

# MALWARE ROUNDUP

Security researchers recently uncovered a new version of the Backoff point-of-sale malware, which offers several new features that make it tougher to find or eradicate.

Here's a roundup of a number of significant recent malware developments:

## ROM

The latest version of the dangerous Backoff malware, tied to numerous POS breaches.

### Characteristics:

- » Encrypts connections between zombie systems and command-and-control servers
- » Disguised as a media player; formerly posed as a Java component
- » Removed: keystroke logging (may be added in again later)
- » New blacklisting capabilities help attackers avoid non-payment-card data



*"Modifications have been made by the malware author for evading detection and hindering the analysis process."*

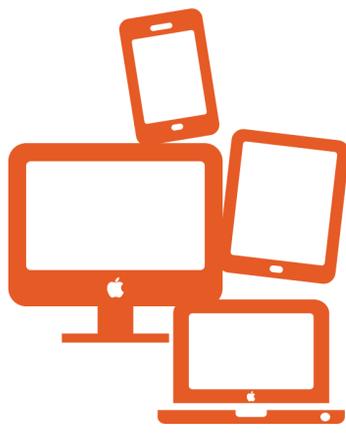
*-Hong Kei Chan, Fortinet*

## WireLurker

Previously unseen malware family targets Apple iOS and Mac OS X devices and is spread via a third-party Chinese app store called Maiyadi App Store.

### Characteristics:

- » Hidden in "Trojanized" versions of applications that appear to function normally
- » Can infect non-jailbroken iPhones
- » Watches for any USB-connected devices that connect to infected Apple OS X computer
- » Hasn't been used for a major attack campaign yet



Infected applications were downloaded more than

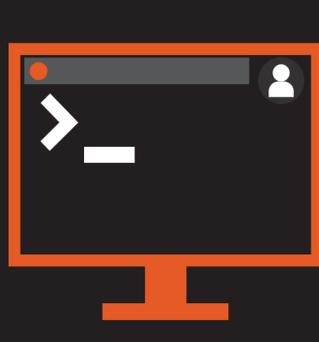
 **356,000 times**

## Mayhem Shellshock

Malware that targets Unix and Linux systems has been updated to exploit Shellshock flaws.

### Characteristics:

- » Used for in-the-wild attacks
- » Performs in heavily locked-down server environments without admin credentials
- » No longer uses a PHP script to compromise machines, instead executes a Perl script



*"This threat has the potential to become a major issue."*

*-Gregory Lindor, Akamai*

## Dyre

This Trojan attempts to steal banking credentials, although it has been seen targeting Salesforce users.

### Characteristics:

- » Bypasses SSL mechanisms of a browser
- » Captures banking website credentials in plaintext format



### Victims:

Bank of America, JPMorgan Chase, NatWest, Royal Bank of Canada, Salesforce

## PinPad

Recent reports indicate ATMs in Europe are being targeted with this specially created malware to conduct cash-out schemes.

### Characteristics:

- » Allows an attacker to tell an ATM to dispense money without a credit or debit card
- » Enables an attacker to use the ATM PIN pad to submit commands to the Trojan
- » Can automatically delete itself if the infection isn't successful
- » Can't be used to infect every type of ATM



View this infographic online

<http://www.databreachtoday.com/infographic-malware-roundup-a-7551>

### Sources

Fortinet, Trustwave, Malware Must Die, Akamai, Palo Alto Networks, Symantec, F-Secure, Stop Malvertising

**Data Breach**

Prevention. Response. Notification. **TODAY**