RANSOMWARE

What we learned.

NOT IF, WHEN.
Our Disaster Recovery Plan Goes Something Like This...

Lessons learned
Lessons learned

WHY LODI?

DISRUPTION
Surface Web

Deep Web

Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription-only information
Some organization-specific repositories

96% of content on the Web (estimated)

Dark Web

TOR
Political protest
Drug trafficking and other illegal activities
Special warning for system administrators, network administrators and third parties:

Do not try to solve this problem by yourselves!
Don't change file extensions! It can be dangerous for the encrypted information!

Your network has been penetrated.
All files on each network host have been encrypted with a strong algorithm.
Backups were encrypted too.
Shadow copies also removed, so F8 or any other method may damage encrypted data but not recover.

Decryption takes from ten minutes up to several hours.
It is performed automatically and doesn't require from you any actions except decoder launching.

DO NOT RESET OR SHUTDOWN SYSTEM — files may be damaged.
DO NOT DELETE reads files. Your system administrators are trying to solve problem by simple file extension changing. This actions seriously increase the time needed to recover your company’s PCs and network servers!

To confirm our honest intentions. Send 2 different random files and you will get them back decrypted.
It can be from different computers on your network to be sure that one key decrypts everything.
We will unlock 2 files for free.
To get info (decrypt your files) contact us at
DavaWittich92@protonmail.com
or
OvershinerAybrie@protonmail.com

You will receive btc address for payment in the reply letter

Ryuk

No system is safe
Protect your backups!

Stop the spread!
RISK MANAGEMENT

CALIFORNIA JOINT POWERS
RISK MANAGEMENT AUTHORITY

Cyber Forensic Experts
Let the Cyber Professionals Help You

Managed communications with the bad actors.

Identified where to find the .exe

Created a report that acknowledged what needed to be patched.

Collected the hard drives that were encrypted to try to establish evidence.
HOW THE HECK DID YOU FIGURE OUT MY PASSWORD

PASS THE HASH ATTACK SEQUENCE

Elevate Privilege
Scrape Hashes
Recon

Elevate Privilege
Scrape Hashes
Recon

Extract Active Directory

Compromise
Client Windows 7
Pass The Hash
Member Server W2K8 R2
Pass The Hash
W2K12 Domain Controller

Leave Backdoor (Optional)
Crack Hashes (Optional)
SECURITY AWARENESS TRAINING
IMPLEMENTING END-USER INFORMATION SECURITY AWARENESS TRAINING
What do you mean 'upgrade' the server? The old one works just fine.

URGENT: CRITICAL UPDATE AVAILABLE!

DETAILS: FIXES AN ISSUE THAT WAS CAUSING RANDOM LAPTOP ELECTRICAL FIRES.

(THIS UPDATE WILL REQUIRE RESTARTING YOUR COMPUTER.)

REMIND ME LATER