NETSURION DEFENSE AGAINST BACKOFF:
How Netsurion Effectively Protected Against Threats

Netsurion™
Powering Secure and Agile Networks

In the wake of the numerous recent data breaches, many consumers are demanding answers as to the how and why surrounding companies who have inadvertently allowed data to be compromised, given security measures accessible today.

After a breach is confirmed, the process typically involves PCI Forensic Investigators spending time researching and investigating compromised networks, logging files, and any other pieces of the system traceable to not only determine how the hackers gained access, but once in control of a machine, how data was removed or retrieved. Investigative reports post-breach have uncovered vast amounts of useful information employed to reactively secure networks going forward. The industry, as a whole, has learned that in many of the instances, the culprit responsible for the data theft is linked to businesses utilizing remote access, or more specifically, insecure remote access.

It should come as no surprise then that the method of choice for many blackhats (a.k.a. computer hackers) looking to enter a system has been identifying insecure remote access. This method includes several different remote platforms, of which you can read more about in the DHS article on Backoff: New Point of Sale Malware. Hackers search for vulnerabilities and once located, it is only a matter of moments before they are able to connect to machines remotely, often times gaining administrative privileges in the process. Once they have these privileges, it is quite easy for them to download the Backoff malware on the machine in order to begin sending credit card data to their destination of choice. Gaining access, however, is only one step of the hacker's overall goal: retrieving sensitive information from systems with malicious intent.

What Backoff Is, And What It Is Not

Before moving forward, it is important to understand that the Backoff malware is not infectious. That is to say, simply visiting a web page will not result in the malware being downloaded onto a machine; rather, it must be installed, much like any other application used for legitimate purposes.

Therefore, the most common way that Backoff, and its latest variants, have infiltrated systems is through the use of insecure remote access. The Department of Homeland Security brief about Backoff points out that of the 1000 plus businesses affected by Backoff, the majority were compromised through the use of remote access lacking sufficient security measures.

Imagine for a moment, if remote access granted to a vendor serving all locations for a particular company were to become compromised, then it is highly plausible that a savvy hacker could penetrate not only the single location, but could obtain access to an entire brand, tarnishing their reputation and ultimately plunging profits in the process.

How Backoff Typically Works

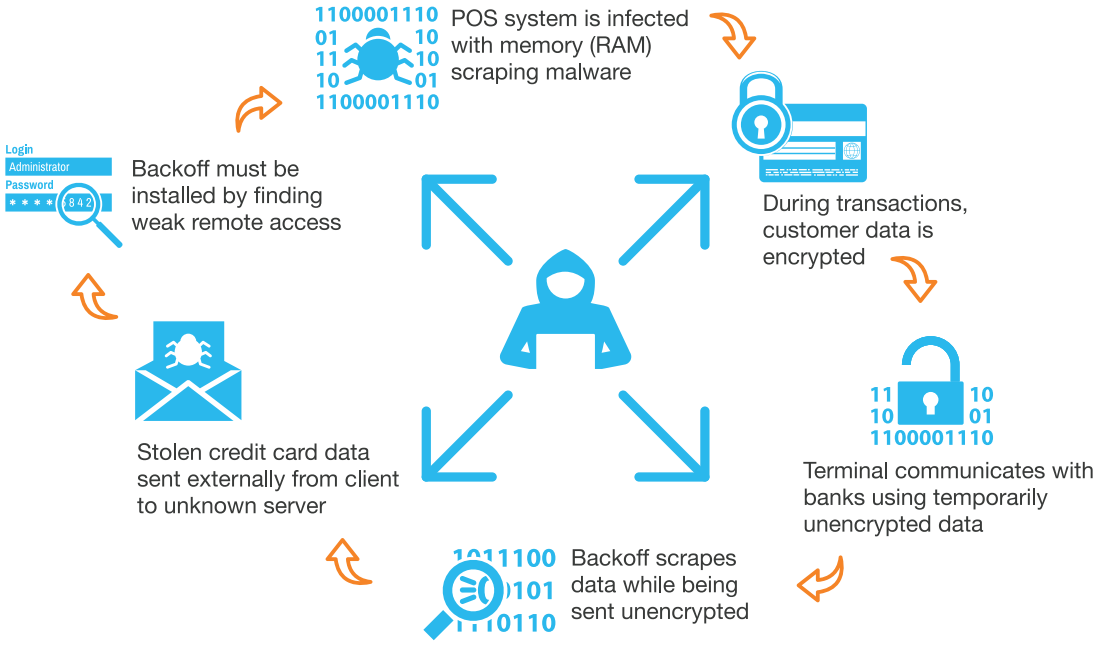
Backoff works by allowing criminals to (remotely) control the infected system, seizing credit card data out of memory, writing files with sensitive authentication data, and ultimately transmitting the stolen information using standard HTML posts. There is nothing particularly innovative about how Backoff works, but the completeness of its design and simplicity has allowed some of the biggest credit card thefts in history. Not only is the software itself fairly simplistic, but hackers can easily obtain a copy of Backoff from the Internet, streamlined so it causes few issues when installing on a remote machine; and it was so well written, it is extremely effective at stealing data once it is in place.

Protecting Against New And Unknown Threats

The original Backoff software sent data in clear text that could be detected using a network sniffer, or

Intrusion Detection System. The sniffer examined the data traveling over the network and could detect credit card data in the stream, preventing malicious traffic from being sent from the POS system.

Clever cyber-criminals, however, tend to stay one step ahead, continually creating new and enhanced versions of malware and other attack techniques. Need proof? Just look at the latest version of Backoff,



Backoff ROM. It was updated with the ability to encrypt outbound credit card data, making sniffer detection and prevention methodology all but ineffective. To a network sniffer, encrypted data appears as gibberish, removing any patterns that would allow the sniffer to recognize the transmission as credit card data.

It typically takes several months for security and anti-virus providers to identify new strains of viruses and react through incorporating added protection into their products and services. Factoring in the time and effort needed to fully deploy the updates, systems have now been unprotected with out-of-date software for months.

The glaring issue here is that software solutions such as anti-virus programs are usually between 6 to 12 months behind major malware releases, and therefore not soon enough to protect against sophisticated threats. It is therefore necessary for companies to embrace a more holistic approach when looking to protect your business.

Maintaining an effective defense against all vulnerabilities, new and unknown, along with forward thinking initiatives to protect against other modes of cyber-attack requires using techniques that focus on blocking the behaviors that attackers use, rather than any one specific attack or malware.

Firewall installation and proper configuration are integral parts to security, but what happens when the firewalls are not set up correctly? Many SMBs rely on internal IT teams lacking the security expertise or discipline required to continually monitor firewall security, keep abreast of the latest threats, and make the adjustments necessary to thwart attacks. A large portion of these businesses mistakenly believe a firewall can be set up once and will continue to provide adequate protection for an infinite amount of time.

However, as we mentioned before, effective firewall protection requires a combination of continually updated technology complemented by expert monitoring and adjustment. Firewall protection falls short when businesses fail to initially configure their firewalls properly, or when they deploy firewalls that may lack particular modes of protection necessary to thwart certain types of attacks like Backoff.

Having a dedicated security expert managing your firewall can make the difference between a costly breach and a bullet-proof defense. A security expert will be able to recognize when an unusual event has occurred, investigate to determine the level of danger posed by the event, and take the appropriate measures to ward off present and future attacks.

A common complaint surrounding data security is that the steps required to maintain protection tend to interfere with efficiency, thus causing employees to blur the line or even outright circumvent the security measures which easily leads to breakdown in the overall protection of the network quite quickly.

This isn't to say that you have to compromise efficiency for security. What is closer to the truth is the need for understanding throughout the company of why security initiatives and processes were determined as best practices in the first place, and continuing to follow through with them.

Protecting Your Business With Secure Remote Access

Some of the methods that protect against Backoff are fairly basic security measures which too many retailers ignore. These methods are recommended regardless of initiatives like the Payment Card Industry Data Security Standard (PCI).

First and foremost, verify that your remote access is secure. This includes using:

- 2-Factor Authentication
- Complex Passwords
- Unique Credentials
- Log Accessditto

In following the advice above you are ensuring that passwords in place are sufficient to deter the time and energy to crack, especially considering that 2-factor authentication is an added security measure hackers rarely have direct access to view. In utilizing a single user per username, or unique credentials, activity can then be tracked back to a specific user.

In addition, developing a proper managed firewall protection program that incorporates limiting both inbound and outbound traffic to the necessary minimum is critical. Consistency in reviewing your practices and updating them when necessary is key to making sure that you are, and stay, protected. Best practices should be followed to minimize risk. For example, firewall segmentation limiting access separates the channels storing information in order to minimize access to sensitive data along with the overall data that can be breached.

How Netsurion Defeated Backoff

During the recent rise in data breaches, Netsurion has remained successful in preventing penetration and data export, even before the Backoff threat was known and understood.

By combining our advanced capabilities such as the double-duty firewall design, DNS blocking and network segmentation with proper firewall configuration, along with testing and continuous updating and adjustment, Netsurion managed firewalls effectively protected from threats, both new and even those unknown at the time.

Installation

Backoff relies upon insecure remote access to penetrate networks. To protect, Netsurion advises the following:

- Strong password required
- Update password every 60-90 days
- Two-Factor Authentication

Netsurion Managed Firewall

Firewall denies unless it has been specifically set to allow or potentially misconfigured at the request of merchant.

- Provides logs
- Ensures safe internet
- Does not allow unknown traffic

IP Data Blocker with DNS Blocking

Provides added protection via IP data blocker with multilayered DNS blocking.

- Unresolved - no packet delivered
- Log states “Will Not Resolve”

Unparalleled Secure Remote Access

Accessing a network remotely is an essential capability for most businesses. Unfortunately, opening up an unsecure port compromises the network’s integrity and can also invite hackers. Some of the largest breaches in recent history can be attributed to weak remote access or unsecured VPN connections. We provide not only secure remote access SSL VPN into a network, but through our partnership with Juniper Networks, we offer Host Checker, a service that performs a check on all endpoint computers ensuring they conform to security requirements before access over the VPN is allowed.

Inbound & Outbound Data Security

Domain Name Servers (DNSs) are the Internet’s equivalent to a phone book. They maintain a directory of domain names and translate them into Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers access Websites based on IP addresses. Our industry leading IP-based web traffic routing technology provides battle-tested protection against malware-based data theft, where other firewalls have fallen short. Unlike most self-managed solutions, and even some third-party solutions, we created outbound traffic restrictions as part of our base configuration. These outbound restrictions were instrumental in stopping Backoff from affecting numerous businesses infected by this malware. As an added layer of security, Netsurion’s centrally managed firewall allows us to control

where network traffic goes, preventing it from resolving to malicious sites or sometimes based on countries, as well as denying traffic requests containing other potential vulnerabilities.

Backoff attempted transmission and was examined by the intermediary DNS security component, determining it suspicious. Data was therefore blocked from being sent to the requested Backoff server address. Because the Web address to which the Backoff server was attempting to send the credit card data was not a known or listed entity, our firewall (and its unique configuration) refused the request, rendering Backoff ineffective.

The knowledge that even the most secure firewall can be accessed, be it via improper configuration or an employee error, is essential. Malware will continue to be a significant issue for businesses accepting credit cards in the foreseeable future, and it is key that all businesses become aware of how to secure their environments. It would be irresponsible to ignore the problem or pretend that it could never happen to you. Taking the appropriate steps today will help you avoid joining the ever-increasing list of businesses that realize they are a hacker's latest victim. Proper management of security and consistent maintenance should be the goal of any security program.

Cybercrime has grown to epidemic proportions, and the effects on multi-location brands, individual franchisees and other small businesses can be devastating and unrecoverable. We believe franchisors, franchisees and SMBs that lack IT resources should be able to access and benefit from enterprise-class network security. Our goal is to ensure our customers' brands are protected from both internal and external threats by providing them robust and powerful network management, security, and compliance services at a fraction of the costs associated with a self-managed solution.

For more information about Netsurion's services, visit netsurion.com

Netsurion™
Powering Secure and Agile Networks