Don’t Get Locked Up by Ransomware

Cryptolocker, Cryptowall, Petya, NotPetya, Locky and WannaCry have become notorious families of malware known as ransomware. Ransomware attacks have exploded since they came on the scene in 2012. **The number of ransomware attacks on businesses tripled last year,** jumping from one attack every two minutes at the beginning of the year to one every 40 seconds by the middle of the year.

AN INDIVIDUAL IS ATTACKED:

JANUARY: every 20 seconds

JUNE: every 10 seconds

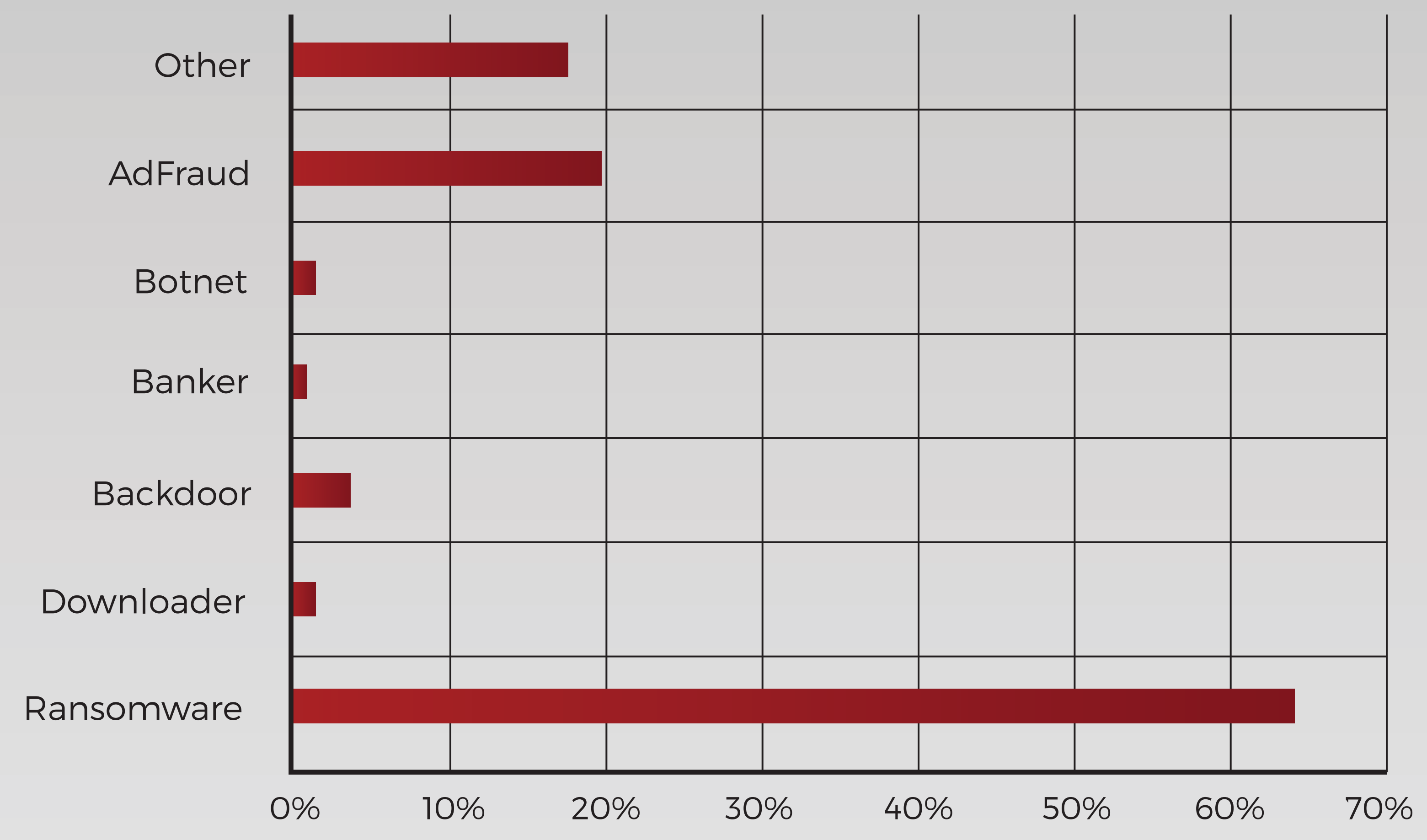
A BUSINESS IS ATTACKED:

JANUARY: every 2 minutes

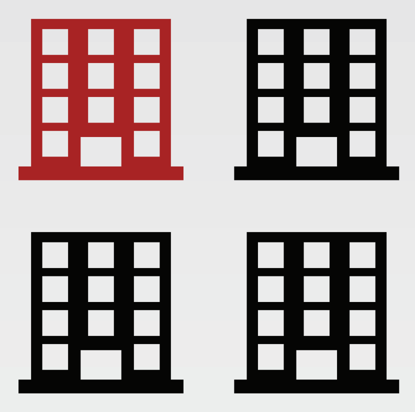
JUNE: every 40 seconds

This year, 60% of malware payloads have been ransomware, with the rest being a mix of ad fraud malware and small traces of everything else. In recent years, malware distribution breakdowns like these have been heavily influenced by whatever it is the major botnets are distributing.

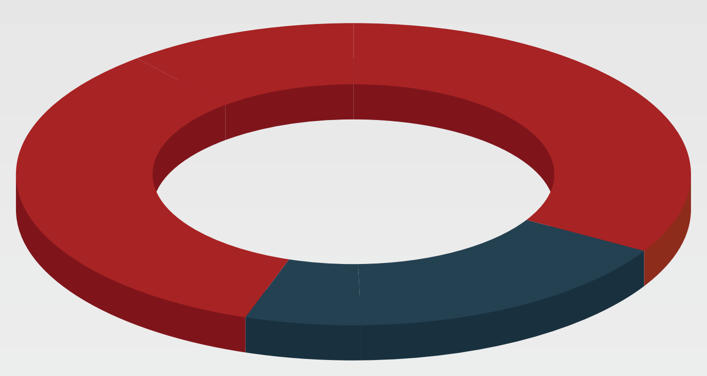
Malware Distribution by Type



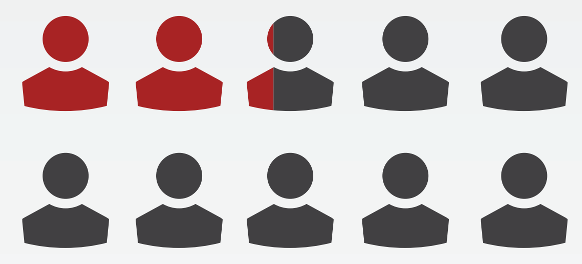
The rise of the ransomware-as-a-service model has been a big factor, making it easier than ever for even novice cyber-criminals with the most basic technical knowledge to launch their own customized attacks.



1 in 4 businesses hit with ransomware have 1,000 employees or more.



71% of companies targeted by ransomware attacks have been infected.



22% of victims had to halt operations.

No surprises here. Even when you have backups, a successful ransomware infection can grind your operations to a halt. And the longer you stay down, the harder (and more costly) it is to recover.

$6 trillion in losses expected by 2021.

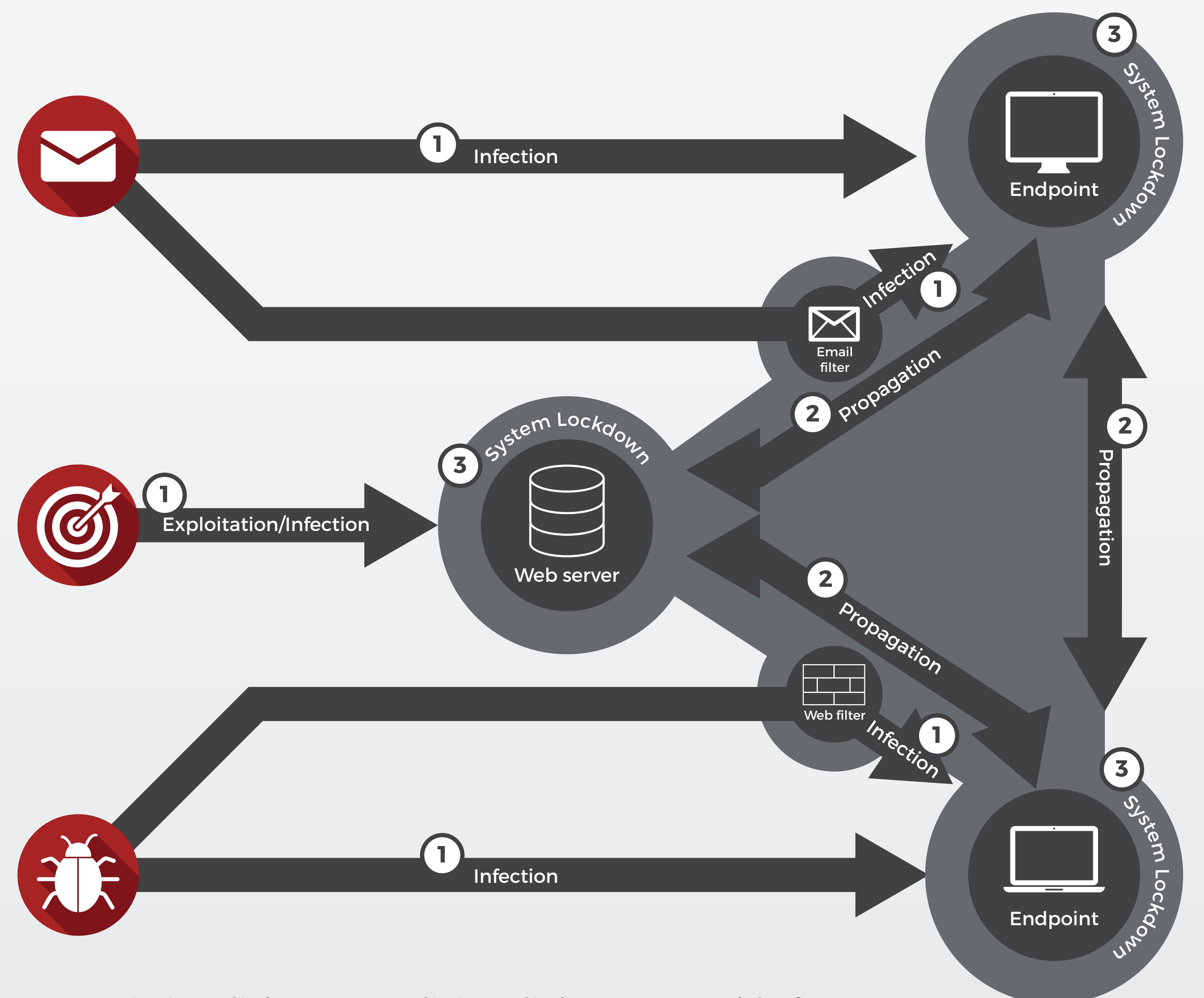
Ransomware and other cybercrime are projected to cost the global economy $6 trillion per year by 2021.

For perspective, that’s 7.5% of the total value of the global economy!

While there is a variety of ways malware can enter a network, ransomware was typically spread through phishing tactics. When users clicked on malicious links in an email or were sent to an infected website, the malware was installed, and locked their data.

The WannaCry ransomworm changed the delivery method by eliminating user action to install the malware remotely and in an automated fashion by pinging systems to find those with known, unpatched vulnerabilities that would allow the attackers to install the malware.

How a ransomware attack infects your systems:



1. Victim clicks on a malicious link or executable from an email and within minutes the malware locks all files on the system
2. Malware spreads through the network by collecting email addresses and credentials to move from system to system
3. Locked or encrypted files cannot be accessed without a decryption key from the attacker or from a vendor that has cracked the encryption and is offering the tool

DEFENDING AGAINST RANSOMWARE

DON’T PAY THE RANSOM

Increasingly, even if the ransom is paid, files are not unlocked as the criminal campaigns are too large and uncoordinated for criminals to track victim payments.

DON’T OPEN SUSPICIOUS EMAILS

You get lots of spam, and it’s difficult to tell which is harmless and which isn’t. That said, do not click on suspicious links or open attachments unless they’re from a trusted source.

UPDATE SOFTWARE

WannaCry and other ransomware code look for known vulnerabilities. Yes, it is inconvenient to patch or update software, but with the newer types of attacks, this will likely protect you more effectively.

BACK-UP YOUR DATA

Again, like patching, this is tedious, but automated tools that back-up and secure your data in the cloud may be a lifesaver.

RANSOMWARE PROTECTION

For $25 or so, a good antivirus solution will prevent the vast majority of ransomware attacks. Go to PCmag.com and search ransomware protection.

secure OPS