SCIT
the digital vaccine

MAJOR SECURITY BREACHES OF THE 21st CENTURY

AN ANALYSIS OF THE POTENTIAL IMPACT OF SCIT

Kapil Sood, SCIT Labs, Inc.; kapil.sood@scitlabs.com

This document examines the major security breaches of the 21st century compiled by CSO magazine (http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html) and analyzes if/how they could have been affected if SCIT had been used.

Following assumptions were used in this analysis:

- We have relied on publicly available information for details of each breach. Links are provided to some of the relevant articles.
- Systems meet the requirements for installation of SCIT i.e. the servers are production systems on which transactions are being performed. As part of our pre-sales process, SCIT requires completion of a questionnaire and discussions with our technical team to ensure client systems of interest meet SCIT installation requirements.

Breach	Description	Protection with SCIT	Links Used
Target – 2013	• Obtained login credentials from HVAC vendor through a phishing attack. • Accessed Target web application server, uploaded file into it. • Navigated through the network to POS systems. Installed malware to scrape memory. • Used Windows **domain account** to send the stolen credit cards details to a central repository within	• After infiltrating the network, the attackers took time to identify their targets – an activity that took multiple days. SCIT cleansing would have disrupted this activity. • Final ex-filtration took place over a 10 day period, from December 2 to its discovery on December 12. In actual fact, the malware to perform the ex-filtration and the file with stolen credit card details was on Target	http://www.securityweek.com/targets-data-breach-commercialization-apt https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

	Target's network. • Ex-filtrated details of more than 40 million credit cards over 10 pay periods during office hours to hide within normal business traffic. • Security warnings were ignored by the Target team because of the large number of false positives being generated.	servers for approximately a month. SCIT cleansing would have removed this file and also disrupted the ex-filtration process. This is demonstrated by the Telos test. • SCIT IT Warning would have reduced the number of false positives, thereby increasing the likelihood that alarms were not missed.	http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html?page=2
Home Depot – 2014	The Home Depot breach was remarkably similar to the 2013 breach at Target: • Attackers obtained login credentials from a Home Depot vendor. • Attackers used a day zero vulnerability in Windows to access the Home Depot network. • They were then able to access POS systems and install memory scraping malware. • Credit card information was ex-filtrated to a system outside the server. • 56 million customers were affected.	As with Target, use of SCIT would have: • Disrupted the attack in the initial stage by not providing attackers the time to identify POS system targets and navigate to them. • Disrupted the ex-filtration process. While the exact steps used in ex-filtration in the Home Depot breach are not clear from available public documents, it would likely have required installation of malware on a server in the Home Depot network – which would have been removed through SCIT cleansing. Note that SCIT would have been effective in disrupting ex-filtration even if the hacker had not used malware but, rather, had accessed files as a privileged user. As the Telos test demonstrates, SCIT can be set up to make it virtually impossible to ex-filtrate large files even for a valid user. This is done by setting the maximum transfer rate and maximum data	https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367?keepThis=true&TB_iframe=true&height=650&width=850&caption=SANS+Information+Security+Reading+Room https://www.bloomberg.com/news/articles/2014-09-18/home-depot-hacked-after-months-of-security-warnings

		volume transferred per access so that ex-filtration of large files is disrupted and connections have to be re-established with every rotation.	
JP Morgan Chase-2014	• In June 2014, attackers were able to infect the PC of one of Chase's employees with malware and thereby obtain the employee's login credentials. • The hacker was able to gain access to the internal network when this employee connected remotely to the corporate network through a virtual private network (VPN). • From that point on, the hacker managed to break through layers of security by unleashing malicious programs designed to penetrate J.P. Morgan's network. • The hacker(s) then successfully obtained the highest level of administrator privileges and were able to take control of more than 90 servers through the use of multiple zero-day vulnerabilities. • To avoid detection, data was stolen slowly over a period of several months. Approximately 83 million customer records were stolen in this fashion. • The breach was discovered accidentally and stopped in mid-August. A security firm discovered a billion stolen usernames and	Hackers were on the JP Morgan Chase systems for 3 months: • Malicious software installed would have been cleansed. • Ex-filtration process would have been disrupted.	https://www.sans.org/reading-room/whitepapers/casestudies/minimizing-damage-jp-morgan-039-s-data-breach-35822 https://www.wired.com/insights/2014/10/a-silver-lining-in-the-jp-morgan-breach-3/

	passwords, some of which belonged to the JP Morgan Chase Corporate Challenge charity site.		
US Office of Personnel Management (OPM) – 2012-2014	Hackers, said to be from China, were inside the OPM system starting in 2012, but were not detected until March 20, 2014. A second hacker, or group, gained access to OPM through a third-party contractor in May 2014, but was not discovered until nearly a year later. The intruders ex-filtrated 4.2 million personal files and security clearance background information on 21 million individuals. In addition, fingerprint data of 5.6 million of these was stolen. In each case, hackers were lodged in the OPM network for more than a year and worked their way to administrative servers and, from there, to target areas, working in a slow, deliberate fashion to avoid raising suspicion.	SCIT's rotation and cleansing strategy would not have allowed hackers to stay in the system long enough to do damage. • Malware introduced would have been removed at the next rotation instance. Hackers who tried repeatedly would likely have triggered alarms with the standard security software in place at OPM. • Similarly, ex-filtration of data sets would have been disrupted and made virtually impossible. Requests to re-establish connections would likely have led to detection. • SCIT IT Early Warning would have detected the presence of malware and triggered an alarm.	https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
eBay – 2014	Hackers obtained login credentials of a few employees through a phishing or social engineering attack. Malware was uploaded to eBay servers. Hackers remained on the system for 229 days. They were able to access user information for 145 million users. However, the hackers were discovered before they were able to get to systems with user financial information.	While damage from this attack was significant – 145 million user records were compromised – it could have been much worse. Hackers were unable to access credit card and other financial information. This is likely because, even though they were on the network for 229 days, they did not have sufficient time to navigate to systems with financial information. Use of SCIT in this case would have reduced time available to hackers to the rotation interval selected i.e. minutes	https://www.scmagazine.com/the-ebay-breach-explained/article/537762/ https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/#7804b24f7492 https://www.bloomberg.com/news/2014-05-21/by-e-mailing-hacking-victims-ebay-opens-users-up-to-more-risk-of-attack.html

		instead of months. This would likely have ensured that no damage was caused by this intrusion.	
TJX Companies – 2006	While there are conflicting accounts about how this breach occurred, the general consensus is that hackers took advantage of weak encryption of wireless network traffic within stores and collected credit card information. This attack was discovered in December 2006 when suspicious software was discovered on its systems. By this time, intruders had been resident on TJX systems for 18 months.	SCIT would not have prevented hacking of the wireless network. The use of up-to-date protocols such as WPA would have assisted in this regard. However, once the intruders accessed the TJX systems, SCIT's rotation and cleansing algorithms would have ensured that attackers did not persist on the systems for more than a few minutes – as opposed to the actual time of 18 months! We believe this is a critical differentiator. Current networks for large enterprises are very complex and have a large number of users. It is insufficient to rely solely on having absolutely no vulnerabilities in such complex environments. SCIT's approach adds a new layer of security to the security tools and protocols already in place.	http://www.computerworld.com/article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html http://www.computerworld.com/article/2538711/cybercrime-hacking/one-year-later--five-takeaways-from-the-tjx-breach.html http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3391&context=cais
Yahoo 2013-2014	In September 2016, Yahoo announced that a security breach in 2014 had compromised 500 million user accounts. Subsequently, in December 2016, it found that another billion accounts had been compromised in a breach that had occurred in 2013. These events jeopardized Yahoo's sale to Verizon and, ultimately, caused the sale price to be reduced by $350 million. • Credentials of a semi privileged Yahoo employee were obtained through social engineering or spear	It is unclear from public information whether any malware was used to access the UDB file and download it. If, as we surmise, hackers needed to use malware once they logged in as the compromised user, SCIT, through regular restoration of servers to their pristine states, would have hindered the ability of intruders to access and ex-filtrate the UDB. A hacker who has acquired the required privileges to perform these tasks, can ex-filtrate a file without the use of malware. However, as the Telos test demonstrates SCIT can be	https://arstechnica.com/tech-policy/2017/03/fbi-hints-that-hack-of-semi-privileged-yahoo-employee-led-to-massive-breach/ https://www.bloomberg.com/news/articles/2017-03-16/here-s-how-russian-agents-hacked-500-million-yahoo-users

	phishing. • Hackers were able to infiltrate the Yahoo network and navigate to the User Database (USB). • The UDB file was ex-filtrated using FTP. • The UDB record for each user contained a nonce which enabled hackers to forge cookies and access accounts without their login credentials.	set up to make it virtually impossible to ex-filtrate large file even for valid users. (Please refer to explanation of potential application of SCIT in the Home Depot case for more details). Also, by requiring repeated connections at every rotation, it would have significantly increased the likelihood of detection.	
Adult Friend Finder – 2016	More than 400 million user records in the websites that comprise the Adult FriendFinder network were compromised. Details of some users were published. Others are vulnerable to extortion attempts. The breach occurred through exploitation of a Local File Inclusion vulnerability in the application. This allowed the hacker to upload malware and access the database used for user authentication.	Malware resident on the Adult FriendFinder (AFF) network would have been disrupted by the use of SCIT. Details of how long the malware was in operation are not known. If, as we expect, malware was resident on the system for more than a few minutes – the typical SCIT rotation interval used – SCIT would have disrupted the intrusion by cleansing the servers and removing malware before any damage could be done. In addition, SCIT IT Early Warning would have detected the presence of malware and generated an alarm. Also, SCIT can be set up to control the data transfer rate and the volume of data transferred per access. This would have increased the time required for ex-filtration, requiring the hacker to reconnect to the system multiple times, thus facilitating detection. As our Telos test demonstrates, SCIT can be set up to make it virtually impossible to	http://www.csoonline.com/article/3132533/security/researcher-says-adult-friend-finder-vulnerable-to-file-inclusion-vulnerabilities.html

		ex-filtrate a large file even when a hacker is able to access the system as a privileged user.	
Heartland Payment Systems - 2008	This breach resulted in compromise of 134 million credit cards. Heartland Payment Systems (HPS) paid out approximately $145 million in compensation for fraudulent payments, • Around May 2008, hackers were able to access the HPS corporate network through an SQL Injection attack on a web form. • Intruders spent 6 months navigating to the payment processing system. During this period, they bypassed and avoided detection by the antivirus packages employed by HPS. • The intruders installed sniffer software that was able to capture payment card data, including card numbers, card expiration dates, and, in some cases, cardholder names as the data moved within Heartland's processing system.	Use of SCIT would have cleansed systems at regular intervals, thereby removing any malware that may have been inserted and preventing attackers from residing on the corporate network for 6 months. Note that, unlike antivirus systems, SCIT does not presuppose specific knowledge of the characteristics and behavior of the malware that has been installed. Consequently, it would been effective in removing initial malware and, later, the sniffer malware that was created by the user.	https://www.phil.frb.org/-/media/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf https://www.secureworks.com/blog/general-pci-compliance-data-security-case-study-heartland http://www.bankinfosecurity.com/heartland-payment-systems-forcht-bank-discover-data-breaches-a-1168
Anthem - 2014	The data breach began in Feb 2014 when a user within one of Anthem's subsidiaries opened a phishing email with malicious content. This launched the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and dozens of other systems within the Anthem enterprise, including Anthem's	Malware was resident on the Anthem network for more than 6 months. Use of SCIT would have ensured that systems would be cleansed and the malware removed periodically. That is, attackers would have been limited to the rotational time interval selected, likely in minutes, to navigate through the Anthem network – a very unlikely scenario.	http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627 http://www.csoonline.com/article/2880352/disaster-recovery/anthem-confirms-data-breach-but-full-extent-remains-unknown.html

	data warehouse. The attacker was able to move laterally across Anthem systems and escalate privileges, gaining increasingly greater ability to access information, including in the data warehouse. Hackers were able to query the data warehouse and obtain and ex-filtrate approximately 78.8 million unique user records prior to detection of the breach in January 2015. Anthem's costs related to the breach are estimated to be $100 million.	Similarly, the ex-filtration process would have been disrupted to such an extent as to make it virtually impossible to ex-filtrate this volume of records. (Please see the results of the test conducted by Telos for more details). SCIT IT Early Warning would have detected the presence of malware and sent an alert.	
Adobe – 2013	In Sept 2013, Adobe announced that hackers had stolen 38 million customer credit card records with hashed and salted passwords along with source code of some of their products. Later, a file with 150 million records was published on a site. Even though passwords were hashed, for many records it was possible to guess the passwords based on values of other fields such as password hints. Adobe suffered significant reputational damage and risked the possibility that vulnerabilities would later be exposed by hackers reviewing their source code. In addition, in 2015, Adobe later also agreed to pay more than $2 million in response to a class action lawsuit. Little is known in the public domain about the specific method used to breach the Adobe system. Experts	Since the specifics of how the hack occurred are unclear, it is not possible to definitively assert if SCIT could have prevented or limited the damage. However, the fact that the breach occurred over 6+ weeks indicates that hackers slowly worked their way through the Adobe system – an activity that could have been disrupted by SCIT. Also, if ex-filtration was performed by malware injected into the network, it, too, could have been disrupted by SCIT.	https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ http://www.darkreading.com/attacks-breaches/hacking-the-adobe-breach/d/d-id/1140620? https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/

	speculate that hackers were on their systems for more than 6 weeks.		
Sony PlayStation Network – 2011	The Sony PlayStation Network (PSN) was hacked between April 17 and April 19, 2011. 77 million customer credit card records were stolen, resulting in losses exceeding $171 million. Details of the method used to breach the Sony PSN are not known.	Since details of the Sony PSN breach have not fully been released to the public, it is not clear if SCIT would have been sufficient in disrupting or preventing this attack. One public forum speculated that hackers obtained login credentials of a sys admin. If all activities were performed as this privileged user and no malware was employed, SCIT's cleansing feature and restoration of servers to pristine states would not have been an effective tool here. However, as mentioned earlier (please see Home Depot case) and demonstrated by the Telos test, SCIT also provides the capability for an admin to configure it to make the ex-filtration of large data sets virtually impossible. In addition, detection is facilitated by requiring connections to be made with every rotation. Note that this occurs even if a hacker obtains login credentials of a user and no malware is installed.	https://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked https://www.cnet.com/news/the-playstation-network-breach-faq/ https://threatpost.com/sony-very-professional-sophisticated-attackers-responsible-psn-hack-050411/75204/
RSA Security – 2011	In March 2011, RSA Security announced that its corporate network had been breached. "Certain information" related to its SecureID authentication was stolen, potentially affecting 40 million customers. By July 2011, RSA had spent $66 million on remediation. Also, customers such as Lockheed and L3 were subsequently attacked. • Phishing emails were sent to some	Use of SCIT would have disrupted the attack in the following manner: • The malware would have existed on the system for up to the rotation time selected by the RSA Admin. Malware would have been removed and systems cleansed to their pristine states before the attacker had time to do damage. • Similarly the ex-filtration process used	https://www.securenvoy.com/blog/2012/04/27/the-rsa-security-breach-12-months-down-the-technology-turnpike/ https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/?mcubz=0&_r=0 http://www.csoonline.com/article/2127820/malware-cybercrime/the-rsa-hack-faq.html

	RSA employees. One employee opened the attached Excel sheet. • The spreadsheet contained malware that exploited a zero day vulnerability in Adobe Flash to install a backdoor. • The hacker installed a Poison Ivy variant malware and, with it, controlled the machine from a remote location. • The attacker secured additional privileges and navigated through the network to the server of interest. • A staging server was setup in the RSA network. Data was copied to this server and then ex-filtrated to an external server.	would have been disrupted by removing malware from the system before any significant amount of data had been ex-filtrated.	https://blogs.rsa.com/category/threat-detection-and-response/
Stuxnet - 2010	Stuxnet is a very complex virus that was used to significantly disrupt and retard progress at the Iranian nuclear facility in Natanz. • An initial beacon virus was introduced, most likely through an unsuspecting worker. • This virus collected and transmitted information on the configuration of the network at the target. • Thereupon, a worm was created to specifically target this configuration that consisted of Siemens SCADA controllers. The worm propagated through the entire network, using multiple zero day vulnerabilities. It	SCIT can potentially protect against a virus such as Stuxnet in the following manner: • Since it is malware that is inserted into a system, its actions will be disrupted by each cleansing and rotation cycle. • While SCIT is currently not supported by Siemens controllers, the next generation of SCIT products will focus on the Internet of Things i.e. such devices and controllers. These will disrupt and cleanse malware in controllers in much the same manner as with server machines.	https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon#t-86712 http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html

	modified operation of centrifuges causing them to become unbalanced by spinning too slowly or too fast and, in some cases, exploding. • In the summer of 2010, a bug caused the virus to propagate to the laptop of a scientist and, from there, to the internet.		
Verisign – 2010	In 2011, Verisign reported that it experienced multiple breaches in 2010. Details of what specifically was compromised are unclear. However, per Verisign: • No critical systems such as DNS servers or the certificate servers were compromised. • One or more files were ex-filtrated from the Verisign corporate servers.	Since details of this breach are not publicly available, it is difficult to assert with confidence, the potential benefits of using SCIT in this scenario. This notwithstanding, we can say the following: • The fact that Verisign was breached multiple times in 2010 speaks to the risk of relying mainly on perimeter based defenses to protect networks. SCIT's benefit is that it does not require prior knowledge of malware to cleanse a system of it. • By dropping the connection with the external server during each rotation, SCIT could potentially have disrupted the ex-filtration of file(s) from the corporate system. Also, the frequent reconnections required would have facilitated detection.	http://www.reuters.com/article/us-hacking-verisign-idUSTRE8110Z820120202 http://www.computerweekly.com/news/2240114786/Verisign-admits-security-breach-of-corporate-network https://www.wired.com/2012/02/verisign-hacked-in-2010/