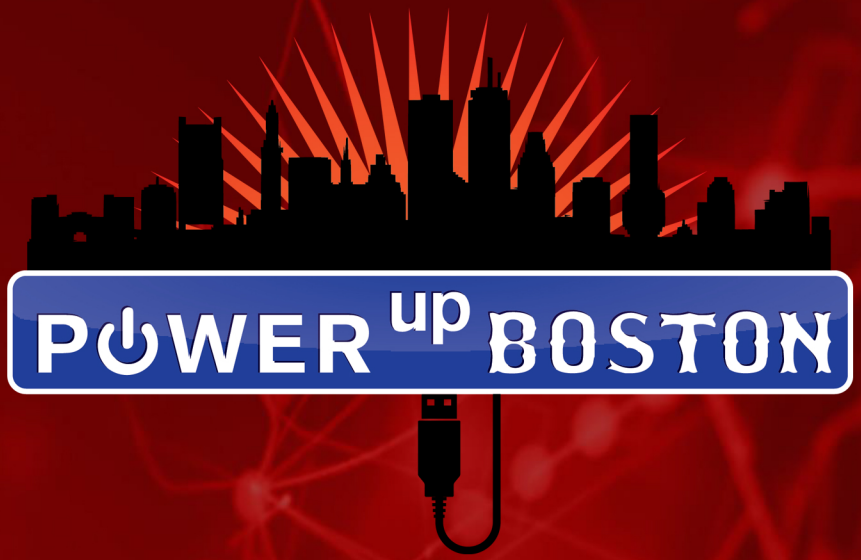


COUNTING DOWN TO THE NEXT ZERO-DAY ATTACKS

WHAT BUSINESSES NEED TO KNOW

It’s another day, and yet another zero-day exploit is making the news. Whatever week you’re reading this, we can guess there’s a zero-day attack in the works. This eBook will help you understand what happens with this type of exploit, give common examples, and share strategies to help you protect your business.

As the 1990s came to a close, we were concerned about Y2K – the threat of a widespread programming shortcut wreaking havoc on our computers had us all worried. Yet, while Y2K didn't have a great impact, one of today's top threats, zero-day attacks, do live up to their hype. Exposing and leveraging vulnerabilities, at first without detection, zero-day exploits create complicated problems for those using the affected software. This eBook will:

- define zero-day exploits;
- explain how they work;
- share recent examples;
- discuss prevention and detection.

Key Distinctions

Zero-day vulnerability – a flaw the software developer is unaware of, so there is no patch yet.

Zero-day exploit – the method hackers use to leverage the vulnerability.

Zero-day attack – when someone uses a zero-day exploit

WHAT IS A ZERO DAY EXPLOIT?

A zero-day exploit is computer code taking advantage of a vulnerability in software. This type of attack hurts business because it's being exploited before developers have a chance to address it. The developer has only just learned about the flaw and has had "zero days" to fix it. Hence, the name zero-day attack.

HOW DOES A ZERO-DAY ATTACK WORK?

You work hard to secure your business network. Unfortunately, hackers are determined to get in. They probe persistently until they find a software vulnerability you don't know about. They use this unknown and unpatched flaw to access your system.

The vulnerability may have been there from the day the software was released, or it may come as the software updates. Threat actors, meanwhile, prod the software and scrutinize the code to find vulnerabilities. Once they find a loophole, they work to write and install an attack before the developer discovers the flaw.

Bad actors can buy zero-day exploits on the Dark Web and customize an attack on your business.

The zero-day attack may be immediate once a bad actor finds a vulnerability, or they might infiltrate the network and wait patiently for the best time to attack. That could depend on their goal, which may be financial gain, hacktivism, corporate espionage, or cyberwarfare.

RECENT EXAMPLES OF ZERO DAY ATTACK

Zero-day hacks can target operating systems, Web browsers, office applications, open-source components, hardware and firmware, or the Internet of Things. That makes for a pretty large threat surface.

A zero-day attacker can steal data, corrupt files, take control of devices, install malware or spyware, and more.

Consider these well-publicized examples of zero-day attacks from the past two years:

- In December 2021, **Amazon Web Services, Microsoft, Cisco, Google Cloud, and IBM** were among the major tech players affected by the Log4j vulnerability in an open-source logging library. Wired reported the exploit, "will continue to wreak havoc across the

internet for years to come." The US's Cybersecurity and Infrastructure Security Agency director described the flaw as "one of the most serious I've seen in my entire career, if not the most serious."

- Earlier in 2021, **Google Chrome** was hit by a series of zero-day threats and issued updates to a vulnerability stemming from a bug in its Web browser's V8 JavaScript engine.

- **Zoom** was targeted in 2020. Hackers were able to remotely access users' PCs if the video conferencing platform was running on an older version of Windows.

- **Apple's iOS** fell victim in 2020 to two sets of zero-day bugs that saw attackers compromising iPhones remotely.

PREVENTION AND DETECTION

The same preventative measures that protect computers against cybersecurity threats can work against zero-day exploits. You'll want to install security patches for software and operating systems when they are released. This is the developer's way of fixing any newly discovered flaws.

Your business will also want to use a firewall. This one thing won't necessarily prevent an attack, but it helps to maximize your system protection. Also, install antivirus tools to help block threats and keep your devices secure.

Detection matters, too. The sooner you can identify zero-day attacks, the better. So, it's best practice to:

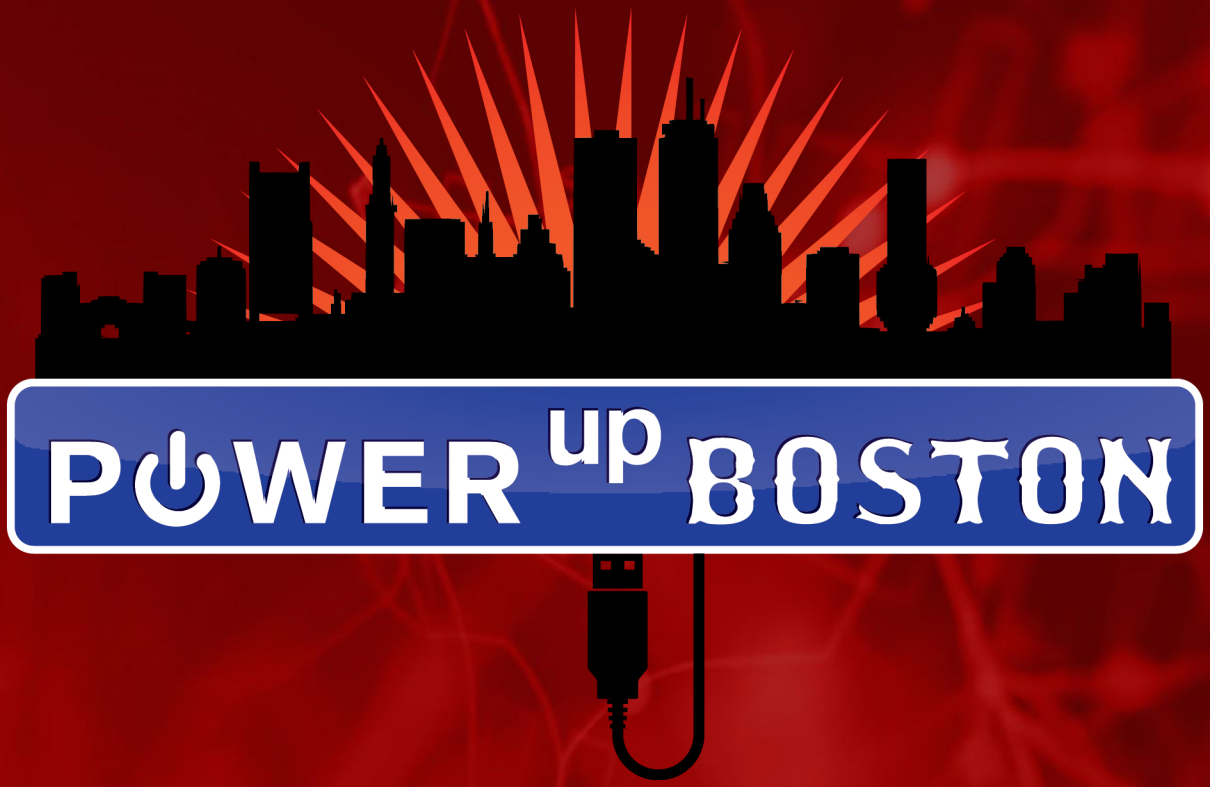
- scan for unexpected traffic and suspicious activity;
- follow malware databases to see what is known about the exploits;
- establish a baseline for safe system behavior – this helps identify interactions that may result from malicious actions.

CONCLUSION

Zero-day attacks are a nightmare for everyone involved. The sooner you act, the better. You can keep an eye on security news. When a zero-day exploit is announced, act quickly to identify where you are vulnerable, and patch that vulnerability.

Still, when you partner with a managed services provider, they'll monitor emerging threats for you. This expedites the response, as they can roll out a system patch without disrupting your work. They can respond quickly, as they know your setup and where you are vulnerable, and they already have access to your systems. They'll also put protection in place to prevent you from becoming a victim of the next exploit to make the news.

Speak to your MSP today about the work they're doing to secure your systems. Want to find out if you're at risk from a zero-day exploit? Contact our IT experts today!



Phone: (508) 617-1310

Email: info@powerupboston.com

Web: www.powerupboston.com

Facebook: facebook.com/powerupboston