



THE MALWARE REPORT

How Safe Are Electronic Voting Machines?

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

The Malware Report Transcript

Title: How Safe Are Electronic Voting Machines?

Episode: 91

Location: http://www.eset.com/podcasts/ESET100608_Electronic_Votin.mp3

October 16, 2008

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant and you're listening to The Malware Report with Randy Abrams. Hi Randy, thanks for being here.

Randy Abrams: Thank you for having me back again.

Matt Grant: We gave our listeners a tease on last week's Malware Report that we were going to be talking today about electronic voting; and some of those machines that are going to be used in the upcoming November election. A growing number of federal and state legislators are expressing doubt about the integrity of these types of voting machines. In this election over 150 million Americans will cast their ballot on one of these machines. How safe are these electronic voting machines?

Randy Abrams: Let me read to you a few headlines of articles that I have in my e-mail: "U.S. investigates voting machines' Venezuela ties," "Diebold voting machine hack exposed," "Hardware hacking a voting machine in four minutes," and "Evaluating the security of electronic voting systems." There's a lot to be worried about out there. One of the worst cases was where Diebold, or their subsidiary now, tried to blame an antivirus company for defects in their voting machine. If they've got antivirus on the voting machine, the voting machine is not properly secured. You shouldn't have the voting machine exposed to codes such that it would need antivirus software. It turned out that the problem was actually a bug in the voting machine software itself where it was dropping votes. That points to bad process, because the voting machine itself should have cross-checks in place that are fairly independent to assure that the proper number of votes are counted. If you put in 20 entries and you get 19 results, it's not that hard to measure and say "hey, there's a problem." On top of that, you should have an external count. When the people come in to vote they sign a register, you count the number of people that sign to vote and that should match the number of votes. There's good reason for concern about electronic voting machines; they haven't done it right.

Matt Grant: How do you monitor the security around these sorts of machines? What records are kept? Obviously with paper ballots, you have the paper ballots.

Those can be recounted to make sure they're legitimate. How do you do that with electronic voting?

Randy Abrams: It's pretty difficult. There should be an audit trail, and there hasn't been. Not that I've seen. Evidently there's some sort of audit trail, because they've figured out it was dropping votes and you have to have some information to figure that out.

Matt Grant: How easy would it be to tamper with some of these machines? Would it be like hacking into a computer? What would the process be?

Randy Abrams: One of the headlines I didn't read was "Hotel mini-bar keys open Diebold voting machines." Diebold actually put a picture of the key to the voting machine on the internet and people figured out that the key that's used in some hotel mini-bars will open a Diebold voting machine. That's the door that protects the memory card that stores the votes. And it's the main barrier to the injection of a virus. You can find that standard key widely available on the internet.

Matt Grant: How knowledgeable are the folks at the polls if somebody is trying to tamper with these devices? It doesn't seem like it would be that difficult.

Randy Abrams: They're kind-hearted sweet people that volunteer to work the polls at the polling places. I suspect it would pretty easy to socially engineer at least some of them and show up in a technician's outfit and say, "There's a problem. We've electronically monitored these machines to make sure they're functioning properly, and this one here is not functioning properly so I have to fix it." And they'll probably be back there with their hotel mini-bar key, opening the machine and tampering.

Matt Grant: We saw these electronic voting machines used four years ago. More than three times the amount of Americans are going to be using electronic voting

machines in this year's election. Has the technology gotten better over the last four years?

Randy Abrams: It should have. I'm not convinced it has.

Matt Grant: It sounds like some of the same vulnerabilities in terms of accessing the machine or hacking the machine, are still the same as they were four years ago.

Randy Abrams: Yes, and I don't know if the voting machine manufacturers have finally figured out to get some external help in figuring out how to secure these things. Manufacturing and computer security are significantly different fields. That's why we saw problems with USB devices coming out with viruses on them. It's because the people that understood manufacturing didn't understand how digital security is required in their manufacturing environment.

Matt Grant: Does it seem like it might be easy to modify a machine so you could alter the results of the election? And, if so, it seems like that would be difficult to detect, wouldn't it?

Randy Abrams: Yes, it's very difficult to detect. However, there are countries that are very happy with their electronic voting systems. Brazil's been using electronic voting for a decade and I haven't heard any reports out of Brazil about problems with their voting machines. Plus, more than 90% of Estonians vote online. We're not talking about a digital voting machine; we're talking about them voting right from their computer. I think far too much greed and too little thought went into the e-voting machines. It was a money maker for the companies making the e-voting machines, but they didn't want to invest in a quality product. And maybe it wasn't that they didn't want to, but they didn't even know they needed to.

Matt Grant: Do you know of any guidelines that are in place? And, if there aren't, should there be guidelines in place for these machines? How would the federal government regulate these types of devices?

Randy Abrams: There definitely need to be guidelines. They need to be written with the help of security experts such as Avi Rubin a professor of computer science at John Hopkins University. He wrote a book called *Brave New Ballot: the Battle to Safeguard Democracy in the Age of Electronic Voting*. He actually has come out saying he's more optimistic about voting systems. People like him that understand the security angles of voting machines need to be brought into the process of creating regulations. And then you have to audit you have to check and make sure that the voting machines are compliant to the regulations.

Matt Grant: Absolutely. I know this is a topic that hopefully we might be able to get to discuss again before the election or possibly after, to see what effects using these machines might have on the election. If you have any questions for us or are interested in talking more about this topic, feel free to send Randy an e-mail at askESET@ESET.com. This has been Matt Grant and you're listening to The Malware Report.

[End of recorded material]