SHADOW BROKERS: "ALL YOUR BASES ARE BELONG TO US"

Back when Shadow Brokers doxxed some NSA hackers, I argued some allusions Shadow Brokers made served as a kind of warning, in that case directed at people who hack for NSA. As I understand it, Shadow Brokers' threats reflected access to specific and accurate information.

Though I haven't confirmed any of these details, yesterday's Shadow Brokers post *seems* to do more of the same, although this time directed at NSA itself.

Consider this passage:

> In April, 90 days from theequationgroup show and tell, 30 days from Microsoft patch, theshadowbrokers dumps old Linux (auction file) and windows ops disks. Because why not? TheShadowBrokers is having many more where coming from? "75% of U.S. cyber arsenal" TheShadowBrokers dumped 2013 OddJob from ROCTOOLS and 2013 JEEPFLEAMARKET from /TARGETS. This is theshadowbrokers way of telling theequationgroup "all your bases are belong to us". TheShadowBrokers is not being interested in stealing grandmothers' retirement money. This is always being about theshadowbrokers vs theequationgroup.

Shadow Brokers starts by saying it just dropped the EternalBlue dump, along with some other files, because "The ShadowBrokers is having many more where [those were] coming from." Shadow Brokers then cites from a detail first reported in a WaPo report (though presents the factoid as a direct quote when it is not): that Hal Martin stole 75% of the US cyberarsenal. The WaPo report actually stated that Martin had stolen "75 percent of TAO's library of hacking tools."

Shadow Brokers then made some assertions that may disprove a claim WaPo made yesterday: "It is not clear how the Shadow Brokers obtained the hacking tools, which are identical to those breached by former NSA contractor Harold T. Martin III, according to former officials." It described exactly where, on the NSA servers, the files came from. "TheShadowBrokers dumped 2013 OddJob from ROCTOOLS and 2013 JEEPFLEAMARKET from /TARGETS." Having suggested it had at least seen file paths or screen caps of the NSA's file system, Shadow Brokers then made its point even more clear: "This is theshadowbrokers way of telling theequationgroup 'all your bases are belong to us'," both making fun of the claims about its broken language but also suggesting takeover (though I'm curious if mis-citation using a plural here is intentional — perhaps these file systems are in different places? — or just one of a some egregious typos in this post).

Again, I haven't confirmed whether those details are accurate. Surely the NSA has doublechecked. If they are accurate, then the other claims made in the post — specifically about the other things it has to dump — will especially merit attention.

> TheShadowBrokers Monthly Data Dump could be being:
>
> - *web browser, router, handset exploits and tools*
> - *select items from newer Ops Disks, including newer exploits for Windows 10*
> - *compromised network data from more SWIFT providers and Central banks*
> - *compromised network*

> *data from Russian, Chinese, Iranian, or North Korean nukes and missile programs*

One more point. Shadow Brokers seems to suggest Oracle and another Microsoft patch were due to notice from former NSA hackers, as if all the former NSA employees are helping their employers clean up holes they've long known about.

> Oracle is patching huge numbers of vulnerabilities but TheShadowBrokers is not caring enough to be look up exact dates.
>
> [snip]
>
> TheShadowBrokers is thinking Google Project Zero is having some former TheEquationGroup member. Project Zero recently releasing "Wormable Zero-Day" Microsoft patching in record time, knowing it was coming? coincidence?

It's not clear whether they'd be doing this because they knew of holes NSA had been using or not.

But it's worth observing that Shadow Brokers is not making vague threats here.