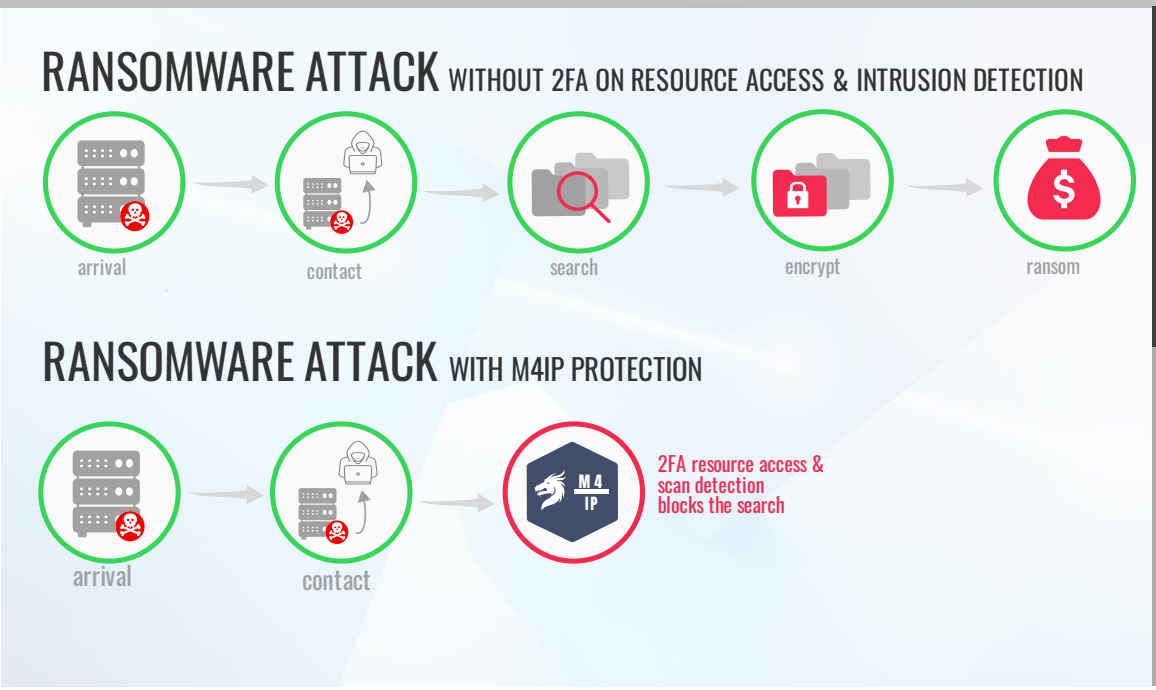
STOP RANSOMWARE

mamori.io



435%

Increase in number of attacks

200K USD

Avg payout

Ransomware

No matter what industry your business works in, ransomware needs to be at the top of your list of threats. It's a simple attack in which a hacker obtains access to your data, encrypts it, and charges money for the decryption software.

These attacks are succeeding in sectors that traditionally do not implement modern security solutions, making them soft targets. The services sector is particularly lucrative to hackers because services companies contain PII data and client system access credentials that can be sold to more sophisticated hacker organizations. This allows the hackers to profit on top of any ransom that is paid.

Asset Targets

Database Files	via OS access
Table data	via DB access
Documents	via shared drives

Attacks by Industry

Prof. Services	18.1%
Health Care	13.8%
Public Sector	12.0%
Software Services	8.0%
Education	9.0%
Other	39.1%

Business Impact

- Business operations disrupted until data recovered.
- Average payout ~USD 200k.
- 13% of services companies lost 50% of their clients. The remainder lost between 11-20%. (Source: NinjaRMM)
- Data sold to other hackers exposes your partners and clients to cyberattacks, and to further liability.

What you can do

To succeed, hackers need to scan you network for resources, and then **access** files, servers, and/or databases. They are stopped by implementing the following safeguards:

Minimum Requirements

- Implement an intrusion detection that blocks unauthorized scans.
- Multi-factor all access to file shares, servers and databases.
- Eliminate use of shared credential and lock down service account credentials by application and IP.
- Reliable and regular backups.

Additional Best Practice

- Replace permanent access to servers and databases with granted permissions that expire based on a policy.
- Restrict ability to update database data without an approved permission (prevents the encryption of database data).
- Provide users access to just required resources (never a whole network subnet).
- Replace error-prone manual access provisioning processes with automated processes.

How Mamori.io can help

Mamori.io offers an integrated security solution that allows you to easily implement, monitor, and audit the minimum and best practice safeguards listed above (excluding backups). The solution can be deployed on-premise or in the cloud.

Features include:

- Device registration
- Multi-factored access to all your internal resources.
- Segmentation of resource by role or individual workload
- Intrusion detection & threat isolation
- Access on-demand workflows
- Activity monitoring, alerts & session recording
- Privileged access management

Key Benefits

COMPREHENSIVE

Secure web applications, direct database, server access and any other IP resource.

COMPLIANT

Meets technical safeguards for all major security and data privacy regulations.