MWR InfoSecurity

Supported by CPNI Centre for the Protection of National Infrastructure

CASE STUDY: ATTACK TYPE – ROGUE UPDATE

CASE STUDY:

Attack Type – Rogue Update

Scenario:

Org 5 is a mid-sized discount retailer specialising in low cost household items. Over recent times, the company has gone through a period of rapid growth followed by significant resource constraints on its IT department. The IT department attempts to manage this rapid growth and keeps everything up to date as much as possible by contracting with its software providers to manage updates.

Org 5 accepts payment card transactions through its merchant acquiring bank and uses an approved off the shelf point-of-sale application, to handle the processing of payment card data from the till through local gateways at each store to the bank. The POS application is sold and managed by a local UK reseller.

Org 5 received complaints from their customers that fraud was starting to show up on cards after having shopped at Org 5 stores. This was followed by a notice from their banks that Visa and Master Card had identified them as a common point of purchase in payment card fraud.

An investigation was initiated at several of the stores where the customers had shopped with cards that had been identified with fraud. Meanwhile, fraud rates were rapidly increasing and many more complaints were coming in daily with the press wanting to know what had happened. Investigators arrived on-site and found immediately that the POS system was logging customer card data to log files in plain text, a software bug that had been updated and fixed by the POS reseller six months earlier.

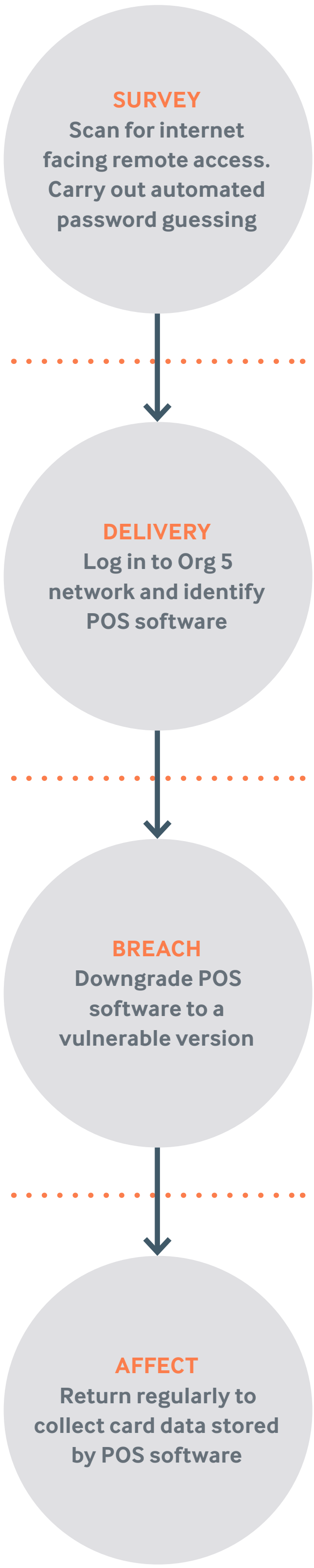
Upon further investigation, it was identified that the remote access credentials used by the POS reseller had a very weak password and had been used to log in from an unauthorised location several times in the past three months. An attacker had guessed the password, logged in and found the updated version of the POS software and re-installed the older version that logs payment card data to debug logs. Since the software continued to work as normal, nobody noticed. In fact, there had been several updates in the past six months and every time the reseller dutifully logged in to update the POS software and the attacker then logged in shortly after to collect stolen data and downgrade the software again.

Eventually, the attacker evidently decided they had stolen enough card data and were at risk of detection. This lead to them selling the stolen card data on the black market, resulting in fraud alerts.

Specific Failures Leading to Compromise

- Poor remote access controls
- No integrity checking on critical software

STAGES OF ATTACK



SURVEY
Scan for internet facing remote access. Carry out automated password guessing

DELIVERY
Log in to Org 5 network and identify POS software

BREACH
Downgrade POS software to a vulnerable version

AFFECT
Return regularly to collect card data stored by POS software

ATTACK TIMELINE

Targeting to Compromise:	8 days (evidence in logs showed persistent password guessing)
Compromise to Exfiltration:	6 hours
Compromise to Discovery:	3 months
Compromise to Containment:	3 months + 1 day
Method of Discovery:	External – third-party notification due to fraud
Threat Actor:	External – targeted organised crime
Assets Compromised:	Point of Sale Gateway (remote access), Point of Sale Terminals (POS software + Logs)