EPIC
Insurance Brokers & Consultants

CLIENT ADVISORY

WEB SHELLS

WEB SHELLS: A LURKING THREAT

A "web shell" is malware that is installed on a hacked web based server and allows the cyber criminal to interact with the victim's server and filesystem. Although a long-standing threat, web shells have emerged as one of today's most popular forms of malware. Cyber criminals use communications that blend in well with legitimate traffic in order to infiltrate networks. Attacks usually occur during non-working hours when their activities are less likely to be discovered and responded to. The rapid move to cyberspace during the pandemic may mean that companies are more vulnerable to these threats. Employees are more distracted and disoriented and IT departments are strained due to an increase in service requests. As a result, an organization's ability to detect and respond to network intrusions and attacks may not be as quick, precise or comprehensive as usual.

DETECTION

Although these attacks are covert, there are clues which companies can look for to determine if a system is compromised:

- Comparisons between suspected web shells and known "good" images do not match
- Web traffic anomalies
- Unusual web signatures
- Unexpected network flows
- Detection by endpoint detection and response (EDR) capabilities

HIDDEN DANGER

As of February 2020, Microsoft reported that it detects around 77,000 active web shells on a daily basis[3]

PREVENTION

Although remote company systems are more vulnerable at this time, there are preventative steps that can be taken to harden systems against web shell attacks and mitigate exposure to loss[1,2]:

- Update web applications regularly and deploy latest security updates as soon as they become available.
- Add permissions for web applications to limit access.
- Monitor file integrity.
- Enable cloud-delivered protection to get the latest defenses against new and emerging threats.
- Segregate networks.
- Harden web servers. Audit and review logs from web servers frequently.
- Check your perimeter firewall and proxy to restrict unnecessary access to services, including access to services through non-standard ports.
- Utilize your network firewall and other intrusion prevention devices to prevent command-and-control server communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
- Educate end users about avoiding malware infections.

The COVID crisis serves as a reminder of the most important steps companies can take to improve their ongoing resistance to infections from malware. The same concepts that apply to our physical well-being apply to our IT systems as well: practice good hygiene (keep your systems clean); stay fit and maintain a healthy diet to improve your ability to resist and fight infection (update security); and maintain a safe distance from others and avoid areas where contact with infection is more likely (be alert of suspicious internet activity to avoid infection).

[1] NSA & ASD: Detect and Prevent Web Shell Malware, April 2020, https://media.defense.gov/2020/Apr/22/2002285959/-1/-1/0/DETECT%20AND%20PREVENT%20WEB%20SHELL%20MALWARE.PDF

[2] Microsoft: Ghost in the shell: Investigating web shell attacks, February, 2020, https://www.microsoft.com/security/blog/2020/02/04/ghost-in-the-shell-investigating-web-shell-attacks/

[3] ZDNet: NSA shares list of vulnerabilities commonly exploited to plant web shells, April 2020, https://www.zdnet.com/article/nsa-shares-list-of-vulnerabilities-commonly-exploited-to-plant-web-shells/