that voting machine came from companies with locations in both China and Russia.

The study is by Interos, a third party risk software company.* In it, the company analyzed both the hardware and software components used in a popular voting machine and then "mapped the supply chain" of the machine, including the companies

further down the supply chain. These fourth- and fifth party (or so-called "subtier") suppliers play a heretofore unstudied role in the creation of countless technology products, from networking gear to cameras and drones to voting machines.

Touchscreen Voting: Made in China

"Our study shows links previously not understood between America's voting infrastructure and countries with a proven aptitude and desire to target elections and the democratic process," **Jennifer Bisceglie**, the founder and CEO of Interos said in a published statement. "We must ensure similar attacks in future elections are thwarted, and that means outfitting organizations with the proper technology to vet all products in their voting infrastructure ecosystems."



Interos research found 20% of voting machine components came from companies headquartered in China or Russia.

Interos said it used its eponymous platform to identify and source data on the components in the electronic voting machine including import and export records, SEC filings and company websites.

Interos has not named the manufacturer of the touchscreen voting machine, which it refers to as "Machine A" in its study. However, it said the machine is "widely used across the United States and functions as a primary point of interface for voters."

The Suppliers' Suppliers Suppliers

The company broke down the voting machine into a list of component parts, identifying 140 digital and physical components. Those 140 components included 38 that it buys directly from another supplier ("Tier 1 suppliers"). Those 38 components were broken down into 50 "known parts" and Interos identified the suppliers of those parts ("Tier 2 suppliers). Those 50 known parts were further deconstructed, identifying a further 70 components. Interos then identified the businesses that provided those components ("Tier 3 suppliers").

Interos's study did not attempt to determine where the individual, component parts originated. Many of the suppliers merely had a presence in a country like China or Russia, which does not imply that its hardware or software products are sourced from that country.

More Questions as Expert Recreates Chinese Super Micro Hardware Hack

However, the nearly one fifth (19.6%) of suppliers who were China-based firms are sure to be a source of concern for voting integrity advocates in the U.S. government and civil society. Among that group of firms, 6 of 38 (16%) of the Tier 1 voting machine components and 16 of 50 (32%) of the Tier-2 components came from companies headquartered in China, Interos found.

Touchscreens and Processors and Tablets…Oh, My!

Among the China-based Tier-2 suppliers Interos identified is one, dubbed "Company A," that supplies hardware for touchscreens used by one of the voting machine's Tier 1 suppliers. Those components "are ultimately packaged as part of Machine A," Interos writes. Another firm, dubbed "Company B" is described as a "Shanghai-based company with locations in Russia." It provides machinery used by a major processor manufacturer to build processors that are used in Voting Machine A, Interos said.

Podcast Episode 120: They Email Ballots, Don't They?

Interos' study only assessed components that are part of the touchscreen voting machine's "core hardware and software." The company notes that the voting machine manufacturer counts many Chinese firms among Tier 1 suppliers of external components including power supply adapters, tablets, machine covers and other elements.

Supply Chain Scrutiny on the rise

In an environment of rising tensions between global players like China and the United States, so-called **supply chain risk has become an acute problem**.

In recent years, the U.S. Government has moved to limit the use of hardware and software from firms with ties to foreign governments including **Kaspersky Lab, the Russia anti-malware firm** and Huawei, the Chinese networking and equipment giant.

As Election Threats Mount, Voting Machine Hacks are a Distraction

The most recent National Defense Authorization Act (**PDF**) went a step further: banning the use or procurement of telecommunications and video surveillance services or equipment by a wide range of vendors from mainland China including Huawei, ZTE, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company.

That decision followed **years of warnings from security professionals** about security vulnerabilities, back door accounts and suspicious patterns of behavior from cameras and other technology manufactured in the People Republic of China. But two stories this week suggest that simply ordering the U.S. government to swear off Chinese hardware is easier said than done.

That may prove harder than the U.S. Government anticipated. In November, the Department of Justice unsealed a complaint that alleges the New York firm Aventura Technologies **engineered a years-long scheme to deceive the U.S. government**: selling Chinese manufactured cameras and other gear to the U.S. Military, the Department of Energy and other government agencies that it claimed were "Made in the U.S.A".

While the security of electronic voting machines has been a frequent topic of conversation within the security community, voting machine makers have been reluctant to open their platforms to scrutiny, beyond what is required by law. In 2018, for example, voting machine maker Election Systems & Software (ES&S) **declined an invitation to participate** in a white-hat hacking event at the **DEF-CON** hacking conference that would have tested the security of voting systems. The company said such hack-a-thons could actually jeopardize election security and invite hackers to disrupt electronic voting systems.

(*) Clarification: an earlier version of this story described Interos as a cyber security firm. It is a third party risk software firm. The story has been updated to reflect that. PFR December 16, 2019

Share this:

Related

Episode 172: Securing the Election Supply Chain

December 31, 2019

Security Holes Opened Back Door To TCL Android Smart TVs

November 12, 2020

As Election Threats Mount, Voting Machine Hacks are a Distraction

August 2, 2018

Tags: China, cyber espionage, elections, hardware, Russia, supply chain, voting machines

Author: Paul Roberts

I'm an experienced writer, reporter and industry analyst with a decade of experience covering IT security, cyber security and hacking, and a fascination with the fast-emerging "Internet of Things."

4 Comments

Anonymous

December 16, 2019 at 16:19

I wouldn't be worried. We've been warned about issues with voting machines for years:
http://www.notablesoftware.com/evote.html

No one cares.

Pingback: Episode 172: Securing the Election Supply Chain | Raymond Tec

Pingback: Seven Years Later, Scores of EAS Systems sit Un-patched, Vulnerable | Raymond Tec

Pingback: Episode 175: Campaign Security lags. Also: securing Digital Identities in the age of the DeepFake | Raymond Tec