The Target Breach

NNT's Perspective

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

Abstract

The breach at Target has not just been big news within the Information Security community; it is worldwide headline news in all mainstream media outlets. This article looks at Brian Krebs'† excellent (as usual) investigation and analysis of the story so far from an NNT perspective.

† We recommend you subscribe to Brian's 'Krebs on Security' blog: it really is a great source of cyber security news and analysis

The Target breach – Facts and Figures

It's not just the scale of the breach – Target themselves (see side panel) estimate that 40 Million payment card numbers have been stolen, along with 70 Million customers' personal information – that makes this such a significant event.

It isn't even the eye-watering potential repercussions that may ensue from this (stolen payment cards sell for between $20 and $100 – that's because in the right (wrong?) hands, a card can be cloned many times and, if used in a disciplined operation, can net $1000's). Numerous Class Action lawsuits are being filed by banks and customers for consequential losses – it costs a bank around $5 to provide a replacement payment card as a pre-emptive action, but fraudulent transactions could cost much more.

But it's the fact that America's 3rd largest retailer can seemingly be turned over in such a spectacular manner. The natural assumption is that all leading retail organizations would be well protected, with substantial security measures in place. However, reports suggest the breach has been perpetrated using what appears to have been a pretty well-understood attack strategy.

> ***"What happened?***
>
> In mid-December, we learned criminals forced their way into our system, gaining access to guest credit and debit card information. The investigation has recently determined that certain guest information was taken. That included names, mailing addresses, email addresses or phone numbers. We have partnered with a leading third-party forensics firm who is thoroughly investigating the breach
>
> ***How many guests were affected by the additional stolen information?***
>
> Up to 70 million individuals may be affected.
>
> ***How many credit or debit cards were impacted?***
>
> Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013
>
> *source: target.com Jan 2014* ***"***

What Have We Been Told About What Happened?

According to Brian Krebs' blog:

- Malware was placed on Target POS systems. Target US stores run Windows XP Embedded and Windows Embedded for POS-based checkout systems.
- The POS Malware is thought to be 'Reedum', a Trojan specifically used for stealing payment card data. Other reports talk about Trojan.POSRAM and BlackPOS.
- A control server was established within the Target network. This collated stolen card data from the infected POS systems. The thieves then downloaded the data from the control server.

Malware Detection – How Effective is Anti-Virus?

In response to the incredulities at *'How could this happen?'* there have been some mitigating excuses provided. In Brian Krebs' initial piece 'A First Look at the Target Intrusion, Malware', he quotes a source close to the Target investigation:

> *'This POS malware was installed in Target's environment (sometime prior to Nov. 27, 2013), none of the 40-plus commercial antivirus tools used to scan malware at virustotal.com flagged the POS malware (or any related hacking tools that were used in the intrusion) as malicious. They were customized to avoid detection and for use in specific environments.'*

Malware Detection – How Effective is Anti-Virus? Continued

> *"*...'AV is always working on old information...a modified malware strain becomes a brand-new, never-before-seen variant, leaving the AV blind to its existence*"*

Unfortunately, this is no real excuse, since anyone in the Information Security industry knows that Anti-Virus is fallible as a malware defense. AV systems work by quarantining any files that score a hit against a repository of signatures of known malware. In addition, a good AV system will also track known patterns of malware behavior. In other words, AV is always working on old information.

The fact is that Malware can be modified to side-step AV operation. A modified malware strain effectively becomes a brand-new, never-before-seen variant, potentially leaving the AV blind to its existence.

File Integrity Monitoring - Detecting Malware that AV Misses, Maintaining Secure Configuration Settings

Since it is well-understood that AV needs help, the security standard developed to protect card data – the PCI DSS – has measures in place to block the loopholes left by AV.

PCI DSS Requirement 11.5 mandates that regular file integrity checks are run on all 'in scope systems'. A file integrity check ensures that all file attributes, security settings and permissions are maintained. In order to detect if a Trojan has replaced an existing system file, a cryptographic hash value is also recorded for each file being tracked. Hash algorithms such as MD5 and SHA1 work in such a way that even a tiny change to the file will result in a significant change to the hash value.

File Integrity Monitoring can also ensure that hardened, 'locked down' configuration settings for 'in scope' devices can be maintained. Again, any change to a config file or setting will be detected and alerted. For example, on a Windows system, configuration settings tracked include registry keys and values, service startup and running states, installed programs and updates, user accounts and Local Security Policy/Resulting Set of Policy. On Linux and Unix systems, process lists can be tracked and all other config files can be tracked directly according to their text content, such as `/etc/hosts.allow`, `/ssh/sshd_config` etc.

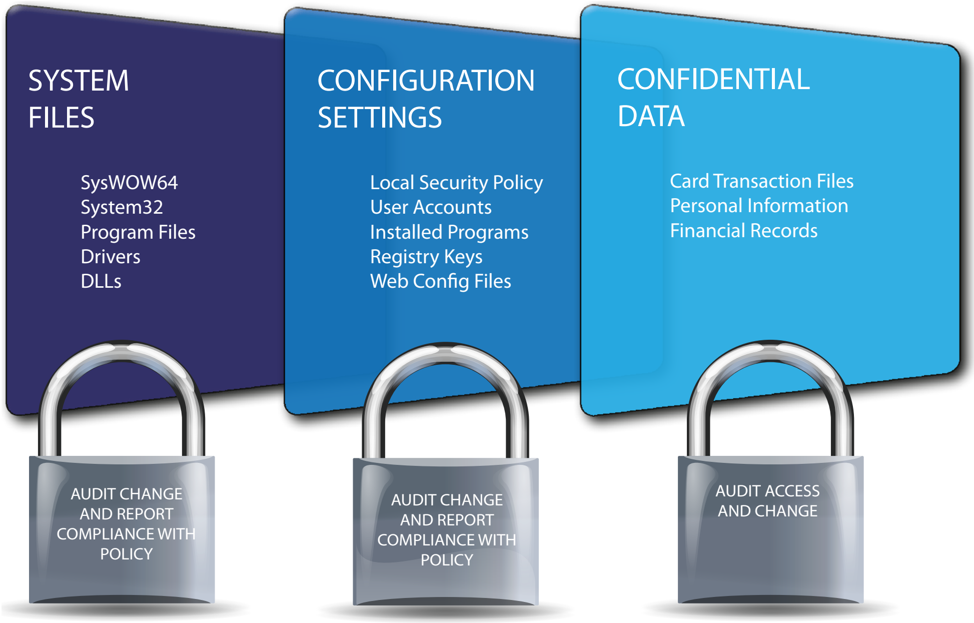
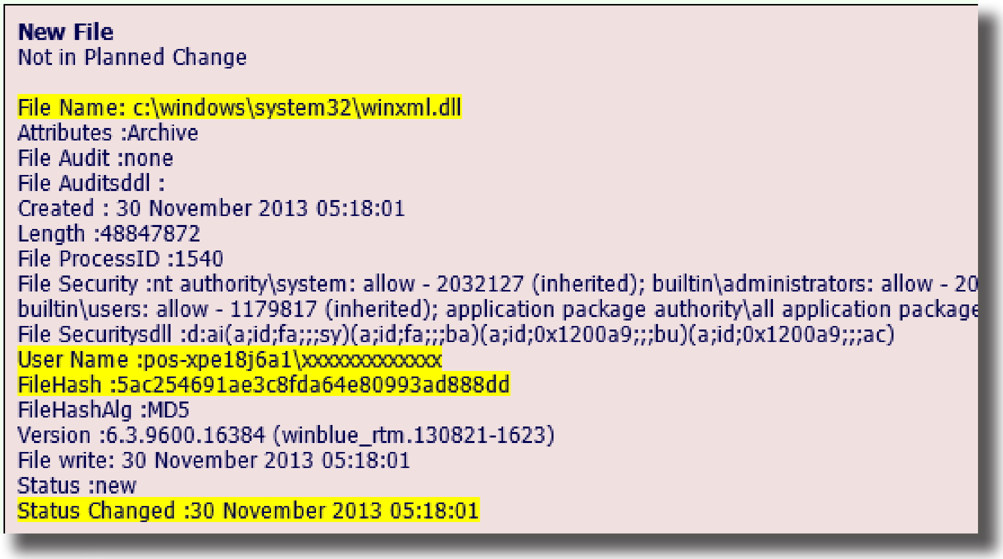


Figure 1: The Anatomy of FIM (Windows) - File Integrity Monitoring has three key dimensions - protecting system and program files, protecting configuration settings and protecting confidential data. These three dimensions require different technologies and approaches to cater for the varying demands of access and change detection

Change & Configuration Management (CCM) with File Integrity Monitoring (FIM) within the context of the Target breach

Now let's assume we are running FIM and CCM against the a POS system similar to those reportedly in use at Target and other 'in scope' servers within the estate.

According to Brian Krebs' research, there are suggestions that the Target malware is related to the 'Reedum' malware (see symantec.com). Reedum uses a Trojan (\system32\winxml.dll) in conjunction with a new service named 'POSWDS' to gather card data from a number of targeted POS program processes. FIM should typically be applied to system files such as executables, DLLs and driver files within the System32 and SysWOW64 locations on a Windows host. Program file locations should also be tracked along with other relevant files and folders for the role/function of the device.On this basis, an effective CCM and FIM solution would have reported changes as soon as the winxml.dll was created and when subsequent changes were made to the file.



```
New File
Not in Planned Change

File Name: c:\windows\system32\winxml.dll
Attributes :Archive
File Audit :none
File Auditsddl :
Created : 30 November 2013 05:18:01
Length :48847872
File ProcessID :1540
File Security :nt authority\system: allow - 2032127 (inherited); builtin\administrators: allow - 20
builtin\users: allow - 1179817 (inherited); application package authority\all application package
File Securitysdll :d:ai(a;id;fa;;;sy)(a;id;fa;;;ba)(a;id;0x1200a9;;;bu)(a;id;0x1200a9;;;ac)
User Name :pos-xpe18j6a1\xxxxxxxxxxxxx
FileHash :5ac254691ae3c8fda64e80993ad888dd
FileHashAlg :MD5
Version :6.3.9600.16384 (winblue_rtm.130821-1623)
File write: 30 November 2013 05:18:01
Status :new
Status Changed :30 November 2013 05:18:01
```

Figure 2: NNT Change Tracker reports all file system changes according to the monitor-ing policy applied: a new file has been added the System32 folder of a Win-dows POS device, and all file attributes are shown, including an MD5 hash to reveal an Trojan impostor. Note also the Windows User Account used to make the change is reported

According to the Symantec report, Reedum also creates new registry subkeys:

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\"POSWDS"**
- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\"LEGACY_POSWDS"**

Any security best practice standard will encourage you to harden systems by, among other changes, remove all unnecessary services from hosts (See PCI DSS Requirement 2). FIM should then be applied to service lists and monitor both the running and startup states of 'allowed' services.

On a Windows XP or Windows Embedded POS system as used by Target, regardless of whether the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\** key is being monitored for changes, or a service list dump taken via a WMI command, FIM would have provided an indicator that suspicious activity has taken place.

Finally, although there is less detail related to the Control Server used, this would have also required services to be created/enabled, and/or drivers to be added/changed, and/or files to be deployed. Each of these changes presents an opportunity to detect the breach and, in line with PCI DSS Best Practices, any potential security incident should be investigated.

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.