Retail Under Attack—Attivo's Unique Deception Solution

Protecting Against Advanced Persistent Threats (APTs)

Summary

Retailers across the U.S. are trying to understand how to detect and protect against a new wave of cybercrime targeting their payment systems and customer databases. During the 2013 holiday shopping season, retail giant **Target** confirmed they had been a victim of a major credit card data breach that impacted up to 70 million customers. Since then, many other retail stores have acknowledged breaches, including **Michaels, Neiman Marcus** and **Goodwill Industries**. On September 8, 2014, **Home Depot** issued a statement around a compromise of their payment data systems, which could represent the biggest retail breach in the U.S. to date.

To implement effective preventive security measures, it's important to understand the mechanics of these attacks and where existing security measures can be breached. In the case of the **Target** attack, preventive measures fell short.

Technical Description

The attack on **Target** was actually extremely complex. It used multiple vectors throughout the lifecycle of the attack to accomplish the cybercriminals' objectives. Thor Olavsrud detailed for **CIO.com** the 11 steps the attackers took to breach **Target's** security (synopsis below).

11 Steps Attackers Took to Crack Target

Step	What the Attackers Accomplished at Each Step
1	Used an email phishing campaign to steal network credentials of a HVAC Vendor
2	Gained access to the HVAC vendor's billing and invoicing web server
3	Used a known PHP exploit to gain access through a web shell
4	Learned network topology; queried Active Directory with internal Windows Tools, using the LDAP protocol, and the DNS servers to get target IP addresses
5	Used an attack technique, called "Pass-the-Hash", to impersonate an Active Director Administrator and gain access privileges
6	Used those Active Directory Administrator's privileges to create a new account and add the new account to the Domain Admins group
7	Used "Angry IP Scanner" to discover which systems were network accessible and then tunneled through those servers to circumvent firewalls and other security measures

http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html

11 Steps Attackers Took to Crack Target (cont)

Step	What the Attackers Accomplished at Each Step
7	Used "Angry IP Scanner" to discover which systems were network accessible and then tunneled through those servers to circumvent firewalls and other security measures
8	Used SQL tools to extract database contents; accessed personally identifiable information of up to 70 million customers. Note, due to measures in place to comply with PCI regulations, the attackers couldn't get credit card data from these databases, so they had to get that data directly from the point of sale (POS)
9	Used network topology (Step 4), remote access (Step 7), and the installation of Kaptoxa on the POS machines to scan the memory of the infected machines and store credit card information to a local file
10	Once the credit card data was obtained, they shared the file remotely on an FTP-enabled machine
11	Once data arrived on the FTP-enabled machine, they used a script to send the file to their C&C server

The Target Breach, by the Numbers

KrebsonSecurity did a deep dive into the numbers and synthesized some of those less-reported numbers that are associated with this epic breach on **Target**:

- **40 million**—credit and debit cards stolen between Nov. 27 and Dec. 15, 2013
- **70 million**—customer records stolen that included the name, address, email address and phone number of shoppers
- **$ 200 million**—estimated dollar cost to the credit unions and community banks that had to reissue 21.8 million cards — note, this represents almost half of the total stolen in the Target breach.
- **$148 million**—charges related to losses that **Target** said would be included in its second quarter earnings report
- **$53.7 million**—estimated income hackers likely generated from the sale of 2 million cards at a median price between $18.00 and $35.70
- **46 percent**—drop in profits at **Target** in the fourth quarter of 2013, versus a year ago

Kill Chain Analysis

A "kill chain" describes the progression an attacker often follows when planning and executing an attack. Analyzing the malware and tools associated with the target helps build a picture of how the attackers gained access to sensitive systems and, ultimately, exfiltrated stolen data. Understanding the process helps identify security controls that can be implemented or improved to detect, deny, and contain a similar attack in the future.

The Reconnaissance phase of the breach, when the attackers were probing the network to understand what assets they were going to target would have been a good place to stop the attack in its tracks.

Reconnaissance

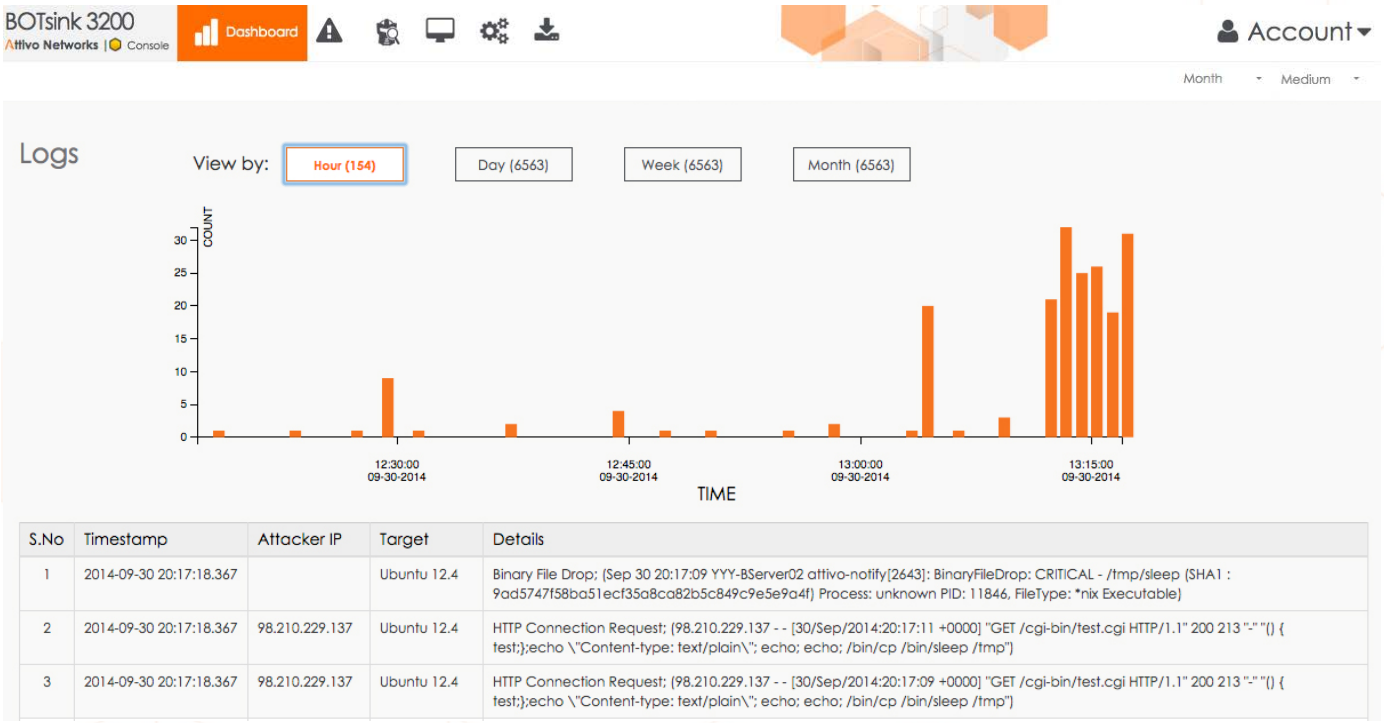
Reconnaissance includes researching and selecting targets. Threat actors behind typical retail attacks use reconnaissance (Steps 4 and 7) to discover targets of opportunity on the network. In the case of Target, they used the "Angry IP Scanner" to discover network accessible hosts from their compromised server. Attivo Networks can detect and alert on this activity, as soon as an attacker tries to establish a connection to an Attivo Engagement Server.

Attivo Networks: A Different Approach to Catching Attackers

Attivo Networks® uses next-generation Deception technology to actively engage and trap attackers. By hosting key network services across multiple virtual machines and IP addresses, Attivo Solutions engages the attackers anywhere across the Enterprise network—clients, servers and services—where the attackers are looking for high-value assets. Attivo then traps the attack activity in a secure sandbox for analysis and forensics and to prevent ongoing communications and propagation.

Once the advanced persistent threat (APT) activity is cataloged and analyzed, the Attivo ThreatMatrix Solution resets its environment, completely destroying it. The Attivo Solutions detect known and unknown APT variants, so you can eliminate the threat. By placing the Attivo Solution in next to high value assets, you will know as soon as there is any suspect activity, including:

- **Reconnaissance**—an attacker probing for the vulnerability.
- **Attempted Attacks**—an attacker targeting your assets.
- **Successful Attacks**—an attacker exploiting the vulnerability to compromise other systems.



S.No	Timestamp	Attacker IP	Target	Details
1	2014-09-30 20:17:18.367		Ubuntu 12.4	Binary File Drop: (Sep 30 20:17:09 YYY-BServer02 attivo-notify[2643]: BinaryFileDrop: CRITICAL - /tmp/sleep (SHA1 : 9ad5747f58ba51ecf35a8ca82b5c849c9e5e9a4f) Process: unknown PID: 11846, FileType: *nix Executable)
2	2014-09-30 20:17:18.367	98.210.229.137	Ubuntu 12.4	HTTP Connection Request; (98.210.229.137 - - [30/Sep/2014:20:17:11 +0000] "GET /cgi-bin/test.cgi HTTP/1.1" 200 213 "-" "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cp /bin/sleep /tmp")
3	2014-09-30 20:17:18.367	98.210.229.137	Ubuntu 12.4	HTTP Connection Request; (98.210.229.137 - - [30/Sep/2014:20:17:09 +0000] "GET /cgi-bin/test.cgi HTTP/1.1" 200 213 "-" "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cp /bin/sleep /tmp")

Attivo's actionable intelligence helps to quickly and effectively shut down any known or unknown exploits and minimizes the impact of these potentially devastating data breaches.

About Attivo Networks

Attivo Networks® provides real-time detection, analysis, and forensic reporting of in-network threats. The Attivo ThreatMatrix Platform efficiently detects stolen credential, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, IoT, and POS environments by deceiving attackers into revealing themselves. Engagement-based alerts and 3rd party integrations accelerate incident response. www.attivonetworks.com