Ransomware Detection

PLATFORM FEATURE UPDATE

While various ransomware attacks use different methods and techniques, at the core, the attack is carried out by encrypting files across a victim's network. In doing so, this process triggers a number of file access events: Write/WriteAttribute (Windows Event ID 4663) and Delete (Windows Event ID 4660).

Adlumin's new **Ransomware Detection Model** monitors the volume of these three events independently of each other per user across the entire network, looking for anomalous spikes in activity during a specific time window using historical data as a benchmark. If the amount of activity (either write or deletion) exceeds a specific threshold relative to the rest of the activity on the network, a detection will be sent for investigation.

In addition to checking the total volume of files accessed, the model also checks the distribution of objects modified across the network. If the majority of activity is focused in a single directory, which could be associated with software installation or updates, the model will not raise a detection. However, if the spike in activity is spread across multiple subdirectories, indicative of system-wide activity, the model will raise a detection.

9	Settings Learning	g Center Reports * Tool	is • Modules	• Tenanta • Support	æ	Gus Warren ot	
24						TENANT: Demonstration Tenant	
) *	Ransomware Detection - 15587 © Detection Time: 2021-07-23 09:16:14 UTC				+ Add Note	d to Investigation	
*	Detection Detail	s					
-8	A machine learning Details:	g algorithm has identified an and		access events.	1725 Total Events 1725 Events Surrounding this De	stection	
е А	Total file write ever	cent file write events detected : nts for s-1-5-18 : 1752	1752	Aggregate	E First Occurance 2021-07-23 09:16:14 UTC	;	
53 ©				information	Last Occurance 2021-07-23 09:17:44 UTC	•	
0	Event Sample Ti	meline					
						=	
	1	■ July 23 2021 @ 09:16:2	14	• July :	23 2021 @ 09:17:94	- July 23 2021 @ 09:17:44	
meline of file	+ 2xly 23 2021 (# 09:16		4	-300-1 (-300-223 3021 (\$ 00.0544)	12201 @ 9917394	(- July 23 2021 @ 00:1744)	
imeline of file	surrounding Eve	4	м			+ Jay 22 22 22 0 09 1744	
imeline of file		ants	• Het			• b/y 22 3221 g 093744)	
imeline of file	Surrounding Eve Show 10 ventries	ants		(-204-21 201-0 00 00 00 0	- 244 77 100 ((KU724)	Search	
imeline of file	Surrounding Eve Show 10 ventries Tape	ants Thee (JPE)	• Hot	900st	- 307 77 2017 @ M17734	Search	
10% Sample imeline of file access events	Surrounding Eve Show 10 ventries Tare	ants The MTE 2014 07-308-17 M UTC	- Hot	о оцин О раз 23 2021 ф 2010 мала О оцин Правол Полонал Полонал и индерски	- 10 17 101 (# 10.1715) - 10 17 101 (# 10.1715)	Search Vew V	Click to view full
imeline of file (ccess events	Surrounding Eve Show 10 ventries Type Dig Object Access	14 2015 2016/0/23 00:17.44 UTD 2016/0/23 00:17.44 UTD	• Het	о оцин Орин Прина и прина и Прина и прина и	- 30 17 201 (# 10.1734)	Search Ver Ver	
Table of files accessed during	Surrounding Eve Show 10 ventries Type In Origent Access Depend Access	A	- Hot States States		- Press	Search Vee 4 Vee 4 Vee	
Table of files accessed	Surrounding Eve Drav 10 ventils Trav (b) Over Annus (b) Over Annus (b) Over Annus (b) Over Annus (c) Over Annus	Image: Section 2016 Section 2016 Image: Section 2016 Section 2016	. Het	о орни орни Орни Парада Калана Парада Калана	- Press	Search Vee 4 Vee 4 Vee 4 Vee 7 Vee 7 V	Click to view full event information

