Back to School Checklist

Check "Backoff" Off Your List

A checklist of good business practices to protect your business from a malware attack.

"Backoff", a family of Point of Sale (POS) malware, was recently discovered on at least three separate forensic investigations, according to the *U.S. CERT Advisory - Backoff: New Point of Sale Malware* issued in July.

DOWNLOAD PDF >

The variants of the "Backoff' malware family are largely undetected by anti-virus (AV) vendors. However, because AV companies will quickly begin detecting the existing variants, it's important to maintain up-to-date AV signatures and engines as new threats such as this are continually being added to your AV solution. Pending AV detection of the malware variants, network defenders can apply Indicators of Compromise (IOC) to a variety of prevention and detection strategies.9,10,11 IOCs can be found in the *U.S. CERT Advisory - Backoff: New Point of Sale Malware advisory, Appendix 1: Technical Malware Analysis.*

The forensic investigations of retail IT/payment network compromises indicate that the network compromises allowed the introduction of memory scraping malware to the payment terminals. Information security professionals recommend a defense in depth approach to mitigating risk to retail payment systems.

Mitigation Strategies

Remote Desktop Access

- ☑ Configure the account lockout settings to lock a user account after a period of time or a specified number of failed login attempts. This prevents unlimited unauthorized attempts to login whether from an unauthorized user or via automated attack types like brute force.
- ☑ Limit the number of users and workstation who can log in using Remote Desktop.
- ☑ Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports (default is TCP 3389).
- ☑ Change the default Remote Desktop listening port.
- ☑ Define complex password parameters.

Network Security

- ☑ Review firewall configurations and ensure that only allowed ports, services and Internet protocol (IP) addresses are communicating with your network. This is especially critical for outbound (e.g., egress) firewall rules in which compromised entities allow ports to communicate to any IP address on the Internet. Hackers leverage this configuration for exfiltration of data to their IP addresses.
- ☑ Segregate payment processing networks from other networks.

Cash Register and POS Security

- ☑ Implement hardware-based point-to-point encryption. It is recommended that EMV-enabled PIN entry devices or other credit-only accepting devices have Secure Reading and Exchange of Data (SRED) capabilities. SRED-approved devices can be found at the Payment Card Industry Security Standards website.
- ☑ Install Payment Application Data Security Standard-compliant payment applications.

For More Information

Visit visa.com/cisp or email cisp@visa.com to learn more about data security tips and resources to help keep your business safe and secure.