Redemption: Real-Time Protection Against Ransomware at End-Hosts

WRITTEN BY:

AMIN KHARRAZ

ENGIN KIRDA

PRESENTED BY:

NICHOLAS BURTON

What is Ransomware?

What is Ransomware?

- Ransomware is malicious software that encrypts user data, and demands a ransom is paid to unlock it.

Well that sucks, how do I get my data back?

Data Retrieval

- The easiest solution: keep a backup of your files.

Data Retrieval

- The easiest solution: keep a backup of your files.
- If and when you system is compromised by ransomware, you can use the backup to get back your files.

I don’t have a backup….

I don’t have a backup….

and I NEED those files!

This is really bad, can I prevent this?

Prevention

- CryptoDrop

Prevention

- CryptoDrop
- SheildFS

Prevention

- CryptoDrop
- SheildFS
- PayBreak

None of those work very well, what now?

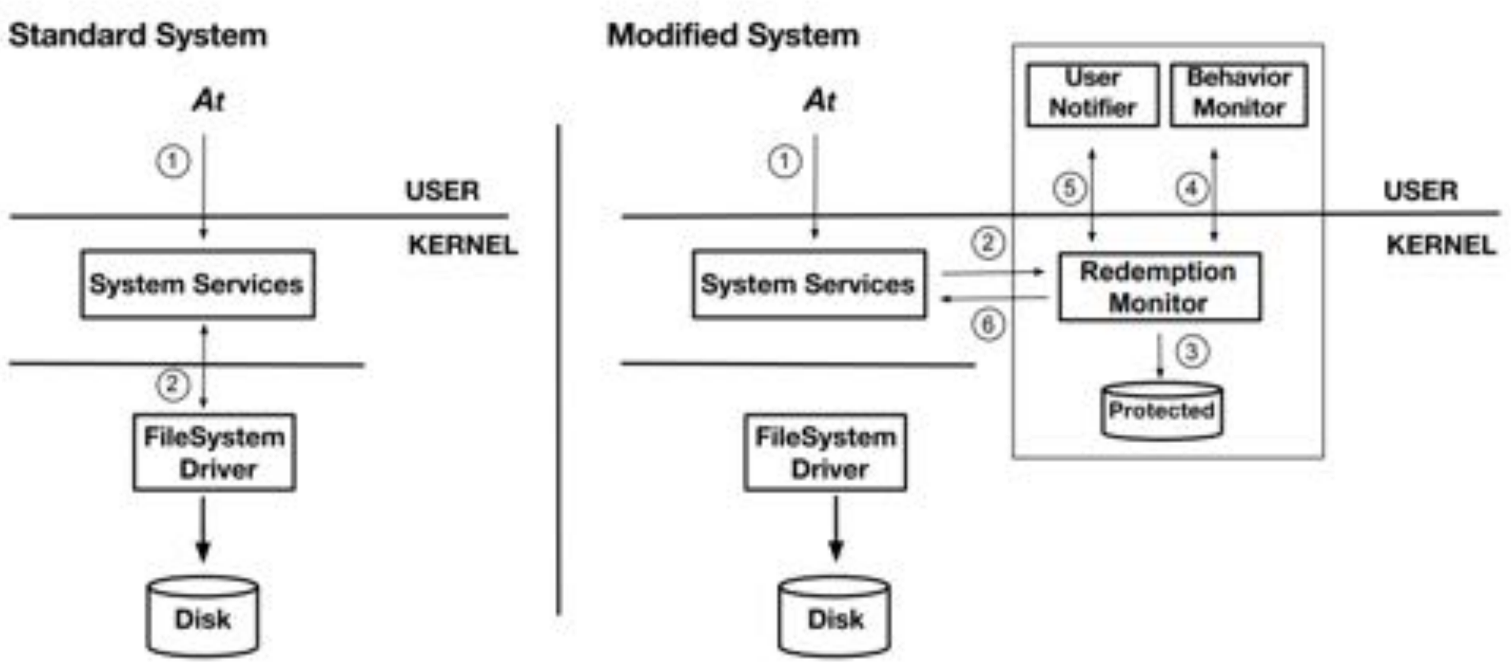
Redemption, Real-Time Protection

Redemption Design Overview

Two Components of Redemption

- A characterization of ransomware behavior based on a large class of current ransomware.
- High performance and integrity mechanism to restore attacked files.

Redemption Design Overview



How to determine Malice Score?

Malice Score

Two Components of Malice Score Calculation

- Content-based features
- Behavior-based features

Content-Based Features

- Entropy Ratio of Data Blocks (Shannon Entropy)

Content-Based Features

- Entropy Ratio of Data Blocks (Shannon Entropy)
- File Content Overwrite

Content-Based Features

- Entropy Ratio of Data Blocks (Shannon Entropy)
- File Content Overwrite
- Delete Operations

Behavior-based Features

- Directory Traversal

Behavior-based Features

- Directory Traversal
- Converting Files to a Specific Type

Behavior-based Features

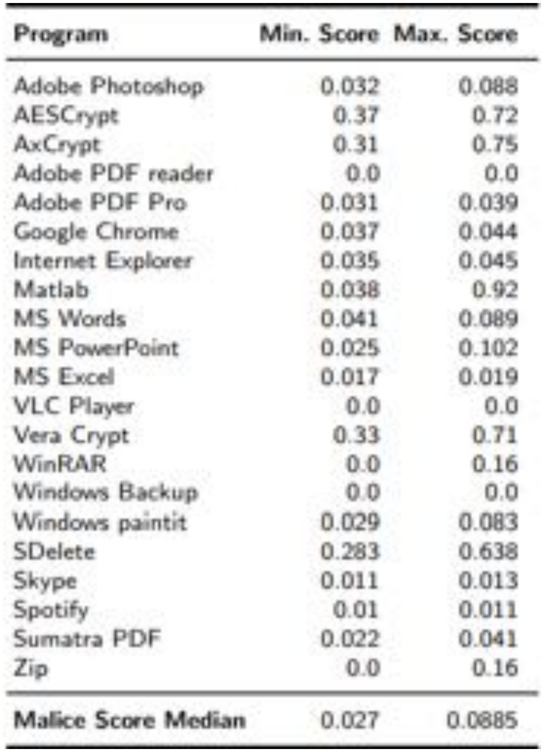
- Directory Traversal
- Converting Files to a Specific Type
- Access Frequency

Why two components of malice score calculation?

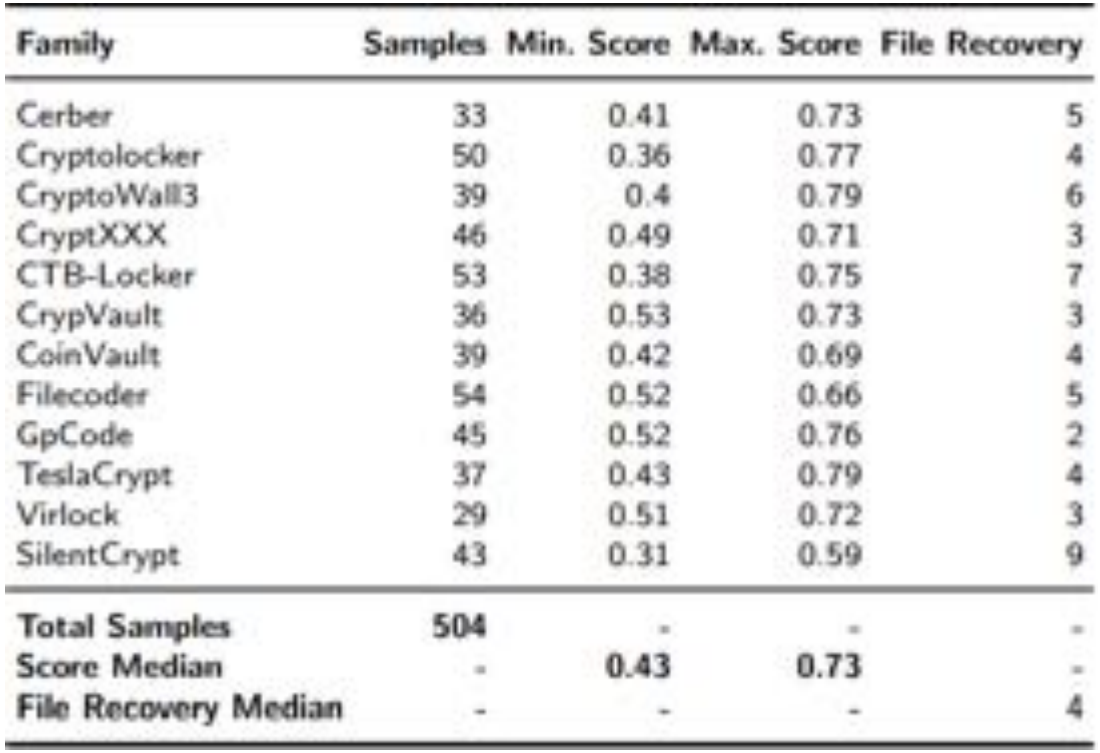
Why two components of malice score calculation?

$$MSC(r) = \frac{\sum_{i=1}^{k} w_i \times r_i}{\sum_{i=1}^{k} w_i}$$

Acceptable Malice Score

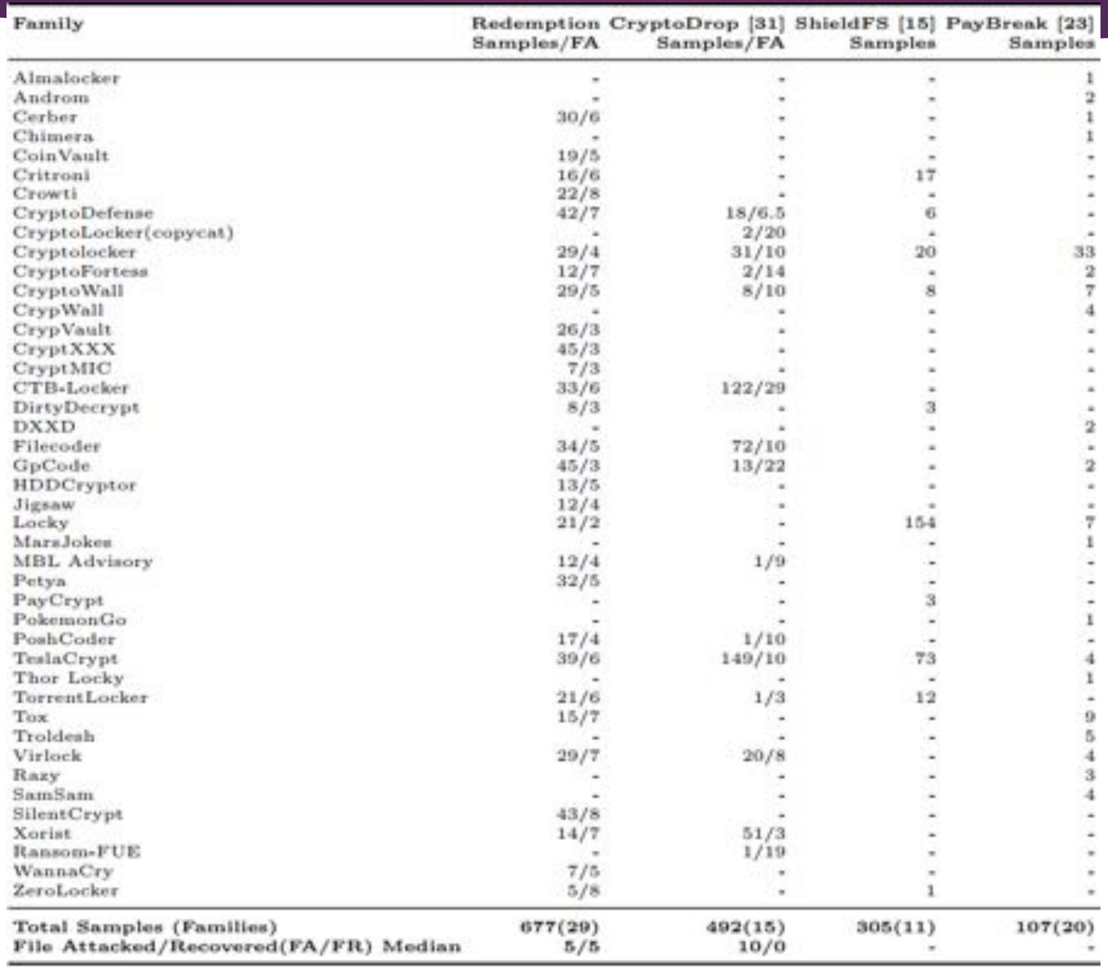


Program	Min. Score	Max. Score
Adobe Photoshop	0.032	0.088
AESCrypt	0.37	0.72
AxCrypt	0.31	0.75
Adobe PDF reader	0.0	0.0
Adobe PDF Pro	0.031	0.039
Google Chrome	0.037	0.044
Internet Explorer	0.035	0.045
Matlab	0.038	0.92
MS Words	0.041	0.089
MS PowerPoint	0.025	0.102
MS Excel	0.017	0.019
VLC Player	0.0	0.0
Vera Crypt	0.33	0.71
WinRAR	0.0	0.16
Windows Backup	0.0	0.0
Windows paintit	0.029	0.083
SDelete	0.283	0.638
Skype	0.011	0.013
Spotify	0.01	0.011
Sumatra PDF	0.022	0.041
Zip	0.0	0.16
Malice Score Median	0.027	0.0885



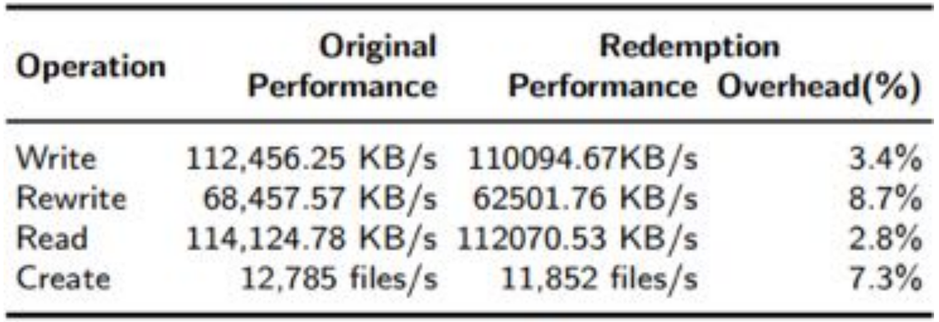
Family	Samples	Min. Score	Max. Score	File Recovery
Cerber	33	0.41	0.73	5
Cryptolocker	50	0.36	0.77	4
CryptoWall3	39	0.4	0.79	6
CryptXXX	46	0.49	0.71	3
CTB-Locker	53	0.38	0.75	7
CrypVault	36	0.53	0.73	3
CoinVault	39	0.42	0.69	4
Filecoder	54	0.52	0.66	5
GpCode	45	0.52	0.76	2
TeslaCrypt	37	0.43	0.79	4
Virlock	29	0.51	0.72	3
SilentCrypt	43	0.31	0.59	9
Total Samples	**504**	-	-	-
Score Median	-	**0.43**	**0.73**	-
File Recovery Median	-	-	-	4

Testing Against Other Anti-Ransomware Applications

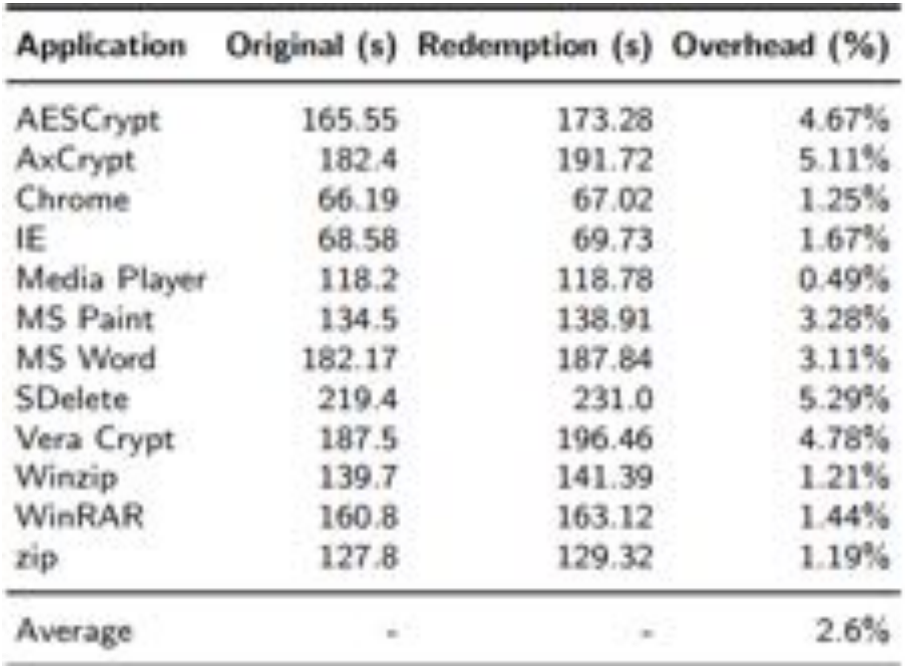


Family	Redemption Samples/FA	CryptoDrop [31] Samples/FA	ShieldFS [15] Samples	PayBreak [23] Samples
Almalocker	-	-	-	1
Androm	-	-	-	2
Cerber	30/6	-	-	1
Chimera	-	-	-	1
CoinVault	19/5	-	-	-
Critroni	16/6	-	17	-
Crowti	22/8	-	-	-
CryptoDefense	42/7	18/6.5	6	-
CryptoLocker(copycat)	-	2/20	-	-
Cryptolocker	29/4	31/10	20	33
CryptoFortess	12/7	2/14	-	2
CryptoWall	29/5	8/10	8	7
CrypWall	-	-	-	4
CrypVault	26/3	-	-	-
CryptXXX	45/3	-	-	-
CryptMIC	7/3	-	-	-
CTB-Locker	33/6	122/29	-	-
DirtyDecrypt	8/3	-	3	-
DXXD	-	-	-	2
Filecoder	34/5	72/10	-	-
GpCode	45/3	13/22	-	2
HDDCryptor	13/5	-	-	-
Jigsaw	12/4	-	-	-
Locky	21/2	-	154	7
MarsJokes	-	-	-	1
MBL Advisory	12/4	1/9	-	-
Petya	32/5	-	-	-
PayCrypt	-	-	3	-
PokemonGo	-	-	-	1
PoshCoder	17/4	1/10	-	-
TeslaCrypt	39/6	149/10	73	4
Thor Locky	-	-	-	1
TorrentLocker	21/6	1/3	12	-
Tox	15/7	-	-	9
Troldesh	-	-	-	5
Virlock	29/7	20/8	-	4
Razy	-	-	-	3
SamSam	-	-	-	4
SilentCrypt	43/8	-	-	-
Xorist	14/7	51/3	-	-
Ransom-FUE	-	1/19	-	-
WannaCry	7/5	-	-	-
ZeroLocker	5/8	-	1	-
Total Samples (Families)	677(29)	492(15)	305(11)	107(20)
File Attacked/Recovered(FA/FR) Median	5/5	10/0	-	-

Overhead



Operation	Original Performance	Redemption Performance	Overhead(%)
Write	112,456.25 KB/s	110094.67KB/s	3.4%
Rewrite	68,457.57 KB/s	62501.76 KB/s	8.7%
Read	114,124.78 KB/s	112070.53 KB/s	2.8%
Create	12,785 files/s	11,852 files/s	7.3%



Application	Original (s)	Redemption (s)	Overhead (%)
AESCrypt	165.55	173.28	4.67%
AxCrypt	182.4	191.72	5.11%
Chrome	66.19	67.02	1.25%
IE	68.58	69.73	1.67%
Media Player	118.2	118.78	0.49%
MS Paint	134.5	138.91	3.28%
MS Word	182.17	187.84	3.11%
SDelete	219.4	231.0	5.29%
Vera Crypt	187.5	196.46	4.78%
Winzip	139.7	141.39	1.21%
WinRAR	160.8	163.12	1.44%
zip	127.8	129.32	1.19%
Average	-	-	2.6%

Getting around Redemption

Social Engineering

- Aggravating a user to the point were they turn off Redemption.

Attacking the Malice Score Calculation

- Selective content Overwrite
- Low entropy payload
- Periodic file destruction

Questions?