Massive breach shows how espionage is carried out in the 21st century

December 21 2020, by Mike Snider and Jessica Guynn

Credit: CC0 Public Domain

Forget KGB agents Russian intelligence officers masquerading as ordinary Americans to slip inside government agencies and steal national security secrets like in television's "The Americans."

The massive cyber assault on the U.S. government and private

companies perpetrated through networked computer systems is what 21st century espionage most commonly looks like. And these kinds of confrontations on a digital battlefield, cybersecurity researchers say, are our new normal.

We are in a state of "unpeace," not quite war but close and potentially just as dangerous. In this case, a nation-state, believed to be Russia, infiltrated the software supply chain on which the nation relies.

"We are currently witnessing the digital continuation of the once-analog spy games that all countries play," said Ross Rustici, global head of security architecture and threat intelligence at ZeroFOX, a Baltimore-headquartered cybersecurity firm.

Still, we think of this internet entity we seamlessly navigate daily as a mundane means of commerce and communication. But its origins were as a backup in case of chaos caused by real-world war. Now, this backup plan is a covert tunnel into places agents might otherwise have had to walk through a front door to access in earlier days.

How did cyberspace become today's battlefield?

Global superpowers strike this way as an alternative to military maneuvers or economic sanctions and as a response to such actions, said Ed Parsons, executive vice president of consulting for F-Secure, a cyber security firm based in Helsinki, Finland.

"For a country like Russia, aggression in cyberspace offers the opportunity to overcome the power imbalance encountered in traditional warfare domains, while offering advantages such as power projection and plausible deniability," Parsons said.

Researchers say neglect of these security vulnerabilities during the

Trump administration has left the country even more exposed.

"The unique concern of today, is not that this activity is ongoing—it has been since the first two towns were created—but rather that the U.S. is more vulnerable to this type of activity than it has been in the past," Rustici said.

Networks are the targets by nation-states and criminal organizations because, in our hyperconnected 21st century world, that's where the information is, says Steve Bellovin, computer science professor at Columbia University School of Engineering.

How hackers pulled off the latest caper

As far back as nine months ago, the infiltrators began penetrating federal and private computer systems through much-used server software from a company called SolarWinds.

The breach was stealthy and sophisticated and likely took years to prepare, Bellovin said.

Massive breaches are most likely caused by simple, but diligent, probing of corporations or agencies, says DvirSasson, head of research for CyberInt, a Tel Aviv, Israel-headquartered security firm.

"They do not come from guys lurking in the shadows trying to crack passwords or physically attack servers," Sasson said. "It can be something as simple as a phishing campaign."

President Trump has been loath to criticize Russia and has not commented on this cyber assault. And a month ago, the president dismissed Christopher Krebs, the Department of Homeland Security's cyber chief, after he said there was no evidence of fraud in the 2020

elections.

Post-election division remains a problem and there's a bumpy transition between the Trump and Biden administrations. "Russia is fully aware of how vulnerable a time it is for the United States," said Lior Div, CEO of Cybereason, a cybersecurity firm headquartered in Boston. "On top of that, leaders have been heads down on the election and working to combat disinformation regarding COVID-19 research and vaccines. This malicious operation into U.S. government agencies could be considered an act of war."

He was not alone in drawing an analogy between the cyber attack and military attacks. U.S. Rep. Jason Crow, D-Colo., said the event "could be our modern day, cyber equivalent of Pearl Harbor."

Microsoft president Brad Smith on CNN said such a parallel description was "appropriate," calling the breach "a wake-up call (and) a moment of reckoning."

But this crisis cannot be totally blamed on Trump, Bellovin says. "Everybody is dumping on Trump for shortchanging cybersecurity and not going after Russia. I won't disagree with any of that," he said. "This was a long-term, very sophisticated plan."

And he says the number of intelligence agencies that could pull it off are in the slim single-digits.

The concern? Increasing rates of cyber aggression by nation-states and criminal actors suggest the international community has not done enough to deter attacks, Parsons said.

He frets that these attacks undermine confidence in the nation's technology and security companies that are the backbone of our digital

economy. What keeps him up at night? That cyber incidents could trigger a military response.

Peter Singer, author of near-futuristic novels he dubs "useful fiction," envisioned how cyber warfare can escalate into real warfare in the 2020 book "Burn-In," written with co-author August Cole. In the book, a cyber attacker bombards Washington, D.C., with a plague including the reddening of the Potomac River (through remote attacks on chemical waste treatment) and drones being manipulated to fly into monuments.

Instead of simply stealing information, intruders "might cause kinetic, physical change through cyber means," he said.

The good news? Governments and private companies are increasingly cooperating to deter such infiltrations.

And so far, individual Americans have not been directly affected by the SolarWinds hack.

"At this point, from what we know now, there is no direct impact on the average person's information," Bellovin said. "This is intelligence agency and their interest is in government secrets."

And their target is not your credit card or bank account, but every computer on a desk in Washington. "Access to you would be called collateral damage," he said.