PayBreak: Defense Against Cryptographic Ransomware

Eugene Kolodenker‡*, Wil Koch*, Gianluca Stringhini†, and Manuel Egele*

⋆Boston University, ‡MITRE, †University College London

INTRODUCTION

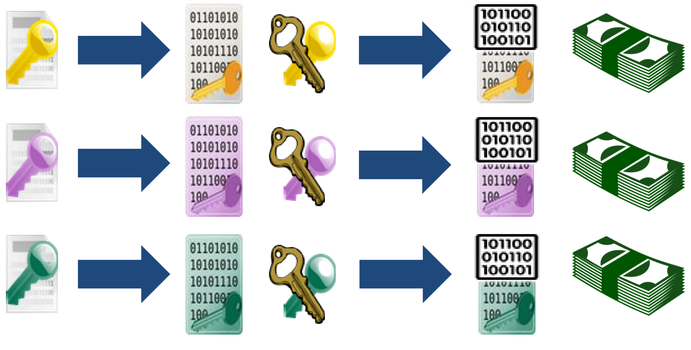
- Cryptographic ransomware is malware that **prevents the victim user access** to some resource by encrypting it, and **extorts a ransom** payment to perform decryption.

CRYPTO RANSOMWARE

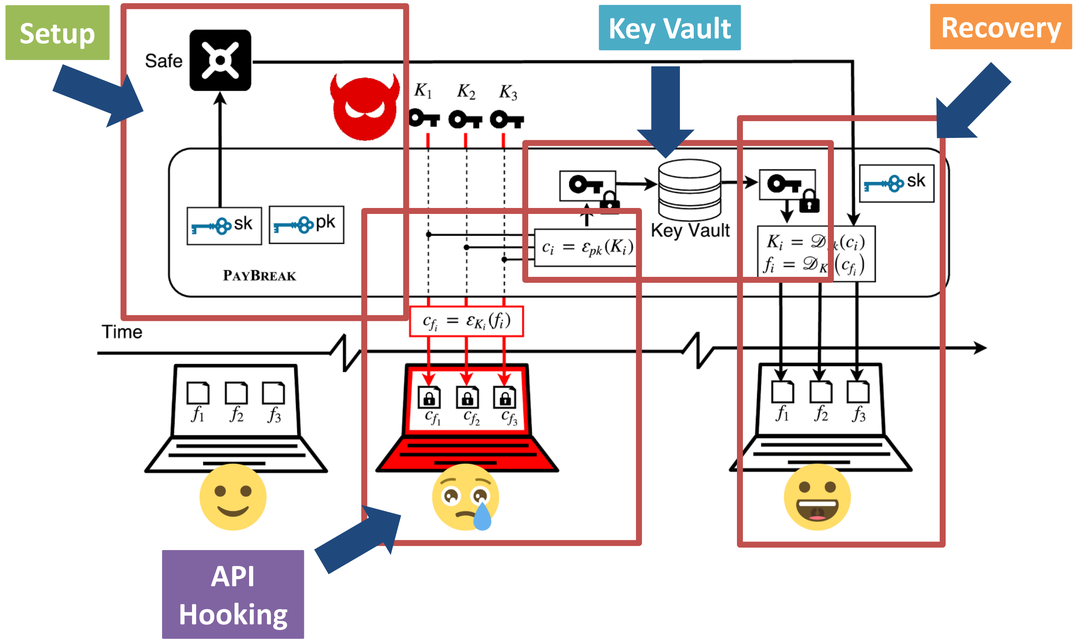
Malware start - Create private-public key pair. Transfer public key to victim to be used later

Victim forced to generate session key per file...

Encrypt each file	Encrypt each session	Pay



OVERVIEW



IMPLEMENTATION

Setup

- Set up systems with a public private-key pair
- Public key is for key vault input and the private key is used during recovery

API Hooking

- Augmented cryptographic library functions with extra code to export out keys
- Hooked dynamically and statically linked functions

Key Vault

- Store exported keys from the API hooking step into a secure container
- Secure with setup key pair and assure integrity

Recovery

- Decrypt the key vault using previously set up private key
- Attempt decryption for each file, at different file offsets, with each key in the key vault

EFFECTIVENESS

- Evaluated against the **largest set of ransomware families at date (20).**
- **Successful file recovery from 9** previously unrecoverable families.

Families	# Samples	Previously defeated	Defeated by	Defeated	Library	Algorithm
Almalocker	1	✓	✓	✓	CryptoAPI	RSA+AES-128-CBC
Cerber	14	✓	✓	✓	CryptoAPI	RSA+RC4-256
Chimera	1	✗	✓	✓	CryptoAPI	RSA+AES-256-ECB
CryptoFortress	2	✗	✓	✓	CryptoAPI	RSA+AES-256-ECB
CryptoLocker	33	✗	✓	✓	CryptoAPI	RSA+AES-256-CBC
CryptoWall	7	✗	✓	✓	CryptoAPI	RSA+AES-256-CBC
CrypWall	4	✗	✓	✓	CryptoAPI	RSA+AES-256-CBC
GPcode	2	✓	✓	✓	CryptoAPI	RSA+AES-256-ECB
Locky	7	✗	✓	✓	CryptoAPI	RSA+AES-128-CTR
SamSam	4	✗	✓	✓	CryptoAPI	RSA+AES-128-CBC
Thor Locky	1	✗	✓	✓	CryptoAPI	RSA+AES-128-CTR
Tox	9	✗	✓	✓	Crypto++	RSA+3DES-128-CBC
DXXD	2	✓	✗	✓	Unknown	XOR with Constant Key
MarsJokes	1	✓	✗	✓	Unknown	ECC+AES-256-ECB
PokemonGo	1	✓	✗	✓	.NET Crypto	AES with Constant Key
Troldesh	5	✓	✗	✓	Unknown	RSA+AES-256-CBC
VirLock	4	✓	✗	✓	Unknown	XOR with Constant Key
Androm	2	✗	✗	✗	Unknown	RSA+AES-256-CBC
Razy	3	✗	✗	✗	.NET Crypto	AES-128
TeslaCrypt	4	✗	✗	✗	Unknown	ECC+AES-256-CBC
Total	20	107	8	12	17	

GENERAL

- Compiled **12 encryption programs** using different crypto libraries, and different compilers at different optimization levels – required **2 signatures** to detect all variations.

PERFORMANCE IMPACTS

- Macro benchmark showed a **a 4.1ms overhead increase** in loading HTTPS webpages, and neglible overhead in 21 common software applications.

We would like to thank the anonymous reviewers for their insightful comments and our shepherd Guofei Gu for helping us improve the quality of the original manuscript. This paper was supported by an EPRSC-funder Future Leaders in Engineering and Physical Sciences Award, by the EPSRC under grant EP/N008448/1, and by the Office of Naval Research under grant N00014-15-1-2948. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the sponsor.

REFERENCES

[1] Cryptowall, teslacrypt and locky: A statistical perspective. http://blog.fortinet.com/post/cryptowall-teslacrypt-and-locky-a-statistical-perspective.
[2] Cybercriminals rake in $325m from cryptowall ransomware: report. http://www.washingtontimes.com/news/2015/nov/2/cybercriminals-rake-in-325m-cryptowall-ransomware/.
[3] Cryptolock (and drop it): Stopping ransomware attacks on user data. In IEEE 36th International Conference on Distributed Computing Systems, 2016.
[4] A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero, and F. Maggi. Shieldfs: a self-healing, ransomware-aware filesystem. In Annual Computer Security Applications Conference (ACSAC), 2016.
[5] M. Egele, M. Woo, P. Chapman, and D. Brumley. Blanket execution: Dynamic similarity testing for program binaries and components. In 23rd USENIX Security Symposium (USENIX Security 14), 2014.
[6] A. Gazet. Comparative analysis of various ransomware virii. Computer virology.
[7] A. Kharraz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda. Unveil: A large-scale, automated approach to detecting ransomware. In 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, Aug. 2016. USENIX Association.
[8] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), volume 9148 of Lecture Notes in Computer Science, Milan, Italy, July 2015. Springer International Publishing.
[9] K. Savage, P. Coogan, and H. Lau. The evolution of ransomware. http://www.symantec.com/content/en/us/enterprise/media/security response/whitepapers/the-evolution-of-ransomware.pdf.
[10] A. Young and M. Yung. Cryptovirology: Extortion-based security threats and countermeasures. In IEEE Symposium on Security and Privacy, Oakland, CA, May 1996.