Point-of-Sale Malware: Why Today's Top Retailers Are Vulnerable to Attacks

Sam Garfield

Abstract

Large retailers are falling victim to a family of malware called Backoff, which exploits vulnerabilities in point-of-sale machines. This type of malware has the ability to access credit card information in the machine's memory, store user-inputted keystrokes, and send this information across a network to an attacker's personal computer. Backoff is a serious threat -- it has already compromised millions of credit cards and infected as many as 1,000 businesses. Here I explore the details of these attacks and formulate a procedure for defense. I also take a deeper look at the underlying issues that keep companies consistently vulnerable and how they can mitigate risk.

Samuel.Garfield@tufts.edu
Fall 2014: Computer System Security
Mentor: Ming Chow

1 Introduction

Everywhere you look, there is a point-of-sale system — the place where you swipe your credit or debit card in order to complete a transaction. Most people use credit cards at retailers for convenient, quick transactions. And yet, more credit card security breaches are made each day. Would you make purchases differently if you knew what happens under the surface? And what makes these companies so vulnerable to the attacks? Though these systems have made it easier for consumers to buy things, there are blatant security flaws, and there is malicious software waiting to take advantage of them. One such kind is called Backoff malware. First brought to light in July 2014, it has been traced to attacks nearly a year prior. [9] In particular, it was the cause of Target's breach in December 2013, and it continued with Dairy Queen this August. According to Damballa, a security firm focused on advanced cyber threats, Backoff malware infections have increased 57% between August and September. [6] What is peculiar is that prevention of Backoff is fairly simple. However, implementing these changes is the more difficult issue.

2 To the Community

It is extremely important for retailers, point-of-sale system vendors, and consumers alike to recognize the vulnerabilities of point-of-sale systems. When millions of credit cards are compromised almost overnight, it is apparent that the security behind these machines is much too weak. Retailers and vendors must take the proper steps to ensure that their systems are being monitored and that these attacks will be prevented in the future. On the other side, consumers

need to understand the inherent dangers of allowing point-of-sale systems to process their credit card data. Point-of-sale systems have turned this important data invisible. Thus, the consumers blindly trust it as long as it works. However, they need to understand that there is a tradeoff. On a personal note, I was a victim of a point-of-sale attack a few years ago. I swiped my debit card at a store where malicious software was installed, and only weeks later did I discover that an anonymous person was using my card's information to make unauthorized purchases. These attacks are happening all the time. This paper will discuss the specifics behind the attacks, present preventative steps, and explore the deeper issues that leave retailers extremely vulnerable.

3 What Is Backoff?

Backoff is a specific type of malware that infects a point-of-sale machine and network through a remote desktop. It comprises the following capabilities:

1. RAM scraping for credit card information
2. Logging keystrokes
3. Command and Control Communication between server and attacker's local computer [9]
4. Injects a watchdog stub to ensure that its process constantly runs [3]

3.1 How Backoff Works

Backoff first has to access a point-of-sale machine's private network. Many of the point-of-sale systems come pre-packaged with remote desktop capabilities. This allows workers and vendors to access the retailer's network through the Internet, usually for troubleshooting purposes. However, many of these remote desktops are badly protected. Backoff detects these weakly

protected computers using widely-used network scanning tools, and then it brute forces weak passwords.

Once in the network, Backoff injects a malicious stub into explorer.exe to make sure that it is always running. It checks its process constantly, and if the malware executable has been deleted, the malicious stub decrypts itself and starts running a new process.

The malware then tries accessing a POS terminal. Inside this is the random access memory, or RAM, that processes the credit card data in cleartext. Backoff uses a blacklist of processes to ignore, and it uses a Windows process API to scrape data from the processes that use credit card data. Backoff then extracts the credit card information, using the data from the magnetic strips on the card (tracks 1 and 2), and it even runs sanity checks before it passes information back through the network. In particular, it checks that the Primary Account Number (PAN) is 16 digits long, that the card holder's name is capitalized, that the expiration date is valid, and that the PAN passes the Luhn algorithm, which is how all credit card companies validate purchases.[2]

Once the data passes these tests, it's passed through the network via Command & Control capabilities. Recently a new version of Backoff, called ROM, was found to use SSL encryption when sending HTTP POST requests in order to hide its network traffic tracks.

Finally, since the malware remains on the POS network, it can log keystroke data and send that back to the attacker's server via C&C communication.

4 Defending Against Backoff Malware

The first step is arguably the most important in preventing Backoff malware. This involves securing remote desktops and preventing Backoff from infiltrating the retailer's network in the first place. A remote desktop user would do well to:

1. Hide the remote desktop behind a firewall.
2. Use two-factor authentication.
3. Establish account lockout after a number of failed login attempts.

In the interest of being thorough, we have to assume that Backoff or any other type of malware can still infect the system. The Payment Card Industry (PCI) has published a Data Security Standard in November 2013 which identifies the many ways retail companies can ensure that their systems are secure beyond just preventing a backdoor intrusion. Among the list are some more essential steps, such as:

1. Do not use vendor-supplied defaults for system passwords.
2. Encrypt transmission of cardholder data across open, public networks.
3. Identify and authenticate access to system components.
4. Track and monitor all access to network resources and cardholder data.

Though this is promising information, in his 2007 paper on Point-of-Sale vulnerabilities, Dr. Neal Krawetz claims that the PCI DSS was a reactive security decision. The PCI DSS released its first version in 2004, after a series of credit card compromises.[4] After compiling the credit card fraud attacks since then, and comparing the new Security Standards to the old, it seems as though history is repeating itself. Version 3 of the PCI DSS has almost exactly the same 12 practices to prevent attacks.[4][5] And since 2004, there have been at least five attacks that have each compromised at least 40 million credit cards and as many as 130 million:

Notable Attacks/Milestones [7]

2005-2007 - TJX Companies - 45.6 million credit cards

Oct 2008 - PCI DSS 1.2 released

Jan 2009 - Heartland - 130 million credit cards

2010 - PCI DSS gets global support

Oct 2010 - PCI DSS 2.0 released

2012 - Adobe - 40 million credit cards

Nov 2013 - PCI DSS 3.0 released

Dec 2013 - Target - 40 million credit cards

Sept 2014 - Home Depot - 56 million credit cards

So if the standards haven't changed, and the same attacks are happening, then who's to blame? According to Dr. Anton Chuvakin of Gartner Inc., "The basics of security are well known; the challenge for many companies is not in 'going advanced,' but in actually *doing* the basics." [7]

4.1 Why Companies Aren't Doing the Basics

"With respect to PCI compliance, in many cases, it cost about 40% more than they estimated," says Derek Brink, vice president of the Aberdeen Group. [7] Understandably, employing security tools to meet required standards can be a huge burden. According to Christopher Strand, a senior director of compliance, staying up-to-date on software, operating systems, and security patches can be difficult and costly, especially if operating systems are reaching their end of life, much like Windows XP POS did in April 2014. The result is costly fees and long hours to replace the entire system. Otherwise, companies will stay stuck with the same vulnerabilities and end up incurring fees from the PCI. [8] Therefore, it's not just the cost, but the technological hoops companies have to jump through as well.

However, the PCI has made progress and has shown that it's committed to improving security and creating awareness. In February 2008, a trend showed that the PCI drove up security

spending. In June 2010, the PCI increased the amount of time businesses could use to update compliant security features. Finally, in August 2012, compliance hit a record high of 97% among Level 1 merchants, proving that awareness in security grew significantly.

4.3 Forward Thinking

In the end, it comes back to the importance of a security-first mindset. Companies who do not plan to secure their systems fall into a hole where they have to decide if implementing security features outweighs the cost. As Derek Brink quotes from his report, "'Research confirms that companies who choose the easier path and take a checkbox approach to PCI compliance (or worse, ignore the PCI altogether) realize inferior results." [1]

5 Conclusion

Backoff malware is certainly a potent and effective family of malware. However, it is not particularly sophisticated. Its entire lifespan hinges on the assumption that it can access a vulnerable network by brute forcing a username and password. If that is ruled out, then Backoff and other point-of-sale malware has little power. Rather than scaring the public, this type of malware should highlight the inherent flaws in today's retail network security and spur motivation for change.

For companies that are struggling to incorporate better security practices into their businesses, there are methods they can take to secure the systems they already have in place. It is encouraged that they reflect on their long-term interests, take on a forward-thinking approach, and make room in their budget for security features that meet standard practices. As Bob Russo,

general manager of the PCI states, “It’s about making PCI compliance part of your business, not a once-a-year, study-for-the-test kind of thing.” [7]

As for new companies, all sources point to having security at the forefront. Building an infrastructure that has strong protection in the beginning is a long-term investment that pays back in greater sales and a better reputation.

Backoff, and many other types of malware, are only as malicious as we let them be. We can stay in old habits and let them get the best of us, or we can use them as tools for growth. If retail companies make security a more integral part of their businesses, they will benefit as much from malware prevention as they will from consumers’ trust in them.

6 Demonstration

The following is a security expert’s demo and basic explanation of Backoff malware:

https://www.youtube.com/watch?v=yXR7VVn9Djs

Provided is also a simple key-logging program which demonstrates the easiness to track sensitive and potentially store it and send it:

https://sgarfield.github.io/Keylogging/keylog.html

References

[1] Aberdeen. (October 4, 2013). “Reflections on Nine Years of PCI DSS.” http://blogs.aberdeen.com/it-security/reflections-on-nine-years-of-pci-dss/

[2] Chan, Honk Kei. (August 7, 2014). “An Analysis of the Backoff PoS Malware.” https://blog.fortinet.com/post/an-analysis-of-the-backoff-pos-malware

[3] Huq, Numaan. (2014). Trend Micro Incorporated. “PoS RAM Scraper Malware: Past, Present, and Future.” http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf

[4] Krawetz, Neal. (August 27, 2007). Hacker Factor Solutions. “Point-of-Sale Vulnerabilities.” http://www.hackerfactor.com/papers/cc-pos-20.pdf

[5] Payment Card Industry (PCI) Data Security Standard. (November 2013). https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[6] “Q3 State of Infections Report.” https://www.damballa.com/q3-state-infections-report-reveals-57-increase-backoff-malware-august-september/

[7] SearchSecurity. (November 2013). “The history of the PCI DSS standard: A visual timeline.” http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

[8] Strand, Christopher. (August 7, 2013). “How to Successfully Manage Retail Compliance and Security.” https://blog.bit9.com/2013/08/07/how-to-successfully-manage-retail-compliance-and-security/

[9] US-CERT. (July 31, 2014). “Backoff Point-of-Sale Malware.” https://www.us-cert.gov/ncas/alerts/TA14-212A