Dellicker STRATEGIES

Cyber Threats to
Schools & Municipalities

SERVICES AVAILABLE

Dellicker Strategies has solutions & services to help public organizations get their cybersecurity under control.

ESSENTIALS PACKAGE
- Security awareness training
- Network vulnerability scan
- Incident response retainer
- Program development

SUSTAINMENT PACKAGE
- Essentials Package plus:
- Additional training seats
- 2nd vulnerability scan
- More tech & program support

COMPREHENSIVE PACKAGE
- Sustainment Package plus:
- Penetration testing
- Advanced endpoint protection
- Additional technical capabilities

Dellicker's delivery partners include Candoris Technologies, and KnowBe4.

Contact us today for a free cybersecurity assessment:
Info@dellicker.com

Prepared by Sarah Choi

WATERING HOLE ATTACKS

Watering hole attacks are slightly different from other social engineering attacks as they are targeted towards specific organizations rather than individuals that happen upon them.

What is a watering hole attack?
They are threats where attackers inject malicious code onto sites that are regularly visited by the targets. The code downloads malware onto the computer, allowing access to the device and network.

Who are the perpetrators?
These are executed by small criminal organizations for financial gain or access to personal information or sensitive computer systems.

How prevalent is a watering hole attack?
Watering hole attacks are uncommon, as they are generally employed against highly secure organizations as they are very difficult to detect, whereas smaller organizations would be more susceptible to smaller scale attacks, which require less time and resources to execute.

How bad is it?
As these attacks would be employed against secure organizations, several layers of security would be breached, and it can be assumed that the exploited information or networks are relatively significant.

What can we do to protect our schools and municipalities?
Organizations can protect themselves by keeping software updated, not adding trusts to third-party sites, blocking sites that are not required for work, and generally being aware of suspicious links.

*Source: Gavin Wright, "What is a Watering Hole Attack," SearchSecurity, April 2020.