Cybersecurity Firm Hacked: Sensitive Data on Sale

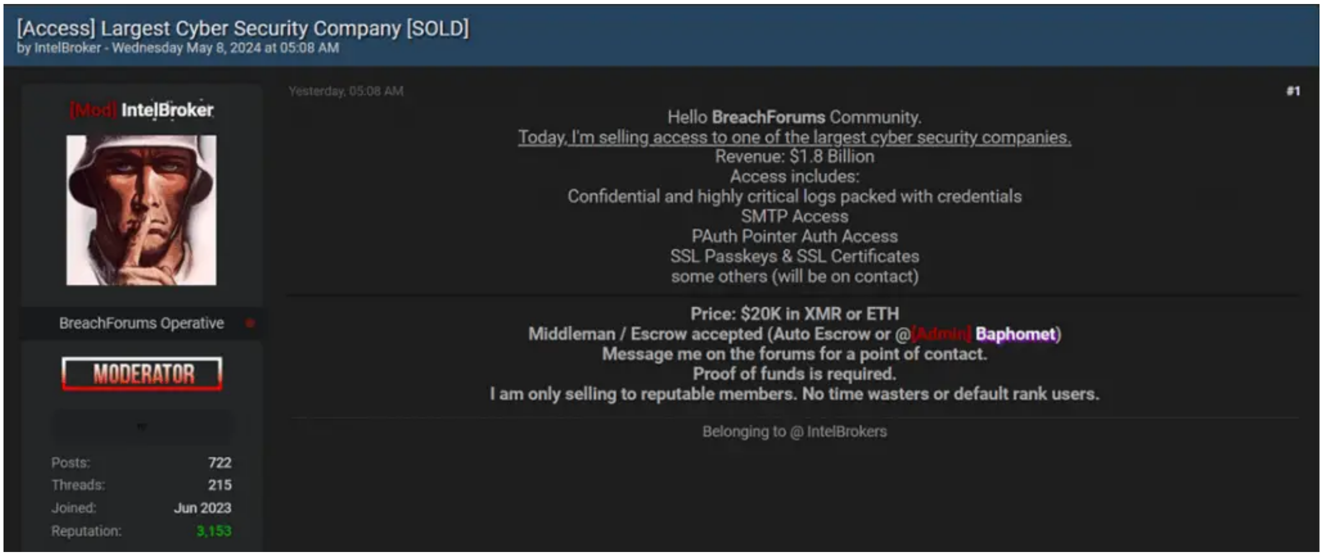
meterpreter.org/cybersecurity-firm-hacked-sensitive-data-on-sale/

ddos

May 9, 2024

Recently, reports have emerged about a significant cyber incident. A hacker, known by the alias “IntelBroker,” claims to have breached the systems of one of the world’s leading cybersecurity companies, which boasts an annual revenue of $1.8 billion.

IntelBroker posted an offer on the notorious cybercriminal forum BreachForums, proposing to sell access to sensitive data and systems of the affected company for $20,000 in the cryptocurrency Monero (XMR). The name of the afflicted company has not been disclosed by the hacker, presumably to prevent it from implementing protective measures before the data is sold.



[Access] Largest Cyber Security Company [SOLD]
by IntelBroker - Wednesday May 8, 2024 at 05:08 AM

[Mod] IntelBroker

BreachForums Operative

MODERATOR

Posts: 722
Threads: 215
Joined: Jun 2023
Reputation: 3,153

Yesterday, 05:08 AM

#1

Hello **BreachForums** Community.
Today, I'm selling access to one of the largest cyber security companies.
Revenue: $1.8 Billion
Access includes:
Confidential and highly critical logs packed with credentials
SMTP Access
PAuth Pointer Auth Access
SSL Passkeys & SSL Certificates
some others (will be on contact)

Price: $20K in XMR or ETH
Middleman / Escrow accepted (Auto Escrow or @[Admin] Baphomet)
Message me on the forums for a point of contact.
Proof of funds is required.
I am only selling to reputable members. No time wasters or default rank users.

Belonging to @ IntelBrokers

Among the stolen information, according to the hacker, are SSL keys, access to the Simple Mail Transfer Protocol (SMTP), confidential logs containing credentials, and access to Pointer Auth Authentication, which may pertain to ARM Pointer authentication.

The hacker has stated that additional details will be provided only after contact with potential buyers and has agreed to use an intermediary or escrow service for the transaction. Furthermore, IntelBroker requires buyers to verify their funds and limits sales exclusively to highly reputable members of the forum.

Since first appearing in the hacking community in October 2022, IntelBroker has been involved in several high-profile data breaches, including those affecting DC Health Link, General Electric, Hewlett Packard Enterprise, Los Angeles International Airport, and the

American contracting company Acuity. Consequently, the cybercriminal has gained a somewhat positive reputation on hacking forums, lending some credence to his claims.

The incident highlights the potential vulnerability of even the most secure cybersecurity systems. If the breach is confirmed, the implications could be significant not only for the company involved but also for its clients and the cybersecurity industry as a whole.

Zscaler, which seemingly fits the description provided by IntelBroker, has already initiated an investigation to determine if its systems have been compromised. According to the company's security updates page, preliminary findings revealed an isolated environment on one of its servers, which "was not hosted on Zscaler infrastructure and had no connectivity to Zscaler's environments" but was nonetheless accessible from the internet. "The test environment was taken offline for forensic analysis."

As of the morning of May 9th, the company assures its clients that there has been no impact on its customers, production, or corporate environments. Nevertheless, Zscaler has engaged an external incident response organization to conduct its independent investigation.

It remains unclear whether IntelBroker was indeed referring to Zscaler when announcing the sale of access, or if it is merely a coincidence that the company discovered "an isolated test environment on a single server (without any customer data) which was exposed to the internet." More dramatic developments related to this story are likely to emerge, and we will certainly report on them.

Share