Emerging Threats

eCommerce Malware

Sam Cleveland
Sr. Risk Analyst
Payment Systems Intelligence
Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.
Agenda

• What is eCommerce malware
• How do attackers gain access
• Common skimming malware
• What to do after a compromise
• How to protect against attacks
eCommerce Malware

- Targets eCommerce transactions
- Shoplift
- MageCart
- Online Skimming
Initial Intrusion

• Admin Login
• Outdated Software
• Insecure Software
• Insecure Server Settings

*Source: Survey of PCI Forensic Investigators
Skimming Malware

- Remote and local
- Hidden in plain sight
- Growing sophistication
  - Steganography
  - Dynamically loaded code
- Persistence mechanisms
I’m compromised! Now what?
Recommended Steps

• Perform a full security audit
  – Review source code and databases for malware
  – Run anti-virus/anti-malware
  – Remove malicious code

• Change administrative passwords

• Update website software
  – eCommerce platform
  – Add-on software

• Validate PCI DSS compliance
How can I prevent an infection?
Recommended Steps

- Document a comprehensive security process
- Perform regular backups
- Enable security and access logging
- Run anti-virus and anti-malware scans regularly
  - External and Internal scans
- Follow industry security standards
  - [https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf](https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf) (Payment Card Industry)
  - [https://www.cisecurity.org/controls/](https://www.cisecurity.org/controls/) (Center for Internet Security)
Recommended Steps

• Web Application Firewall
  – Blocks suspicious and malicious requests from reaching your website

• Secure and limit access to your administrative portal
  – Limit administration accounts to those who need them
  – Require strong passwords (use a password manager for best results)
  – Enable two-factor authentication if available

• Update and Evaluate your software regularly

• Choose a secure payment solution (PCI DSS Compliant)
  – iFrame checkout forms
  – Fully hosted checkout
Questions?

paymentintelligence@visa.com

https://usa.visa.com/support/merchant/library.html
Thank you