'o-day exploit middlemen are cowboys, ticking bomb' | ZDNet

Ryan Naraine

Prominent privacy rights advocate Christopher Soghoian is calling on the security research community to blackball middlemen companies that trade in vulnerabilities and exploits to governments.

During a presentation at the recent Kaspersky security analyst summit (see important disclosure), Soghoian warned of the risk of "blowback" if a weaponized zero-day sold to a foreign government is used against critical infrastructure in the U.S.

Soghoian (right) pinpointed VUPEN, FinFisher and HackingTeam among a handful of companies that buy and sell zero-day vulnerabilities, exploits and remote monitoring tools to governments around the world.

"As soon as one of these weaponized zero-days sold to governments is obtained by a 'bad guy' and used to attack critical U.S. infrastructure, the shit will hit the fan," Soghoian warned.

"It's not a matter of if, but when," he added.

Soghoian said these companies are purchasing vulnerabilities and exploits at prices ranging from $50,000 to $100,000 and work hard to keep these a secret forever. It's well known that companies like VUPEN never report vulnerabilities to vendors like Microsoft or Adobe and Soghoian said this presents a danger to the general public.

[SEE: 'Offensive security research community helping

bad guys']

"What if a low-paid, corrupt police officer sells a copy of one of these weaponized exploits to organized crime or terrorists?" Soghoian asked. "What if 'Anonymous' hacks into a law enforcement agency's network and steals one of these weaponized exploits?"

Noting that the security industry is completely unregulated, Soghoian said the current free-for-all encourages anyone to create weaponized exploits and sell them to shady agencies around the world. In addition to some of the companies he named, Soghoian said there are many middle-men vulnerability brokers who operate under the radar.

[SEE: Ten little things to secure your online presence]

"Governments are going to use zero-days, we have to deal with this," he declared. "But the middle-man firms that buy exploits and resell them to governments are a ticking bomb. Security researchers should not be selling zero-days to middle man firms."

"This trade is not legitimate and we should not legitimize them.

"These firms are cowboys and if we do nothing to stop them, they will drag the entire security industry into a world of pain," Soghoian added.