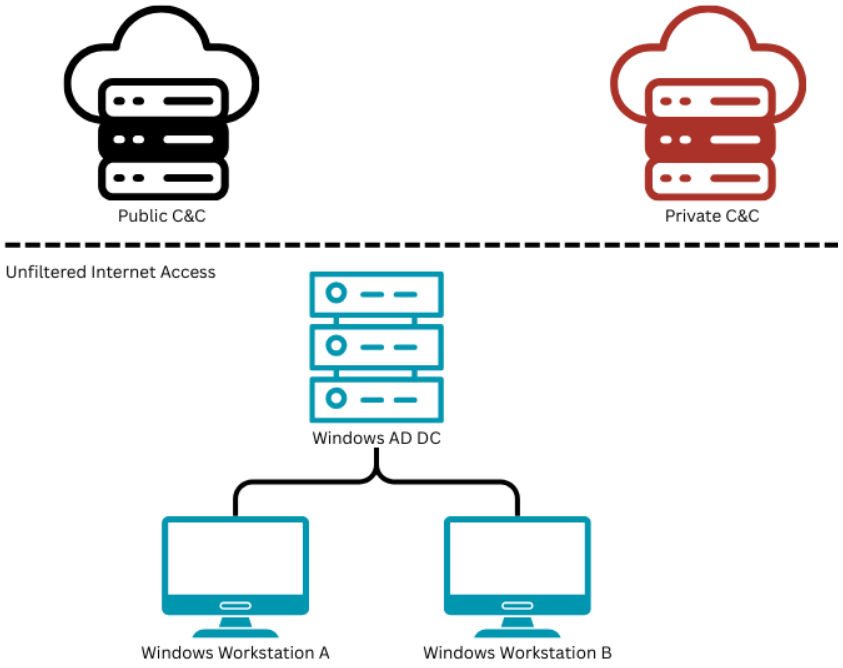
Ransomware Impact Methodology

Table of Contents

1. Goal

This evaluation aims to test security solutions responsible for protecting against post-intrusion ransomware attacks. This methodology is focused on endpoint solutions. Addendums can be used to tailor the rating system for other solutions.

2. Environment



The target environment consists of two protected Windows 11 workstations enrolled in a Windows Server based Domain Controller. Exact versions of operating systems are specified in the test schemes and each accompanying report.

Unfiltered internet access is provided for samples to connect to either a publicly available C&C or for the Artifact team to serve crafted samples as necessary.

The target Workstations contain commonly used files to in an office deployment as a target for ransomware encryption. The collection of these files is made available to participants and publicly upon report.

3. Attack Corpus

The attack test corpus contains prevalent ransomware families at the time of the test. An overview of the families and targeted operating systems are presented as part of the test plan. Publicly available samples and bespoke, crafted scenarios based on knowledge of existing ransomware trends and techniques can be part of the corpus.

The attack corpus is split into Public Threats and Crafted Attacks. Threats are collected and verified on a base clean Windows 11 Pro image without any security product installed. They are delivered to the target workstation using an external server that can fulfil real-world distribution channels.

Public Threats

Public Threats are sourced from known families. These are used to validate the effectiveness of the solution against known techniques.

Crafted Attacks

Crafted attacks can contain public samples with added evasion techniques to the base sample or new samples crafted by the Artifact Lab team.

Attacks are split into two sequences *intrusion* and *infiltration*.

Intrusion is defined by the initial delivery mechanisms employed by the attacker against the victim.

Infiltration is defined by the attacker executing and taking actions upon successful intrusion. I.e. deploying ransomware on the initial target.

Note: Propagation to other systems may naturally occur during the detonation of the samples with samples that include lateral movement or affect remote locations accessible by the target. The rating only focuses on the total each sample has done to the protected system irrespective of how it detonates.

4. Attack Rating

Solutions are expected to minimise the impact of ransomware deployment during the **infiltration** phase of the attack. Assuming a target workstation of up to 1000 files across local and remote locations.

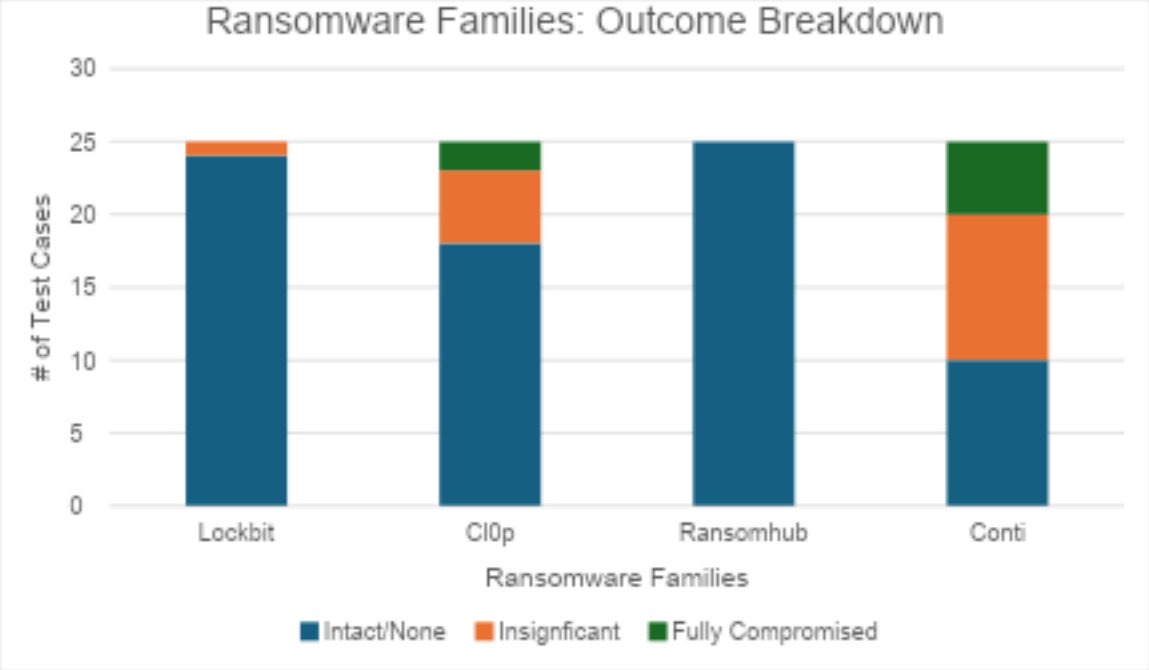
Severity	Insignificant	Low	Medium	High	Very High	Fully Compromised
# of Files	1 ≤ 4	5 ≤ 15	16 ≤ 50	51 ≤ 100	100 <	Complete
Rating	+10	+7	+4	+2	0	-10

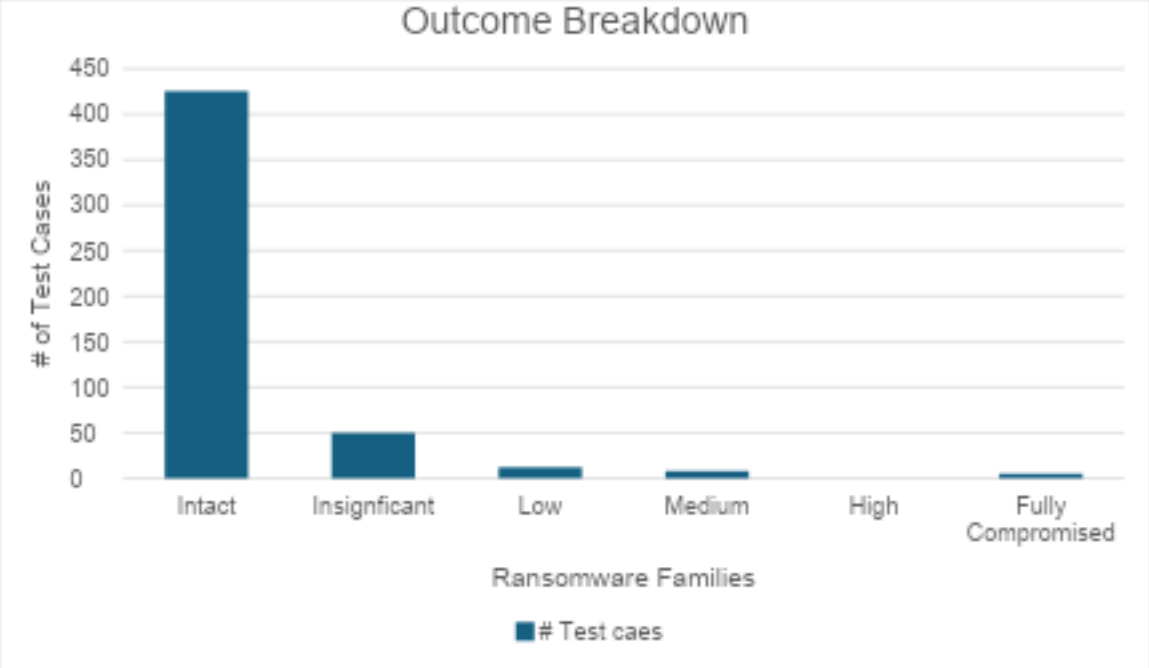
Remediation: Where possible, *s*uccessful remediation of files post compromise will shift the rating back to the Severity level achieved.

Definition of important files: non-system field, files added or created by users. In our test environment this is a mix of Office files & productivity related files.

A complete total accuracy rating is calculated using the Impact Severity Ratings.

Sample threat rating tables





5. Configuration disclosure

Product are deployed under recommended configuration, where possible under defaults. A full configuration and licencing disclosure is taken as part of any public report. If possible, this will be hosted under Artifact Security website or a trusted 3rd party repository. Linked references to the tested vendor resource are also acceptable.

6. Change Log

20/12/2025 – Ransomware Impact Methodology v1 – Identifier: RNSM2025v1