ABOUT THE LOCKHEED MARTIN HACK

As first started leaking last week, Lockheed Martin seems to have been hacked.

> Last weekend was bad for a very large U. S. defense contractor that uses SecureID tokens from RSA to provide two-factor authentication for remote VPN access to their corporate networks. Late on Sunday all remote access to the internal corporate network was disabled. All workers were told was that it would be down for at least a week. Folks who regularly telecommute were asked to come into nearby offices to work. Then earlier today (Wednesday) came word that everybody with RSA SecureID tokens would be getting new tokens over the next several weeks. Also, everybody on the network (over 100,000 people) would be asked to reset their passwords, which means admin files have probably been compromised.

What seems to have happened is hackers used information gotten in the RSA Data Security hack to try to break Lockheed's own security—basically, Lockheed noticed that hackers were trying to use the keys they stole in March to open a bunch of locks at Lockheed. Lockheed appears to have discovered the effort and in response, started shutting down remote access on parts of its network.

> Lockheed Martin, the Pentagon's No. 1 supplier, is experiencing a major disruption to its computer systems that could be related to a problem with network security, a defense official and two sources familiar with the issue said on Thursday.
>
> Lockheed, the biggest provider of information technology to the U.S.

> government, is grappling with “major internal computer network problems,” said one of the sources who was not authorized to publicly discuss the matter.
>
> [snip]
>
> The slowdown began on Sunday after security experts for the company detected an intrusion to the network, according to technology blogger Robert Cringely. He said it involved the use of SecurID tokens that employees use to access Lockheed’s internal network from outside its firewall,
>
> [snip]
>
> Loren Thompson, chief operating officer of the Lexington Institute, and a consultant to Lockheed, said the company monitored every node on its vast global computer network from a large operations center in a Maryland suburb near Washington, D.C.
>
> “If it sees signs that the network is being compromised by outsiders it will shut down whole sectors of the network to protect information,” Thompson said.
>
> He said Lockheed had advanced networking monitoring tools that gave it a “much better understanding of their systems’ status than most other organizations, including the Department of Defense.”

In other words, Lockheed may have prevented a much bigger breach into their own systems. But the assumption of many is that other companies might not have noticed what Lockheed did. Stories on this hack all feature a list of other defense contractors—like Boeing and Raytheon and Northrup Grumman—who “decline to comment,” which might mean they’re scrambling to address the same problem Lockheed is, only trying to do so without all the bad PR.

Now, most observers of this hack have suggested that the hackers—who might work for a state actors or some other sophisticated crime group—were after Lockheed's war toy information (which partly explains why you'd ask Lockheed's aerospace competitors if they'd been hacked too). But remember that Lockheed does a lot for the government besides build planes. Of particular note, they're a huge NSA contractor. Maybe the hackers were after info on jet fighters, or maybe they were after the data and data collection programs our own government hides from its own citizens.

Which is all a reminder that, amidst the sound and fury directed at WikiLeaks (which after all shared important information with citizens who deserved to know it), there's a whole lot more hacking we don't learn the results of, hacking that either might result in others adopting our lethal technologies, or in third parties stealing the data we're not even allowed to know.

Now, granted, Lockheed has far far better security than DOD's SIPRNet does. At least they're trying to protect their data. But it's not clear they—or their counterparts—are entirely successful.