

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

By Lawrence Abrams

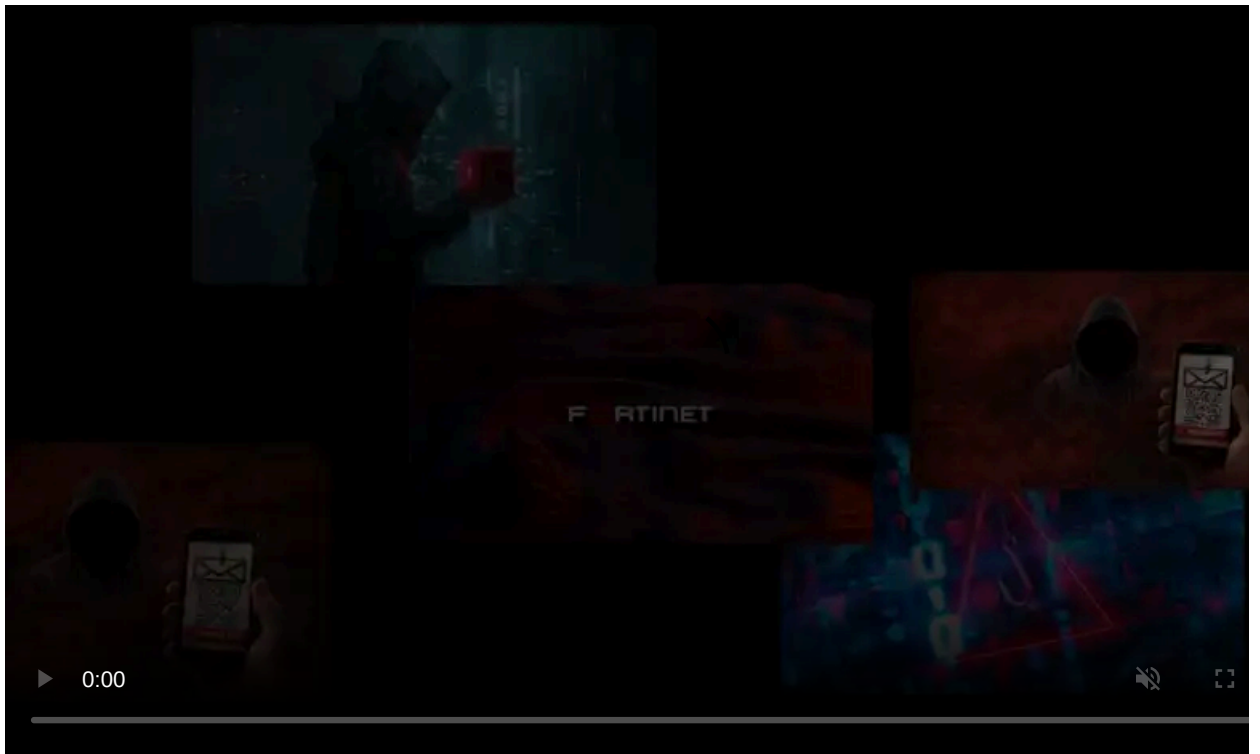
Published: 2020-12-03 · Archived: 2026-04-06 00:43:12 UTC



Clop ransomware is claiming to have stolen 2 million credit cards from E-Land Retail over a one-year period ending with last month's 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](#).



Visit Advertiser website [GO TO PAGE](#)

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.

1043048	4364		=		0000;
1043049	6258		=		1581;
1043050	4518		=		0000;
1043051	5188		=		0000;
1043052	5137		=		0000;
1043053	4092		=		0000;
1043054	6360		=		0002;
1043055	3779		=2		0000;
1043056	4599		=		0000;
1043057	5430		=		0799;
1043058	6258		=		2471;
1043059	3779		=2		0000;
1043060	6556		=		0001;
1043061	6573		=		0051;
1043062	4902		=		0002;
1043063	4092		=		0099;
1043064	5594		=		0000;
1043065	5580		=		0002;

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.

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.



[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/ransomware-gang-says-they-stole-2-million-credit-cards-from-e-land/>