BACKOFF MALWARE

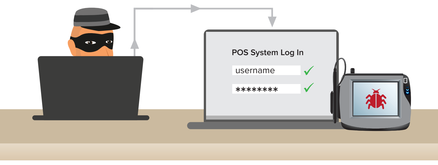
WHAT YOU NEED TO KNOW

New point-of-sale malware known as Backoff has been linked to numerous remote-access attacks, putting smaller merchants at greatest risk. Here's what you need to know about this growing threat:

1,000 BUSINESSES HIT

A Department of Homeland Security advisory says more than 1,000 U.S. businesses have had their systems infected by Backoff.

HOW IT WORKS

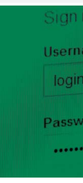


The Run-Down:
In a typical Backoff attack, hackers exploit remote-access vulnerabilities, such as weak passwords. With compromised remote-access credentials, attackers infiltrate the merchant's point-of-sale system through a remote portal and install Backoff. The malware then gathers cardholder data and other transactional information stored within the system and exfiltrates it.

Remote Desktop Applications Commonly Compromised:
LogMeIn, Join.me, Microsoft's Remote Desktop, Apple Remote Desktop, Chrome Remote Desktop, Splashtop 2, Pulseway

Source: Department of Homeland Security

Trustwave, which first identified and named Backoff, says remote-access compromises have been to blame for all of the Backoff infections it has investigated to date.



"In the cases we've reviewed, poor passwords with remote access were to blame. Many companies use remote access, and if you're not using two-factor authentication, it makes it easier for hackers to brute-force those passwords."

-Chris Hague, Trustwave

ADVISORIES ISSUED

DHS issued a July 31 advisory about the risk posed by Backoff.

PCI Security Standards Council issued a bulletin on mitigation steps.

Among those affected:

Mizado Cocina

Period of compromise:
May 9, 2014 – July 18, 2014

Compromised information:
Credit/debit card numbers, cardholder name, expiration dates, card verification value

Total Cards Compromised:
Unknown

Description:
The New Orleans restaurant said a breach that compromised credit and debit card transactions was the result of the Backoff malware.

Dairy Queen

Period of compromise:
N/A

Compromised information:
Unspecified customer data

Total Cards Compromised:
N/A

Description:
The restaurant chain says it was recently notified by federal authorities that a limited number of its stores may have been hit by Backoff.

Other possible victims include: UPS Stores, various Delaware restaurants and customers of Information Systems & Supplies Inc.

Sources: Department of Homeland Security, PCI Security Standards Council, Trustwave, Mizado Cocina, Dairy Queen, UPS Stores, Delaware Restaurant Association, IS&S.

View this infographic online
http://www.databreachtoday.com/backoff-malware-what-you-need-to-know-a-7261

ISMG Network Sources
http://www.databreachtoday.com/1000-businesses-hit-by-pos-malware-a-7230
http://www.databreachtoday.com/pci-council-issues-malware-alert-a-7241
http://www.databreachtoday.com/new-breaches-tied-to-evasive-malware-a-7216
http://www.databreachtoday.com/dairy-queen-another-backoff-victim-a-7244

Data Breach TODAY
Prevention. Response. Notification.