TARGET DATA BREACH

Fang Liu
fbeyond@vt.edu
Aug.25, 2016
The breach occurred between November 27, 2013 and December 15, 2013.

During this period
- 40 million credit and debt card numbers stolen.
- 70 million records of personal information.
- Over 200 million dollars in cost to credit card unions for reissuing cards
# Timeline

<table>
<thead>
<tr>
<th>September</th>
<th>November 15</th>
<th>November 27</th>
<th>November 30</th>
<th>December 2</th>
<th>December 12</th>
<th>December 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacked compromised Fazio Mechanical Services.</td>
<td>Attackers broke into Target’s network and tested malware on POS machines.</td>
<td>Attackers began to collect credit card data.</td>
<td>POS malware fully installed.</td>
<td>Attackers began to move credit card data out.</td>
<td>Department of Justice notified Target.</td>
<td>Target removed most malware.</td>
</tr>
</tbody>
</table>
ATTACK STEPS

1. Phishing attack against Fazio Mechanical Service
2. Accessing the Target network
3. Gaining access to vulnerable machines
4. Installing malware on PoS terminals
5. Collecting card information from PoS
6. Moving data out of the Target network
7. Aggregating stolen card and person data
seen on underground forums since February 2013

Believed to be the major malware used in the data breaches at Target (2013), P.F. Chang’s (2013), and Home Depot (2014).

The malware is a form of memory scraper that takes a chunk of a system’s memory and looks for credit card numbers.

Evading Detections
- Multi-phase data exfiltration
- Constrained communication
- Data encryption
- String obfuscation
- Self-destructive
- Customized attack vector
THINGS THAT TARGET DID WRONG

- Target did not investigate into the security warnings generated by multiple security tools.
- Target did not take correct methods to segment their systems, failing to isolate their sensitive network assets from easily accessed network sections.
- Target did not apply proper access control on verities of accounts and groups, especially the ones from third party partners.
- Target did not harden their point of sale terminals, allowing unauthorized software installation and configuration.
AFTER THE BREACH

- The CEO Greg Steinhafel has stepped down.
- They appointed a new Chief information Officer.
- Target promised to spend 100 million on security upgrades.
- They are updating their cash registers to use chip and pin technology that is safer than the magnetic strip.
REFERENCES

- B. Krebs, “The Target breach, by the numbers,” May 2014.
- B. Krebs, “Email attack on vendor set up breach at Target,” February 2013.