Issued 6/7/17

The Secret to Detecting Malware

Are there new tricks to finding malware that most people aren't aware of? On the consumer/home user side, the easiest and most obvious answer is visual indicators. Ransomware takes over your screen and has popups making demands of payment. Adware and PUA (potentially unwanted applications) often put system tray icons or popup windows randomly containing ads or websites you didn't visit. Also, browser toolbars that were never there, icons on your desktop, or start menus you don't recognize. Physical indicators could be that the fan on your computer is running at full speed for long periods of time or powering off at random times. These indicators are easy and often result in family members contacting me about their "computers acting funny". However, most malware today leaves no indicator. In fact, you can't tell it's running on your system at all.

This is why consumers rely so heavily on anti-virus to keep their systems clean of malware. Also, giving them clear indicators when they have landed themselves in trouble. What the industry calls "nextgen anti-virus" is the way of the future. Rather than looking for specific malware, it looks for malicious behavior in general. This helps close the gaps on what we call "0-day threats". Malware that exists with no coverage from anti-virus. The best advice I can give to consumers is use trusted anti-virus, don't be hesitant to patch all your software, and be leery of all email attachments. On the enterprise side, there have been a lot of new innovations including the previously mentioned "nextgen

anti-virus" and EDR (Endpoint Detection & Response) that has me really excited. To put simply, EDR opens the door to endpoints in an enterprise network, a previously massive blind spot to IT professionals. It records every process running on the box and how that process was executed. It gives full process trees of everything running on the endpoint, what it's doing to the system and what it's connecting out to on the internet.

With this visibility, no malware can hide, it will be recorded, evaluated by the EDR technology and flagged for an incident responder to review. This also gives massive visibility to threat hunters, professionals whose sole mission is to find evasive malware/actors in networks and identify them. This combination of visibility, threat intel, technology and humans is really the pinnacle of where enterprises need to move IT Security programs to today.