Deception Centric Defense Against Ransomware

by admin | Aug 7, 2017 | Blog |

Team Acalvio

It is estimated that in 2017, damages due to the ransomware will exceed $5 billion.[8] When successful, ransomware can not only infect the endpoint, it can also spread across the network extending its exploit. The initial versions of ransomware like CryptoWall, CryptoFortess, DMA-Locker, CryptoLuck used mapped and unmapped drive for lateral movement. WannCry[3] exploited SMB remote code execution vulnerability (MS17-010) and affected 150 countries; and Petya[2] used the same vulnerability (MS-17-010) along with WMI with stolen passwords for lateral movement and impacted 65 countries.

Despite the fact that detection approaches, algorithms such as detonation in virtualized environment, machine learning based detection algorithms, etc have been employed to detect ransomware, ransomware continues to penetrate the defenses and cause damage to organizations.

In the first part of the blog, we discuss evasion techniques that have been employed by ransomware to avoid detection by traditional defenses. We then discuss deception centric detection solutions and its inherent advantages over the current detection approaches.

Limitations in the existing detection architecture:

We classify traditional detection architecture into three broad categories : Sandbox based detection architecture, Endpoint based detection architecture and Intrusion prevention systems.

Sandbox Based Detection Architecture: Sandbox based architecture monitors email and web traffic. It extracts the file which is delivered over network and detonates the file

in a virtualized environment. Based upon the behavior of a file it is classified as malicious or benign. The architecture is prone to evasions [9]. As an example, if a ransomware employs a new file type, then the virtualized environment might have to be updated for the detonation of new file type. Deployment of an updated environment will take time and will lead to the opening of the window of opportunity for exploitation by a threat actor.

Endpoint Based Detection Architecture: Endpoint based detection architecture typically uses machine learning based detection algorithms. Machine learning algorithms such as random forest , extreme random forest can be used to classify a file malicious or benign. These algorithms are also prone to evasions. As an example, if a ransomware employs a new file type for delivering a malicious payload, then a new set of features might have to be extracted for the new file type. Deployment and development of an algorithm for the new file type will take time and will open a window of opportunity for exploitation. Also, if the ransomware enumerates processes on the endpoint, and if it finds Anti Virus agent installed on the end point, it can hide its behavior.

Network Based Inspection: Many families of Ransomware will initiate command and control communications to download the public keys which is used during process of encryption. This malicious network communication can be detected by network based inspection devices. Network based inspection approaches are prone to evasions [7]. Also, not all families of ransomware such as Sopra initiate command and control communication to download the public keys.

For further details about evasions employed by ransomware we would encourage you to refer to our previous blog titled Ransomware:catch me if you can.

In the following section, we first explain the deception centric architecture and outline its inherent advantages over the traditional detection architecture.

Deception Centric Architecture:

Deception centric architecture as a part of the first step, deploys bread crumbs, honey traps on the end host and in the network. When a ransomware infects the end host, it perform a set of discrete activities such as: encrypt the files on the infected host, delete the shadow backup, etc. It may perform other malicious activity as well such as creating a registry entry for persistence, may drop a copy of itself, may perform code injection, disable UAC, etc. Some families of ransomware moves laterally to mapped and unmapped files shares, databases and encrypts the files in the mapped and unmapped drives. These malicious activities triggers the events on the honey traps. Once these events get generated, these gets validated for the presence of ransomware. If the

validation algorithm confirms that ransomware has infected the end host, then the infected endpoint is isolated from the network, limiting the damage caused by ransomware.

Since deception sensors gets triggered during the actual execution of ransomware, deception centric architectures affords the following inherent advantages:

1. Detection is independent of the file type delivering malicious payload.
2. Detection is independent of the delivery vector i.e. ransomware can be delivered over web, email or by a threat actor, it will get detected by deception solution.
3. With or without command and control communication generated by a ransomware, deception solution will detect it.
4. Since the Detection solution uses alerts from honey traps for validation of ransomware, it results in a fast and accurate detection.
5. Since the Deception solution makes use of distributed deceptions for detection, it is capable of independently detecting infection at multiple places. It can detect ransomware on the end host over the internal network, at the mapped, unmapped drives. This capability of independently detecting ransomware at multiple places helps identify new variants employing different behavior. For example, if a ransomware, infiltrates the network, copies itself to the mapped /unmapped file shares and get activated at a precise date, a deception solution will be able to raise an alert even before the ransomware gets activated.

The following table outlines the different architectural approaches to detect Ransomware.

Types of Solution	**Known Evasions**	**Handles New File Types**	**Supports all delivery vector(Email, Web, Threat Actor)**	**Timely Detection**	**Detect infection at Multiple Places (Endhost, Mapped Drives..)**
	N	N			

Endpoint Anti-Virus	Enumerate process and find process specific to an endpoint agent.	Might have to build a new classifier	Y	Y	N
SandBox Behavioral Based	N Check for VM based upon execution environment [9] etc.. Differentate between human or automatd analysis systems based upon mouse movement, Number of CPU etc..	N Environment might have to be updated to detonate the new file format.	N SAMSAM ransomware. [6] (Compromising the network and installation of ransomware was done by a threat actor.)	Y	N
Intrusion Prevention System	NRansomware might not have C&C or capability to spread.	Y	Y	Y	N
Analytics	Y	Y	Y	N	N
Deception Centric Solution	Y	Y	Y	Y	Y

Summary:

Ransomware today is the leading threat which an enterprises faces and requires immediate attention. In this blog we summarize the inherent advantages of deception centric architecture over other traditional detection solutions. Since the deception centric architecture provides inherent advantages over other traditional architectures, we believe deception based approaches for detection and remediation of ransomware

should be a part of your security solution strategy.

Please join us for a webinar with Splunk, discussing the ShadowPlex-R ransomware solution and the Splunk Adaptive Response Initiative, and how we have partnered to deliver a unified, effective solution. Tuesday, August 22, 10am PST.

Register for Ransomware Webinar

Reference:

1. Ransomware catch me if you can, http://blog.acalvio.com/ransomware-catch-me-if-you-can
2. Technical Analysis of Petya Ransomware, https://acalvio.com/technical-analysis-of-petya
3. WannCry Ransomware analysis, Lateral movement propagation http://blog.acalvio.com/wannacry-ransomware-analysis-lateral-movement-propagation
4. Spreading Technique used by Ransomware, https://www.virusbulletin.com/virusbulletin/2016/12/spreading-techniques-used-malware/
5. Petya Ransomware Outbreak, here is what you need to know. https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know.
6. SAMSAM Ransomware, http://www.intelsecurity.com/advanced-threat-research/content/Analysis_SamSa_Ransomware.pdf
7. Evasion in Intrusion Prevention/ Detection System, https://www.virusbulletin.com/virusbulletin/2010/04/evasions-intrusion-prevention-detection-systems
8. Ransomware demand is a billion dollar crime and now growing, http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646
9. Hot Knives Through Butter: Evading file based Sandboxes. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/file/fireeye-hot-knives-through-butter.pdf

Search

Recent Posts

MarketWatch – This 18-Year-Old's Hacking Side Hustle Has Earned Him $100,000 — And It's Legal

BrightTALK – TAG-Cyber's Ed Amoroso Interviews Acalvio

3 Minutes Until the Apocalypse – Technical White Paper

TAG Cyber Interview of Acalvio's John Bradshaw

Security Week – Outdated DoD IT Jeopardizes National Security: Report

Archives

July 2018

June 2018

May 2018

April 2018

March 2018

February 2018

January 2018

December 2017

November 2017

October 2017

September 2017

August 2017

July 2017

June 2017

May 2017

April 2017

March 2017

February 2017

January 2017

December 2016

November 2016

October 2016

September 2016

August 2016

July 2016

Categories

Analyst Reports

Blog

Data Sheets

E-Books

Events

In the News

Press Releases

Resources

T-Shirts

Video

Webinars

White Papers

Acalvio provides Advanced Threat Defense (ATD) solutions to detect, engage and respond to malicious activity inside the perimeter. The solutions are anchored on patented innovations in Deception and Data Science. This enables a DevOps approach to ATD, enabling ease of deployment, monitoring and management. Acalvio enriches its threat intelligence by data obtained from internal and partner ecosystems, enabling customers to benefit from defense in depth, reduce false positives, and derive actionable intelligence for remediation.