The 5 Types of Ransomware Attacks

You can practice your scared face, but you won't need it.

In 2020, cybercrime

cost over **$4B**

increased **69%** over 2019

The Rubrik/ePlus partnership is key to the detection and remediation of a ransomware attack. Rubrik uses ML to inspect backups and detect when data has been changed by ransomware. Uninfected copies of that data can then be identified and used to surgically restore from the attack. Otherwise, entire systems must be recovered, resulting in the loss of uninfected data.

*FBI Internet Crime Report 2020

Here's What You're Up Against

1 Encryption Ransomware

TARGETS

Personal files, folders and NAS shares (i.e. documents, archives, pictures, videos, etc).

WHAT HAPPENS

Affected files are deleted once encrypted. Users generally encounter a text file with instructions for payment in the same folder as the now-inaccessible files. The problem may only be discovered when someone attempts to open one of the encrypted files. Some types show a "lock screen."

RECOVERY

Requires identifying infected files/systems and restoring them to a safe point.

EXAMPLES

Maktub Locker, CryptoLocker, WannaCry, Cerber, CryptoWall

2 NAS Ransomware

TARGETS

NAS systems; also shadow volumes kept by the OS as backups.

WHAT HAPPENS

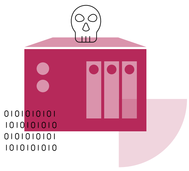
Scans the network for NAS and SMB devices, which often hold user files like home directories, host VMs for hypervisors, and are backup repositories. Encrypts and/or deletes the files so they're unusable by users, hypervisors, or backup protection software. When backup software and hypervisors are involved this can be particularly impactful.

RECOVERY

Compromised, if backup images are attacked.

EXAMPLES

Strains of SamSam, WannaCry, Ryuk



3 Lock Screen Ransomware

TARGETS

The computer's screen (no personal files are encrypted).

WHAT HAPPENS

Locks the computer's screen and demands payment via a full-screen image that blocks all other windows. Often easily removable in safe mode with anti-virus recovery tools.

RECOVERY

Involves booting into safe mode and removing the new lock screen.

EXAMPLES

WinLocker, MoneyPack

4 Hardware Locker

TARGETS

The Master Boot Record (MBR) on the computer's hard drive.

WHAT HAPPENS

Interrupts the normal boot process and instead displays a ransom demand on the screen at the boot cycle.

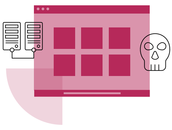
RECOVERY

Requires fixing the MBR or recovering data to a new system.

EXAMPLES

safe-data.ru, MBRLocker AKA DexLocker

5 Application/ Web Server Encryption



TARGETS

Files and web servers via application vulnerabilities.

WHAT HAPPENS

They replace index.php or index.html files on web servers with content that has the ransom instructions.

RECOVERY

Requires finding infected files and recovering them to their previous state.

EXAMPLES

CBT-Locker

Ransomware can take several kinds of attack vectors.
You only need one to fight back:

The Rubrik/ePlus solution

Get a Readiness Assessment

You've begun your datatude adjustment and realized that backup is just the beginning of what the Rubrik/ePlus solution can do for you. Now it's time to take the next step by having our engineers perform a thorough analysis of your current infrastructure, needs, and processes. We'll make strategic recommendations that show you a path to simpler data management, smart automation, and considerable cost savings.

Visit **datatude.eplus.com**