ShadowBrokers Dump More Equation Group Hacks, Auction File Password

By Michael Mimoso

Published: 2017-04-10 · Archived: 2026-04-05 12:52:33 UTC

The ShadowBrokers' latest dump of Equation Group hacks focuses on UNIX systems and GSM networks, and was accompanied by an open letter to President Trump.

The mysterious ShadowBrokers, long thought to have given up their cause, released on Saturday additional hacking tools allegedly belonging to the Equation Group, along with the password guarding the original set of exploits the group planned to auction off.

The password was at the tail end of a rambling open letter to President Donald Trump in which the ShadowBrokers expressed their discontent with the administration's actions in Syria, its defeat on Obamacare, the removal of Steve Bannon from the National Security Council and more.

"Respectfully, what the f%&k are you doing? TheShadowBrokers voted for you. TheShadowBrokers supports you. TheShadowBrokers is losing faith in you," the letter begins.

As for the tools, as in past leaks it appears these are older exploits. They run the gamut from remote code execution attacks against enterprise operating systems such as Solaris, Netscape Server, FTP servers, various webmail clients and more.

There are also a number of antiforensics tools that the Equation Group, linked in many circles to the National Security Agency, uses to clean up its tracks after an intrusion.

Saturday's dump also includes a number of backdoors and post-exploitation remote access shells for UNIX and SPARC systems, as well as keyloggers, network monitoring tools and kernel-level implants for UNIX systems.

"What is stunning is the way it specifically targets Solaris/HP-UX systems that are most likely used in big corporations or telecoms companies," said a researcher who goes by the handle x0rz. "Which means they are in for the big fish."

The extent of the Equation Group's reach into its targets is illustrated in a long list of compromised hosts and tools used against them, including UNIX backdoors PITCHIMPAR and INTONATION.

X0rz was among a handful of researchers who examined the dump over the weekend and posted the files and an index for other researchers to examine. X0rz said the Equation Group was particularly invested in exploiting and attacking GSM core networks. GSM stands for Global System for Mobile Communication, used primarily in Europe, and is the telephony system for data compression and transmission; there are estimated five billion GSM phone users worldwide.

In one instance, it appears the Equation Group had access to the Pakistan Mobilink GSM network.

“From what I understand they have tools to collect CDRs (Call detail record) that are generated on GSM core networks for billing purpose (who is calling who, etc.),” x0rz said. “They are deep into these systems.”

There are more than 1,000 files included in the dump and it’s unknown whether any of the vulnerabilities being exploited remain unpatched.

Edward Snowden, the NSA whistleblower, said in a series of tweets on Saturday that the latest dump does not represent the totality of the NSA’s hacking tools.

In January, the ShadowBrokers said they were done and were deleting all of their accounts. The group did first put a set of Windows exploits for sale for 750 Bitcoin which included a zero-day exploit for a Windows SMB protocol flaw. Researcher Jacob Williams looked at the screenshots and surmised the zero day by the price the ShadowBrokers are asking.

“Note that most of the tools have apparently been through multiple revisions, adding apparent legitimacy to the claim that these exploits are real,” Williams said. “Though another screenshot hints at a possible zero day SMB exploit, there’s no indication of which exploit names involve SMB (or any other target service).”

The identity of the ShadowBrokers remains open for debate, and the candidates could be anyone from an intelligence outfit, to a NSA insider. Saturday’s letter gives no concrete clues as to who they may be, or their motivations.
