staff around their security responsibilities is key when staff are not in the corporate office.

The uncertain new normal

This all may seem like a lot of work – and it is. But organisations can take some comfort that these efforts to revisit GDPR compliance are worth the effort. As and when we gradually emerge from the global pandemic, working from anywhere is predicted to become a core part of the new normal, and the processes laid down today will remain relevant for years to come.

Even if the majority of the workforce does indeed choose to return to the office, an organisation can be confident that it's prepared, should any similar event happen in future, and that it can offer more-flexible working practices should its employees demand it.

About the author

Marc Lueck is CISO EMEA at Zscaler (www.zscaler.com). He is a senior security practitioner with over 20 years' experience crossing multiple industry sectors, from financial services to publishing, specialising in enterprise security management, threat intelligence, compliance and security architecture.

Facing ransomware: an approach with private cloud and sentinel software

Holzen A Martínez-García

Holzen A Martínez-García, TecNM/Technological Higher Institute Progreso

Data and information are assets that carry a high value for organisations – and cyber criminals know this. They try to take advantage of this fact and have adopted various hacking techniques. One of the most current and dangerous is the infection of devices with cryptographic ransomware. Currently there are many approaches to countering this threat focused on the detection and mitigation of risks, but only a few of them consider an imminent infection and take on proactive data recovery techniques.

Ransomware is a type of malware that uses encryption algorithms and techniques to hijack a virtual computer asset, such as data or operating system functionalities. The modus operandi of this type of malicious software consists of encrypting files on the disk or blocking access to the system completely or partially until the user pays the creator of the malware, usually with a digital currency such as Bitcoin. According to Bhardwal et al, ransomware is a digital extortion that: infects a computer system; attacks from a variety of vectors; and can be implemented via browser exploits, the downloading and installation of freeware applications, through email attachments and ads that offer cash and other incentives to invite potential victims to fall for the deception.[1]

The main categories of ransomware are classified into two, according to the method of extorting the victim. These two variants are ransomware-crypto (or cryptographic ransomware) and ransomware-locker. Ransomware-locker focuses on the operating system or its functionalities, which has allowed users with technical knowledge in computing the possibility of retrieving the data and reinstalling the affected functionality. The impact and effectiveness of this ransomware is lower in comparison with the cryptographic method, which is why attacks of this type are decreasing.

Cryptographic ransomware represents the most widespread ransomware infection today. The success and effectiveness of this kind of attack is in large part thanks to social engineering. Although the use of this technique is not unique to ransomware, it is popular because it exploits certain human characteristics, manipulating people psychologically or exploiting the urge to do (or fail to do) some sensitive operation that allows the cyber criminal to continue the attack.[2] Social engineering techniques can be varied, with a lot of crossover between methods and their use.[3]

How the proposal works

This work presents an approach based on a generic network architecture that consists of an adaptable private cloud that contains a Linux-based storage server with open-source sync file software included. This stores real-time versioned copies of the files synchronised with the endpoint devices. The client layer also contains installed sync and share software, and sentinel software – specifically designed software that emerged as a product of this research. Figure 1 describes the proposal graphically.

The sentinel software works like a monitor of the folders on the client device previously configured by the user. The language used for coding was C# .NET and its main function is to block the monitored folders when there is suspicion

that cryptographic ransomware is active. It uses a SQLite database locally that updates from a server, which for the purposes of this work is the same cloud server.

This sentinel protects each client computer individually. Its basic function is to provide alerts of changes made to the working directory, lock the folders and prevent the ransomware from continuing to successfully encrypt files. Its operation is briefly described in Figure 2.

The sentinel software is configurable and can protect all files on the host computer. It is a program that installs individually on client computers that are running the Windows operating system. It manages an internal database in SQLite, which allows it to get updates with information about new, potentially dangerous extensions.

This software provides a graphical interface, which is shown in Figure 3, and it contains three main modules. The first module is the monitoring program, which records the events that arise during the monitoring of the established folders. The second contains the libraries module, in which the folders to be protected are established. You can observe the folders that are already monitored, remove any folders from the monitoring activity, check if they are active or not, and it's possible to activate them if they are not already active. Finally, in the configuration section, the parameters to associate with the server are set. In this section, it is possible to specify the data necessary to connect to the server database, perform a connection test and download the updates from the blacklist.

The sentinel software sends alerts when a monitored file is attacked with a change in its extension. Subsequently, if no record of the extension is found in the database, it asks the user if that extension should be allowed and added to the whitelist. When the user gives a negative response, it is added to the blacklist and immediately blocks the affected folder, allowing no further changes unless the same software releases the protection that has been applied. The sysadmin can now make a determination as to which is the best path from here. The sequence of steps is shown in Figure 4.

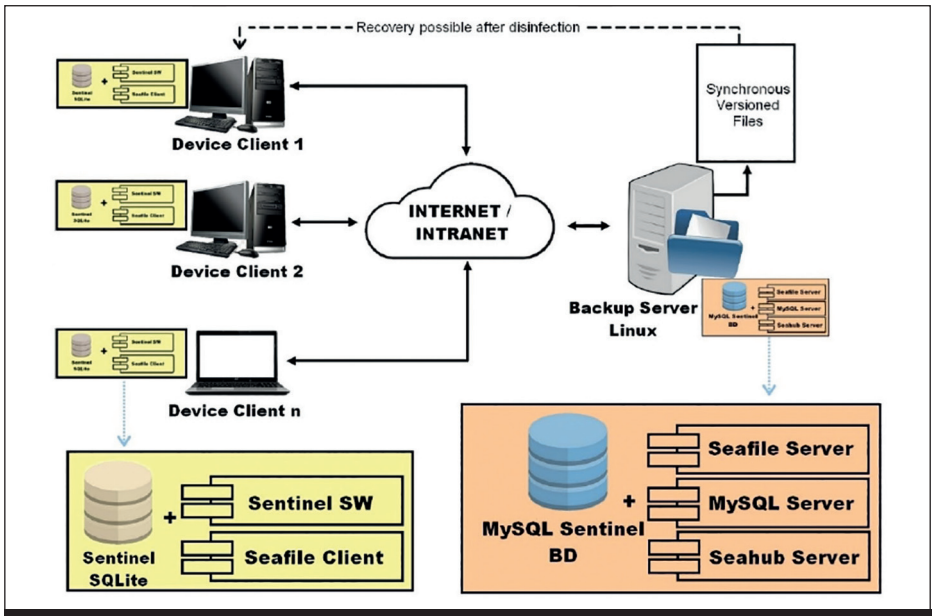

Figure 1: Proposed architecture with private cloud and sentinel software.

Experimentation and results

Now that we understand the sentinel software process, the steps followed in the experiment were as follows:

a) Interconnect the experimental group to the proposed network architecture.
b) Install the sentinel software in the machines of the members of the experimental group.
c) Verify that the control group is outside the proposed network architecture.
d) Infect both groups with the Hidden Tear open-source ransomware.[4]
e) Verify the files in both groups.
f) Ask the participants to try to recover the encrypted files without using the storage system.
g) Ask the participants to try to recover the encrypted files through the storage system.
h) Record the results obtained.

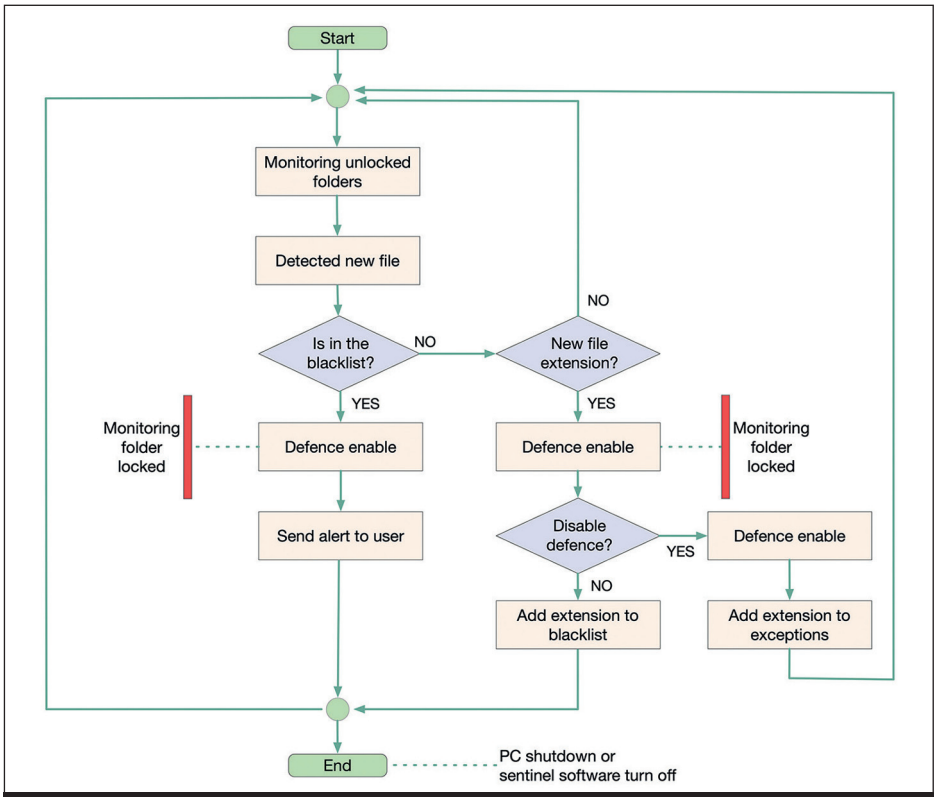

Figure 2: Workflow of the sentinel software on client devices.

With the exception of a particular case in which there were persistent problems with the network, all the other clients of the experimental group performed the test as planned, from the infection with ransomware to the recovery in a click from the web interface of the synchronous storage server.

Although in the experimental group there was an instance of a communication problem with the network, the element was counted as valid since the communications are part of the system. This decision was made in order not to bias the study and keep it as complete and reliable as possible.

To obtain additional data, we proceeded to create a cross-referenced table, in which it can be observed that all cases of effective recovery occurred when the proposed storage system was used, with an effectiveness of 92.3%, with a failure representing 7.7% of the total as a result of the communication error in the system.

After the experimental phase, a Likert test with many questions was performed on the experimental group of the test, to discover their attitudes towards the proposal. The scale was from 1 to 5, where 1 represents total disagreement and 5 total agreement, with the value 3 being neutral.

Finally, the experiment allowed a comparison of the perception of participants and the observation made with respect to the effective recovery of files. Figure 5 shows the data obtained from the applied test, which coincides closely with the external observations made. The person who is neither in agreement nor in disagreement represents 7.7%, the same percentage of the experimental team that had problems with the network and did not therefore obtain the projected data recovery (although the copies of the files in the server remained intact).

Observations

With the implementation of the proposed architecture, it was possible to design a generic storage system which consisted of a server using the Linux Mint operating system. This incorporated the cloud data storage software. The update is synchronous and includes version control, which allowed the user to recover images of data via the web interface provided by the system.

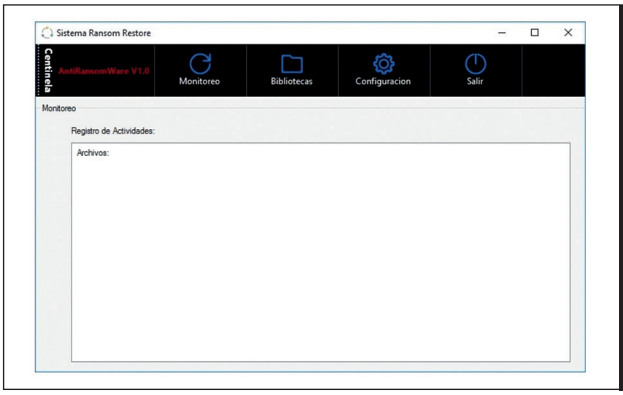

Figure 3: The main interface of the sentinel software.

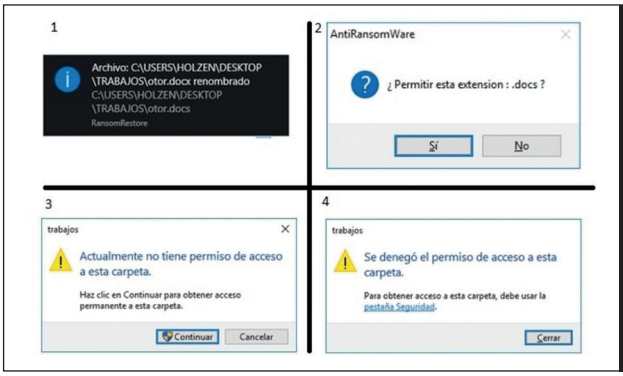

Figure 4: Alerts from the sentinel software.

Additionally during the course of the investigation, the development and implementation of the sentinel software emerged. This allows monitoring of the folders of the client systems that connect to the server, and blocks them in case of a ransomware attack or any unauthorised modification in monitored data.

With the data obtained and the hypothesis test raised, it is possible to affirm that the proposed system satisfactorily complied with the projected aims, since it was able to reverse the corruption of data caused by cryptographic ransomware infection, restoring files to optimal conditions. This represents an alternative mitigation and recovery method for updated data against the threats of cryptographic ransomware.

This proposal is mainly focused on dealing with cryptographic ransomware and an imminent infection. As long as the server data with previous versions of the files remains intact, recovery will always be possible, without spending time trying to decipher the encryption algorithm or worry about it being an unknown new strain. However, as version control and effective recovery are handled in a few steps, it is feasible also that it can be used as a recovery alternative if there is data corruption due to physical or other damage.

Implementation issues

On the issue of implementation, the proposal is generic and scalable. In the case of established and consolidated organisations, this should not be a problem. Given the infrastructure and security implementation levels they should have, adaptation should be easy. In addition to its layers of protection that include firewalls, intrusion detection systems, anti-virus solutions and other protection technology, it is worth noting that the inclusion of this proposed system is just one more layer within the security scheme. Although the protective systems in the organisation are focused on not letting the cryptographic ransomware penetrate the organisation's network, the surplus value of this proposal is that there is an alternative for recovering updated data in case the cryptographic ransomware penetrates the systems described above.

In the case of medium-sized organisations or personal users who do not have

the budget for multi-layer security solutions, this proposal would be sufficient to add greater security to their data against cryptographic ransomware. By using a Linux-based operating system, the proposal could be supported on development cards or computers with cheap embedded systems, such as the Raspberry Pi. These cards support the installation of a Linux operating system and the sync file software, with the user responsible for configuring and supporting the overall physical data storage, either using hard drives or devices that connect to the installed server.

The research project was completed successfully, with the achievement of the primary objective of verifying the use of a versioned synchronous storage system as a tool to mitigate and neutralise the effects of cryptographic ransomware. However, this work gives rise to other possible studies. For example, its generic architecture could be combined with some other layers of extra security to test the behaviour and efficiency of the computer system. Another possibility is that the server can be in a local cloud environment, as demonstrated in this research, or deployed on dedicated Internet hosting.

The sentinel software, which detects any effects in the folders indicated by modifications of the extensions of the files, also offers some additional possibilities worth exploring. This same sentinel software could be studied and optimised to experiment and protect against threats other than ransomware – such as file intrusion by other types of malware or actions by cyber criminals.

About the author

Holzen A Martínez-García is associate professor in the Computer Systems Department at TecNM/Technological Higher Institute Progreso (www.progreso.tecnm.mx). He has completed a PhD in computer systems at South University, México. He has a certification in PSP from Carnegie Mellon University and has completed complementary studies at Stevens Institute of Technology, Hoboken, New Jersey. His research interests are the IoT applications, computer security and machine learning.

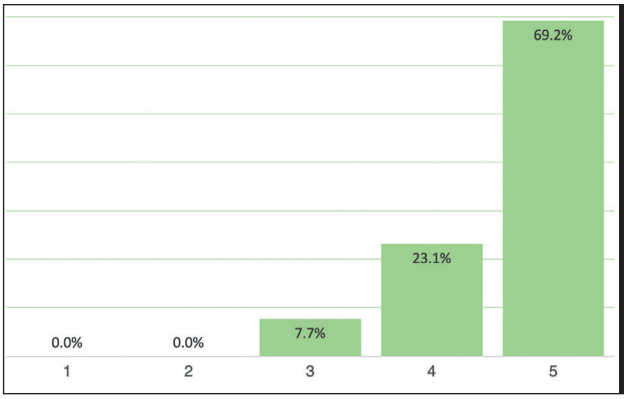

Figure 5: Attitude of the participants regarding the effectiveness and efficiency of the proposal. A rating of one represents disagreement that the system achieved its goals, while five is full agreement, with three being neutral.

Resources

- Kharraz, A; Robertson, W; Balzarotti, D; Bilge, L; Kirda, E. 'Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks'. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Jul 2015, pp.3-24. Accessed Jul 2020. http://193.55.114.4/docs/dimva15_ransomware.pdf.
- theZoo aka Malware DB, home page. Accessed Jul 2020. https://thezoo.morirt.com/.

References

1. Bhardwaj, A; Avasthi, V; Sastry, H; Subrahmanyam, G. 'Ransomware Digital Extortion: A Rising New Age Threat'. Indian Journal of Science and Technology, Apr 2016, pp.1-5. Accessed Jul 2020. www.researchgate.net/profile/Hanumat_Sastry/publication/286301708_Ransomware_A_Rising_Threat_of_new_age_Digital_Extortion/links/5763ae5908ae9964a16badd0/Ransomware-A-Rising-Threat-of-new-age-Digital-Extortion.
2. Mieres, J. 'Ataques informáticos: Debilidades de seguridad comúnmente explotadas'. EvilFingers, Jan 2009. Accessed Jul 2020. www.academia.edu/8522766/Ataques_inform%C3%A1ticos_Debilidades_de_seguridad_com%C3%BAnmente_explotadas.
3. Zhou, Y; Jiang, X. 'Dissecting Android Malware: Characterization and Evolution'. 2012 IEEE Symposium on Security and Privacy, 2012, pp.95-109. Accessed Jul 2020. https://ieeexplore.ieee.org/iel5/6233637/6234400/06234407.pdf.
4. Martínez-García H; Chuc-Us, L. 'Hidden Tear: Análisis del primer Ransomware Open Source'. Avances y perspectivas de la innovación, investigación y vinculación, 2015, vol.1, pp.31-54. Accessed Jul 2020. http://utmetropolitana.edu.mx/Publicaciones/recursos/may.112016123644Libro%20avances%20y%20perspectivas%20de%20la%20innovacion.pdf#page=30.