Guardicore

# Winning Against Ransomware

How Guardicore Centra Protects Against Ransomware

## Preface

Ransomware is a form of malware designed to encrypt important files on a device, rendering them unusable. The malware operators then demand a price (ransom) for a decryption key or software that can restore the files to their original data. Over the last few years, ransomware attacks became increasingly prevalent, and there's been an additional surge with Covid-19. Some ransomware also began exfiltrating their victim's data to hold as additional leverage[1].

Ransomware attacks are multi-faceted - an initial breach is not enough. An attacker or malware must also spread across the network before beginning encryption to maximize the damage. If only a single computer is encrypted they will not have enough leverage to demand a ransom. This fact, that forces ransomware operators to move laterally across the network, opens many opportunities for detection and mitigation points. Preparing your network beforehand with Guardicore Centra can reduce your attack surface and help mitigate and contain any possible damage from ransomware before you're even aware you're hit. Using Guardicore Centra visibility features can both detect malware presence faster and react to it sooner.

The United States Cybersecurity & Infrastructure Security Agency (CISA) has recently published a ransomware guide[2] to help companies deal with and prepare for ransomware infections. The guide's recommendations and best practices include segmentation and asset management as tools to prevent and deal with ransomware. Guardicore Centra visibility and segmentation features are exactly the tools for the job - Setting up policies to prevent and contain an initial breach, but also alert on lateral movement and other suspicious behaviours to help detect any malware sooner, while the easy and quick segmentation will allow you to react to it faster. Guardicore Centra also has other features to allow you to deal with threats even faster, like policy templates. We will cover all of that in this document.

Note: while the actions described below will reduce your network attack surface and stop different ransomware attacks from damaging your network, additional steps are still highly recommended. Like, credentials hygiene, backups detached from the network, routine patching.

[1] https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/
[2] https://www.cisa.gov/publication/ransomware-guide

# Prepare for the Worst, Hope for the Best

## Preventive Measures and Mitigations Before You Get Hit

Ransomware is an operation - the attack doesn't end when the malware reaches an organization's computer, it merely starts there; There is a long kill chain before the actual ransomware is deployed. The operator behind the ransomware may stay in the network for a long time, all the while propagating and increasing their reach in the network. In recent cases, before encrypting the network, hackers also exfiltrated important data and files and threatened to publish them online unless paid - as another leverage against victim companies.
Because a ransomware operation is multi-faceted, by having multiple layers of defence, you can prevent widespread damage and have multiple mitigations ready to cut the killchain early.

## Prevent initial infection

The first vulnerable spots for any network are its points of contact with the internet. While many ransomware operations rely on (spear)phishing, nothing prevents them from breaching your internet exposed services. Use Guardicore Centra visibility to monitor services exposed to the Internet and limit their exposure with policy:

1. Remote access services (Eg. RDP, SSH, TeamViewer, AnyDesk, VPNs).
2. Potentially vulnerable services (Eg. Apache, IIS, Nginx).
3. Potentially vulnerable machines (detect machines with an unpatched operating system using Guardicore Insight).
4. Unwanted exposed services (Eg. Databases, Domain Controllers, Internal web or file servers).

Reducing your network's outside visibility will hinder potential attackers and force them to spend more time at the intelligence gathering phase, which gives you more opportunity to discover them.

## Cutting The Killchain

Try as you might, networks eventually get breached. This could be due to a user infected by a spear-phishing campaign or a server running a vulnerable service that was not mitigated properly. With this mindset, we should prepare for this and have proper mitigations set beforehand.

Assuming a machine has been breached, and the attackers have a foot in the door, we would want to limit them from propagating from it inside the network. Consider the following guidelines:

1. Block any communication between laptops/workstations.
2. Block SMB (TCP 445) communication across your network, especially across apps and segments and between endpoints, except to your *Domain Controllers*.
3. Restrict FTP (TCP 21) access to file servers that share files over FTP to only machines and assets that need those shares - This will hinder attackers from exfiltrating data to later hold as leverage against you.
4. Block RPC (TCP 135) and WinRM (TCP ports 5985/6) to prevent remote service creation attempts and tools like PSexec.
5. Block communication from processes running with “powerful” domain users privileges, like *Domain Administrators*.
6. Block RDP communication across your network as much as possible - Allow it only from specific IT machines with their specific user. Consider creating Jumpboxes for RDP and restricting access to and from them to only specific personnel that absolutely need them (E.g: IT members, domain administrators, key app owners, etc...)
7. Limit users that can execute processes on your servers
8. Limit access from laptops/workstations to data center servers and cloud instances.
9. Split the network to minimal operational blocks that can work independently, and don’t allow communication between operational blocks, for example:
    - a. Isolating a database cluster and the app that relies on it from the rest of the network - They can continue to work and serve customers without risk of infection from the rest of the network.
    - b. Separating departments from each other so they can continue working. An infection starting at one point can’t affect the whole organization then and is contained to that department.
      E.g: Desktop machines belonging to the Accounting department and the Accounting app server.

## Backups and Their Protection

To maximize damage, Ransomware campaigns usually target the organization's backup application in order to encrypt the stored backup data. Use Guardicore Centra to limit access to your backup servers. Minimize communication to/from them using custom process-level micro-segmentation policy rules.

## Segment Critical Data Services

Your data services and servers are targets. Use Centra to segment and ring-fence critical data services such as your databases and file servers and limit the access to them from outside the network and also from regions in your network that do not need to access them. Limiting your data services' exposure to only the operational minimum will reduce the risk factor to those services and mitigate ransomware exposure and propagation paths.

## Detailed Response Plans

Create and plan your breach mitigation policies in advance, to reduce response time once a malware is detected.

Consider the following guidelines for your mitigation policy:

- Consider cutting off file servers and SMB from desktop machines - ransomware usually looks for network shares on the victim machine and encrypts them first. Don't let your file server be compromised by cutting it off from any machine that mustn't have it for operational continuity.
- Restrict Lateral Movement even more - while you may need to leave some remote control channels open for your IT department, block the rest. The channels that you do leave open, restrict heavily with both machine and user policies.

You can also create plans for the recovery process - consider which applications and sections you need to bring online first and create according policies to keep them secure while you restore the rest of the network.

# The Early Bird Gets the Worm

## Detection and Response Measures Once You're Hit

Vigilance is important when dealing with cyber threats and ransomware. The quicker you can react and put your walls up, the less damage and chaos the attacker can inflict before they are contained. Guardicore Centra has many capabilities that put it in an excellent position to both help in detection and in response - this section will cover those capabilities.

## Detection

Using Guardicore's Centra full set of capabilities, generate alerts to quickly find anomalies and threats inside your network.

### Policy Violations

Once your policy is in place and fully configured, any alert should be an indicator of an anomaly - something unexpected going on inside the network. Together with Guardicore Centra visibility and the initial lead from an alert, look for indicators of compromise and raise the alarm if you find traces of malicious activity.

### Guardicore Insight

We have integrated OSQuery into Guardicore's agent to give you even more visibility options on the asset scope. Utilize the querying framework to quickly detect anomalous activity that might be an indicator of compromise:

- Detect ransomware's most common pre-encryption action - Volume Shadow Copy operations - using OSQuery:

  ```
  Select * from file WHERE directory = 'C:\\Windows\\Prefetch\\' and filename like '%vssadmin%';
  ```

- Detects trojans used to deliver ransomware by searching for a common process hollowing technique that hides malware under svchost.exe, a legitimate windows process:

  ```
  select p.pid, p.path, p.parent, p.cmdline, par.name as parent_name, par.cmdline as parent_cmdline from processes as p
  inner join processes as par on p.parent=par.pid
  where p.name='svchost.exe' and (par.name!='services.exe' or p.path not like '%windows\system32\svchost.exe' or p.cmdline not like '%-%');
  ```

### CSA ThreatHunting

For customers with the Cyber Security Analyst (CSA) service, Guardicore CSA team runs periodic Threat Hunting techniques and raises the alarm on any anomalous behaviour they find. Techniques include analyzing incoming and outgoing internet connections and their associated GeoIP, looking for new executables that have increasing network presence that can indicate propagation and analyzing asset connections to find indication of lateral movement through neighbor count anomalies.

## Immediate Response

Once you've detected a threat or ransomware inside your network, use Guardicore Centra to quickly deploy the mitigation measures discussed in previous sections to prevent the threat from propagating inside the network and causing further damage.

### Segmentation Policy

Use Guardicore Centra labelling system to categorize machines into infected and clean groups, to keep track of the infection scope and cleaning process.

If you prepared plans in case of breach like what was proposed in Cutting the Killchain and Detailed Response Plans, deploy them as soon as possible. If you haven't, use the guidelines proposed there to quickly break your network into isolated operational hubs, to contain the spread of the malware.

Following those guidelines, Guardicore created two policy templates to help with ransomware response. Using the templates allows you, in a few mouse clicks, to deploy a policy to mitigate and contain ransomware spread and reduce the infection scope to a minimum.

There are two templates:

- **Ransomware Lateral Movement Mitigation -** Prevents RPC, RDP, WinRM and SSH across the network to stop ransomware from propagating from breached machines while allowing the bare minimum to keep the network functional.
- **Ransomware File Share Restrictions -** Prevents access to SMB and FTP servers from most of the network to protect them from ransomware, as it can cause the most damage there due to the amount of data they hold.

## Infection Scope Assessment

While some ransomware is self-spreading[3], there are still many that are spread using active attacker presence and campaigns[4]. Beginning the recovery process without thoroughly disinfecting the network can lead to the ransomware operators sabotaging your network again or damaging your network even more.

### Increasing Infection Visibility Incrementally

With your initial lead or indicator of compromise, you can start looking for other indicators. Use Guardicore Centra maps and filters to find all assets with this indicator (E.g: All assets communicating to the C2, all assets communicating to a unique port, or all assets running a malicious process). Armed with this map, you can look for other similarities across infected machines or traces of propagation:

- Other C2 or download servers
- More spawned processes for the malware or other process names
- Connection logs of RPC that might indicate lateral movement

### Finding Patient Zero

Once you've maximised your infection visibility, look for the earliest event that occurred - does it look like the initial breach method? If the answer is no, look at the other processes on the machine - maybe you missed the dropper? Is there a document reading program running at the same time (E.g: Microsoft's Office or Adobe Acrobat Reader - Documents are common first stagers for spear phishing campaigns). Are there suspicious incoming connections? Maybe you missed a machine in the previous step and haven't maximized your visibility. Keep repeating those steps until you find the initial breach location. Then look at all the outgoing connections to make sure there's no other machine that could have slipped your notice.

Leaving even a single machine infected can allow an attacker to spread themselves inside the network once more, and with more ease as they already have all the necessary intelligence gathered.

### Guardicore CSA as Incident Response

Guardicore's Cyber Security Analyst (CSA) team can assist with breach containment endeavors and incident response. Feel free to contact them for help in any breach or ransomware event - Those are professionals familiar with Incident Response, Threat Hunting and Reverse Engineering and will surely enrich any breach investigation going on.

[3] WannaCry, NotPetya, Lockbit
[4] Ryuk, Maze, REvil

## Disinfection and Recovery

Once you have a list of all infected machines and all IoCs, you can start disinfecting machines. Use policy rules and labels to mark infected, recovering and clean machines and to stop communication between them. Keep recovering machines isolated and monitored, in case there's an installed persistency method that slipped your analysis. Once you're sure a recovering machine is clean, you can change its label accordingly and begin restoring it from backups, or move on to other machines.

We've included a policy template, called ***Ransomware Recovery Process Policies***, to help you to quickly deploy those guidelines, and easily keep track of your recovery process while keeping your network secure. The template isolates infected machines by blocking all communication from them, but allows clean machines to operate normally. Recovering machines that need to be monitored further, are allowed to operate normally but not to use lateral movement.