**Today**



[**kim@lancesoft.com Senior Security Analyst**](http://localhost:3011/ldms/qradar/incidentscollaboration)2:08:59 PM

@John @Dave @Stuart it seems that we are dealing with WannaCry

I'll start to contain the spread, @Dave please update the CISO about this incident



[**dave@lancesoft.com Security Analyst**](http://localhost:3011/ldms/qradar/incidentscollaboration)2:09:07 PM

I'm on it



[**john@lancesoft.com Senior Threat Analyst**](http://localhost:3011/ldms/qradar/incidentscollaboration)2:09:13 PM

I found that **Shadow Broker** leaked an SMB exploid named \*EternalBlue\*. SMB is the transport protocol used by Windows machines for a wide variety of purposes such a file sharing, printer sharing and access to remote Windows services. SMB operates over TCP ports 137, 139 and 445. This vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target's computer. As a mitigation I suggest blocking any outbound traffic on TCP prots 137, 139 and 445.



[**kim@lancesoft.com Senior Security Analyst**](http://localhost:3011/ldms/qradar/incidentscollaboration)2:09:18 PM

@John can you create an IOC list?



[**john@lancesoft.com Senior Threat Intelligence Analyst**](http://localhost:3011/ldms/qradar/incidentscollaboration)2:09:259 PM

On it!

**Completed task in 2mins 2secs**