Prinect

Technical White Paper
Preventing Ransomware.

HEIDELBERG

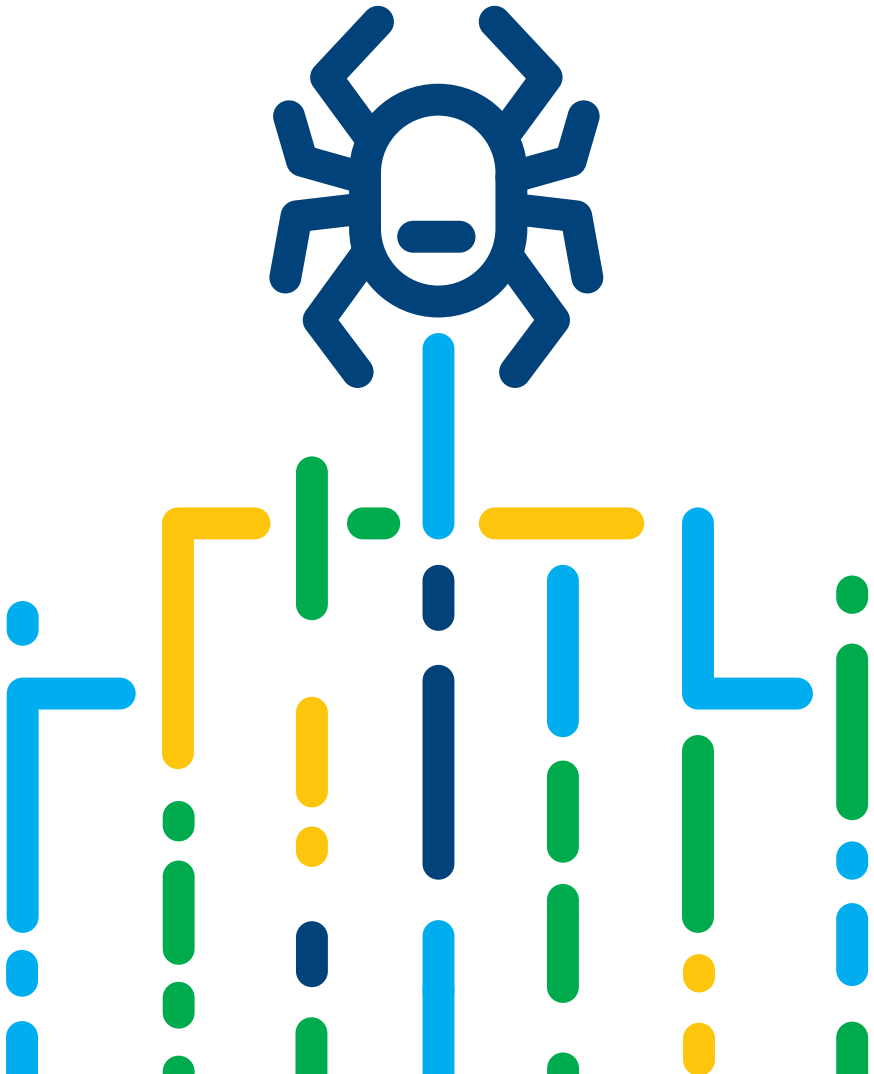
Don’t put your shop at risk. Ransomware is a serious problem.

Ransomware is potentially a very serious problem. It can cost a lot of money and affect the reputation of your business – no matter how big or how small your business. Security-related attacks are increasing, and victims experience major disruption to their production.

When preventing Ransomware, your choices are **limited:**

- Invest time and money in prevention.
- Invest time and money to mitigate your damages after being hit by Ransomware (then, subsequently, investing time and money in prevention for the future).
- Hope nothing bad ever happens.

To view or download all of our Technical White Papers visit: https://news.heidelbergusa.com/whitepapers/



Contents

*The information provided herein is being delivered to you "as is" and Heidelberg makes no warranty as to its accuracy or use. Any use of the technical documentation or information contained herein is at the risk of the user.

What can I do to prevent Ransomware?

Here are 9 steps you need to take:

1 Apply the Latest Software to your Systems

You want to make sure you are applying the latest software updates to your systems; especially security-related updates:

a. Microsoft® Windows™ Operating System updates on your Servers and Workstations as well as Firmware and BIOS updates.
b. MacOS Operating System updates on your Apple® Workstations.
c. Software Updates on all your infrastructure appliances like your firewalls and network switches as well as software applications particularly your Web Browsers.

CAUTION: Updates are not the same as Upgrades. Updates apply software fixes within an OS Version while Upgrades migrate you to a completely new version of the OS typically with new features. You should NEVER do Upgrades unless the new OS version is officially supported by the Heidelberg Prinect® Workflow as well as other applications you may use.

2 Implement Anti-Virus Software

Implement Anti-Virus software on all your servers and workstations – implementing on only a few will create the risk that the Ransomware gets in and propagates to another. Anti-Virus software can slow down the system performance including your Prinect applications. Heidelberg does not recommend any specific Anti-Virus product or vendor, and has no direct guidance on configuring the various settings for balancing security/performance as these vary from product to product.

3 Follow Vender and Industry "Best Practices"

Follow vendor-recommended and industry-accepted "Best Practices" for hardening all the equipment used in your plant. There are various security standards: for example, PCI-DSS or HIPPA may provide some information may be applicable to your plant.

4 Always Run Backups

Maintain regular backups of your business systems.

5 Implement a Domain

If you are not already on a domain, consider implementing one where you can administrate security policies from a central location.

6 Executing Policies and Procedures

Put policies and procedures in place to minimize your chances of a successful attack.

a. Users should avoid accessing personal e-Mail on your business systems.
b. Users should avoid installing unwanted software on your business systems.
c. Users should avoid accessing their social media on your business systems.
d. Users should not click on links in e-Mail from unknown or suspicious senders.
e. Users are required to have strong passwords.

7 Only Use Commercial Grade Products

Use "commercial-grade" products in your plant. Besides being more durable and performing more consistently, they typically have more robust controls over security.

8 Eliminate End-of-Life Products from your Plant

Eliminate end-of-life products from your plant, where there is little or no support as well as a lack of the latest security technologies. For example, if you are still running Microsoft Windows Server 2003 in your plant which Microsoft has ended support a few years ago. When there is no support, there are no new security updates.

9 Protect your Heidelberg Workflow

a. Keep your Prinect Workflow software up-to-date using the Prinect Maintenance Center.
b. Ensure users are logging in with their own user account and use the OS Login setting.
c. Do not give every user Administrator rights for production systems.
d. Do not use the "Prinect" user for normal production and make sure you have changed any factory default passwords.
e. Harden the shares used in the Workflow. They do not need to have Full Control for the Everyone Group. Heidelberg Prinect Production Manager does not use the Hidden Administrative Shares, but take caution that they are not used by any other software in your plant such as IT Management Tools.
f. Use the Prinect Security Tool in Cockpit Administration.

Please Note: Heidelberg has no way to enforce the things above, and our customers vary in size as well as their security needs, but the more you can do to address plant security, the better off you will be.

How do I know if I have Ransomware?
The symptoms are as follows:

Files Won't Open
All of the sudden you cannot open files, and errors show up saying "file is corrupted" or "has the wrong extension."

Strange Names in Files
There are files in the folders with names like "HOW TO DECRYPT INSTRUCTIONS.HTML."

Unable to Close Windows
A window has opened to a Ransomware program that you cannot close.

Instructions to Pay for Files
Your desktop background contains instructions on how to pay to unlock your files.

A Countdown Warning
A program warns you that there is a countdown until the ransom increases, and you will not be able to decrypt your files.

How did I get Ransomware?
Here are the most common ways:

Opening Suspicious e-Mails
If you receive an e-Mail with an attachment or link to a software download, open the attachment or click the link without verifying its authenticity, you can get a Ransomware infection. **This is, by far, the most common way Ransomware gets on a computer.**

Downloading Unverified Files
Ransomware infections can also happen via downloads when you visit a compromised website with an old web browser (or plug-in/add-on). What happens is the compromised website runs what is called an "Exploit Kit," which checks for vulnerabilities such as unpatched operating systems.

Hackers
Another way Ransomware infections occur is hackers offer free software. This often includes "cracked" versions of expensive games or software, free games or mods to games, adult content, screensavers, cheats for online games or a "get around" for paying for access to a website. This is how a hacker can bypass any firewall or email filters because you downloaded the file directly. When you install it, the software also installs the Ransomware that activates itself days, weeks, or even months later.

Remote Desktop Protocol (RDP)
Internet-exposed Remote Desktop Protocol (RDP) sessions are used to remotely log in to Windows computers and allow a user to control that computer as if he were sitting in front of it. RDP typically uses port 3389 to communicate, and if your business allows this kind of traffic from the Internet through your firewall, hackers can use these exposed computers to spread Ransomware within your network.

What do I do once I am infected?

Here are 4 steps you need to take:

1 Disconnect Immediately

Disconnect any infected computer from your network as soon as possible. Unplug any Ethernet cable, turn off any wireless capabilities such as Wi-Fi or Bluetooth, and unplug any storage devices such as USB or external hard drives.

Make note of the following for the infected computer:

- Mapped or shared folders from any other computers
- USB drives of any kind
- Cloud-based storage such as Microsoft OneDrive, Google Drive, DropBox, etc.

2 Check Your Computers

Inventory all computers and check for signs of encryption.

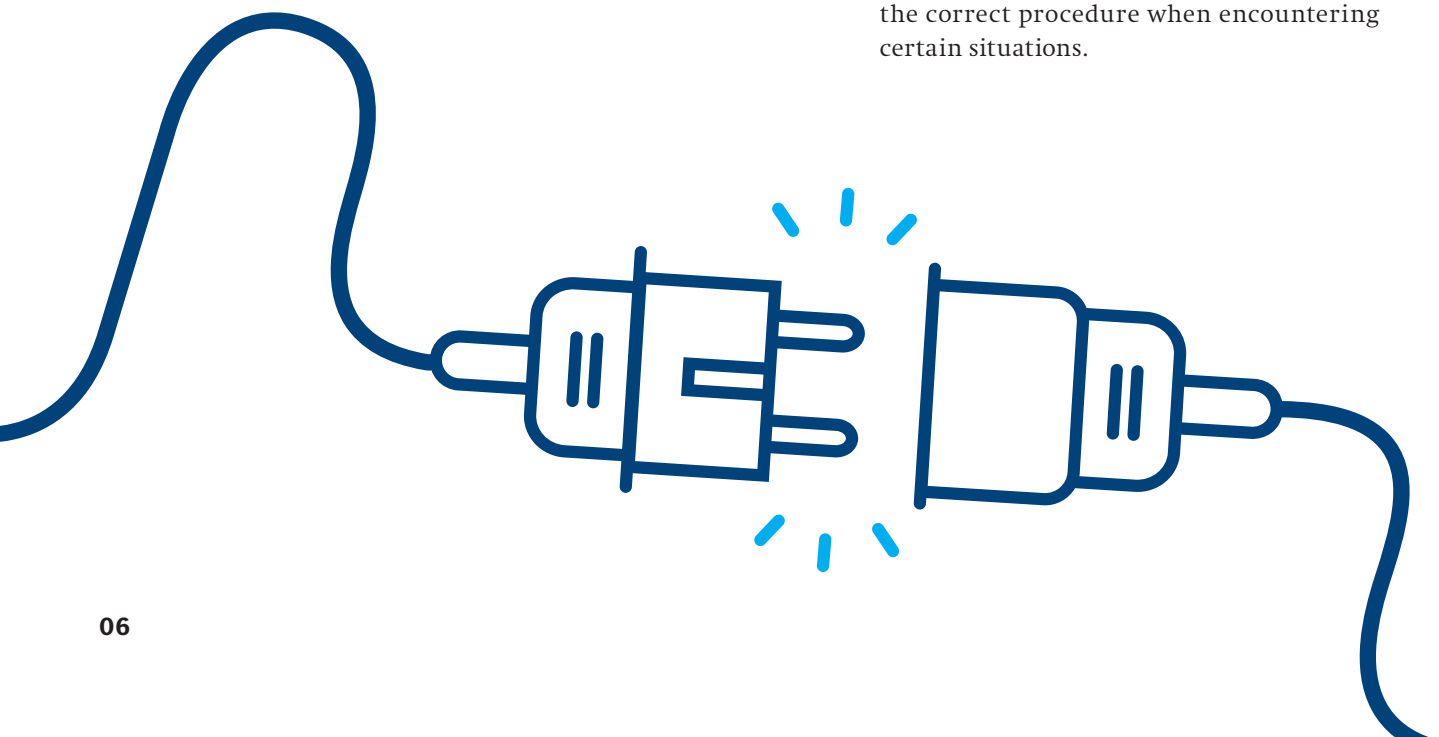
3 Find Out the Following:

- What strain of Ransomware you were hit with
- If other computers on your network were also infected
- Which computer was the so-called **"Patient Zero" or the first one infected – the entry point.** This is typically done by looking to see who the owner of the encrypted files is. To encrypt a file, the Ransomware must open and write back to a file, which means that the file ownership will change to the user who was infected.

4 Decide What 3 Options You Want to Do:

- **OPTION 1:** Redeploy the system and reinstall the software. This means either starting fresh or, if you have a good backup, restoring your data and configuration. This assumes you have a recent backup, it is known to be good, and you are sure you have eradicated the Ransomware from your plant.
- **OPTION 2:** There are some tools that purport to remove Ransomware. Heidelberg does not endorse any such tools, but you can certainly try them – particularly, if you do not have a good current backup of your system. In the event you go down this path, you have to decide if you feel comfortable using them, or if it makes more sense to hire a professional who is experienced. This route may or may not work.
- **OPTION 3:** Pay the ransom – this assumes you have or know how to obtain Bitcoin, which will (most likely) be the form of payment required, and that you have a TOR Browser. Hackers will often direct you to a site hosted on the TOR network. Paying the ransom is no guarantee you will get back in operation or won't be infected again. This is an option that you probably want to avoid if at all possible.

For the Future: Implement plant-wide prevention for the future. This must include Security Awareness Training for your users as, most likely, your plant was infected by advanced social engineering, lack of knowledge on common threats, or just not knowing the correct procedure when encountering certain situations.



What can Heidelberg do if I have been infected?

Unfortunately, there is very little Heidelberg can do once the Ransomware infection has occurred. First you will need to eradicate the virus, we can then redeploy the system(s) and reinstall the software. **Please Note:** Recovery from viruses is not covered by service contract or warranty, these services are billed at prevailing rates.

What other things can I do to protect my plant?

You may want to consider integrating Cyber-Insurance into your Risk Management Program. Keep in mind that this does have certain requirements. For example, you may be required to identify a Chief Information Security Officer (CISO), create an Incident Response Team, and have a tested plan in place. In addition, almost all Cyber-Insurance policies will require timely breach reporting. Surprisingly, Cyber-Insurance probably makes more sense for smaller printers that do not have a dedicated IT Staff with a strong focus on security.

Summary

Hopefully you will never have to deal with Ransomware. On average, it will take 3 days and cost around thirty-thousand dollars to recover. Ransomware is a problem that is better taken care of sooner than later – the old adage "An ounce of protection is worth a pound of cure" really applies. Security in your plant should be assessed and budgeted accordingly to address any gaps in protection. Heidelberg has several white papers that can provide guidance.

Be sure to:

- Establish an acceptable-use policy
- Harden your plant infrastructure
- Harden your network switches
- Harden your Prinect servers

Please direct any questions regarding this document to Eugene F. O'Brien, Senior Technical Support Analyst at:
(770) 794-6205 or
eugene.obrien@heidelberg.com

Heidelberg USA
1000 Gutenberg Drive
Kennesaw, GA 30144
Phone 800 437 7388
info@heidelberg.com
www.heidelberg.com/us