Kevin Richards
Managing Director, North America and Strategy & Risk Lead

(Full transcript)
June 2017

(FULL VIDEO)

Building Resilient Healthcare Systems
iDefense® Malware Analysis

Kevin Richards
At iDefense®, part of Accenture Security, we understand that today's security executives and practitioners require a new way to consume dynamic intelligence so they can investigate threats and take action. In order to fulfill this requirement, Accenture Security has developed the iDefense® IntelGraph, an innovative new tool to capture and link all facets of the cyber threat landscape together.

This data-driven security intelligence application allows practitioners to quickly understand the diverse threats they are facing, investigate additional risks to their organization, allocate resources effectively and determine the proper courses of action to take. In this use case, we'll show how the iDefense® IntelGraph enables practitioners to investigate suspicious DNS queries and network traffic by simply searching on a domain.

We'll ask questions like: Is the domain malicious? When was it last used? Which malware family is the domain associated with? Is it a targeted attack or widespread across the internet? Which vertical or region does the malware target? Which tactics, techniques and procedures are related to the attack or the campaign? Where does the malware originate from? What kind of data can be stolen? Are there any signatures or indicators of compromise to detect or block the malware?

Let's say during daily monitoring, you identify a DNS query and suspicious network traffic to the domain grouptumbler .COM. To start your iDefense® IntelGraph query, type the name of the domain, in this case, grouptumbler .COM, into the search field. The right-side nodal diagram shows the connections. A search for the keyword yields a number of results, including: Associated domains: grouptumbler .COM and news dot grouptumbler .COM. And an email address potentially associated with the threat actor, postmaster at grouptumbler .COM.

There are also multiple intelligence alerts for "TOR File-Wrapping Malware Linked to the "OnionDuke"" and "MiniDuke" threat campaigns. The domain registrant, postmaster at grouptumbler .COM, also registered the domains nostressjob .COM and overpict .COM. The domain overpict .COM was used as part of the "OnionDuke" threat campaign.

The "OnionDuke" malware analysis provides detection signatures to identify various attack phases and a list of indicators that can be entered into a SIEM. Through the use of iDefense® IntelGraph, you can easily find information and visualize connections among alerts, malware families and threat campaigns.

With iDefense® IntelGraph, you can find IOCs and signatures to leverage for detection and mitigation activities, uncover potential previously unknown security risks, and prioritize your security resources more effectively.

To learn more, go to Accenture.com/iDefense.

END