WEBINAR SUMMARY

July 15, 2021

Thwarting Extortion: New and Old Research Directions in Ransomware Detection and Prevention

Dr. Katie Paxton-Fear, Application Security Engineer, Bugcrowd
Matt Wixey, R&D Lead, Cyber Security Practice, PwC

KEY TAKEAWAYS

- Reviewing the ransomware landscape starts with understanding current approaches to ransomware detection and prevention.
- A work in progress: Five new approaches that may help thwart extortion.
- Future visions of ransomware: possible ways attacks may evolve.
- Lessons learned from a real-world ransomware attack.

in partnership with

bugcrowd

OVERVIEW

Ransomware detection and prevention is a hot topic, as ransomware is constantly in the headlines these days and as organizations of all sizes in all industries are susceptible to attack. While keeping systems updated and fostering a security culture can help protect businesses, technical detection and prevention solutions are also necessary to further fortify the defenses.

Not only are researchers exploring existing methods to better understand how and when various methods work best to protect the business, but they are looking into new methods that can improve defenses and thwart extortion.

CONTEXT

Matt Wixey shared insights from his research into existing and new approaches to ransomware prevention and detection, as well as a vision of where ransomware attacks could be headed. Dr. Katie Paxton-Fear discussed lessons learned from the real-world ransomware attack she experienced.

KEY TAKEAWAYS

Reviewing the ransomware landscape starts with understanding current approaches to ransomware detection and prevention.

Matt Wixey shared an overview of current encryption-based ransomware detection and prevention approaches for Microsoft Windows systems. He found a reliance on sandboxing and he determined that two areas—honeyfiles and deception—were under-explored.

Overview of current approaches to ransomware detection and prevention on Windows	
Static analysis	Uses signature matching and code analysis to infer traits and predict what the ransomware is going to do. This approach is rapid and effective when it works, but has some challenges that include: – Is easy for attackers to bypass deliberately. – Can't always keep up with the rapid deployment of new iterations of malware and ransomware. – Does not work on targeted deployments aimed at a particular organization.
Dynamic analysis: filesystem	Ransomware has to enumerate the filesystem and encrypt files. This approach detects an attack by: – Looking for changes to files/extensions. – Comparing files to known good hash values. – Checking the frequency of read/write operations; ransomware typically overwrites a large number of files in a short period of time. – Looking at the use of vssadmin to make shadow copies; this is done using an open-source tool called Raccine. The filesystem approach can be bypassed by threat actors by slowing down or randomizing the speed of their operations and what they are doing with the file system. The solution also does not scale well, especially for hash value comparisons.
Dynamic analysis: application programming Interface (API) calls	Used in conjunction with machine learning (ML) or statistical analysis, this approach forms an impression based on the sequence of API calls. This approach is difficult for threat actors to circumvent but is also more technically challenging to implement and can be resource intensive.

Overview of current approaches to ransomware detection and prevention on Windows (continued)	
Dynamic analysis: cryptography	While this approach is typically used for post-infection behavior, PayBreak can be used for detection and prevention. The solution monitors the system continuously for the use of symmetric keys and copies any that are found to a vault. If a ransomware incident is detected, the organization can use the captured keys to decrypt the data. This solution may not be used today, but if it becomes widely used, threat actors are likely to circumvent it and even target PayBreak.
Dynamic analysis: honeyfiles	Bait and decoy files are put in the system in a place where users are unlikely to interact with them. The files are constantly monitored, and if they are accessed, it means an attack is occurring, and the user is alerted. They are a lightweight, first-line of defense.
Dynamic analysis: power/central processing unit (CPU)	While more applicable for detecting crypto-miners, looking for distinctive spikes in power/CPU resources may have some application to ransomware. This is an underexplored area and, because it uses signature matching, has the same challenges as static analysis.
Dynamic analysis: traffic	Monitors network traffic for relevant activity, and attempts to fingerprint ransomware traffic, whether across multiple families of ransomware or specific fingerprints for variants. This approach requires a sandbox environment, so it is often used post-infection.
Dynamic analysis: ransom notes	Uses image analysis, optical character recognition (OCR), and computational linguistics to identify ransom notes once they are displayed. This approach requires a sandbox environment, so it is often used post-infection and post-encryption.

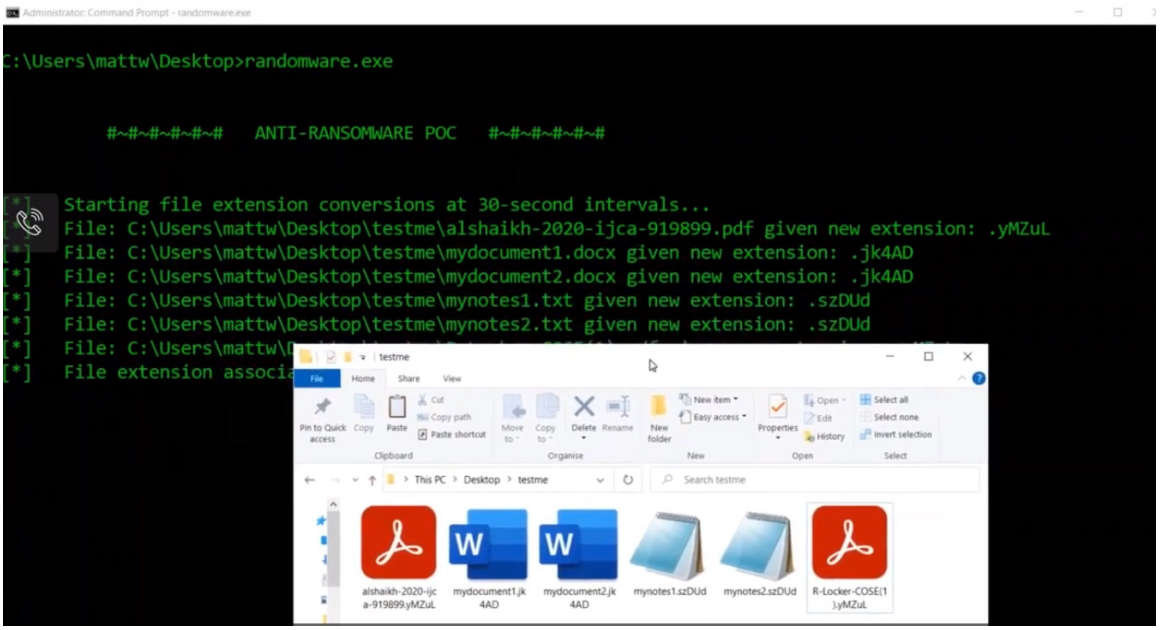
> Ransomware is a significant threat; there's barely a day when it's not in the headlines.
>
> *Matt Wixey, PwC*

A work in progress: Five new approaches that may help thwart extortion.

Wixey shared some of the new approaches he is currently researching, both those that are theoretical at this time and those that have working proofs of concept.

1. **Reconnaissance analysis** is a theoretical (not yet tested) approach that uses case linkage, a statistical technique used by criminal investigators to match separate crimes committed by the same offender based on similarities and offending behaviors. By applying the same principal to the hostile reconnaissance activities that occur weeks or months before a ransomware or malware attack, it may be possible to detect these attacks before they begin.
2. **API call analysis** is a theoretical (not yet tested) approach that also adopts case linkage analysis, this time looking at the API calls the ransomware makes. New processes are monitored, and API calls are recorded and analyzed to determine whether the process is malicious or not. This approach is potentially technically challenging to implement and resource intensive.
3. **Randomware** is a working proof of concept that randomizes file extensions at specific intervals, making it more difficult for ransomware that targets specific extensions to gain a foothold in the system. The software using the files is made aware of the new extension (e.g., a Microsoft Word .doc file that is changed to a .jk4AD file, as in the example below, could still be opened by the program). This approach is only applicable to ransomware that seeks out file extensions to change.

Figure 1: Randomware changes file extensions at specific intervals so ransomware can't target those file types



4. **Honeyfiles and countermeasures** is a working proof of concept where the honeyfiles are placed in a directory that is constantly monitored. When the monitor detects that the files are accessed, usually above a certain number of times, one or more of several countermeasures is launched. Scalability and a good placement of honeyfiles can be concerns with this method.

   Countermeasures in this approach include:

   - *Shut down:* The system is shut down to prevent further access.
   - *Quarantine:* Network adapters are shut down to prevent the system from interacting on the network.
   - *Sinkhole:* The system recursively creates new folders and junk files, which the ransomware will get stuck on attempting to decrypt.
   - *Kill:* Stopping the process ID of the process to end it.
   - *Alert:* Users are alerted to the ransomware via an email or other alert process.

5. **Deception** is a theoretical (not yet tested) approach that makes a real environment look like a sandbox environment. Malware and ransomware often check for sandbox environments, avoiding those systems because they may alert an organization to the attacker's presence more quickly.

> This is a continual arms race between attacker and defender. If the defenders can come up with innovative ways of trying to prevent ransomware, they better off we'll be.
>
> *Matt Wixey, PwC*

Future visions of ransomware: possible ways attacks may evolve.

The research and development team at PwC has come up with five possible ways that ransomware attacks may evolve in the future.

- **Frameware.** This frames a user for an illegal activity they didn't actually commit, such as downloading illegal images. An ML model detects when the user is at the machine and performs the activity over time, and then the attacker blackmails the user.
- **Smart ransomware.** This approach targets both commercial and industrial smart devices, such as white goods, cars, machinery, and infrastructure. This could lead to bigger ransoms and more disruption but is also likely to put threat actors under more scrutiny.
- **Health ransomware.** Medical devices are held at ransom, including hospital equipment, pacemakers, and other implants, threatening harm or death if the ransom is not paid. Private medical records could also be held ransom and released.
- **Data integrity ransomware.** Focused on companies with regulatory requirements, the attacker makes small changes to data rather than encrypting it and demands a ransom in exchange for reverting back to the original information or telling the company what was changed and where.

Lessons learned from a real-world ransomware attack.

Dr. Katie Paxton-Fear shared lessons learned from a ransomware attack she experienced when she was a data scientist and developer in her first tech job at a small utility broker. The business caught the attack before encryption completed, and had backups, which they were able to restore, but not without downtime that cost the company in sales and productivity.

> An attack can happen to any business, large or small. No business is immune to the threat of ransomware.
>
> *Dr. Katie Paxton-Fear, Bugcrowd*

This attack took advantage of an out-of-date Windows server and a known exploit in the remote desktop protocol (RDP). It could have been prevented if the company had:

- **Updated its software.** Keeping the Windows server and software on the system—and in the organization—closes known exploits.
- **Received professional security advice.** Penetration testing seems like an unnecessary expense but could have alerted the organization to gaps. This is often less costly than an attack.
- **Cultivated a better security culture.** Most employees saw security as not their problem and didn't engage with security practices.
- **Learned from the previous attack.** This was the second attack. Performing a retrospective and applying the lessons learned after that first attack could have prevented the second one.

BIOGRAPHIES

Dr. Katie Paxton-Fear

Application Security Engineer, Bugcrowd

Dr. Katie Paxton-Fear is an application security engineer at Bugcrowd, a lecturer, and a security researcher. Her PhD was titled "Understanding Insider Threats Using Natural Language Processing" and she has published her research into insider threats and particularly how to better understand insider threats using a holistic approach. Passionate about education and security, she creates video lectures enabling others to grow in security, with over 50 videos and 30,000 subscribers on YouTube in a little over a year. A former developer and data scientist, she finds her success is directly related to being able to understand the technical and human aspects of security.

Matt Wixey

R&D Lead, Cyber Security Practice, PwC

Matt Wixey is the R&D lead for PwC UK's cyber security practice and is a part-time PhD candidate at the UCL Dawes Centre for Future Crimes. He previously worked as a penetration tester, and prior to joining PwC led an R&D team in a law enforcement agency. He has spoken at Black Hat USA, DEF CON, ISF Congress, BruCon, 44Con, and various other security conferences. His research interests include RF hacking, unorthodox attack vectors, and social engineering.