Another Hacker Selling Access to Charity, Antivirus Firm Networks

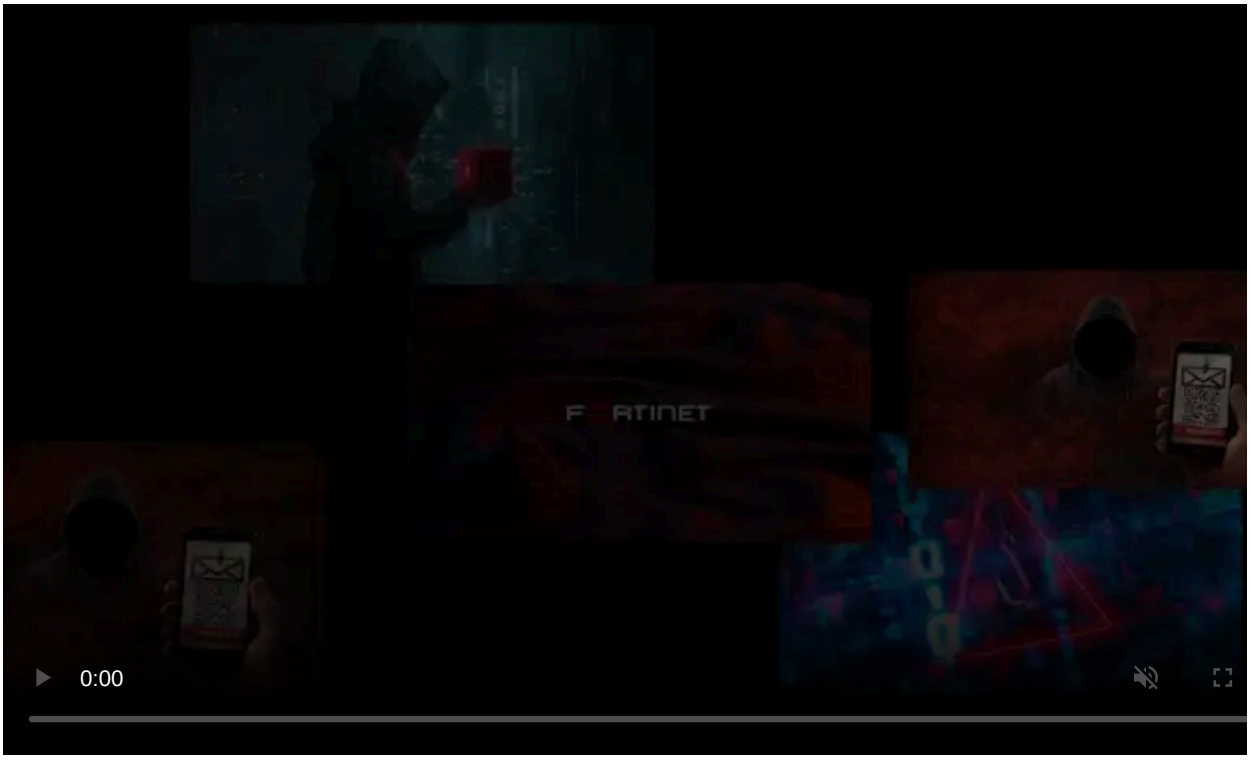
By Ionut Ilascu

Published: 2019-06-06 · Archived: 2026-04-05 21:25:02 UTC

A threat actor observed on underground hacker forums peddling internal network access to various entities claims to have breached the infrastructure of notable organizations such as UNICEF and cybersecurity companies Symantec and Comodo.

The hacker uses the online name Achilles and offers to sell details for a way in for modest prices, between $2,000 and $5,000, depending on the value of the target. Their activity jumped over the past seven months particularly in Fall 2019 and Spring 2019.

This appears to be a different threat actor than Fxmsp, who advertised access to antivirus companies with offices in the U.S., namely Symantec, McAfee, and Trend Micro. While Fxmsp is believed to be a group of Russian-speaking hackers, the new seller speaks English and may be Iranian.

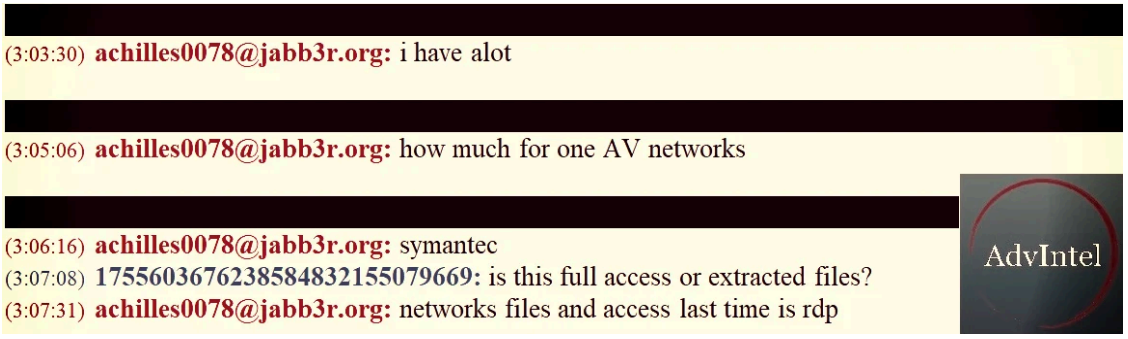

F RTINET
0:00

Hacker built a good reputation

A report from fraud prevention company Advanced Intelligence (AdvIntel) notes that Achilles enjoys a good reputation and positive reviews on the forums they advertise on and has a record of sales. To increase credibility, the hacker insists that payment for some deals be completed through the forum's escrow service.

In conversations with potential buyers, Achilles said they could get into internal networks belonging to Symantec, cybersecurity company Comodo, 3-D software maker Hash Inc, and children's rights protection advocate UNICEF.

The hacker states in private messages that Symantec's internal infrastructure is possible through a remote desktop connection. The same type of illegal entry was advertised for Hash Inc.

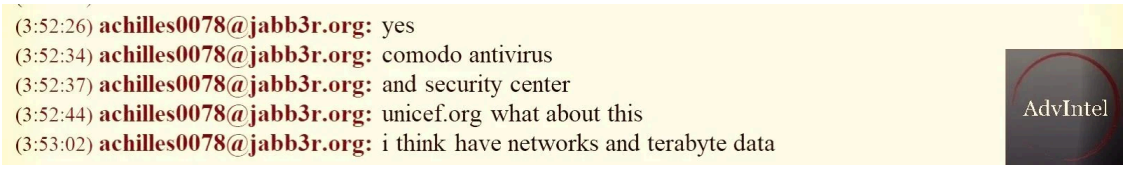


Answering our request for comments, a Symantec spokesperson provided the following statement to BleepingComputer.

“At this time, Symantec has no evidence of a network intrusion, nor do we believe there is a reason for our customers to be concerned.”

Unsupported claims

The claims of having access to Comodo's network is shown in in private messages between Achilles and potential buyers. There is no evidence that such access exists and Comodo and has not responded to BleepingComputer's queries regarding the alleged access.



According to AdvIntel, the hacker also tried to sell entry into the corporate network of Transat, a Canadian holiday travel company. They claim to have breached their network on May 12 or May 13.

Although the affirmations are bold, all this could be just talk, despite the good reputation the actor has on underground forums. The report from AdvIntel report comments that the hacker provided no evidence to support their claims about breaching the networks of Symantec, Comodo, and Transat.

Terabytes of UNICEF data

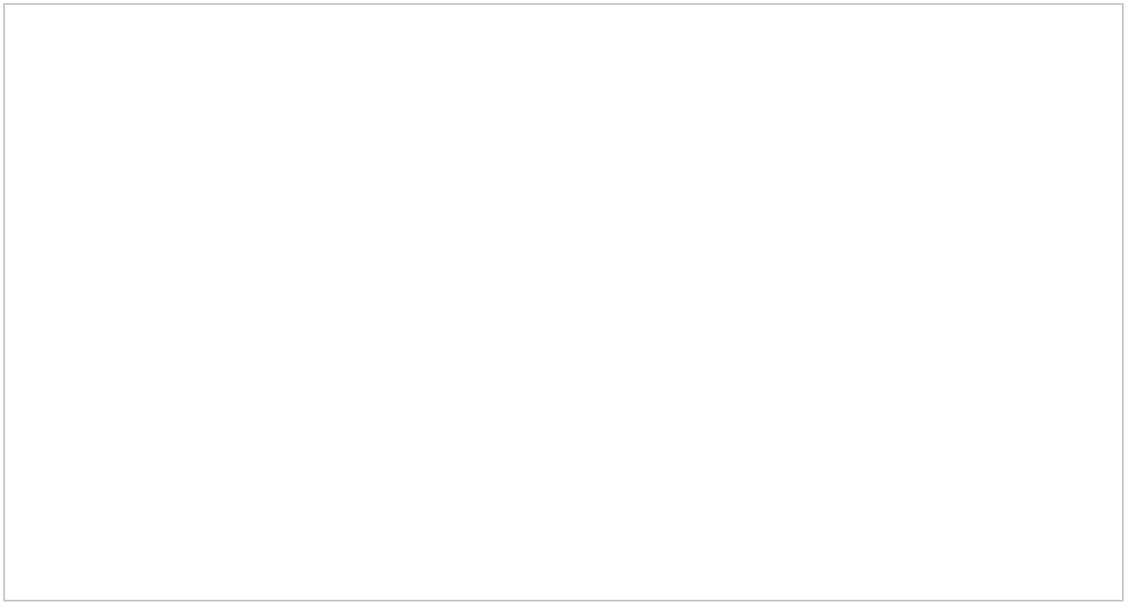
For UNICEF, though, the hacker stated that they had direct network access and offered to sell it for $4,000.

For this money, the buyer would also be able to snoop through and download a large volume of data - about 3.6 terabytes.

The statement is backed by screenshots from the hacker and obtained by AdvIntel, which show that Achilles could access documents allegedly belonging to UNICEF.

Folders included information relating to the activity of various UNICEF committees, meetings, policies, and country-specific policy guidance.

In one of the pictures, it appears that the hacker could get to two network locations, one of them being a 4TB drive that had only 388GB of free space.



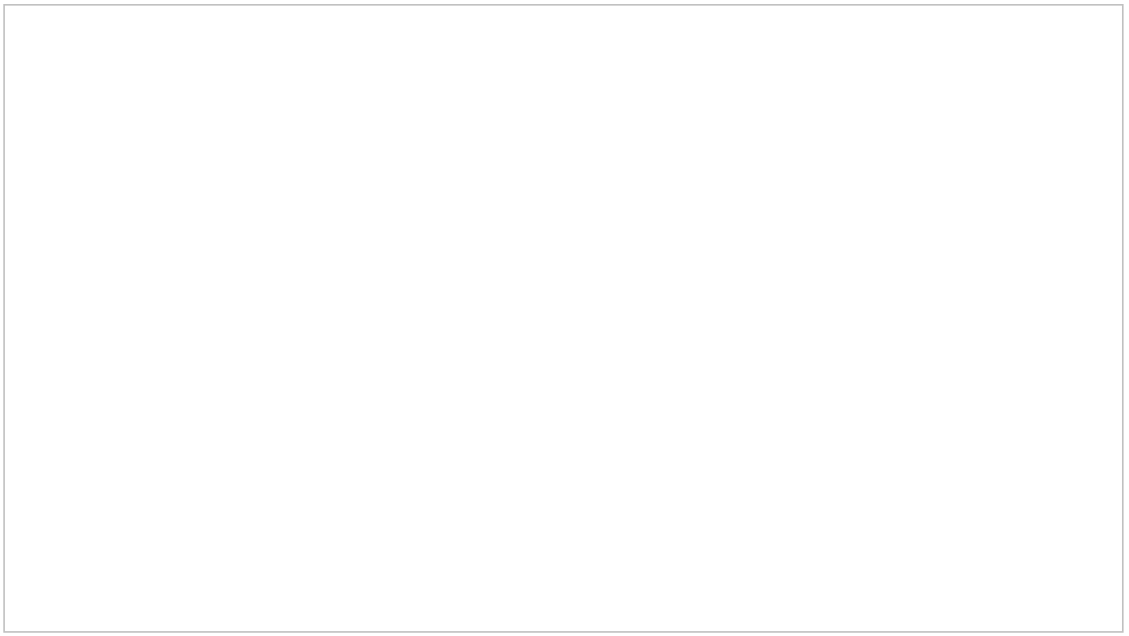
BleepingComputer has also seen images showing more detailed information on the type of data the attacker allegedly has access to and that belongs to Unicef. Due to the nature of these images, we have decided not to publish them.

BleepingComputer has contacted Comodo, UNICEF, Hash Inc, and Transat for statements and did not receive a reply from any of the three organizations at publishing time.

Achilles' work

By offering compromised network access on multiple hacking forums, Achilles was able to build the reputation of a trustworthy seller. On l33t, they advertised DNS server access for several domains managed by the UK government.

The hacker suggested that this could be used for phishing and that they could change the DNS records for any of the listed domains. A buyer could get the entire package for $300.



In April, the actor posted on the same forum that they had 600GB of data from various companies in the UK along with RDP access to them.

Furthermore, AdvIntel says that Achilles also pushed details and credentials of employees from GoDaddy, DHL, Citrix, BBC, and Facebook.

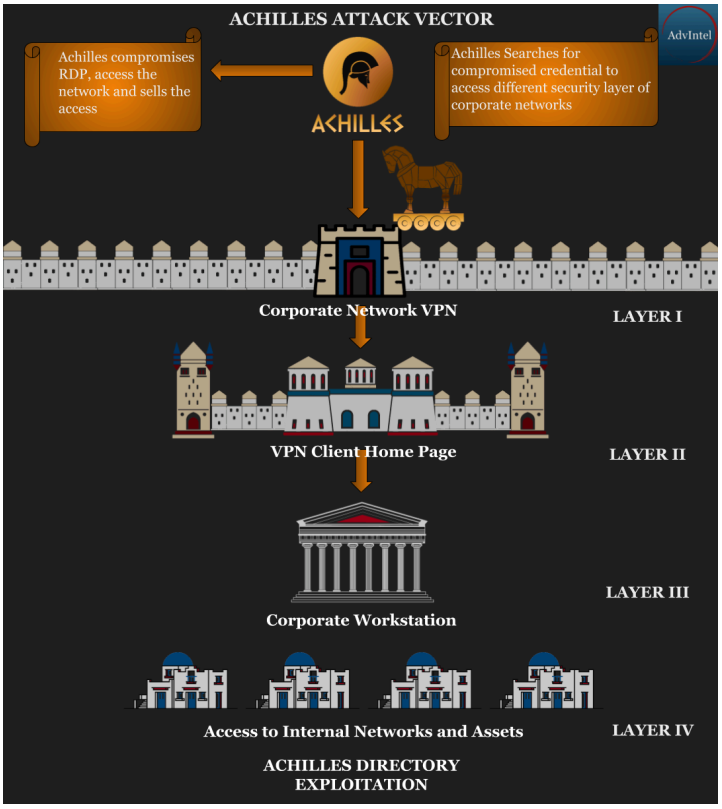
Most of the victims are from the private sector but the hacker's list of targets is diverse, including entities from the defense, energy, tourism, finance, real estate, and information technology verticals.

For a typical intrusion, "they either compromise a Remote Desktop Protocol (RDP) or leverage stolen credentials to establish stable and secure external Virtual Private Network (VPN) access into the victim's network," says Yelisey Boguslavskiy, director of security research at AdvIntel.

Information obtained by the researcher indicates that Achilles tries to avoid malware and adopts a living-off-the-land strategy that counts on utilities and services already available on the target systems. This usually makes detection more difficult because the traffic comes from legitimate sources.

Boguslavskiy says that a common tactic of this threat actor is to use a brute-force attack to get passwords to a company's external portal and remote services.

Once in, Achilles tries to elevate privileges and sets sight on Active Directory (AD) servers, which are responsible for authenticating and authorizing computers in a Windows domain type network.



Who is Achilles?

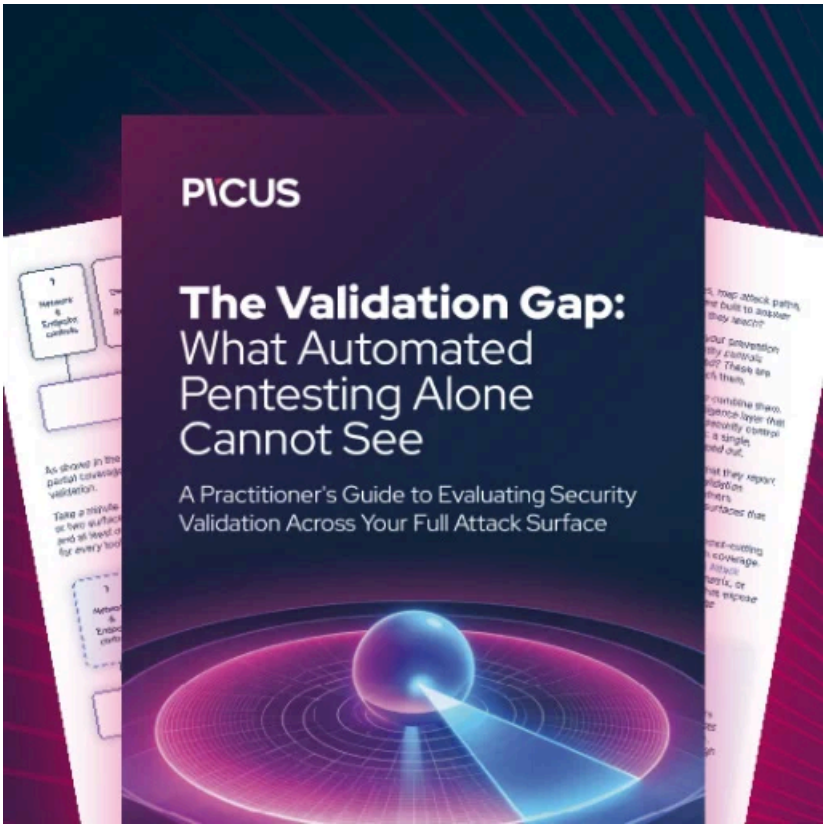
Some of the clues uncovered by AdvIntel indicate that Achilles has ties with at least some Iranian hackers that made headlines. One of them is Mr. Xhat, who is blamed for compromising the control panel for Tajikistan's domain registrar website (domain.tj) and changing the DNS records.

The incident happened in 2014 and resulted in redirecting visitors of localized versions of Yahoo!, Twitter, Google, and Amazon sites to a defaced webpage under the control of the attacker.

Another theory, fueled only by conjecture, is that the attacker is linked to the Iranian hacker group Iridium. One that could point to this conclusion are the use of password spraying tactics used by both Achilles and Iridium. Another is Achilles talking about Citrix VPN systems at a time when Iridium had allegedly breached Citrix; the hacker's activity on forums and messengers also increased.

The Iranian connection is also supported by an incident affecting a shipbuilder in Australia. According to press in Australia, an Iranian-based hacker was responsible. Achilles offered access data for a defense shipbuilder on l33t and KickAss forums, and "additional evidence provided by Achilles suggests that the information was stolen from an Australian shipbuilder Austal," the researcher adds in the report.

Even if these incidents are not related to Achilles, Boguslavskiy noticed that the hacker's activity follows the timezone in Iran. Also, when asked if they'd rather talk in Farsi, Achilles reply was that more trust was required to switch the language.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/another-hacker-selling-access-to-charity-antivirus-firm-networks/