



What is Ransomware?

Ransomware is one topic that doesn't seem to be losing momentum any time soon.

Every day, companies across all industries are paying ransom to retrieve their data from the clutches of malicious hackers.

Why? Because ransomware!

What's that you ask? Great question!

Here are the facts about ransomware to which every business owner should know...

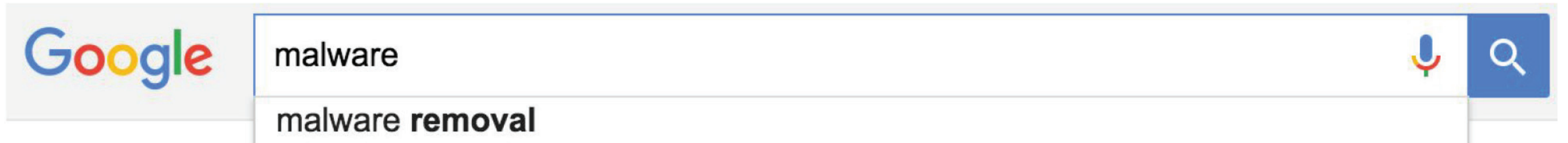


Ransomware comes in quite the variety pack these days, but let's start by cancelling out some definitions.

Ransomware is Not...

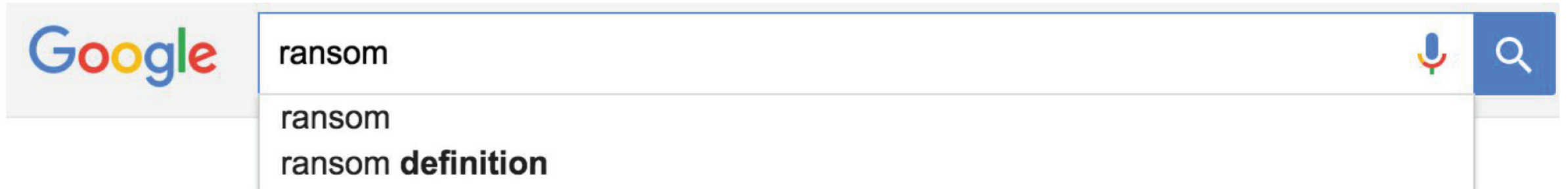


Ransomware ≠ Malware



'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

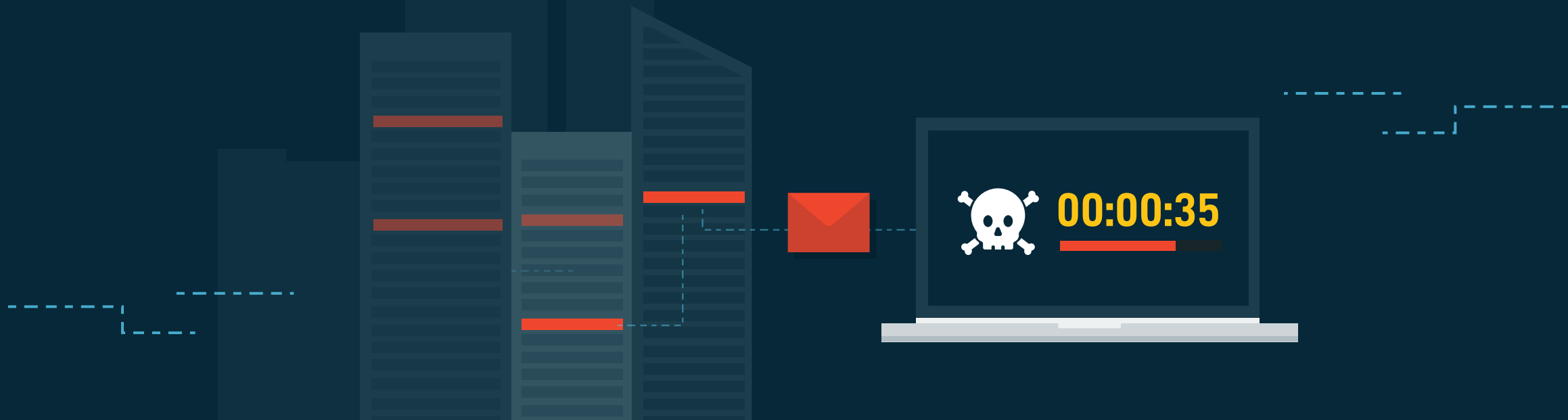
Ransomware ≠ Ransom



Ransom is the practice of holding a prisoner or item to extort money or property to secure their release, or it may refer to the sum of money involved. In an early German law, a similar concept was called weregild.

While ransomware is a form of malware, it's definitely unique in what it does. Sprinkle in some 'ransom' and you've got a malicious virus that keeps your data encrypted until ransom is paid (usually in bitcoins).

So as an SMB, why should you care?
The numbers tell a dark tale!



So what's the current state of ransomware?



On average there are more than **900,000**
ransomware detections each year.

Source: [Symantec](#)

It's pretty contagious!

As opposed to individual devices, more ransomware attacks are spreading across entire networks. The healthcare industry has recently experienced this.

Source: CIO



And It's Not Cheap To Recover From!



**Businesses lose an average of \$133,000
per year in recovery costs following
ransomware incidents.**

Source: [Sophos](#)

Not only is ransomware becoming more common, but it's also expensive and can halt an entire system.

As an SMB, it's painful to your bottom line. We decided to ask some IT professionals for their thoughts and noticed a common trend...

Business Continuity.



While business continuity can't prevent ransomware from attacking, it can prevent it from succeeding!

When it comes to ransomware, it's not a matter of IF but WHEN.

Business continuity will give you access to your captive data.
No hostages here!





For more information please contact:

Todd Painter | | Phone: 864.278.0202 | Email:
tpainter@unginc.com | Unified Network Group |
<https://www.unifiednetworkgroup.com>