Dom Moore
Threat Analysis + Kill Chain

Target company: Target Cyberattack December 2013

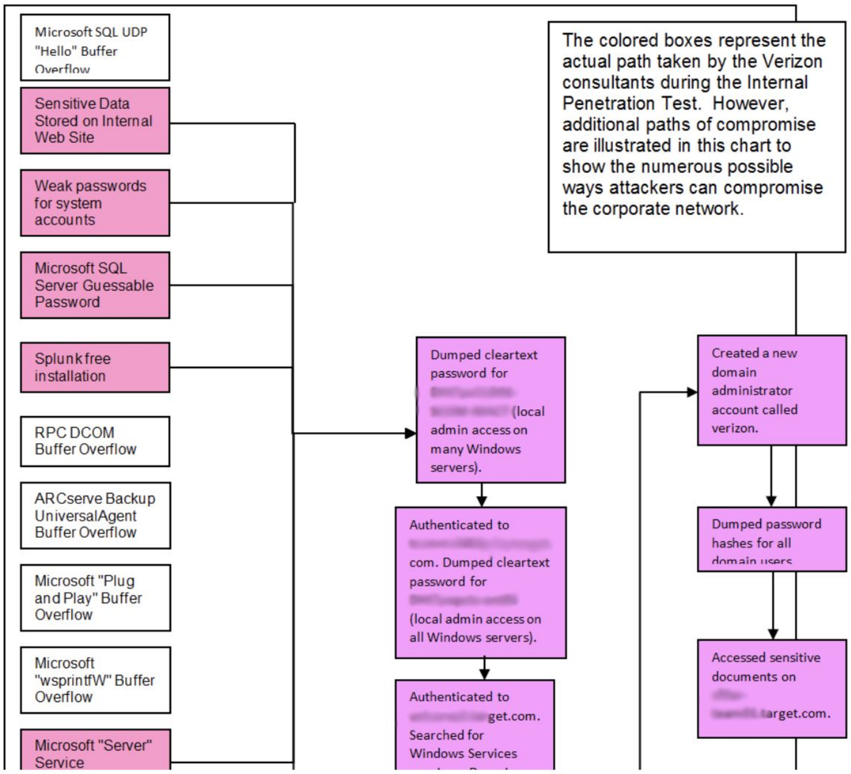
The Advanced persistent threat analysis is based on information provided by KrebsonSecurity where detailed reporting was done into the attack, interference to vulnerabilities, cause, and effect of the breach correlation with similar attacks, and the remedies implemented due to attack. Target hired security experts from Verizon to conduct an analysis of their network after the breach was identified to assess the weaknesses of their system.

Key Features of Attack:

1. The breach was associated with a vendor of Target being breached initially.
2. Citadel- password sniffing bot was used (a derivative of the **ZeuS** banking trojan)
3. Malware delivered through Email payload
4. SQL, UDP buffer
5. Password policies, not implemented
6. Patch management policies not implemented

Images provided by KrebsonSecurity

Campaign

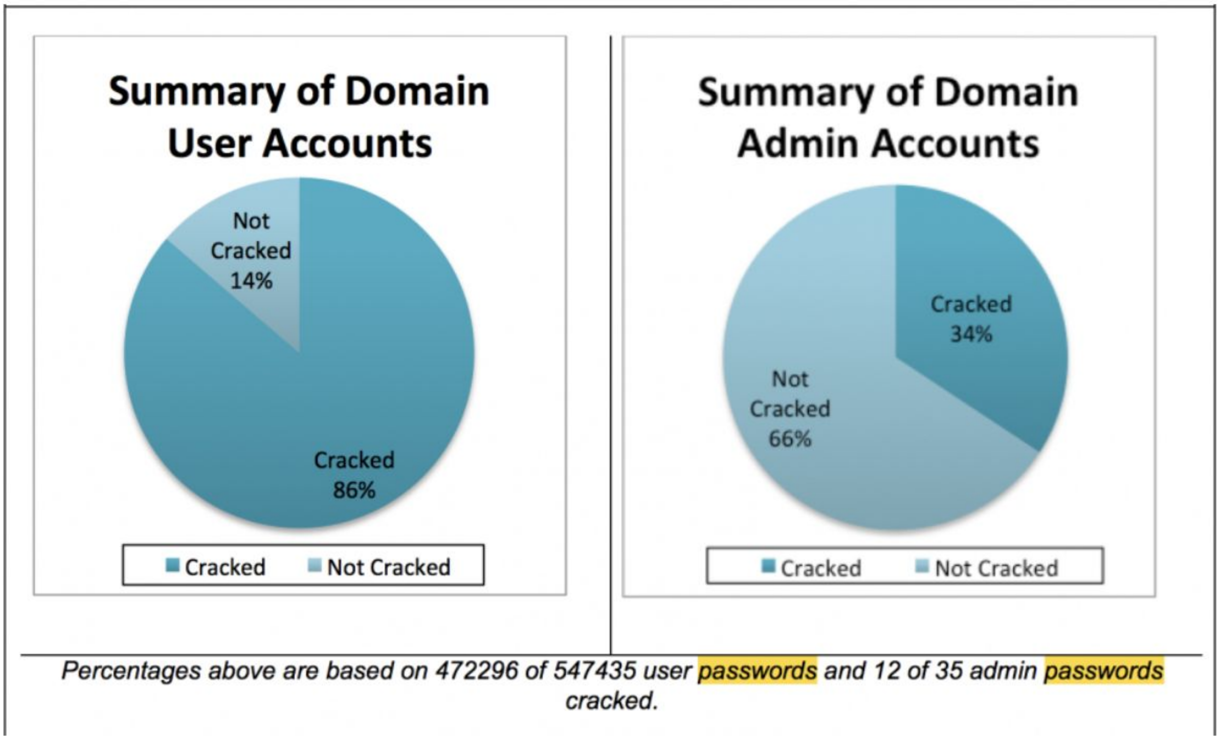

Microsoft SQL UDP "Hello" Buffer Overflow
Sensitive Data Stored on Internal Web Site
Weak passwords for system accounts
Microsoft SQL Server Guessable Password
Splunk free installation
RPC DCOM Buffer Overflow
ARCserve Backup UniversalAgent Buffer Overflow
Microsoft "Plug and Play" Buffer Overflow
Microsoft "wsprintfW" Buffer Overflow
Microsoft "Server" Service
Dumped cleartext password for [redacted] (local admin access on many Windows servers).
Authenticated to [redacted] com. Dumped cleartext password for [redacted] (local admin access on all Windows servers).
Authenticated to [redacted]get.com. Searched for Windows Services
Created a new domain administrator account called verizon.
Dumped password hashes for all domain users
Accessed sensitive documents on [redacted]target.com.

The colored boxes represent the actual path taken by the Verizon consultants during the Internal Penetration Test. However, additional paths of compromise are illustrated in this chart to show the numerous possible ways attackers can compromise the corporate network.

A high-level graphic showing the various routes that Verizon penetration testers were able to use to get all the way down to Target's cash registers in 2013 and 2014.

The target breach is associated with the alleged initial breach of an HVAC vendor working with a single branch within the organization. Though an email malware payload the attackers were able to gain access to the passwords and internal information of target servers, the passwords gained led to a sophisticated intrusion of targets internal system servers allowing the attacker to test pos malware and eventually gain access to nearly all devices within a target network.

Analysis of breaches passwords



Percentages above are based on 472296 of 547435 user passwords and 12 of 35 admin passwords cracked.

A summary of the user and administrator account passwords that Verizon experts were able to crack within one week of finding them on Target's network.

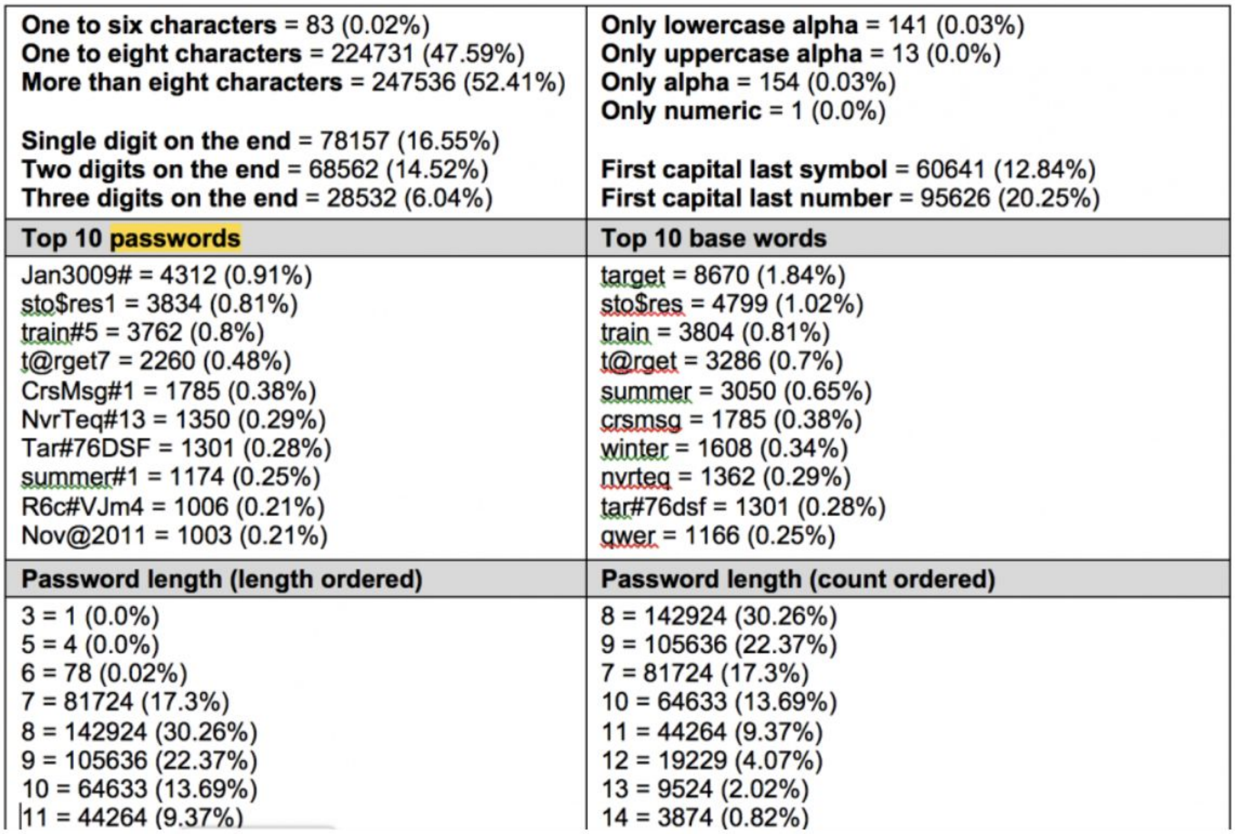
The target of the attack and impact

This attack was targeted at the entire Target network and internal devices, the attackers were able to gain access to POS registers and servers as well as any system hosted on the network. With the ability to escalate the privilege of user accounts and system administrator. The breach resulted in an estimated data infiltration of 110 million customer information and with upwards of 40 million customers banking and personal information and upwards of 420 million in financial damages due to the breach.

PHASE I: RECONNAISSANCE

This was a high skilled attack organized through email malware and passwords policies not implemented within the Target organization. Once the attackers gained entrance to the network they were able to escalate privilege undetected and test various malware on other internal systems (cash registers, apache web servers, Microsoft SQL servers) and within a week was able to compromise 472,308 of Target's 547,470 passwords.

Common Passwords discovered



One to six characters = 83 (0.02%) **One to eight characters** = 224731 (47.59%) **More than eight characters** = 247536 (52.41%) **Single digit on the end** = 78157 (16.55%) **Two digits on the end** = 68562 (14.52%) **Three digits on the end** = 28532 (6.04%)	**Only lowercase alpha** = 141 (0.03%) **Only uppercase alpha** = 13 (0.0%) **Only alpha** = 154 (0.03%) **Only numeric** = 1 (0.0%) **First capital last symbol** = 60641 (12.84%) **First capital last number** = 95626 (20.25%)
Top 10 passwords	**Top 10 base words**
Jan3009# = 4312 (0.91%)	target = 8670 (1.84%)
sto$res1 = 3834 (0.81%)	sto$res = 4799 (1.02%)
train#5 = 3762 (0.8%)	train = 3804 (0.81%)
t@rget7 = 2260 (0.48%)	t@rget = 3286 (0.7%)
CrsMsg#1 = 1785 (0.38%)	summer = 3050 (0.65%)
NvrTeq#13 = 1350 (0.29%)	crsmsg = 1785 (0.38%)
Tar#76DSF = 1301 (0.28%)	winter = 1608 (0.34%)
summer#1 = 1174 (0.25%)	nvrteq = 1362 (0.29%)
R6c#VJm4 = 1006 (0.21%)	tar#76dsf = 1301 (0.28%)
Nov@2011 = 1003 (0.21%)	qwer = 1166 (0.25%)
Password length (length ordered)	**Password length (count ordered)**
3 = 1 (0.0%)	8 = 142924 (30.26%)
5 = 4 (0.0%)	9 = 105636 (22.37%)
6 = 78 (0.02%)	7 = 81724 (17.3%)
7 = 81724 (17.3%)	10 = 64633 (13.69%)
8 = 142924 (30.26%)	11 = 44264 (9.37%)
9 = 105636 (22.37%)	12 = 19229 (4.07%)
10 = 64633 (13.69%)	13 = 9524 (2.02%)
11 = 44264 (9.37%)	14 = 3874 (0.82%)

PHASE II: WEAPONIZATION

The alleged source of the breach was linked to the email malware Citadel and later discovered that Target had lacked to implement patch management on key servers within their network resulting in vulnerabilities to the internal infrastructure.

PHASE III: DELIVERY

No delivery method has been confirmed, reports suggest it started with the infiltration of a scale within the deli department or through SQL server penetration.

PHASE IV: EXPLOITATION

The attackers took advantage of weak password protection policies and a lack of patch management that was in place for Target Corp. It utilized a password sniffer malware which targets credentials stored in password managers and exploits its vulnerabilities for gathering credentials. Once the credentials have been obtained the attacks used this information to navigate throughout the systems gaining access to other servers and sysadmin credentials until they possessed enough information to gain access to any system or device within the entire corporation’s network.

PHASE V: INSTALLATION

Target never confirmed an installation or where the attack originated, reports suggest that after gaining access to passwords the attackers were able to manipulate user credentials and system admin credentials allowing them to hide on the system undetected as they tested various forms of malware on POS systems.

PHASE VI: COMMAND & CONTROL

The attackers within days on the network were able to upload and began testing their card stealing software that was placed on cash registers, they started with a small test sample of registers and within a month had the software on the majority of target pos registers where they began to actively collect user data.

PHASE VII: ACTIONS ON OBJECTIVES

The main objectives of the attack were to infiltrate the in an attempt to escalate privilege to have the ability to make changes to the system undetected. The goal of the attack was for financial gain, where the attackers were able to obtain 40 million debit and credit cards, which is assumed to have resulted in a data drop using FTP to Russia, this has not been confirmed.

RECOMMENDATIONS

This breach resulted in Target increasing their awareness of cyber attack and creating a cyber fusion center within their organization and committing to being a leader in cyber defenses in the future. Some of the measures that may have prevented this attack are the implementation of password requirement policies, it was determined that server and system were set up and managed using the default password, the investigation also documented that servers were lacking updates patch management which lefty systems vulnerable, there could be an automated process of patch management update incorporated in the security policies procedures.