Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cover Corporate Tracks Or Risk 'Back Door' Cyberattacks

Law360, New York (September 03, 2014, 6:21 PM ET) --

Mauricio F. Paez

Cyber criminals have yet another tool in their arsenal of malware based-attacks, called Backoff Point-of-Sale Malware. In their recent advisements, the U.S. Computer Emergency Readiness Team, U.S. Secret Service and National Cybersecurity and Communications Integration Center[1] describe Backoff as a form of malware used by cyber criminals to scrape credit/debit and card account information from point-of-sale terminals. Backoff capitalizes on an old vulnerability — the exploitation by malicious actors of poorly executed remote access controls to open “back doors” to corporate information technology networks and point-of-sale terminals. The Secret Service recently alerted that more than 1,000 U.S. businesses have been effected by the malware.[2] If a company has POS systems in its network, the threat posed by Backoff requires an immediate response.

Remote Access Vulnerabilities

Remote access systems allow a mobile workforce to “log in” remotely, for example from home, a hotel, the local cafe or anywhere that offers an Internet connection. Such access permits the use of network corporate email and proprietary data without being physically present in the office. Remote access systems and connectivity typically utilizes two components: (1) a network access device, such as a server, that enables and permits a virtual system connection, and (2) a remote client, such as the employee’s computer, that initiates and sustains the connection with the network access device, permitting the client to interact with servers, network shares and other networked devices and resources. To verify identity, most remote access systems use single factor authentication — a username and password — to verify the identity of the user. The most common form of remote access is web-based access to email.

Remote desktop application software allows a user to interact with a desktop environment remotely, as if the user was sitting at an office keyboard connected to the host computer. These programs, commonly available within all major operating systems, allow a user to log in and directly control the host machine, giving the user full control and use of any aspect of the host machine allowed by such user’s account, including other accessible networked resources. Most remote users have seen this in action when IT personnel work remotely to repair or update the user’s desktop or programs accessible from the user’s desktop. Indeed, RDA is commonly used today for remote management, configuration and maintenance of the host system and networked devices.

In the case of POS terminals, RDAs allow an IT department to maintain hundreds of such terminals, often scattered over a large geographical area. Rather than having to drive to each store at which a POS terminal is located, an RDA allows the POS systems to be updated and maintained by IT from a single, centralized location. Despite these advantages, however, the Secret Service has recently stated that "[i]t is important to recognize that with the convenience of remote access comes the inherent risk of creating a 'back door' for unauthorized access." In other words, what makes network access convenient for legitimate users likewise permits a vulnerability that can be exploited by malicious actors.

Remote access is often accompanied by one or more common vulnerabilities. For example, remote access ports associated with a company's IP address space are often easily identifiable by malicious actors from simple network scans. Enabling RDA with default or weak access credentials that are easily guessed using brute force techniques allow malicious actors easy access to the POS terminal and other corporate IT systems, and the means by which to deliver malware to an intended corporate target, be it a POS terminal or other connected systems. Finally, the shared use of a password across a large geographical area means one compromise can affect hundreds of other sites and POS terminals. Backoff provides a notable example of these vulnerabilities.

Backoff is a Point-of-Sale Malware that Exploits RDA Vulnerabilities

To distribute Backoff, malicious actors have attacked RDAs. The malicious actors use brute force techniques to access administrative and other accounts, including entry at login of all combinations of usernames and passwords until finally guessing the correct set. The actors then deploy Backoff to acquire a variety of payment card and consumer-related data, including customer names, mailing addresses, credit/debit card numbers, phone numbers and email addresses.

Backoff includes several variants that have been in use from October 2013 to today. The variants are generally capable of: (1) scraping data while in the memory of the infected computer (i.e., before the data is deleted or stored in encrypted form); (2) recording keystrokes typed by users of the infected computer; and (3) uploading data to a central malware controller, updating the malware itself and uninstalling the malware in an effort to avoid detection. It is one of several examples involving remote access exploits and is likely a harbinger of remote access exploits to come.

Proactive Risk Mitigation Measures

There are certain obvious implications inherent to the loss of data targeted by Backoff in particular, and to the susceptibility of remote access applications to known vulnerabilities in general. The most notable risks are the loss of sensitive company and customer payment data, and the obligation companies have to report the loss of data to their financial institutions and card brands, and potentially the affected customers. This, of course, can have a significant impact on a company's brand and reputation. However, companies can take certain proactive measures and technical steps to mitigate related harms and potential liabilities.

First, with respect to Backoff itself, the Secret Service has made available certain Backoff indicators that can be used by a company's network security team to search for the existence of Backoff on company systems.

Second, companies should employ a defense-in-depth mediation strategy designed to have layers of security in place. Too often, businesses are protected by a single password that, if exposed, allows for full access. Instead, companies should create an approach to sensitive data and systems that requires verification and places limits on physical access as well as the use and removal of key data. A few practical steps are listed below, described for IT personnel in a technical manner. Most do not require the purchase of expensive equipment. Rather, they are security protocol choices that can be implemented within an existing network:

- Change the communication port at which an RDA listens to accept connections.
- Log connections through the port, and only allow POS terminals to accept communications from known IP addresses.
- Limit the number of failed login attempts and trigger a shutdown of the RDA to a POS device upon the requisite number of failures.
- Require multifactor authentication to start all RDA sessions.
- Require RDA connections to be made using secure communication methods.
- Implement monitoring on the POS terminals that track all changes made to file structure.
- Review all POS software updates from vendors before they are installed.
- Track and limit outbound traffic from POS terminals and have an IT response team check such traffic regularly.
- Regularly review RDA logs and POS terminal logs, and use a centralized logging system to enable IT staff to see malicious patterns across access data.
- Have consultative capabilities set up to assist IT in reviewing logging results and investigate indicators of compromise.

Third, companies should revise remote access policies to incorporate best practices relating to remote access availability and use. For example:

- Limit the availability of remote access to those within an organization that need it to perform the functions of their employment.
- Limit the systems to which those employees have remote access.
- Prohibit unsafe practices in general, such as sharing remote access authentication credentials, maintaining remote access authentication credentials in writing in close proximity to a laptop or other access device and using remote access authorization credentials as the access credentials for other systems (e.g., web-based email or websites accessed for personal use).

In addition to the recommendations outlined above, companies should reassess enterprise-wide data privacy and security policies and procedures to ensure that POS terminals are adequately protected and that obligations for compliance with applicable laws and industry standards (e.g., Payment Card Industry Payment Application and Payment Card Industry Data Security Standard) are met. Companies also should expand information management and governance policies to reflect the specific nature of the risks uniquely posed by POS systems and should consider routine pen testing, vulnerability reviews, vendor assessments and the like as part of an effective information governance program.

We anticipate that companies affected with Backoff will learn of their status from the Secret Service in the coming weeks and that malicious actors will continue to target remote access policies to open “back doors” to corporate IT networks and POS terminals. That this is now a known attack vector will likely mean regulators will place a higher burden on companies to maintain adequate security measures to guard against it.

—By Mauricio Paez and Richard J. Johnson, Jones Day; Jonathan Fairtlough, Kroll Cyber Security

Mauricio Paez is a partner in Jones Day's New York office. Richard Johnson is counsel in Jones Day's Dallas office.

Jonathan Fairtlough is managing director and deputy practice leader for Kroll Cyber Security in Kroll's Los Angeles office.

The opinions expressed are those of the authors and do not necessarily reflect the views of Kroll or Jones Day, their clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] The announcement is located at http://www.us-cert.gov/ncas/alerts/TA14-212A.

[2] The latest announcement is located at [https://www.documentcloud.org/documents/1279345-secret-service-malware-announcement.html.