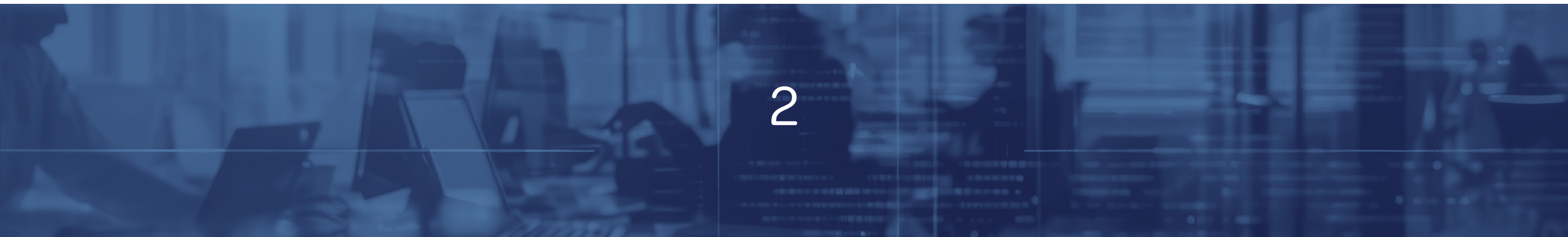
Ascend TECHNOLOGIES

MALWARE RESPONSE GUIDE:

5 THINGS YOU NEED TO CONSIDER

TABLE OF CONTENTS



Malware Happens

No matter how hard you try or train, an end user is going to click on something they shouldn't. The question then becomes, how effective are you at stopping it from spreading? A quick and thorough response is key to avoid the loss of passwords, intellectual property, or worse.

Here's a crucial piece of information to know upfront: Just treating the individual machine is not enough. More on that later, but we see that mistake time and time again.

Having defense-in-depth measures in place is vital to fully combat malware. It can be difficult to convince those not in the security field of the full ramifications that a malware infection can have on a network. We created this guide as a tool to help build a case for further investigation.

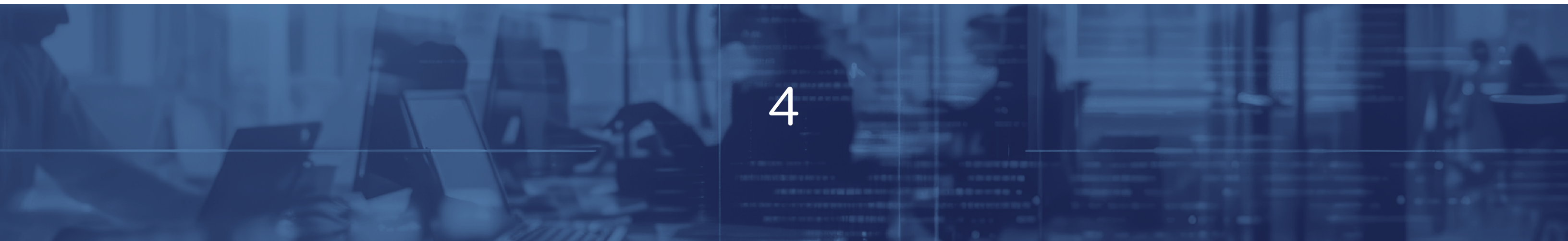
This eBook contains the 5 biggest factors organizations fail to consider when they find malware in their environment.

Credentials May Have Been Taken

After finding malware, your first and only mission in life is to figure out if credentials have been taken. If they have, you have a litany of other issues and scenarios to consider.

Once a hacker has valid credentials, they don’t need malware anymore. They can log into your network legitimately and access any information that the user has access to. This makes them much more difficult to spot, unless you know exactly what you’re looking for. Searching your logs for odd login times to the Virtual Private Network (VPN) (or users accessing machines that they wouldn’t normally have any business accessing) can usually start to point you in the right direction.

So can End Point Detection & Response (EDR). An Endpoint Detection & Response solution actively monitors endpoints in your network for the type of suspicious activity that can be a sign of a larger attack.



Possible Password-Stealing & Keylogger Components

Most malware today contains some kind of password-stealing or keylogging component. In this scenario, hackers are able to obtain passwords not only in the domain, but essentially to anywhere. How many sensitive things are typed on your end users' computers every day?

With this information, the possibilities are endless for a hacker. Bank accounts, intellectual property, and credit card numbers (just to name a few) are only a click away. We've seen organizations become aware of malware but not act quickly enough to resolve it — leading to drained bank accounts as a result.

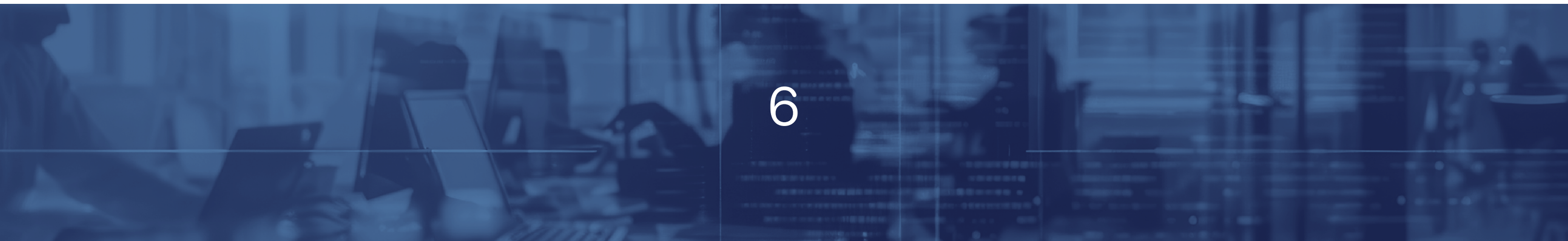
Don't let that be you.

The Attack Could Still Be In Progress

Malware may not be the end game — in many attacks, it’s just the beginning.

Attackers can use the malware as simply an entry point into your network, then use valid credentials or a backdoor to stay persistent and continue the attack. Using lateral movement techniques, they can explore different accounts, machines, and information within the network without drawing attention to their presence.

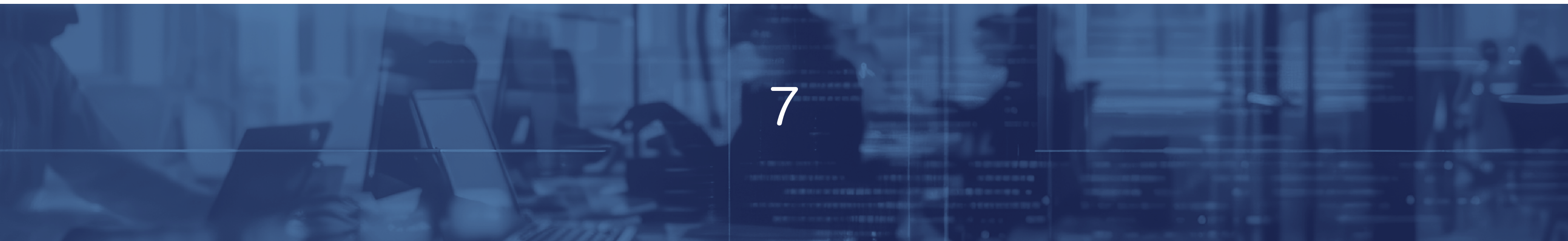
After malware has made its way into your network, the attack can continue quietly (and malwarelessly) unless you’re prepared to identify other signs of an attacker’s presence.



Clients' Information Could Be Stolen

Buying and selling stolen data is big business these days. A very organized black market exists to sell remote access to hacked organizations, stolen credit card numbers, and stolen healthcare records. The ramifications of your organization being told by law enforcement or, even worse, media outlets that your customers' data is being sold are huge. It's better to get ahead of the attack and respond appropriately than to have Brian Krebs break the news, trust us.

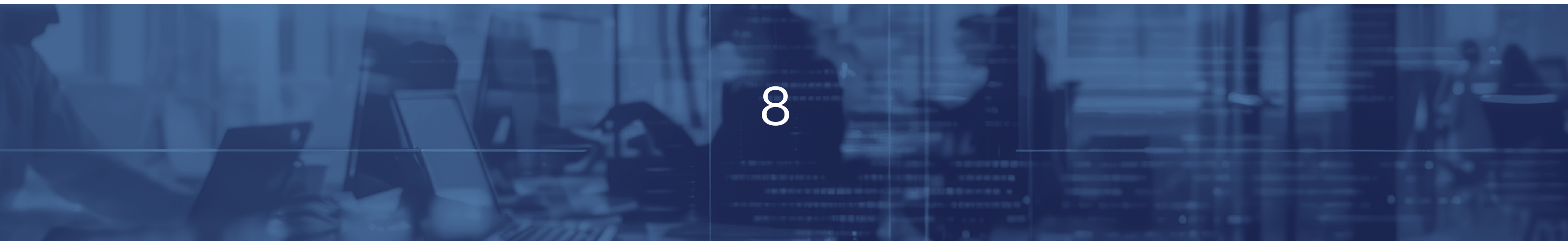
Not only are there PR issues to consider, but there are legal ones too. Many US states, as well as countries around the world, have enacted legislation requiring private, governmental, or educational entities to notify individuals of any loss of Personally Identifiable Information (PII). This means your organization has a legal responsibility to inform clients or customers that you have lost their data. If you ignore that possibility by not performing due diligence, you're opening yourself up to huge amount of legal and financial risk.



Reformatting Won't Work…

Malware exists today that writes to the BIOS/UEFI/Master Boot Record. What does that mean? Even if you re-format a computer, the malware may still be present on the machine. On top of that is the fact that malware can spread to more machines within an environment extremely quickly. Hackers are smart, and can remain relatively quiet in your network for long periods of time until they find something of value. It could be days, weeks, or even months to see visible evidence of an infected machine.

Continuing to just reformat infected machines is what we like to call the 'whack-a-mole' approach to mitigating malware. Unless you deal with the root cause of the attack and investigate fully, malware will continue to pop up across your network. This scenario can move quickly from mild frustration to a full-blown breach if a malware incident isn't remediated properly.



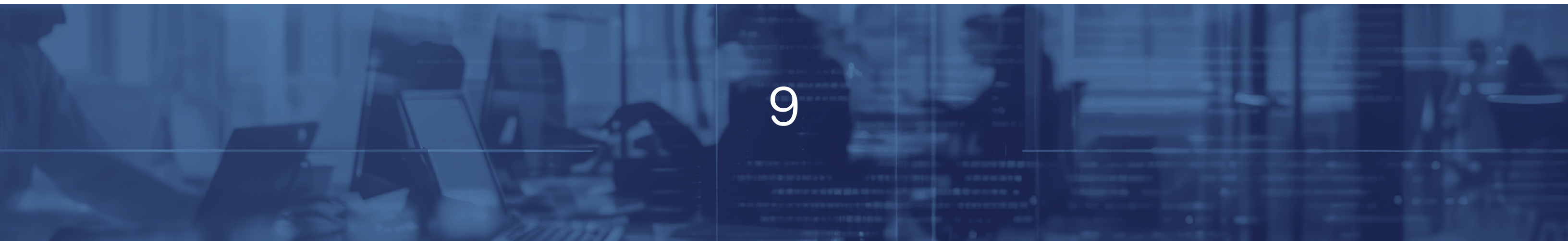
Time is of the Essence

We always try to stress that it is better to respond quickly and appropriately than to wait and see. The longer you wait, the longer malware has a chance to spread and do further damage to your network. When it comes to cybersecurity, there's no time to hope for the best.

So what do we recommend?

Our solution is less complicated and costly than experiencing a full-blown breach. When we respond for our clients, our first step is to quickly and easily deploy technology in their environment that will give us some visibility into the threats inside your network. The key there is to get a complete and accurate picture of the extent to which the malware has done damage, which then allows you to triage and respond appropriately. By getting to the root of the problem immediately, you save yourself time, money, and the headache that waiting could cause.

Having anti-malware technology and a detection & response solution in place can put you ahead the next time malware gets past your defenses.



Ascend
TECHNOLOGIES

NEED HELP MITIGATING A MALWARE ATTACK?

Partner with a reputable response team with proven cybersecurity expertise.

LEARN MORE ABOUT INCIDENT RESPONSE