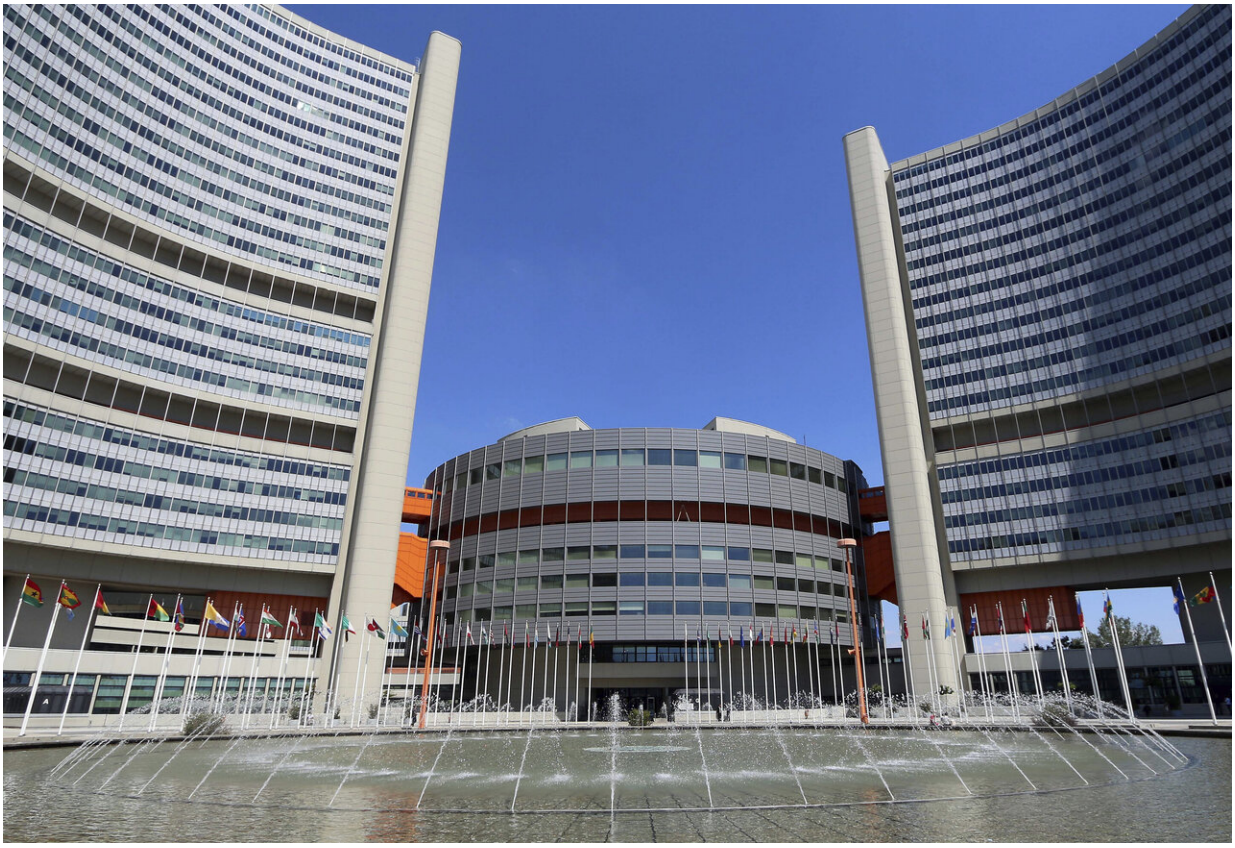
Leaked report shows United Nations suffered hack

January 29 2020, by Jamey Keaten and Frank Bajak



In this June 18, 2014, file photo flags fly outside the United Nations building in Vienna, Austria. An internal confidential document from the United Nations, leaked to The New Humanitarian and seen by The Associated Press, says that dozens of servers were "compromised" at offices in Geneva and Vienna. (AP Photo/Ronald Zak, File)

Sophisticated hackers infiltrated U.N. networks in Geneva and Vienna last year in an apparent espionage operation that top officials at the world body kept largely quiet. The hackers' identity and the extent of the data they obtained are not known.

An internal confidential document from the United Nations, leaked to The New Humanitarian and seen by T he Associated Press, says dozens of servers were compromised including at the U.N. human rights office, which collects sensitive data and has often been a lightning rod of criticism from autocratic governments for exposing rights abuses.

Everything indicates knowledge of the breach was closely held, a strategy that information security experts consider misguided because it only multiplies the risks of further data hemorrhaging.

" Staff at large, including me, were not informed," said Geneva-based Ian Richards, president of the Staff Council at the United Nations. "All we received was an email (on Sept. 26) informing us about infrastructure maintenance work." The council advocates for the welfare of employees of the world body.

Asked about the intrusion, one U.N. official told the AP i t appeared "sophisticated" with the extent of damage unclear, especially in terms of personal, secret or compromising information that may have been stolen. The official, who spoke only on condition of anonymity to speak freely about the episode, said systems have since been reinforced.

Given the high skill level, it is possible a state-backed actor was behind it, the official said. "It's as if someone were walking in the sand, and swept up their tracks with a broom afterward," the official added. "There's not even a trace of a clean-up."

The leaked Sept. 20 report says logs that would have betrayed the

hackers' activities inside the U.N. networks—what was accessed and what may have been siphoned out—were "cleared." It also shows that among accounts known to have been accessed were those of domain administrators— who by default have master access to all user accounts in their purview.

"Sadly ... still counting our casualties," the report says.

Jake Williams, CEO of the cybersecurity firm Rendition Infosec and a former U.S. government hacker, said the fact that the hackers cleared the network logs indicates they were not top flight. The most skilled hackers—including U.S., Russian and Chinese agents—can cover their tracks by editing those logs instead of clearing them.

"The intrusion definitely looks like espionage," said Williams, noting that the active directory component— where all users' permissions are managed—from three different domains were compromised: those of United Nations offices in Geneva and Vienna and of the Office of the High Commissioner for Human Rights.

"This, coupled with the relatively small number of infected machines, is highly suggestive of espionage," he said after viewing the report. "The attackers have a goal in mind and are deploying malware to machines that they believe serve some purpose for them."

Any number of intelligence agencies from around the globe are likely interested in infiltrating the U.N., Williams said.

The hack was not severe at the U.N. human rights office, said its spokesman, Rupert Colville.

"We face daily attempts to get into our computer systems ," Colville said. " This time, they managed, but it did not get very far. Nothing

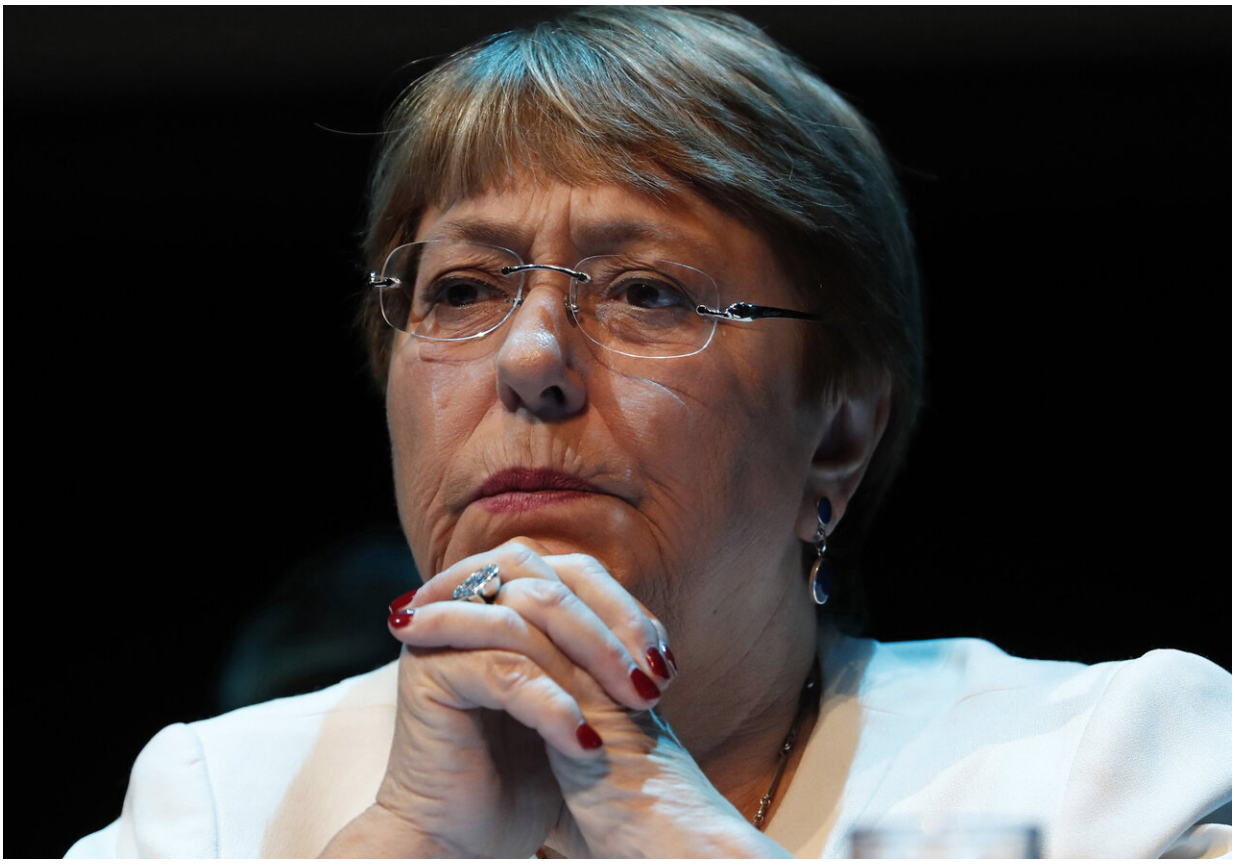
confidential was compromised."

U.N. spokesman Stephane Dujarric said the attack "resulted in a compromise of core infrastructure components" and was "determined to be serious." The earliest detected activity related to the intrusion occurred in July and it was detected in August, he said in response to emailed questions.

He said the world body does not have enough information to determine the author but added"the methods and tools used in the attack indicate a high level of resource, capability and determination.

"The damage related to this specific attack has been contained, and additional mitigation measures implemented," Dujarric wrote. "Nevertheless the threat of future attacks continues, and the United Nations Secretariat detects and responds to multiple attacks of various level of sophistication on a daily basis."

Peter Micek, general counsel of the digital civil liberties nonprofit AccessNow, said U.N. leadership made a "terrible decision" from an information-security standpoint by denying staff information about the breach.



In this April 9, 2019, file photo Michelle Bachelet, United Nations High Commissioner for Human Rights, attends a press conference at the Cultural Center of Spain, in Mexico City. An internal confidential document from the United Nations, leaked to The New Humanitarian and seen by The Associated Press, says that dozens of servers were "compromised" at offices in Geneva and Vienna. Those include the U.N. human rights office, which has often been a lightning rod of criticism from autocratic governments for its calling-out of rights abuses. (AP Photo/Marco Ugarte, File)

"It's best practice to alert people, let them know what they should look out for (including phishing attacks and social engineering) and inform them of what steps are being taken on their behalf," he said.

Otherwise, you are compounding the threat, and a missed opportunity for a teaching moment becomes an example of "intransigence and obfuscation, which is unfortunate," said Micek, who works with U.N. human rights workers to shore up their cyber-defenses.

The internal document from the U.N. Office of Information and Technology said 42 servers were "compromised" and another 25 were deemed "suspicious," nearly all at the sprawling Geneva and Vienna offices. Three of the "compromised" servers belonged to Human Rights agency, which is located across town from the main U.N. office in Geneva, and two were used by the U.N. Economic Commission for Europe.

The report says a flaw in Microsoft's SharePoint software was exploited by the hackers to infiltrate the networks but that the type of malware used was not known, nor had technicians identified the command and control servers on the internet used to exfiltrate information. Nor was it known what mechanism was used by the hackers to maintain their presence on the infiltrated networks.

Security researcher Matt Suiche, the Dubai-based founder of the cybersecurity firm Comae Technologies, reviewed the report and said it appeared entry was gained through an anti-corruption tracker at the U.N. Office of Drugs and Crime.

The report mentions a range of IP addresses in Romania that may have been used to stage the infiltration, and Williams said one is reported to have some neighbors with a history of hosting malware.

Technicians at the United Nations office in Geneva, the world body's European hub, on at least two occasions worked through weekends in recent months to isolate the local U.N. data center from the i nternet, re-write passwords and ensure the systems were clean. Twenty machines

had to be rebuilt, the report says.

The hack comes amid rising concerns about cyber espionage.

Last week, U.N. human rights experts asked the U.S. government to investigate a suspected Saudi hack that may have siphoned data from the personal smartphone of Jeff Bezos, the Amazon founder and owner of The Washington Post, in 2018. On Tuesday, the online civil rights sleuths at Citizen Lab published a report on the attempted hack of the T he New York Times's bureau chief in Beirut, Ben Hubbard, about the same time by a Saudi-linked group.

The United Nations, and its human rights office, is particularly sensitive, and could be a tempting target. The U.N. High Commissioner for Human Rights, Michelle Bachelet, and her predecessors have called out, denounced and criticized alleged war crimes, crimes against humanity and less severe rights violations and abuses in places as diverse as Syria and Saudi Arabia.

Dozens of independent human rights experts who work with the U.N. human rights office have greater leeway—and fewer political and financial ties to the governments that fund the United Nations and make up its membership— to denounce alleged rights abuses.

Richards expressed concern about the safety of U.N. networks .

"There's a lot of our data that could have been hacked, and we don't know what that data could be," said Richards of the U.N. Staff Council. Potentially affected, for example, are staff in the office of the special envoy for Syria carrying out sensitive investigations and human rights staffers interviewing witnesses.

"How much should U.N. staff trust the information infrastructure the

U.N. is providing them?" Richards asked. "Or should they start putting their information elsewhere?"