Evading the rise of ransomware

Ransomware, malicious software that takes users' files "hostage" and demands payment from users to get back their files, has become a popular income stream for cybercriminals. While not all ransomware attacks are effective money earners, they often cause immense disruption for key services such as the healthcare industry. In the case of ransomware, prevention is often better than cure, and ***Professor Elisa Bertino*** *at Purdue University is designing tools to do exactly that – prevent the ransomware infection from ever taking hold with the possibility of stopping the millions of pounds of damage these attacks can cause.*

Ransomware dominated the daily news in May 2017, with the arrival of WannaCry. An unwelcome arrival on personal and company computers alike, the software took files hostage and demanded payment for users to be able to get their files back. WannaCry is probably one of the most famous examples of ransomware, malicious software that makes the victim's files inaccessible through encryption. Encryption 'locks' the data, making it unreadable to anyone without a very specific 'key'.

What made WannaCry such an exceptional attack was the sheer number of infected computers (thought to be around 200,000) and also the nature of some of the organisations affected. Alarmingly, one high-profile victim was the UK's National Health Service hospital computer systems. This affected not just the computers relied upon for administrative tasks, but those responsible for the analysis of test results and the operation of equipment like MRI scanners.

While the prevalence of ransomware in the media may seem like a recent phenomenon, the first ransomware attack occurred in 1989, also targeting the healthcare industry. However, this attack was largely a failure due to a design flaw: rather than encrypting files, it simply renamed them, making it easily reversible. Now though, attacks have become more technologically sophisticated and the availability of anonymous currencies, like Bitcoin, has made it harder than ever to trace the source of such attacks.

Researchers like Professor Elisa Bertino and her group at Purdue University are now fighting back. Breaking the ransomware encryption to recover files is often nearly impossible but Professor Bertino has another clever trick. Rather than trying to break the encryption on affected files, she focuses on prevention approaches that stop the initial encryption process, rendering the ransomware essentially useless. Her research group have already demonstrated this approach to be highly successful in stopping ransomware infections and these tools may be the answer to avoiding a repeat of the WannaCry events.

KEEPING SECRETS

The encryption process is at the heart of how malicious software or 'malware', like ransomware, operates. Encryption is a way of hiding information so that anyone who wants to read the real information must possess a special kind of key.

Reversing the encryption processes on a file, or 'decrypting' it, is not always a trivial or easy task. Encryption

www.researchoutreach.org

Reversing the encryption processes on a file, or 'decrypting' it, is not always a trivial or easy task

comes in many flavours and strengths. Some keys are kept entirely secret, so only the 'sender' and 'receiver' of the information have a copy. Others, counterintuitively, are publicly available and rely on the generation of a paired private, or secret, key for encryption. The generation process relies on an algorithm that can be used to generate more simple or complex keys depending on the security requirement.

Breaking encryption could be done by interception of the keys or by trying to guess the correct key. A brute force approach, where a computer tries to guess all the possible combinations that could comprise the key, means that a correct guess on a reasonable timescale is highly implausible. Where things get even harder is that some malware can require a unique decryption key for each infected computer.

This is why Professor Bertino's approach is so successful. Her tool essentially lies in wait for the signs of a malicious attack. This could be the sudden encryption of a large number of files, resulting in a change to the computer's filesystem. In conjunction with this, it looks for any anomalies in the processes that read and write to the filesystem, that are the signals for the encryption process to occur. This early warning detection system allows the tool to spot an attack very early and halt the encryption.

PREVENTION TACTICS

Professor Bertino is not the first to attempt the search for warning signs to stop ransomware. However, approaches that either just look for file encryption events or anomalous process requests tend to flag a large number of false positives and are generally ineffective in halting real attacks. They can be fooled by the ransomware encrypting files more slowly or trigger when the user is trying to encrypt their own files.

The joint approach of Professor Bertino has proved highly effective for 15 different types of ransomware attack. When the early warning system triggers in the event of an attack, it can stop further encryption but, if some files are already encrypted before the process is blocked, the tool can record the parameters used for the process and, depending on the specific ransomware, recover even the decryption keys. This makes it incredibly straightforward to undo any damage caused by the malware and restore the files to operation.

THE FUTURE FIGHT

Professor Bertino and two of her PhD students in the Computer Science Department at Purdue University, Anand Mudgerikar and Shagufta Mehnaz, are working to further develop this approach. One strategy is to deploy decoy files, that would be of no interest to the user but equally likely to be targeted by the ransomware, as another part of the early warning detection system. Attempts to encrypt those files would be a strong indication of a ransomware attack as users would not usually encrypt such files. She and her students are also focusing on ransomware attacks aimed at different targets, such as IoT (Internet of Things) devices.

Given the increasing volume of sensitive data stored on systems and networks that are connected to the internet, it is likely that ransomware will continue to seem a lucrative tactic for cybercriminals. However, with tools like Professor Bertino's, malware will need to become even more sophisticated to be effective.

Behind the Bench

Professor Elisa Bertino

E: bertino@cs.purdue.edu **T:** +1 765 496 2399 **W:** www.cs.purdue.edu/people/bertino

Cyber2SLab
Purdue University
Department of Computer Science
305 N. University Street
West Lafayette, IN 47907
USA

Collaborators

- Shagufta Mehnaz (CS Dept. Purdue University)
- Anand Mudgerikar (CS Dept. Purdue University)

Bio

Elisa Bertino is the Samuel Conte Professor of Computer Science at Purdue University. She serves as Director of the Cyber Space Security Lab (Cyber2Slab). In her role as Director of the Cyber2Slab she leads multi-disciplinary research in IoT security, data security and privacy, security for mobile systems and projects in the area of cyberinfrastructure for scientific research.

Research Objectives

Professor Bertino's work spans many areas in the fields of information security and database systems. In particular, she is currently working on an approach to combat ransomware attacks.

Funding
NSF

Q&A

Do you think having 'anti-ransomware' software will become as common as an antivirus?

Today there is awareness that data security is a key requirement. Therefore tools for in-depth protection of data are being developed and deployed by industry in many different application domains. A notable example of such tools is represented by data leakage protection tools aimed at preventing data from being stolen by skilful adversaries. Blocking and recovering ransomware attacks is today another relevant frontier for data cybersecurity. Good practices involve frequent backup of files – so that files can be recovered in the event of a ransomware attack – and anomaly detection tools, like the ones we are developing. At present, state-of-the-art, anti-ransomware tools are still complex and are still in an early research stage. However, once these tools are engineered for wide-scale deployment, they will be used by organisations with important data assets.

Are organisations like hospitals particularly vulnerable?

Organisations where timely access to data is critical are certainly vulnerable. Also the vulnerability of organisations depends on their maturity status with respect to the adoption of security practices and tools, and the security training of their staff. In this respect, hospitals are a perfect target for ransomware as critical care for patients relies on timely access to up-to-date information from patient records. Without real-time access to drug histories, surgery directives and other information, patient care can get delayed or halted, with serious consequences. In addition, medical information systems and networks are today very complex – thus making difficult their comprehensive protection, and hospitals often to do not have IT security staff. Therefore, it is not a surprise that many hospitals have been targeted by ransomware and have preferred to pay the ransom rather than endanger patients' health.

What is the most technically challenging aspect of creating your prevention tool?

The most challenging aspect has been to identify the features that allow our tool to distinguish between encryption performed by a user – and thus legitimate – from encryption performed by ransomware, e.g. malicious encryption. To understand such differences, we performed a user survey to better assess whether users encrypt their files, and which files they encrypt.

How do you think 'better user behaviour' can be encouraged to prevent some of the issues with malware?

Better user behaviour is always critical for enhancing security. As with all malware, it is important that users be aware of suspicious messages requiring for example the user to click on certain websites or to download and open an e-mail message attachment. Also installing an antivirus and backing up files are good practices that may drastically reduce the number of successful ransomware attacks.

Professor Bertino's approach is highly successful in stopping ransomware infections