

Heists go Hollywood with DefCon hacks

August 9 2015, by Glenn Chapman



Hollywood-style heists took on real-world potential as hackers at a Def Con gathering showed how to crack safes in full view of security cameras without ever being seen

Hollywood-style heists took on real-world potential as hackers at a Def Con gathering showed how to crack safes in full view of security cameras without ever being seen.

Independent computer researchers Eric Van Albert and Zach Banks found a way to pull off the movie-script ploy of intercepting [surveillance](#)

[camera](#) streams and then looping back video of nothing amiss while, ostensibly, safes or vaults are being emptied.

"We set out to create our own device as close to the movies as possible," Van Albert said as the pair demonstrated their work to an overflow crowd.

"To see how possible this kind of attack actually is."

They spent about \$500 to build a device they could splice into an ethernet cable carrying imagery from surveillance cameras to screens being watched by guards.

The creation, a box of electronics, re-routes incoming video feeds to their computer, where software tends to the job of creating harmless looking footage that is then fed to guards to mask a heist.

As in films, a team planning a theft would need to get access to the cable handling surveillance video. After that, a video signal intercept could be controlled from a far off location, according to the hackers.

Once a safe or vault was emptied and the team is safely away, the device could be removed with a victim being none-the-wiser.

Or it could be left in place to taunt guards by routing messages to their video screens or even playing back the heist.

"So, now they go and try to chase you down and stop the robbery, while you are 100 miles away and they are wondering what is going on," Banks said.

Cracking a smart safe

The looping video hack came just hours after researchers for security firm Bishop Fox showed how to hack open a smart safe made by Brinks using a computer thumb drive.

A key to cracking the computerized safe was plugging into a USB port built into one side to allow technicians to fix problems, such as it refusing to open.

The safe cracked by Daniel Petro and Oscar Salazar was designed to scan currency to track how much money was put in by merchants and use the Internet to credit bank accounts accordingly.

The safe has touch screen controls that could have also worked for the hack, but opting for the USB port was much faster because a more powerful computer could be used, according to the researchers.

"You need physical access to do the hack," Petro said. "But you need physical access to carry away the cash, so it is required either way."

Looping [video](#) from surveillance cameras might help with that but it could be too late. Petro and Salazar said they shared their research with Brinks, which came up with a fix.

© 2015 AFP

Citation: Heists go Hollywood with DefCon hacks (2015, August 9) retrieved 17 May 2024 from <https://phys.org/news/2015-08-heists-hollywood-defcon-hacks.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--