

In a recent survey we conducted with 60 companies who suffered successful ransomware attacks during the last 12 months, **100% reported they were running antivirus at the time of the attack.**

That may not come as a big surprise if you eat, breathe, and sleep InfoSec, but if security is just one of your many IT responsibilities (or if you're an executive who doesn't deal with security day-to-day) it may be a bit of a **wakeup call.**

Antivirus wasn't the only security solution that came up short, however. Victims reported using a variety of products that unfortunately weren't able to prevent the attack:

Ransomware vs. Traditional Security Solutions

Based on survey responses from 60 successful ransomware attacks

- **100% of the attacks bypassed antivirus**
- **95% of the attacks bypassed the victim's firewall(s)**
- **77% of the attacks bypassed email filtering**
- **52% of the attacks bypassed anti-malware**
- **33% of the attacks were successful even though the victim had conducted security awareness training**

This highlights a glaring gap in protection, and judging by the survey responses, it's not one they know how to clearly address, even after they've been made painfully aware it exists.

What do most companies do after a ransomware attack?

More of the same.

One surprising reaction to the attacks is that instead of branching out and investing in new forms of protection, the majority of respondents chose to simply double down on the same poor-performing solutions in the list above.

Investment in Additional Protection Following the Attack

- **26% (re)invested in email filtering**
- **25% (re)invested in security awareness training services**

- 20% (re)invested in antivirus
- 17% (re)invested in firewall(s)
- 43% didn't invest in any additional solutions

Are we giving up on ransomware prevention?

One way to read these reactions is that, lacking obviously better options but still feeling the pressure to do *something*, companies are taking the only immediate path they see forward — adding more of the basic, foundational security solutions that have widely-accepted benefits even though they also have widely-acknowledged holes.

It's companies reacting to their castle being invaded by either making the moat they had wider or adding *another* moat in front of the old one argument.

Sure, the invaders had no trouble bypassing the old moat during their first attack, but generally speaking, everyone still agrees moats are good defense, so let's start there. Besides, the castle is bound to be invaded at some point no matter what we do, so let's just stick to what we know.

(That's not exactly the most productive mindset.)

To be fair, though, the fact that a whopping 43 percent of respondents chose not to invest in *any* additional security solutions whatsoever is also an indication that, when it comes to preventing ransomware, IT pros simply don't see many good options (new or established) they feel like they can trust.

Supporting that interpretation are the responses from IT pros at many of the victim organizations who simply preferred to address vulnerabilities and make improvements on their own. Two thirds responded to the attacks by conducting their own user awareness initiatives. Nearly half reacted by making updates to their existing security policies.

Are backups making us complacent?

Another contributing factor to the general feeling of complacency may stem from confidence in backups.

While backup is unquestionably a necessity and while it has undoubtedly helped save many an IT pro's bacon, it's also far from a given that every ransomware scenario will be able to be quickly remedied with a simple wipe and restore.

[In a separate survey we conducted earlier this year with over 330 IT pros](#), 81 percent were confident backup would provide them with complete recovery from a ransomware attack. But less than half of those who had actually experienced an attack were able to fully recover their data with backup.

The idea of increasing widespread reliance on backup, a solution that's really meant to be used as a last resort, makes many security experts nervous. There's also the worry that [some ransomware variants make copies of encrypted data](#) that criminals can later sell or post publicly.

The rise of [multi-stage ransomware attacks](#) that launch credential stealing payloads in addition to encrypting payloads also means the emphasis should be on proactive prevention rather than reactive recovery.

How to proactively prevent ransomware attacks

Not to get all militaristic, but [the simplest way to prevent ransomware infections is to take aim at its key delivery channels and stop it from gaining a beachhead.](#)

That means focusing on three things:

1. **Stopping ransomware from being delivered via email**
2. **Stopping ransomware from being delivered via exploit kit**
3. **Stopping ransomware from effectively launching on an endpoint**

1) Stopping ransomware from being delivered via email

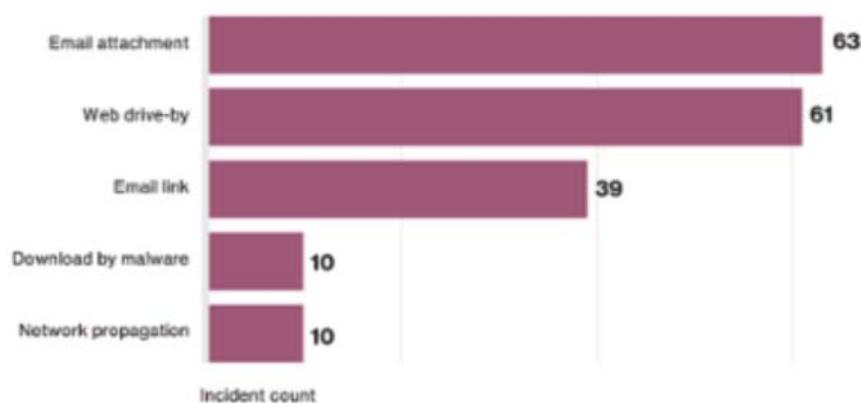


Figure 34.

Top five malware varieties within Crimeware, (n=135)

According to the [2016 Verizon DBIR](#), email is the #1 delivery channel for malware. And what percentage of that malware delivered over email is ransomware? [According to Proofpoint, over 96 percent.](#)

Top Malware Payloads by Percent of Total Message Volume, July-September 2016

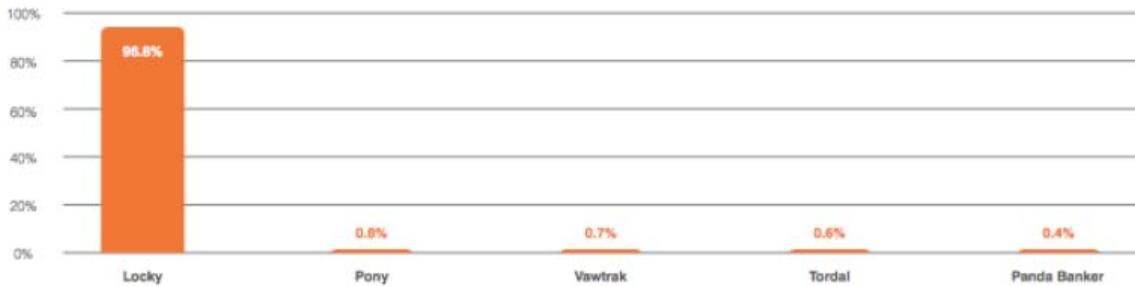


Figure 2: Top malware payloads distributed via email in Q3

Ransomware authors have a clear delivery method of choice, ladies and gentlemen. And the bad news is it's an incredibly effective one. The Verizon DBIR reports phishing emails have an average open rate of 30 percent, which is really just a data-supported way of saying what we already know — [users click things](#).

So how do we stop the wrong user getting the wrong email and clicking something they shouldn't from causing a company-wide data-encrypting disaster?

Well, thanks to our ransomware victim survey data, we know that email filtering unfortunately isn't a reliable solution (if you recall, it was bypassed in 77 percent of successful attacks).

That leaves an option that admittedly no self-respecting IT pro is going to be completely comfortable or satisfied with — training users how to spot phishing emails and avoid falling for them.

I know, I know. It's not great. [But there are approaches that have proven to be at least partially effective](#).

Remember, security isn't about finding one magic, silver-bullet solution. It's about lowering risk incrementally across the board. With that in mind, let's move on to focal point #2...

2) Stopping ransomware from being delivered via exploit kit

2) Stopping ransomware from being delivered via exploit kit

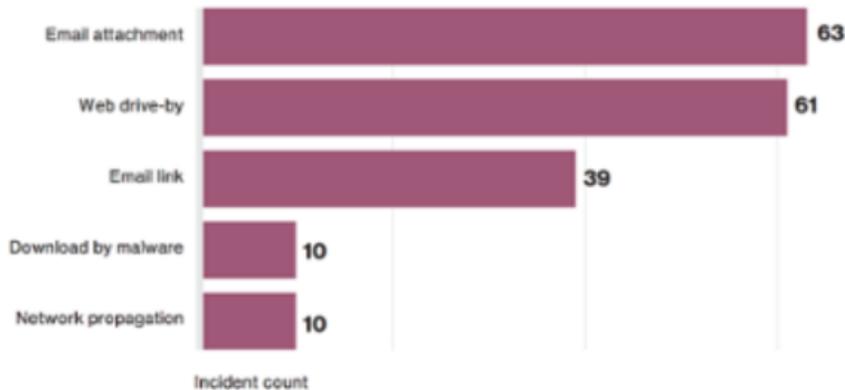


Figure 34.
Top five malware varieties within Crimeware, (n=135)

Verizon lists the #2 delivery channel for malware as "web drive-by", which means victims are infected when they visit a compromised website and a program they're using has a vulnerability that an attacker is able to take advantage of with an exploit kit ([you can learn all about how exploit kits work here](#)).

Two ways to prevent infections from exploit kits are to install an ad blocker, which can protect users from malicious web advertisements, and stay on top of patch management. Depending on the size and complexity of your organization, keeping systems and apps updated can be an ordeal.

Luckily, there are solutions that can help you automate things, and even starting small focusing on patching the 10 most frequently exploited vulnerabilities (CVE-2001-0876, CVE-2011-0877, CVE-2002-0953, CVE-2001-0680, CVE-2012-1054, CVE-2015-0204, CVE-2015-1637, CVE-2003-0818, CVE-2002-0126, CVE-1999-1058) can make a big difference.

((GOTO National Vulnerability Database:
<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-0876>

3) Stopping ransomware from effectively launching on an endpoint

Assuming ransomware does find its way onto one of your machines (with [nearly 50 percent of companies getting hit](#) you have to assume it eventually will), your next best bet is to make it more difficult for ransomware to effectively run.

By this point, the ransomware has already made it past your antivirus. It's in the process of launching and doing the things it needs to do in order to start encrypting your files.

The trick here is to have defenses in place that can not only recognize that those initial behaviors signal an attack is being launched, but that can stop those behaviors in their tracks, preventing the attack from fully executing and doing any damage.

There are several system settings you can adjust — disabling MS Office macros (easy), [using Software Restriction Policies to block executables from running in specific locations](#) (more complex) to stop particular strains of ransomware from running.

..a more comprehensive, hands-off way of blocking early ransomware behaviors...