Casting a wide intrusion net: Dozens burned with single hack

March 7 2021, by Frank Bajak

In this Feb. 23, 2021 file photo, SolarWinds CEO Sudhakar Ramakrishna speaks during a Senate Intelligence Committee hearing on Capitol Hill in Washington. The victim count in the mega-hack of a file-transfer program popular with big companies continues to grow. Much like the SolarWinds hacking campaign, the hack of dozens of Accellion customers on at least four continents suggests both government and the private sector have been falling far short in a digital age core mission: Protecting sensitive data.(Demetrius Freeman/The Washington Post via AP, Pool)

The SolarWinds hacking campaign blamed on Russian spies and the "grave threat" it poses to U.S. national security are widely known. A very different—and no less alarming—coordinated series of intrusions also detected in December has gotten considerably less public attention.

Nimble, highly skilled criminal hackers believed to operate out of Eastern Europe hacked dozens of companies and government agencies on at least four continents by breaking into a single product they all used.

The victims include New Zealand's central bank, Harvard Business School, Australia's securities regulator, the high-powered U.S. law firm Jones Day—whose clients include former President Donald Trump—the rail freight company CSX and the Kroger supermarket and pharmacy chain. Also hit was Washington state's auditor's office, where the personal data of up to 1.3 million people gathered for an investigation into unemployment fraud was potentially exposed.

The two-stage mega-hack in December and January of a popular file-transfer program from the Silicon Valley company Accellion highlights a threat that security experts fear may be getting out of hand: intrusions by top-flight criminal and state-backed hackers into software supply chains and third-party services.

Operating system companies such as Microsoft have long been bull's-eyes—with untold thousands of installations of its Exchange email server being violated globally in the past few weeks, mostly after the company issued a patch and disclosed that Chinese state hackers had penetrated the program.

The Accellion casualties have kept piling up, meanwhile, with many being extorted by the Russian-speaking Clop cybercriminal gang, which

threat researchers believe may have bought pilfered data from the hackers. Their threat: Pay up or we leak your sensitive data online, be it proprietary documents from Canadian aircraft maker Bombardier or lawyer-client communications from Jones Day.

The hack of up to 100 Accellion customers, who were easily identified by the hackers with an online scan, puts in painful relief a digital age core mission at which both governments and the private sector have been falling short.

"Attackers are finding it harder and harder to gain access via traditional methods, as vendors like Microsoft and Apple have hardened the security of the operating systems considerably over the last years. So, the attackers find easier ways in. This often means going via the supply chain. And as we've seen, it works," said Mikko Hypponen, chief research officer of the cybersecurity firm F-Secure.

Members of Congress are already dismayed by the supply-chain hack of the Texas network management software company SolarWinds that allowed suspected Russian state-backed hackers to tiptoe unnoticed—apparently intent solely on intelligence-gathering—for more than half a year through the networks of at least nine government agencies and more than 100 companies and think tanks. Only in December was the SolarWinds hacking campaign discovered, by the cybersecurity firm FireEye.

France suffered a similar hack, blamed by its cybersecurity agency on Russian military operatives, that also gamed the supply chain. They slipped malware into an update of network management software from a firm called Centreon, letting them quietly root around victim networks from 2017 to 2020.

Both those hacks snuck malware into software updates. The Accellion

hack was different in one key respect: Its file-transfer program resided on victims' networks either as a stand-alone appliance or cloud-based app. Its job is to securely move around files too large to be attached to email.

Mike Hamilton, a former Seattle chief information security officer now with CI Security, said the trend of exploiting third-party service providers shows no signs of slowing because it gives criminals the highest return on their investment if they "want to compromise a broad swath of companies or government agencies."

The Accellion breach's impact might have been dulled had the company alerted customers more quickly, some complain.

The governor of New Zealand's central bank, Adrian Orr, says Accellion failed to warn it after first learning in mid-December that the nearly 20-year-old FTA application—using antiquated technology and set for retirement—had been breached.

Despite having a patch available on Dec. 20, Accellion did not notify the bank in time to prevent its appliance from being breached five days later, the bank said.

"If we were notified at the appropriate time, we could have patched the system and avoided the breach," Orr said in a statement posted on the bank's website. Among information stolen were files containing personal emails, dates of birth and credit information, the bank said.

Similarly, the Washington state auditor's office has no record of being informed of the breach until Jan. 12, the same day Accellion announced it publicly, said spokeswoman Kathleen Cooper. Accellion said then that it released a patch to the fewer than 50 customers affected within 72 hours of learning of the breach.

Accellion now tells a different story. It says it alerted all 320 potentially affected customers with multiple emails beginning on Dec. 22—and followed up with emails and phone calls. Company spokesman Rob Dougherty would not directly address the New Zealand central bank's and Washington state auditor's complaints. Accellion says fewer than 25 customers appear to have suffered significant data theft.

A timeline released March 1 by the cybersecurity firm Mandiant, which Accellion hired to examine the incident, says the company got first word of the breach on Dec. 16. The Washington state auditor says its hack occurred on Christmas.

The notification timing issue is serious. Washington state has already been hit by a lawsuit, and several have been filed against Accellion seeking class action. Other organizations could also face legal or other consequences.

Last month, Harvard Business School officials emailed affected students to tell them that some Social Security numbers had been compromised as well as other personal information. Another victim, the Singapore-based telecommunications company Singtel, said personal data on about 129,000 customers was compromised.

Too often, software companies with hundreds of programmers have just one or two security people, said Katie Moussouris, CEO of Luta Security.

"We wish we could say that organizations were uniformly investing in security. But we're actually seeing them just dealing with the breaches and then vowing to do better in the future. And that's been sort of the business model."

Dougherty, the Accellion spokesman, said the attacks "had nothing to do

with staffing," but he would not say how many people directly assigned to security the company employed in mid-December.

Cybersecurity threat analysts hope the snowballing of supply-chain hacks stuns the software industry into prioritizing security. Otherwise, vendors risk the fate that has befallen SolarWinds.

In a filing this past week with the Securities and Exchange Commission, the company offered a bleak outlook.

It said that as supply-chain hacks "continue to evolve at a rapid pace" it "may be unable to identify current attacks, anticipate future attacks or implement adequate security measures."

The ultimate, painful upshot, the document added:

"Customers have and may in the future defer purchasing or choose to cancel or not renewal their agreements or subscriptions with us."