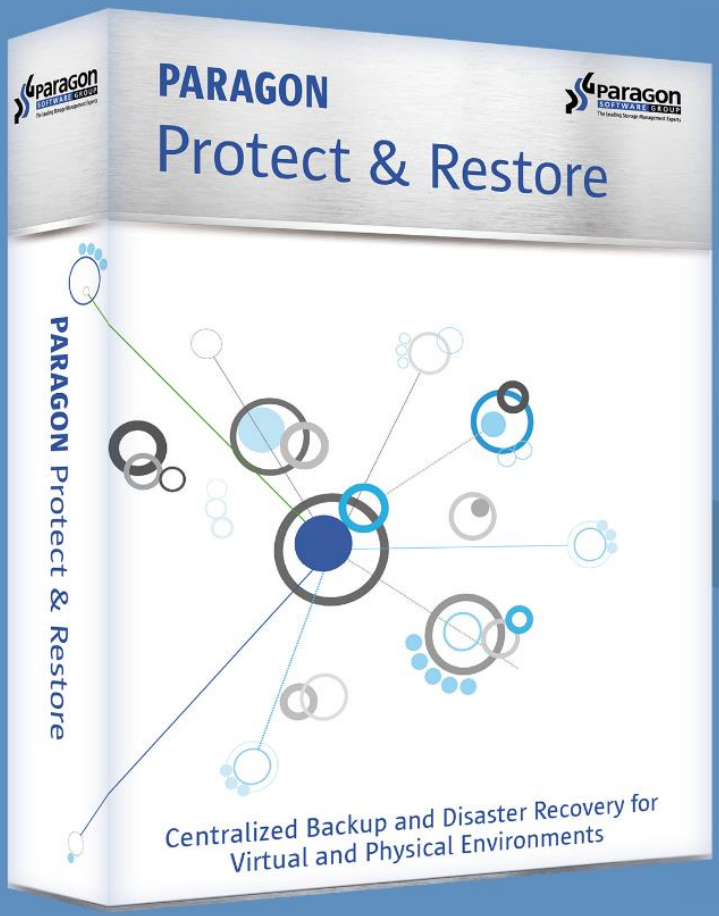
Ransomware (CryptoLocker) Paragon Protect & Restore to the Rescue

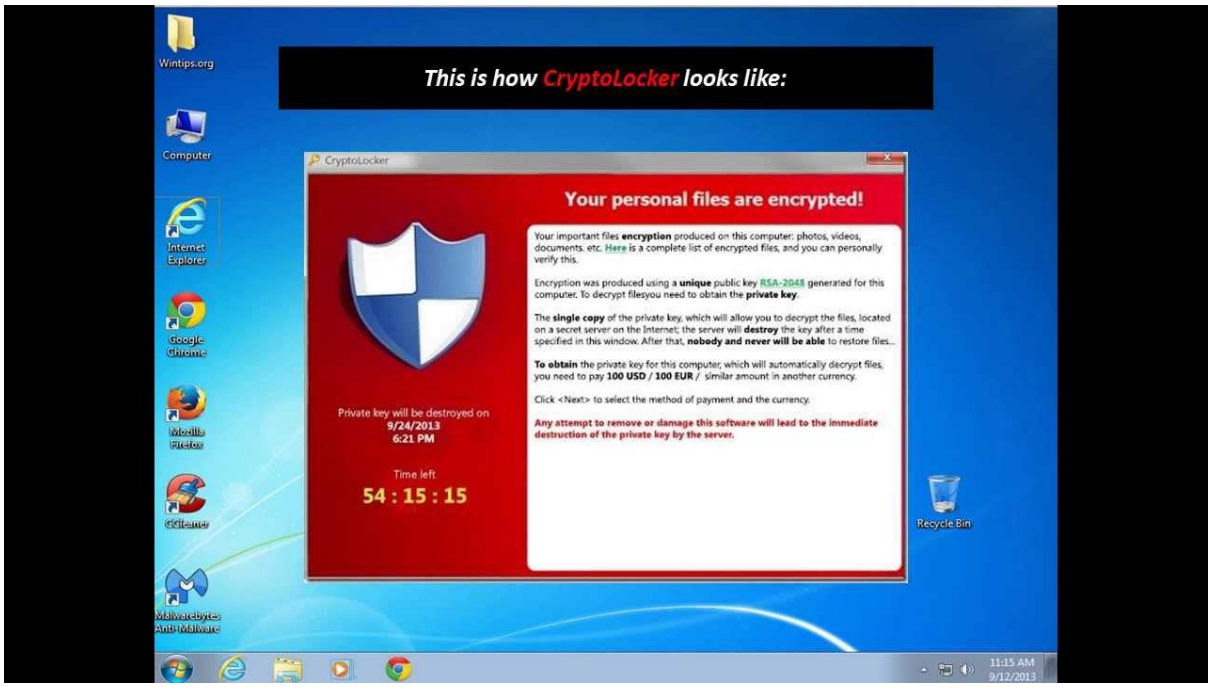


ABSOLUTE SOLUTIONS

Paragon SOFTWARE GROUP

What is Ransomware?

Ransomware is a type of malware that prevents or limits users from accessing their system or accessing their important files. Usually the victim is forced to pay ransom amount to gain access to the system and/or file/s. In most cases the ransomware infection encrypts files (Cryptolocking)



The infected user is asked to pay a certain amount ranging from $USD 24 to $USD 600 as ransom. However, there is no guarantee that even after paying the ransom amount, user will get their data back.

Ransomware attack can occur from various sources. It can be downloaded through malicious or compromised websites. It can arrive as payload, dropped or downloaded by other malware. It can infect through downloaded files from torrent or file sharing websites. Recently a lot of ransomware is delivered as attachments to spam emails. However, sometimes the spam emails are so well disguised that it is very difficult to confirm their authenticity.

Facts

- First developed around 2005 – 2006 in Russia. Ransom amount $USD 300
- During its initial phase, ransomware were typically files that encrypt particular file types (.DOC, .XL, .DLL, .EXE, just to name a few)
- By 2011 SMS ransomware threat, in which users with infected systems were asked to dial a premium SMS number
- Ransomware infection was initially limited to Russia. But its popularity and profitable business model soon found its way in other countries across Europe
- By March 2012, ransomware infections spread across Europe (and the United States, Canada
- The Rise of Reveton or Police ransomware
- The Evolution to CryptoLocker In late 2013
- Rise in infections in 2014
- 2015 – Infections spreading in other parts of the world including Saudi Arabia
- Currently 13 different new variants of ransomware
- Over 50 known ransomware families
- $USD 325 Million lost due to 1 ransomware family in 2015
- Security experts predicting a huge rise in ransomware infections with new variants

Prevention

- ✓ Email and Web protection
- ✓ Server Protection
- ✓ Network Protection
- ✓ Endpoint Protection
- ✓ Strong backup policies for servers and endpoints (Paragon Protect & Restore)

Best Practices

- ✓ Avoid opening unverified emails or clicking links in them
- ✓ Do not open unknown attachments
- ✓ Backup important files with 3-2-1 rule i.e. create 3 backup copies on 2 different media with 1 backup in separate location
- ✓ Do not rely on Windows backup
- ✓ Use encrypted backups for all your important data
- ✓ Regularly update your softwares to protect against latest vulnerabilities

How Paragon Protect & Restore can help?

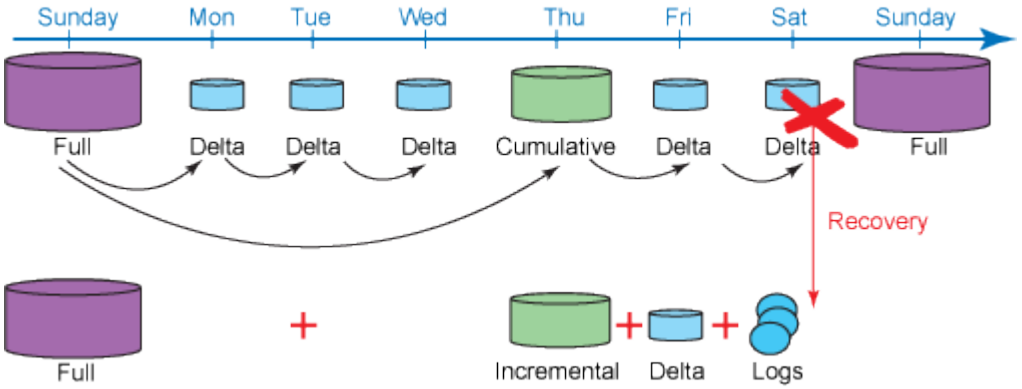
Prevention is better than a cure. In this case, unless you have already taken preventive measures, there can be no cure for a ransomware infection. Once an infection has been triggered and user files have been encrypted, they cannot be decrypted. You will lose your important data forever.

If you have Paragon Protect and Restore as your data backup tool, you can easily recover your lost / affected data.

You can either use the bare-metal recovery feature of Paragon to recover all your data to a new machine. Or you can clean your existing (infected machine) system using an antivirus and then restore your data on the same machine. The same applies to both, servers and work stations. With Paragon's incremental backup feature, network administrators can define policies based upon the machine criticality. A more critical machine can be backed up more frequently than a less critical machine.

Typical Scenario with PPR

In a typical scenario, a critical machine can be fully backed up every week and incremental backups can be scheduled daily. Let's say in this scenario, a full back up was taken on Sunday and incremental backups were taken for next six days. With a cumulative backup on Thursday. On next Saturday, an infection was detected. The system can be rolled back to Friday's state with minimal downtime. The users will receive all their data from Tuesday with no data loss.



Conclusion

Without Paragon Protect & Restore, the machines can be cured, but files that are encrypted cannot be recovered. You will lose your critical data once an infection occurred.