Ransomware gang says they stole 2 million credit cards from E-Land

bleepingcomputer.com/news/security/ransomware-gang-says-they-stole-2-million-credit-cards-from-e-land/

Lawrence Abrams

By
Lawrence Abrams

- December 3, 2020
- 02:02 AM
- 0

Clop ransomware is claiming to have stolen 2 million credit cards from E-Land Retail over a one-year period ending with last months ransomware attack.

E-Land Retail, a subsidiary of E-Land Global, operates numerous retail clothing stores, including New Core and NC Department Store.

Last month, E-Land Retail had to shut down 23 NC Department Store and New Core locations after suffering a CLOP ransomware attack.

At the time of the attack, E-Land Retail stated that sensitive customer data was safe as it was encrypted on another server.

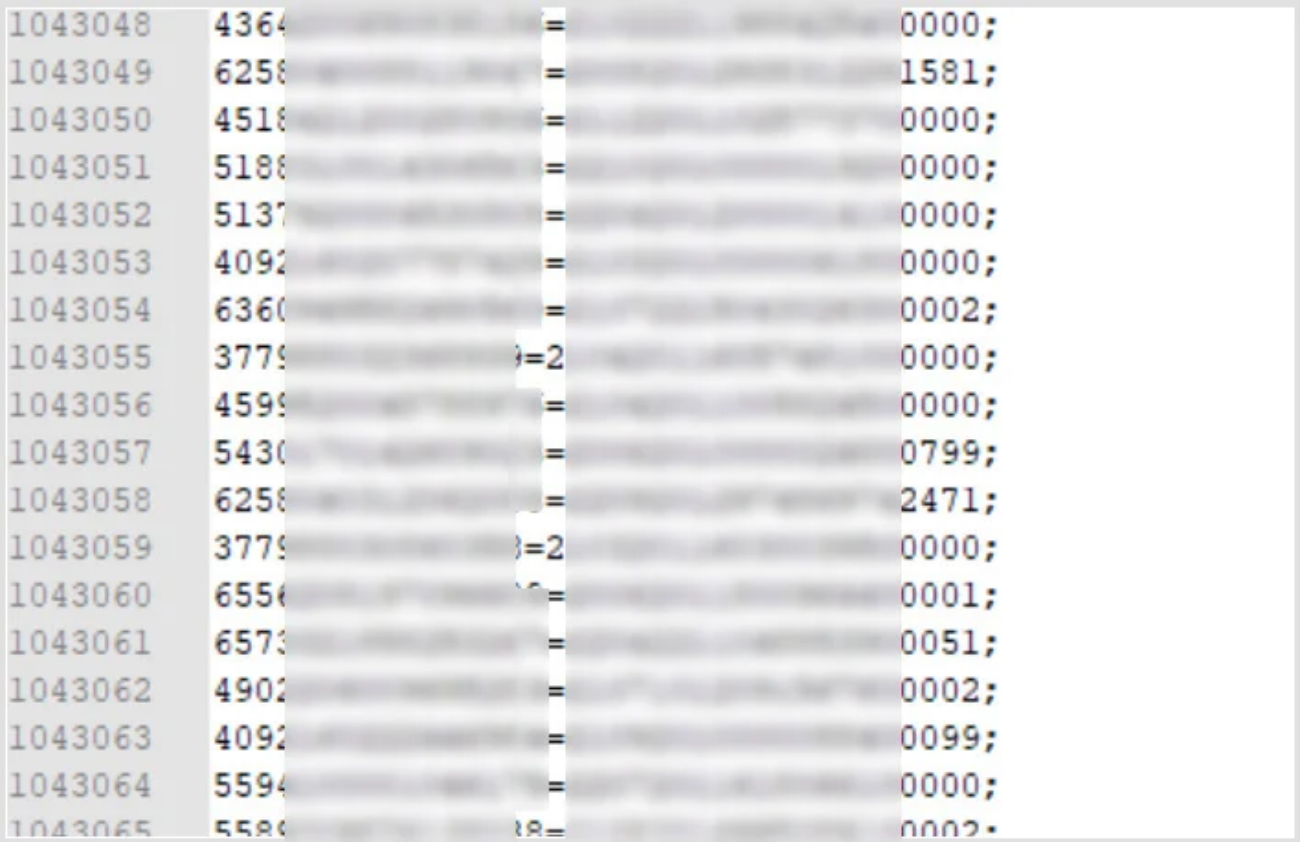
"Although this ransomware attack caused some damage to the company's network and system, Customer information and sensitive data are encrypted on a separate server."

"It is in a safe state because it is managed," E-Land Retail CEO Chang-Hyun Seok disclosed in a notice on their web site.

However, in an interview with BleepingComputer, the CLOP ransomware operators claimed to have breached E-Land over a year ago and have been quietly stealing credit cards using POS malware installed on the network.

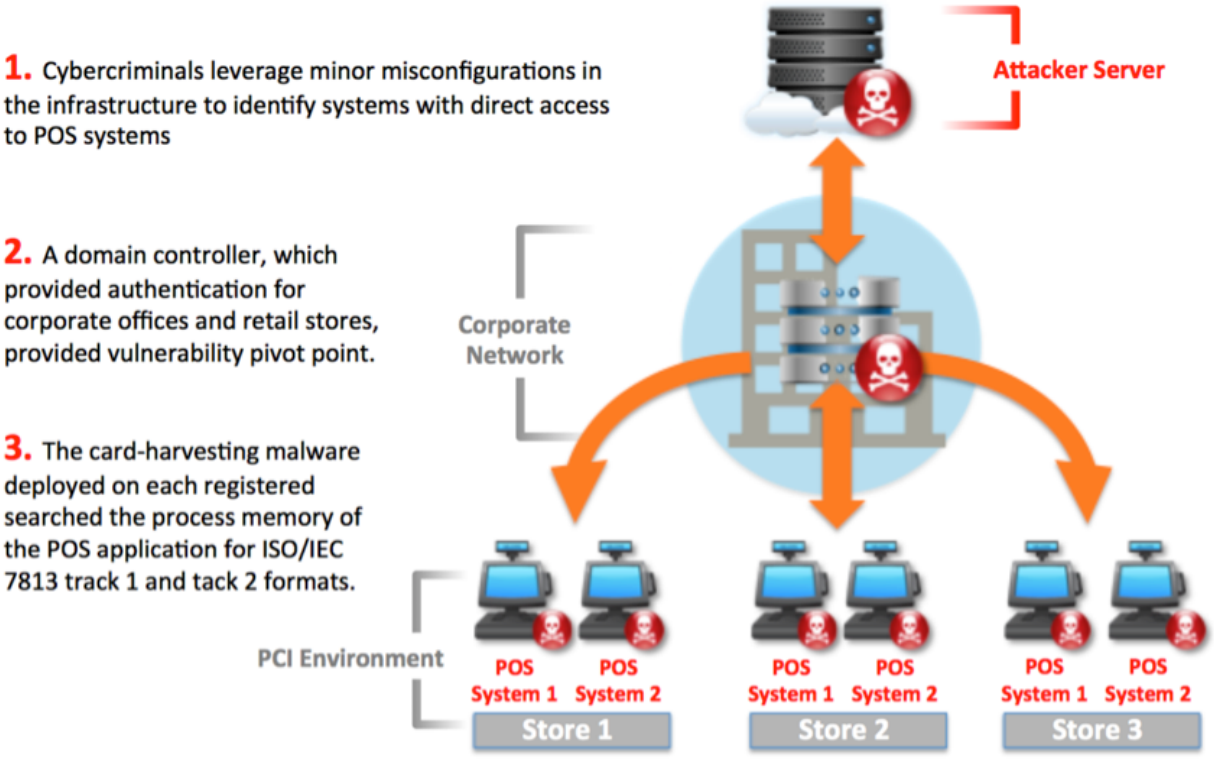
"Over a year ago, we hacked their network, everything is as usual. We thought what to do, installed POS malware and left it for a year. Before the lock, the cards were collected and deciphered, for a whole year the company did not suspect and did nothing," the CLOP gang told BleepingComputer.

Using the installed POS malware, CLOP told BleepingComputer that they stole the Track 2 data for 2 million credit cards over the past year.



Redacted sample of Track 2 data allegedly stolen by CLOP

POS malware is used to scan the memory of point-of-sale (POS) terminals as credit card transactions occur. When credit card data is detected, the malware copies the credit card information as Track 1 or Track 2 data and transmits it back to the threat actor's server.



POS malware attack model (*Carbon Black*)

The stolen credit cards that CLOP claims to have stolen are in the form of Track 2 data, which includes a credit card number, the expiration date, and other information. It does not, though, contain a credit cards CVV code, so threat actors can only use it to create fake credit cards for in-store purchases.

CLOP also told BleepingComputer that they targeted approximately 90k IP addresses, but are unsure as to how many were actually encrypted.

BleepingComputer has made repeated attempts to contact E-Land Global and E-Land Retail but have not received a reply to our emails.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New 'Cheers' Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

Microsoft: Credit card stealers are getting much stealthier

- Clop
- Credit Card
- E-Land

- E-Land Retail
- POS Malware
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: