Iridium cyberespionage gang behind Aussie parliament attacks

By Doug Olenick

Published: 2019-03-02 · Archived: 2026-04-05 18:57:23 UTC

Content

Iranian actors that are possibly backed by segments of that nation's government are likely behind an on-going cyberespionage campaign that most recently targeted the Australian Parliament.

The group named Iridium is the likely culprit, reported Resecurity in a recent report, which gave an extensive look at the gang, its targets and some of its past operations. The company did not directly tie Iridium to Iran, but laid out a the circumstantial evidence that may point in that direction.

The Australian attacks began on December 23, 2018, when two government agencies were penetrated resulting in a two-stage attack taking place in January and February 2019.

Resecurity said the first stage was oriented toward Windows-based server-side environments with the second state of the attack happening in February 2019, leveraging targeted email compromise through a government Global Access List. This list gave Resecurity one of its best clues to indicate Iridium had penetrated into the Australian system as the security firm found the list in a file confirmed as being used by Iridium.

"It stands as evidence of a successful email compromise because a threat actor needs to have hacked into at least one account on the Parliament server to have dumped this information. Once access has been gained and the network intrusion has been conducted, IRIDIUM uses proprietary developed tradecraft and also web shells and back-connect backdoors that are available on the dark web and through public sources.," the report stated.

Resecurity through its research was able to put together a dossier on Iridium. The gang acts on behalf of an intelligence agency focused on foreign politicians and whose multi-year campaign with spikes in activity just after anti-Iranian activity takes place on the world stage such as when the Iran nuclear deal was revoked by the U.S. Australia is not a signatory of the deal, but late last year considered pulling its endorsement, or after an event marking 70 years of friendship between Australia and Israel.

Generally, Iridium attacks sensitive government, diplomatic, and military resources in the countries comprising the Five Eyes intelligence alliance, Australia, Canada, New Zealand, the U.K. and the United States.

The group itself is not just comprised of Iranians, but also includes Syrians, Lebanese, Palestinians and for hire black hats. Their contributions can make final attribution difficult, Resecurity said.

Other bits of evidence that point to Iran are that the tools, techniques and procedures associated with these attack patterns are almost identical to those of the Mabna Hackers and other actors having close ties with the Iranian Revolutionary Guard Corps, Resecurity said. Mabna is also believed to have conducted a massive strike last year against 320 universities in 22 countries.

The attacks were severe enough to warrant having the parliamentarians change their passwords, Resecurity said.

Doug Olenick

Related

DevSecOps Scanning Challenges & Tips

Bill BrennerOctober 26, 2021

There are many ways to do DevSecOps, and each organization — each security team, even — uses a different approach. Questions such as how many environments you have and the frequency of deployment of those environments are important in understanding how to integrate a security scanner into your DevSecOps machinery. The ultimate goal is speed […]

It Should Be 'Cybersecurity Culture Month'

Bill BrennerOctober 19, 2021

It's Cybersecurity Awareness Month, but security awareness is about much more than just dedicating a month to a few activities. Security awareness is a journey, requiring motivation along the way. And culture. Especially culture.That's the point Proofpoint Cybersecurity Evangelist Brian Reed drove home in a recent appearance on Business Security Weekly."If your security awareness program […]

Get daily email updates

SC Media's daily must-read of the most current and pressing daily news

---

Source: https://www.scmagazine.com/home/security-news/apts-cyberespionage/iridium-cyberespionage-gang-behind-aussie-parliament-attacks/