The top 40 ransomware techniques and how to mess with them

An active defense and deception guide

Table of Contents

Introduction

Most intros to ransomware white papers/ guides/reports are predictable. Plaster the first paragraph with 'cost of ransomware' statistics, give an honorable mention to recent variants, and briefly talk about the industries that have been most affected before moving to the useful bits.

We don't need to throw more 'doom and gloom' commentary at you to tell you what you already know – no one likes ransomware, it's bad for business, and organizations get hit by it every year.

As defenders, we need to get better at dealing with it.

Why We Wrote This Guide

You're already doing a ton to deal with security threats. But even as the world's most well-protected organizations will attest to, no security measure can be 100% full-proof. However, there are simple things you can do right now without deploying complex tooling or spending a ton of money that will put you in a better position to defend against ransomware.

This guide aims to help you do just that – do things that are in your control to defend against ransomware. The goal of this guide is to help you limit the spread of ransomware and reduce its impact.

Why Active Defense and Deception for Dealing With Ransomware

Most solutions to security problems take a siloed approach. Want to defend endpoints? Cover them with an EDR. More visibility? NTA. Malicious behavior? UEBA.

Ransomware is capable of interacting with all parts of your IT environment. Focussing your efforts on just one part of it will have diminishing returns. Dealing with something like ransomware demands a holistic approach. Your strategy needs to cover critical areas of the environment to be effective.

'Active Defense' helps you do that. The approach is use case-driven and balanced in its outcome. You can pick the use case (in this instance, ransomware) and focus on where you want to be most effective (see implementation advice).

How Does Active Defense Help With Ransomware?

- Creating a fake attack surface using Deception to disrupt adversary playbooks.
- Reducing the attack surface using highly effective controls to eliminate options from the adversary playbook.
- Finding nifty and highly effective ways to monitor the open attack surface, to trap adversaries when they execute unavoidable parts of their playbook.

Implementation Advice

We recommend that you focus your eforts on the following areas of your environment:

- DMZ
- Active Directory
- Critical Server Segments
- Privileged User Accounts
- Privileged Workstations

Once you've covered these, feel free to consider broader implementation based on effort and resource availability.

We are aware that some of the techniques in this guide require an investment of time and effort. Defense cannot and never will be zero-effort. That is why we have only covered strategies that have an asymmetric impact on your detection and protection efforts.

Who Is the Guide for?

- Defenders with an interest in beating ransomware with dirty tricks
- Senior SOC analysts
- SOC Managers
- Anyone concerned about ransomware

> You don't have to implement everything recommended in this guide. It's only prescriptive. **But doing even some of it can help you control and reduce the attack surface available to ransomware. That on its own is a huge win.**

Let's Go

We've tried to simplify this as much as possible. Below, you'll find a list of ransomware techniques and corresponding active defenses that will either detect the technique early on or limit its ability to spread. We've also provided implementation recommendations for each 'Active Defense' and mapped them to MITRE Shield techniques.

	RANSOMWARE TACTIC / TECHNIQUE	ACTIVE DEFENSE	WHY DO THIS?	HINTS, TIPS, TRICKS, AND RECOMMENDATIONS	MITRE SHIELD MAPPING
1	**INITIAL INFECTION** Infects publicly-facing assets with known vulnerabilities (like Wordpress/CMS, etc.)	Create decoy applications on the Internet that intercept ransomware targeting public-facing assets with known vulnerabilities.	Creates a fake attack surface and presents a seemingly vulnerable target to the ransomware operator to disrupt its operations.	Create decoys mimicking Joomla or Wordpress CMS' as we've seen attackers targeting these often.	Decoy Diversity > Application Diversity >
2	**INITIAL INFECTION** Password spraying on well known applications.	Create decoy applications with known default passwords. These will intercept ransomware that attempts password spraying.	Creates a fake attack surface and presents a seemingly vulnerable target to the ransomware operator to disrupt its operations.	Create decoys of applications like Apache Tomcat and PhpMyAdmin.	Decoy Diversity > Application Diversity >
3	**INITIAL INFECTION** Exploit recently disclosed vulnerabilities (e.g. the Microsoft Exchange vulnerability).	Attackers often target applications with recently disclosed vulnerabilities. Create decoys of these applications to draw out the ransomware operator.	Creates a fake attack surface and presents a seemingly vulnerable target to the ransomware operator to disrupt its operations.	Create decoys of applications like Microsoft Exchange and F5 that have been in the news for disclosed vulnerabilities.	Decoy Diversity > Application Diversity >
4	**INITIAL INFECTION** Brute-force publicly accessible RDP servers.	• Block in-bound access to RDP port 3389 from host/network firewall. • Restrict RDP from known IP addresses only (especially cloud servers).	Reduces the attack surface available to the ransomware operator by making RDP servers inaccessible. This directly helps limit the spread of ransomware.	Use Windows Firewall or the Cloud Console to block access to RDP.	Security Controls > Network Manipulation > Isolation >

	RANSOMWARE TACTIC / TECHNIQUE	ACTIVE DEFENSE	WHY DO THIS?	HINTS, TIPS, TRICKS, AND RECOMMENDATIONS	MITRE SHIELD MAPPING
5	**INITIAL INFECTION** Take advantage of applications that are run with administrator privileges.	Run DMZ applications with least privileges.	Run DMZ applications with least privileges.	Run applications with least privileges.	Admin Access >
6	**INITIAL INFECTION** Use of PowerShell	• Block PowerShell using GPO/App Control where its usage is not required. • Monitor PowerShell making outbound connections using Windows Firewall. • Script-block Logging.	• Stops commodity ransomware from executing. • Gives you visibility into Internet connections made by PowerShell in a critical segment. • Gives you visibility into PowerShell scripts that were run.	Use GPO functions to block PowerShell, enable auditing, and control firewall access.	Secuity Controls > Baseline > Standard Operating Procedure >
7	**INITIAL INFECTION** Connects to C2 servers from the infected DMZ segment.	Restrict outbound Internet access from DMZ to a whitelist.	While infection may be possible, C2 call back will fail from the segment and disrupt ransomware operations.	Use egress firewall and corporate proxy in combination to block Internet access.	Secuity Controls > Baseline > Standard Operating Procedure >
8	**INITIAL INFECTION** • Embeds itself in a macro. • Uses DDE to execute code.	• Strip macros via GPO. • Disable DDE via GPO. • Enable Protected View via GPO. Deploy the GPO strategically to privileged users and users who don't need the functionality.	Slows down ransomware operations. Strips adversaries of the ability to use common techniques to embed malicious code used for initial infections.	Use GPO templates to control MS Office capabilities. Use email security capabilities to achieve the same outcomes.	Email Manipulation > Standard Operating Procedure >

	RANSOMWARE TACTIC / TECHNIQUE	**ACTIVE DEFENSE**	**WHY DO THIS?**	**HINTS, TIPS, TRICKS, AND RECOMMENDATIONS**	**MITRE SHIELD MAPPING**
9	**PERSISTENCE** Installs persistence via Registry.	Audit registry run keys.	Gain visibility into persistence tactics used by ransomware.	Audit popular targets like Run Keys and Startup Keys for creation and modification.	Baseline > Hunting >
10	**PERSISTENCE** Installs persistence via ScheduledTasks.	Audit scheduled task creation.	Gain visibility into persistence tactics used by ransomware.	Keep an eye out for Windows Event ID 4698. It is generated when a scheduled task is created.	Baseline > Hunting >
11	**PERSISTENCE** Installs persistence via WMI.	Audit WMI event subscription creation.	Gain visibility into persistence tactics used by ransomware.	Use Sysmon to detect WMI event manipulation. Usually, by default, most systems have just two pre-configured WMI subscriptions.	Baseline > Hunting >
12	**DEFENSE EVASION** Kills security processes.	Create decoy security processes to intercept ransomware that's killing security processes.	Detect the ransomware when it kills a well-known security process.	Create decoy processes for common AVs as ransomware operations target these.	Decoy Process >
13	**DEFENSE EVASION** Stops Services.	• Monitor registry for security services being stopped. • Decoy Backup and Database Services. • Monitor backup and database services being stopped.	Alerts defenders to the presence of an adversary when they attempt to disable key services.	When services are stopped, the start value of the service registry key changes to 4. Use decoy services like Veeam, MSSQL, and Oracle as they are commonly targeted.	Decoy Process > Behavioral Analytics >

	RANSOMWARE TACTIC / TECHNIQUE	ACTIVE DEFENSE	WHY DO THIS?	HINTS, TIPS, TRICKS, AND RECOMMENDATIONS	MITRE SHIELD MAPPING
14	**DEFENSE EVASION** Installs a lightweight headless VM.	Audit headless starts for common VMs like VirtualBox, VMware, and Hyper-V to baseline on systems where they should not be installed	Allows the detection of techniques that bypass inspection by endpoint detection and response solutions (EDRs).	Write rules to match file hashes to executables that allow headless starts. Monitor process starts for command line arguments.	Baseline › Hunting ›
15	**PRIVILEGE ESCALATION** Local Administrator password brute-force or reuse.	• Use LAPS to secure local administrator accounts. • Disable local administrator account logons over the network. • Decoy local admin account credentials in unattend files.	Contain and disrupt the impact of Local administrator password reuse.	Insert passwords into unattend.xml into C:\Windows\Panther and monitor for access	Decoy Content › Security Controls › Standard Operating Procedure ›
16	**PRIVILEGE ESCALATION** Domain Administrator password brute-force (applies to other privileged accounts as well)	• Create decoy domain administrator account. • Lockdown domain admin accounts to be used on domain controller only. • Audit domain admin logon attempts from unauthorized locations.	Protect, detect and confuse ransomware operations when it targets privileged account.	• Create a decoy account and add it to privileged AD groups. • Use the logonworkstation attribute to control where Domain Admins can login. • Monitor logon events 4624, 4625, 4768, 4771, 4776.	Decoy Content › Standard Operating Procedure › Baseline › Hunting ›

	RANSOMWARE TACTIC / TECHNIQUE	ACTIVE DEFENSE	WHY DO THIS?	HINTS, TIPS, TRICKS, AND RECOMMENDATIONS	MITRE SHIELD MAPPING
17	**PRIVILEGE ESCALATION** Credential theft from browsers and software.	Plant decoy credential lures lures pointing towards decoy systems.	Misdirects the ransomware to target a fake attack surface thereby disrupting its operation and slowing its spread.	Add decoy credentials to Chrome, Edge, IE, Putty, and use decoy systems and applications as the target that the lures point to. Optionally, these credentials can be tied to decoy accounts from Active Directory.	Decoy Account › Decoy Credentials › Decoy System ›
18	**PRIVILEGE ESCALATION** Credential theft from memory.	• Plant decoy credentials in CredMan and memory. • Create protected Users Group for privileged accounts. • Lockdown permissions for privileged accounts • LSASS protections.	Reduces the attack surface for in-memory credential theft of privileged accounts. Detection via decoy credentials disrupts ransomware operations on use of decoy credentials.	Protected Users Group is a powerful option to prevent credential storage in memory but it has a few operational drawbacks that must be evaluated. Apply to highly privileged accounts.	Standard Operating Procedure › Admin Access › Decoy Credentials › Security Controls ›
19	**PRIVILEGE ESCALATION** Attempts to compromise accounts with Group Policy creation rights.	• Create decoy accounts with GPO rights. • Lockdown accounts with GPO rights to login to domain controller only. • Hunt for usage of GPO accounts from non-standard locations.	Disrupts the ransomware's hunt for GPO rights by detecting when the account is enumerated and used. Prevents GPO account credentials from leaking to non-domain controller systems.	Detect enumeration of decoy accounts with GPO rights by enabling auditing of various attributes of the account. Use the logonworkstation attribute to control where GPO Admins can login.	Standard Operating Procedure › Admin Access › Decoy Credentials › Security Controls › Hunting ›

	RANSOMWARE TACTIC / TECHNIQUE	ACTIVE DEFENSE	WHY DO THIS?	HINTS, TIPS, TRICKS, AND RECOMMENDATIONS	MITRE SHIELD MAPPING
20	**PRIVILEGE ESCALATION** Attempts to compromise the SCCM administrator accounts.	• Create decoy SCCM accounts. • Create decoy SCCM system with entry in Active Directory. • Restrict SCCM account usage to certain servers only. • Hunt for usage of SCCM accounts from non-standard locations.	Disrupt the ransomware's hunt for SCCM rights by detecting when the account is enumerated and used or when the SCCM servers are enumerated.		Standard Operating Procedure > Admin Access > Decoy Credentials > Security Controls > Hunting >
21	**PRIVILEGE ESCALATION** Active Directory attacks like Kerberoasting.	Create decoy kerberoastable accounts.	Disrupt password attacks that give easy access to privileged credentials.	Make any decoy account kerberoastable by setting the SPN attribute. Ensure password is at least 30 characters long to mitigate brute-force.	Decoy Account >
22	**TARGET SELECTION** Scans the local DMZ segment.	Add decoy systems in the DMZ.	If the initial infection is successful, doing this will detect the ransomware in its discovery phase.	Make sure that decoys carrying file shares are placed in the DMZ.	Decoy System >
23	**TARGET SELECTION** Selects target systems from Active Directory computers.	• Create decoy systems in the Active Directory and enable auditing to log enumeration attempts against them. • Baseline and investigate all accounts and systems that enumerate active directory.	A combination of decoys and baselining makes it easier to spot enumeration attempts against Active Directory and take quick action.	• Place decoy systems in different OUs. • Add hostnames that make the ransomware target lists like "srv" or "server". • Add attributes like operating system and version to help meet selection criteria.	Decoy System > Baseline >

RANSOMWARE TACTIC / TECHNIQUE	ACTIVE DEFENSE	WHY DO THIS?	HINTS, TIPS, TRICKS, AND RECOMMENDATIONS	MITRE SHIELD MAPPING
24 **TARGET SELECTION** Discovers mapped drives and shares on the infected host.	Plant decoy credentials. Create decoy systems advertising shares.	Misdirects the ransomware to scan decoy file shares if it is performing enumeration via the endpoint and scanning.	CredMan is a popular location to store information about mapped shares. Hidden drives can be created in registry	Decoy Credential › Decoy System ›
25 **TARGET SELECTION** Discovers shares from Active Directory.	Create decoy accounts in Active Directory with file share indicators in attributes.	Misdirects the ransomware towards decoy file shares if the enumeration tactic is via Active Directory.	Attributes like profilepath, homedirectory and scriptpath are parsed to discover files hares.	Decoy Account › Decoy Credential ›
26 **TARGET SELECTION** Discovers subnets from Active Directory Sites and Subnets.	Create decoy subnets with decoy systems.	Disrupts the ransomware operation by misdirects it towards decoy networks.	Add a description to the subnet to make it an interesting target, e.g. Critical Server Segment	Decoy System › Decoy Network ›
27 **LATERAL MOVEMENT** Scans network for lateral movement ports – Most commonly, 135, 445, 3389, and 5985/5986.	• Add decoy systems to the DMZ and key server segments. • Isolation to reduce inter-segment discovery towards DMZ and key server segments. • Enforce 2FA requirements to interact with business-critical servers. • Hunt for connections to these ports with the DMZ segment as the source.	• Prevents ransomware from moving laterally where business impact is most likely to occur. • Additionally, provides detection when the ransomware attempts to breach critical targets.	• Use decoy systems for detection and best effort isolation to reduce the attack surface available to ransomware. • Baselining of traffic on key lateral movement ports from the DMZ can quickly bubble up anomalies.	Decoy Account › Isolation › Network Manipulation › Hunting ›

	RANSOMWARE TACTIC / TECHNIQUE	ACTIVE DEFENSE	WHY DO THIS?	HINTS, TIPS, TRICKS, AND RECOMMENDATIONS	MITRE SHIELD MAPPING
28	**LATERAL MOVEMENT** Scans network for databases.	• Add decoy systems with databases in the DMZ and key server segments • Isolation to reduce inter-segment discovery towards DMZ and key server segments. • Baseline connections from the DMZ segment. • Hunt for connections towards common database servers.	• Prevents ransomware from moving laterally where business impact is most likely to occur. • Additionally, provides detection when the ransomware attempts to breach critical targets.	• Use decoy systems for detection and best effort isolation to reduce the attack surface available to ransomware. • Baselining of traffic on key lateral movement ports from the DMZ can quickly bubble up anomalies. • Hunt for connections with destination port 1433, 3306, and 1521.	Decoy System > Decoy Diversity > Isolation > Baseline > Hunting >
29	**LATERAL MOVEMENT** Distributes encryption payload over SMB, e.g. PsExec	• Best effort SMB block. • Add decoy systems to allow SMB interactions. • Disable admin$ share to prevent tools like PsExec from running.	• Best effort SMB blocking completely neuters any ransomware whose MO is to use SMB to spread. This severely dents the impact of ransomware. • Decoys allow detection.	Block SMB inbound between workstations to reduce the attack surface available to ransomware.	Decoy System > Isolation > Admin Access > Security Controls >
30	**LATERAL MOVEMENT** Distributes encryption payload via GPO.	Monitor creation of group policy, especially those that distribute scheduled tasks and registry keys.	Get an alert when a GPO is created for distribution of Scheduled Tasks and Registry keys.	Set GPO creation auditing. Optionally setup auditing on the Policies folder in C:\Windows\Sysvol\ and monitor for file creation for ScheduledTask.xml and Registry.xml	Baseline > System Activity Monitoring >

	RANSOMWARE TACTIC / TECHNIQUE	**ACTIVE DEFENSE**	**WHY DO THIS?**	**HINTS, TIPS, TRICKS, AND RECOMMENDATIONS**	**MITRE SHIELD MAPPING**
31	**LATERAL MOVEMENT** Distributes encryption payload via SCCM or other software deployment tools.	• Monitor creation of SCCM policies • Distribute SCCM policies on a set schedule. • Track usage of SCCM accounts.	Get alerted when an SCCM policy is created or pushed outside of normal hours.	Monitor SCCM account usage via Windows Event ID 4768 and 4624. Pay attention to the source of the login.	Basline › System Activity Monitoring › Hunting ›
32	**PRE-ENCRYPTION CHECKLIST** Terminates debuggers.	Create decoy process for debuggers.	Detect the ransomware operation when a decoy process is terminated.	Create a fake process for windbg.exe and procmon.exe	Decoy Process ›
33	**PRE-ENCRYPTION CHECKLIST** Checks mutexes to prevent reinfection.	Drop mutexes for recent ransomware.	Makes the host an unviable target for ransomware.	Useful if you are under imminent threat from a specific strain of ransomware.	Pocket Litter ›
34	**PRE-ENCRYPTION CHECKLIST** Checks if operating in a VM environment and avoids infection.	Decoy Registry keys with VM references. Decoy processes and services consistent with VM environments.	Makes the host an unviable target for ransomware.	Use process names like vmware-vmx.exe	Decoy Content › Pocket Litter › Decoy Process ›
35	**PRE-ENCRYPTION CHECKLIST** Kills database and MS Office processes to avoid file locks.	Decoy processes for MS Office products.	Detects the ransomware operation when it terminates process.	Use process names like winword.exe and EXCEL.exe	Decoy Process ›
36	**PRE-ENCRYPTION CHECKLIST** Exfiltrates important files as proof of access for ransom demands.	Decoy files to detect data exfiltration.	Detection of data exfiltration can be the last line of defense. Gives you an opportunity to reduce business impact.	Add file names like passwords.xls, assets.xls, SEC disclosure.docx, etc.	Decoy Content › Pocket Litter ›

RANSOMWARE TACTIC / TECHNIQUE	ACTIVE DEFENSE	WHY DO THIS?	HINTS, TIPS, TRICKS, AND RECOMMENDATIONS	MITRE SHIELD MAPPING
37 **PRE-ENCRYPTION CHECKLIST** • Deletes volume shadow copies. • Deletes Windows Checkpoints by deleting all backups using wbadmin. • Disables recovery mode in boot configuration using bcdedit.	Hunt for suspicious process creation and command line arguments.	Alerts defenders to impending infection of the host.	Hunt for process starts by vssadmin.exe, bcdedit.exe, and wbadmin.exe	Hunting › System Activity Montoring ›
38 **ENCRYPTION** Encrypts files with common and important extensions.	Decoy files that meet ransomware criteria.	Detection of data encryption as the last line of defense with an opportunity to reduce business impact.	Add extensions like .txt, .pdf, .pst, .bak, etc.	Decoy Content › Pocket Litter ›
39 **ENCRYPTION** Renames file extension.	Renames file extension.	Detection of data encryption as the last line of defense with an opportunity to reduce business impact.	Set auditing on a decoy file and create a rule to track when the log line indicates the decoy file name with an extension different from the one initially configured.	System Activity Monitoring ›
40 **ENCRYPTION** Follows symlinks, mapped drives, and shares.	Decoy symlinks, mapped drives, and shares	Misdirects ransomware towards the fake attack surface providing the opportunity to reduce business impact.	Add a symlink to the desktop.	Decoy Content › Pocket Litter ›

Closing Thoughts

Practice security with ransomware.

Ransomware is a fascinating subject. Everyone on the security team, from the CISO to the analyst, should attempt to understand how it works and what strategies and tactics can be employed to best limit its impact. And what to do if you get hit with it. Here's why:

1. Ransomware is industry-agnostic.
2. Ransomware is capable of interacting with all parts of the IT environment, from perimeter, to internal network, to endpoint, active directory, applications and cloud.
3. It is the one singular threat today which can completely disrupt operations and bring business to a grinding halt.

Ransomware will test every part of your security program – Protection, detection, response, incident preparedness, vulnerability management, compliance, governance, disaster recovery, security awareness, skill sets, expertise, and communication.

Active Defense against ransomware is a worthy goal. Choose it because ransomware impact will be felt by your board, shareholders, customers, contractors, and employees.

And ransomware tactics have so much overlap with other types of threats, that if you get a decent handle on this problem, you, by default, will end up addressing some of the most pressing fundamental problems in organizational security today.

More Resources

Threat Detection With Deception Technology

Threat Detection and Active Defense With Deception Technology

Download the Whitepaper >

Adopting the MITRE Shield Framework With Smokescreen

Adopting the MITRE Shield Framework With Zscaler Deception

Download the Blueprint >

Building an Active Defense Plan From a Pen Test Report

Building an Active Defense Plan From a Pen Test Report

Get the Handbook >

Defend Your Network, Endpoints, Cloud, and AD With Deception

Get a Demo >

About Zscaler

Zscaler accelerates digital transformation with its Zero Trust Exchange, a SASE-based platform that provides fast, secure connections between users, devices, and applications over any network. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

zscaler™

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com