A Summary on the Target Breach

A Summary on the Target Breach Target announced it had been breached by attackers who made away with 70 M customer personal identifiable information and 40M credit cards. An email containing malware was sent to a refrigeration vendor, Fazio Mechanical, two months prior to the credit card breach. Malware the attackers installed on the POS systems may have been Citadel [2]. The credentials were used to access the 'Ariba' web application, target's property development zone web application and the partners online web application. The attackers found a vulnerability in the web application by managing to upload a file name 'xmlrpc.php', this is a php file which leveraged the vulnerability within the web application. The file was uploaded due to either an upload functionality meant to upload legitimate documents or no security checks were performed in other to check the uploaded of executable. The attackers managed to gather intelligence on Target's internal network and find the relevant Servers that held credit cards and credit card holder's information by running queries on the active directory. Once the attackers found the names of their targets, whether SQL servers or POS machines they obtained respective IP addresses by querying the DNS server, which is co-located on the Active directory server. The attackers then gained privileges of a domain admin account and created a new domain account. After creating the domain account, they also by passed the fire walk rules and other network based solutions put in place by target as controls. The attackers used the windows internal remote desktop (RDP), to assess whether s target is valuable. The attackers extracted 70M personal identifiable information from the PCI-compliant database, using the SQL protocol from a previously propagated computer. Because the database was PCI complaint, no credit cards are stored on it. They went on to install the kaptoxa malware on all POS systems, according to a January 2014 ISIGHT analysis, Kaptoxa had a 0% detection rate among the major commercial anti malware products They sent the credit card data to a local file, which arrives on a FTP enabled machine with Targets internal network. A script on the machine sends the file to the attacker's controlled FTP account. The attackers made away with 40M credit card data extracted from the POS systems.

References

[1] Posted and M. Rouse, "What is Kaptoxa? - definition from WhatIs.com," Search Security, 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/Kaptoxa. Accessed: Dec. 3, 2016.

[2] [Online]. Available: https://www.sans.org/readingroom/whitepapers/casestudies/case-study-critical-controls-preventedtarget-breach-35412. Accessed: Dec. 3, 2016.

[3] Dutton, J. (2015) IT governance Blog. Available at: http://www.itgovernance.co.uk/blog/staysure-fails-to-comply-with-the-pcidss-and-is-fined-175000-by-the-ico/ (Accessed: 4 December 2016).

[4] Copyright (2016) ICO fines insurance firm after hacked card details used for fraud. Available at: https://ico.org.uk/about-the-ico/news-andevents/news-and-blogs/2015/02/ico-fines-insurance-firm-after-hackedcard-details-used-for-fraud/ (Accessed: 4 December 2016).