Equinix data center giant hit by Netwalker Ransomware, $4.5M ransom

By Lawrence Abrams

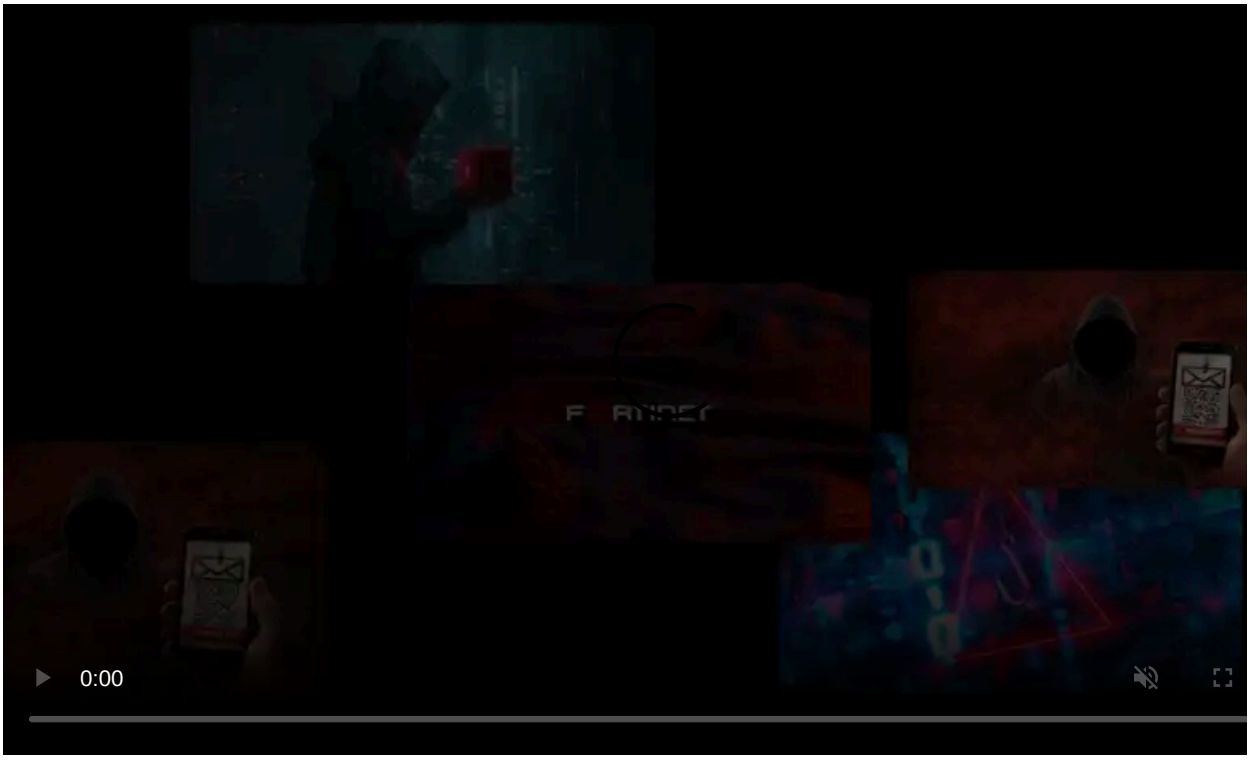
Published: 2020-09-10 · Archived: 2026-04-06 03:20:43 UTC

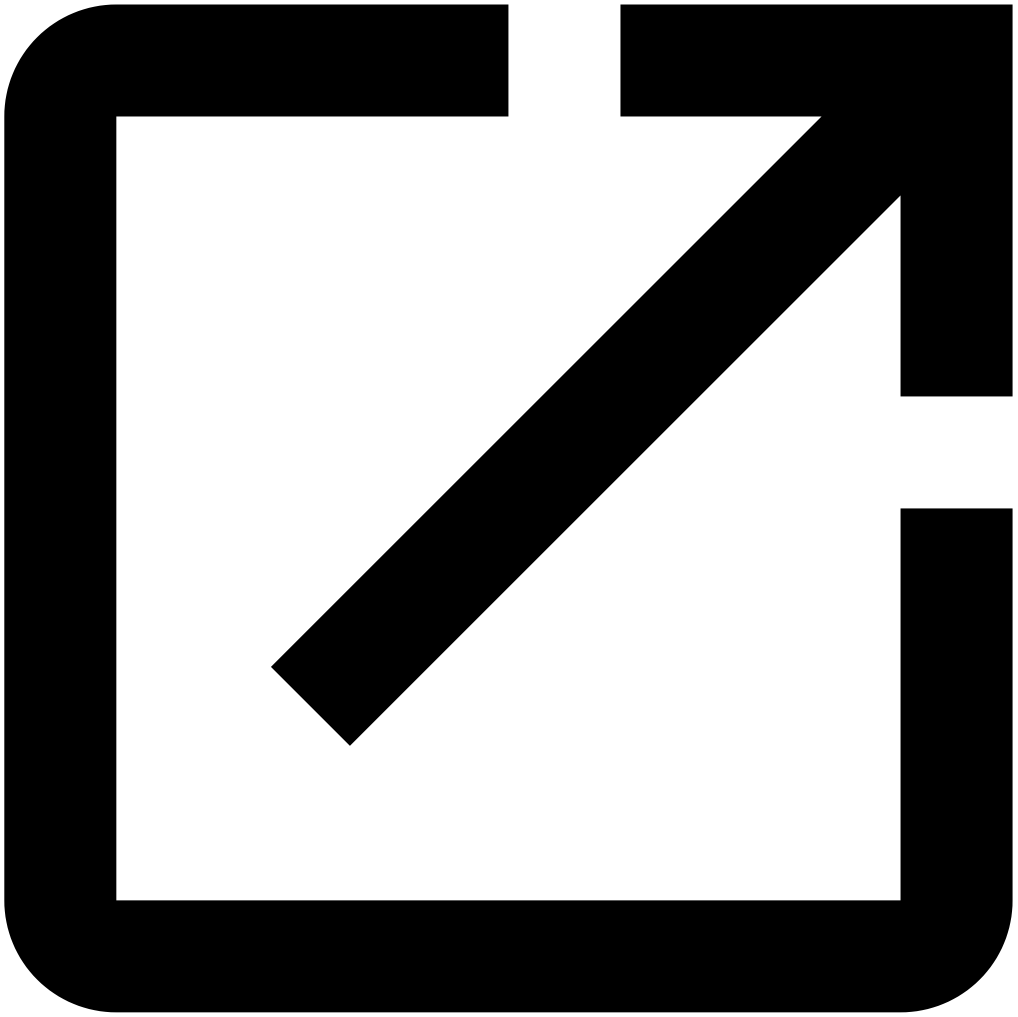
Data center and colocation giant Equinix has been hit with a Netwalker ransomware attack where threat actors are demanding $4.5 million for a decryptor and to prevent the release of stolen data.

Equinix is a massive data center and colocation provider with over 50 locations worldwide. Customers use these data centers to colocate their equipment or to interconnect with other ISPs and network providers.

The attack on Equinix

Early this week, a source shared a Netwalker ransom note with BleepingComputer that was allegedly from an attack on Equinix that occurred over the Labor Day holiday weekend.

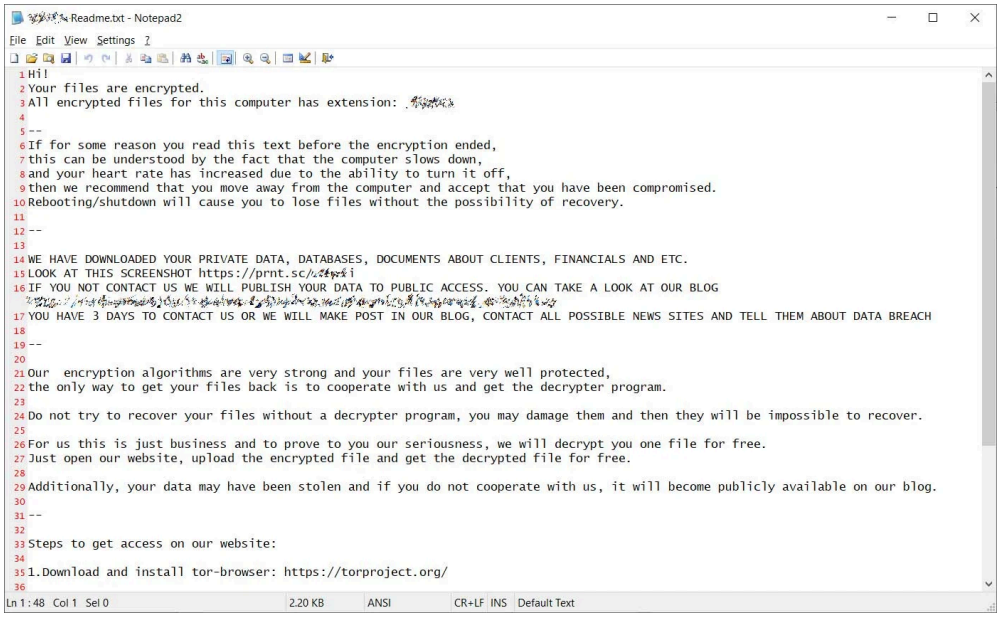

0:00



This note gives us clues about how Equinix was compromised, when the attack occurred, and what data was stolen.

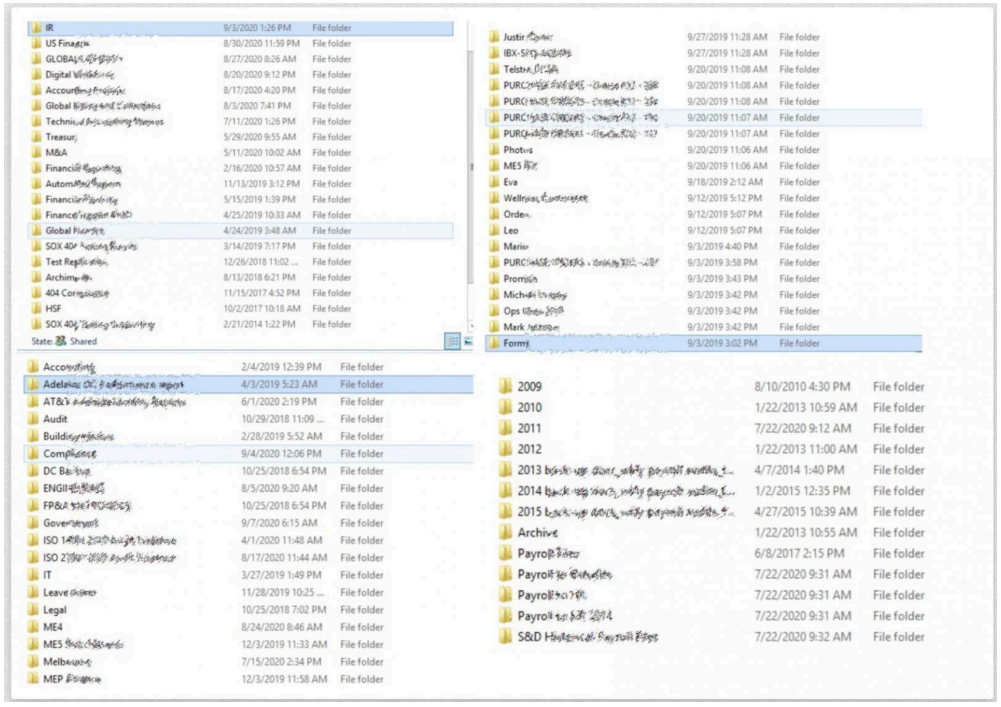
Unlike most Netwalker ransom notes seen by BleepingComputer, this note has a specific message for the victim that included a link to a screenshot of allegedly stolen data.

"LOOK AT THIS SCREENSHOT https://prnt.sc/[redacted]
IF YOU NOT CONTACT US WE WILL PUBLISH YOUR DATA TO PUBLIC ACCESS. YOU CAN TAKE A LOOK AT OUR BLOG [redacted]
YOU HAVE 3 DAYS TO CONTACT US OR WE WILL MAKE POST IN OUR BLOG, CONTACT ALL POSSIBLE NEWS SITES AND TELL THEM ABOUT DATA BREACH "



Equinix ransom note

The screenshot, which we redacted below, contain numerous folders whose names indicate they include financial information, payroll, accounting, audits, and data center reports.



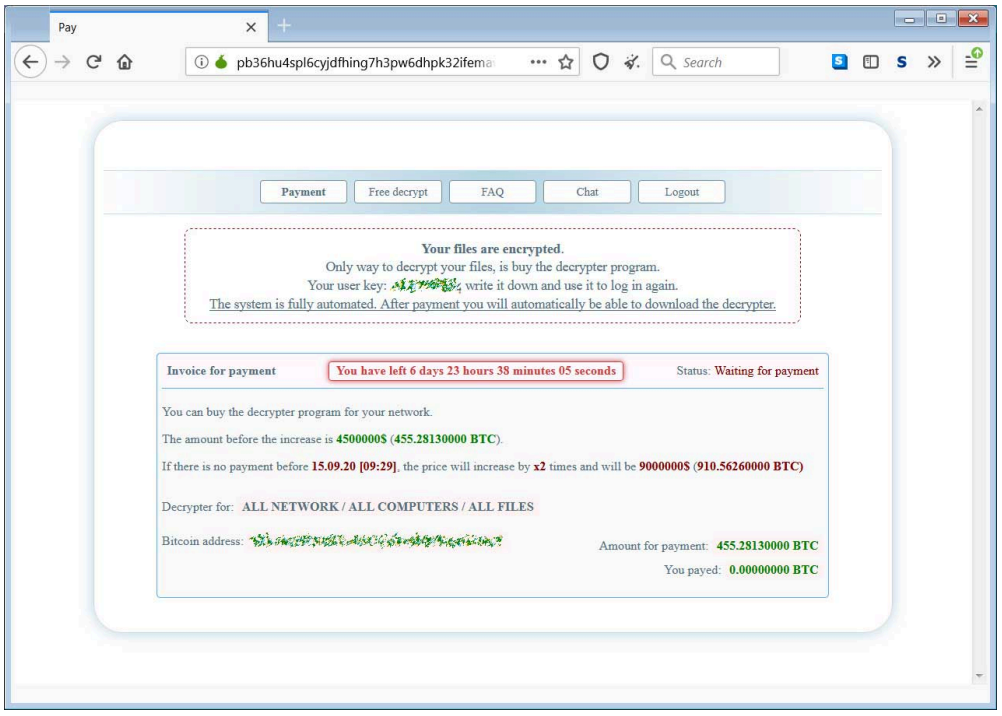
Screenshot of alleged stolen data

Folder names in the screenshot reference data centers and engineers who work in Australia, indicating that their Australian offices were likely compromised.

The latest timestamp on the folders is 9/7/20, which corroborates the claims that the attack occurred over the weekend.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731.

The ransom note includes a link to the Netwalker Tor payment site that shows a $4.5 million, or 455 bitcoin, ransom demand. If the payment was not paid after a certain amount of time, the ransom would double to $9 million.



Ransom demand

After reaching out to Equinix about this attack yesterday, the company went public with a statement that they shared with BleepingComputer late last night.

"Equinix is currently investigating a security incident we detected that involves ransomware on some of our internal systems. Our teams took immediate and decisive action to address the incident, notified law enforcement and are continuing to investigate. Our data centers and our service offerings, including managed services, remain fully operational, and the incident has not affected our ability to support our customers. Note that as most customers operate their own equipment within Equinix data centers, this incident has had no impact on their operations or the data on their equipment at Equinix. The security of the data in our systems is always a top priority and we intend to take all necessary actions, as appropriate, based on the results of our investigation."

Equinix has numerous RDP servers exposed

Exposed remote desktop servers are the most common method used by hackers to compromise a network.

After learning of this attack on Equinix earlier this week, BleepingComputer spoke to Advanced Intel's Vitali Kremez about this attack,

According to Advanced Intel's Andariel intelligence platform, there are 74 known Equinix remote desktop servers and their login credentials being sold in hacker marketplaces and private sales.

August	2020,			Equinix Australia Pty Ltd	equinix.com
August	2020,			Techrep Services Pty Ltd	equinix.com
August	2020,			Equinix Australia Pty Ltd	equinix.com
August	2020,			Equinix Brasil RJ	alog.com.br
August	2020,			Techrep Services Pty Ltd	equinix.com
August	2020,			Equinix Brasil RJ	alog.com.br
August	2020,			Equinix Australia Pty Ltd	equinix.com
August	2020,			Equinix Brasil SP	equinix.com
August	2020,			Equinix Brasil SP	equinix.com
August	2020,			Equinix Australia Pty Ltd	equinix.com
August	2020,			Equinix Australia Pty Ltd	equinix.com
August	2020,			Equinix Australia Pty Ltd	equinix.com
August	2020,			Equinix Brasil RJ	alog.com.br
August	2020,			Equinix Turkey Internet Hizmetleri Anonim Sirketi	equinix.com
August	2020,			Equinix Turkey Internet Hizmetleri Anonim Sirketi	equinix.com
August	2020,			Equinix Turkey Internet Hizmetleri Anonim Sirketi	equinix.com
August	2020,			Equinix Turkey Internet Hizmetleri Anonim Sirketi	equinix.com

Exposed RDP servers

Of the 74 remote desktop servers, most are concentrated in Australia, Turkey, and Brazil.

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.
