## How to view the New Infection Detected in a device via Email alert

Endpoint manager has the feature of viewing the new infection detected in a device via Email alert. The email alert consists of newly infected device name and the "Follow the link to see details." option to view the malware that caused the infection.

**Infected Device Name** - The email has infected device name. By clicking the device name, the users can get the Device summary information.

"Follow the link to see details" - To see the details about the New Infection, click the "link". This link will redirect the user to the malware that caused infection in the device. The details of OS, Device name, application name, package name, file path, file hash, signature, detection date about the malware are available in the Current Malware list.

This feature is explained with a below example:

A New Infection Detected in a device is sent to a user email.

When the user clicks the infected device name "DESKTOP-ETJM9P5" in the email, it will redirect the user to the infected device's summary information.

×		
EM Warning: New Infection Detected! From: Noreplies ksm-noreply@c1notifications.com Date: 2020-12-15 09:04 - Show pictures		Encoding: worldwide (utf-8) 🗸
	You are receiving this e-mail because you are using Endpoint Manager product. 2020-12-15 03:04:31. New Infection Detected on device DESKTOP-ETJM9P5. Follow the <u>link</u> to see details. Best Regards, EM Team	
	Sincerely, Endpoint Manager team.	

## The infected device's ("DESKTOP-ETJM9P5") Summary Information is given below

×					
Endpoint Manager	D	levice List / <u>WIN-952102DLV9R</u> / Summary		License Op	tions 💿 \Lambda Logout
DASHBOARD     DEVICES     Device List     Buik Installation Package	>	WIN-952102DLV9R Owner:	20 D C S C C C C C C C C C C C C C C C C C	کو ce Owner	
CONFIGURATION TEMPLATES  SECURITY	>	Device Name Summary Networks Asso	vacages intermation	nagement Groups Logs	
NETWORK MANAGEMENT	>	Device Summary	_	OS Summary	
APPLICATION STORE     APPLICATIONS     LICENSE MANAGEMENT	>	Custom device name Name Tags Notee	WIN-952102DLV9R WIN-952102DLV9R Not set	OS OS name OS version	Windows Microsoft Windows Server 2016 Standard (x64) 10.0.14933 Version 1607 (05 Bruikt 1.4393.447)
🔅 SETTINGS	>	Logged in user AD\LDAP Domain\Workgroup	Administrator N/A WORKGROUP	Service pack Build version Reboot time	N/A 14393 2022/07/27 10:20:34 AM
		Formfactor Model Communication Client version	Windows Server Virtuallox 7.1.42722.22060	Reboot reason	The process C:Windows\system32\shutdown exe (WIN-952102DLV9R) has initiated the restart of computer WIN-952102DLV9R on behalt of user WIN-952102DLV9R\dministrator for the following reason: No tills for this reason could be found Reason Code: 0x800000f Shutdown Type: restart
		Processor Serial number System model	Intel(R) Core(TM) I3-2120 CPU @ 3.30GHz 0 VirtualBox		Comment:

To view the infection details , click the "link" in the email

🖹 Write \ 🖓 Forward \ 🛞 View \ 😓 \ 🗶 \						
EM Warning: Nev From: Noreplies <itsm-i Date: 2020-12-15 09:04  Show pictures</itsm-i 	w Infection Detected! noreply@c1notifications.com> 4	Encoding:	worldwide (utf-8)	~		
	You are receiving this e-mail because you are using Endpoint Manager product.					
Follow the <u>link</u> to see details.						
	Best Regards, EM Team					
	Sincerely, Endpoint Manager team.					

This "link" will redirect user to the Current Malware List tab. This tab has the infected device name, application name, package name, file hash, signature and detection date.

Endpoint Manager		urc+esse License Options 💿 요 Logout (
DASHBOARD >		
DEVICES	Search group name	< Te Device List Current Malware List Quarantined Files Android Threat History Autoruns Items
<u>A</u> USERS >	요 Show all	📴 Delete Malware 🛛 Ignore Malware 🔄 Quarantine Malware 🖉 Rate as Trusted 🚥 More 🦿 🍸
CONFIGURATION TEMPLATES	+ 🖶 Carey	OS DEVICE NAME APPLICATION NAME PACKAGE NAME / FILE PATH FILE HASH SIGNATURE
NETWORK MANAGEMENT	+ 🖶 Default Customer	
APPLICATION STORE	÷ 🖶 KGF	
APPLICATIONS >	主 🖶 Steve_Smith	Results per page: 20 Displaying 1 of 1 results
$\bigcirc$ security sub-systems $~~{\scriptstyle \lor}~$		
Security Dashboards		
Containment		
Application Control		
Valkyrie		
Antivirus		
Device Control		
Data Loss Prevention BETA		
LICENSE MANAGEMENT		
☆ SETTINGS >		