Cymulate

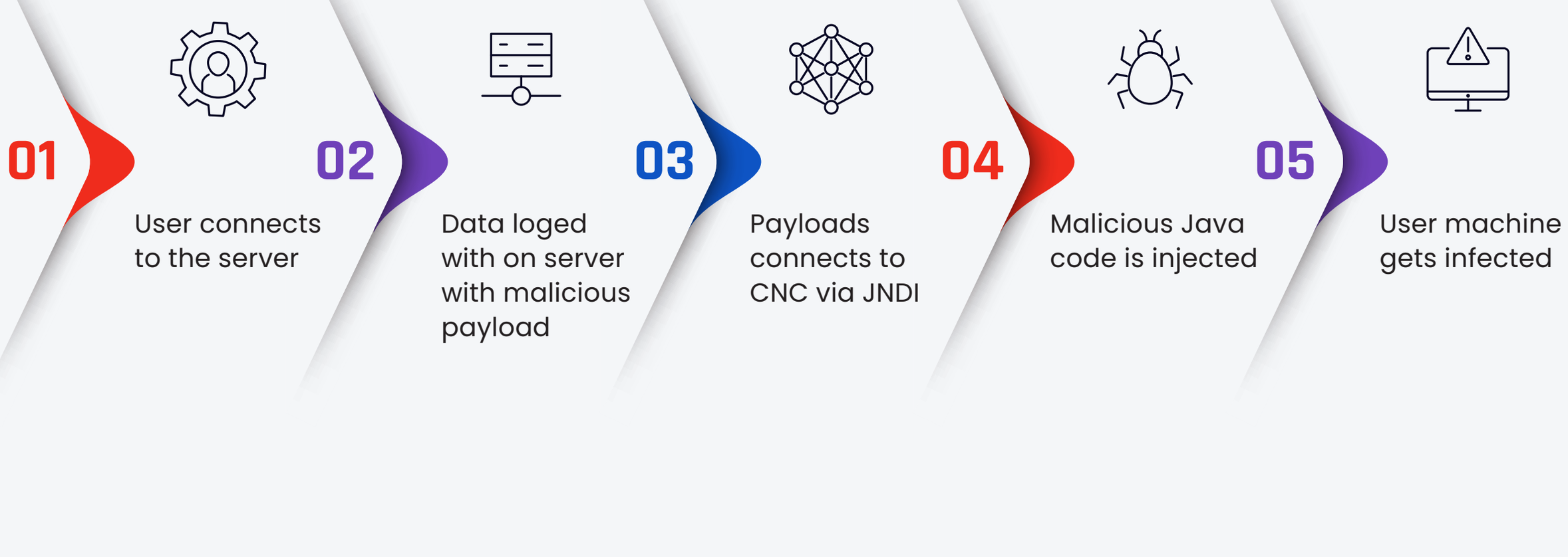
# Log4Shell Attack
## Quick Guide for First Response

The new Apache Log4j 2 vulnerability (CVE-2021-44228) is hopefully the last major issue of 2021 (though there's still a couple of weeks left). Even if it is the last attack we see this year, the impact has the potential to stick around well beyond the holiday season.
Threat actors and adversaries can potentially execute their own code on your systems, which means they can disrupt operations and could potentially access data. This vulnerability can be exploited to enable remote code execution on servers all around the globe, including a variety of major technology brands and services that have been using Log4j as part of critical infrastructure. While we may not know how long the threat actor community knew about the vulnerability, we do know that large-volume scanning for the flaw by threat actors began nearly instantly after public disclosure of it. In the time it took most organizations to begin patching/upgrading efforts, there were recorded incidents of the vulnerability being used to compromise systems.

## Breaking Down the Log4j Exploit

Apache log4j 2 is an open-source java-based logging package. While its primary purpose is to provide logging methodologies for java web apps, it has been utilized to provide functionality in a large variety of platforms. No matter how it's implemented, a specific transmitted payload can cause the log4j library to perform Remote Code Execution (RCE). Such an RCE can allow an un-authenticated threat actor to perform operations on the system running Log4j.

The vulnerability specifically exists in the Java Naming and Directory Interface (JNDI) implementation and can be triggered using an malformed LDAP request, making it easy for an attacker to retrieve a payload from a remote server and execute it locally.
Here is a common example of such a command:



## Key Lessons

While this particular vulnerability became highly publicized very quickly, it is a good reminder that any flaw in an operating system or critical software platform can become a major threat without much warning.
In many cases, the threat isn't even due to the actions of your organization; but rather programming code and packages provided by a third party, and outside your direct influence. There are a couple of major takeaways from events like this:

### Be proactive!

Fact - your security posture is in a state of constant drift. You can keep up with this drift and minimize its impact by running simulated attacks and mapping your attack surface regularly. Continuous security validation technologies provide this capability – make sure you are using the one that gives you the broadest picture and highest visibility.

### Be quick!

These kinds of exploits are a magnet for cybercriminals. They monitor vulnerability announcements and have the people and skill to very quickly create methods to use newly-found vulnerabilities to create attacks in hours – not days. Therefore, most organizations – which do not have a large group of experienced cybersecurity testers - need a system that provides the latest threat information so they can test and fine-tune their compensating controls without massively expanding their already overwhelming workload.

## What to do?

**01 Learn**

CVE details are available on MITRE website here

**02 Investigate**

Find internal and third-party usage of Log4j vulnerable configurations – don't forget that many 3rd-party platforms which use Apache may also use Log4j!

**03 Patch**

Since this is a vulnerability of high impact, a patch has already been released by the Apache Software Foundation and must be installed as soon as it becomes available for the platforms and tools you use.
In addition, Apache has released an updated version of the impacted library, Log4j 2.15.0, for all those who are managing Apache servers.

**04 Test – not just for this attack vector, but for others as well**

Cymulate customers and prospects can simulate attacks against their Apache servers (and the rest of their infrastructure) to test their cyber defenses and find out if this vulnerability can be exploited in their infrastructure before threat actors do.

## About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.

Contact us for a live demo, or get started with a free trial

**Test now!**

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632