westchester LIBRARY SYSTEM

570 Taxter Road, Suite 400
Elmsford, NY 10523
phone 914-674-3600
fax 914-674-4185
www.westchesterlibraries.org

WLS Malware / Virus Issue Summary

Week of January 14, 2019

First sighting of the infection
Eight known libraries infected
Staff dispatched to libraries to initiate re-image protocol

Week of January 21, 2019

Sites previously cleaned continue to have reinfection
More drastic measures taken: Network audit to identify potential "seed" computer

January 25, 2019

Appearance of infection on WLS servers
Easily removed from servers, but regularly attempts at reinfection
Staff authorized for late night and weekend hours to mitigate

January 26, 2019

While trying to mitigate the infection on one server, an IT staff person made a critical error and corrupted the configuration of the server that connects users to the Virtual Desktop environment.

January 27 – 29, 2019

Virtual Desktop connection server failure disconnected staff workstations. Brought back online on January 30.

Monday, February 4, 2019

New security measures on network implemented. Staff continue to mitigate recurring infections at libraries. Smaller libraries seem to stay clean after mitigation. Larger libraries continue to see recurrence. Focus turns to non-WLS devices.

Week of February 11, 2019

Infections following new network filtering settings seems to have slowed. Persistent in three large libraries.
Infections at libraries continue to attempt to spread to WLS servers, but are being caught.

February 16, 2019

DHCP server infected, anti-malware protected the system, but corrupted server in process.
Server restored within 3 hours of notice to Help Desk.

Week of February 19

PT staff person brought in full-time for additional support
Third-party vendor being engaged to investigate and identify further countermeasures
Additional lockdowns on servers initiated
Additional security software being tested and ordered