ON REFLECTION

# THWARTING A TAKEOVER

EXTRAHOP TAKES THE BITE OUT OF RANSOMWARE.

***by Patrick Marshall***

**YOU'RE HARD AT WORK** when suddenly a window pops open unbidden on your screen and proclaims: "Your personal files are encrypted!"

Your first reaction is likely a feeling of being violated. Your second — as you read how many bitcoins you're going to have to cough up to obtain the key to decrypt your files — is most likely outrage.

What to do? Is there any alternative to paying the ransom? The FBI urges you to report the incident to www.ic3.gov. But while that may eventually help corral some of the culprits, it won't retrieve your data.

Ransomware incidents have soared in recent years, with hospitals being hit particularly hard.

In the vast majority of cases, by the time that message from the ransomware program arrives, it's too late to do anything about it unless you have an offline, secure backup


you can restore. ExtraHop, a Seattle-based network analytics platform, has come up with a new way for businesses to protect data from encryption by ransomware.

"The traditional way to deal with things like this is you look for signatures," explains CIO John Matthews. "You try to have your firewalls inspect all inbound and outbound traffic, you look for signature files that you know have a likelihood of being bad or come from a bad location, and you sniff your systems and hope that you catch everything that goes on."

ExtraHop, which has long experience analyzing network traffic, takes a different approach. While looking for ransomware signatures is an important step, says Matthews, to catch unknown ransomware before it does damage you actually have to observe the behavior inside your data center in real time. The ExtraHop Ransomware bundle, a set of triggers, alerts and dashboards that can be added to the ExtraHop platform, monitors all storage activity and uses behavioral analytics to isolate potential attacks in real time.

"We can actually observe action as it is happening and we flag activities that look suspicious and are likely ransomware attacks," says Matthews. If an unexpected surge of encryption begins, for example, he says, "Within minutes of an attack being underway, you can actually stop an attack in flight and you can sequester a system that is behaving poorly and stop the damage very, very rapidly."

Matthews notes that the flow of events in the real world works something like this: "Bad stuff happens, things break and it costs money, IT fixes it, then auditors want to know what happened. From a senior IT position, I need to be able to prove to the board and prove to the auditors what happened when."

The ExtraHop platform goes further, Matthews says, by offering a "look back" feature, which allows IT staff to track back across network activity to determine where the threat came from and what the exact scope of the damage might be.

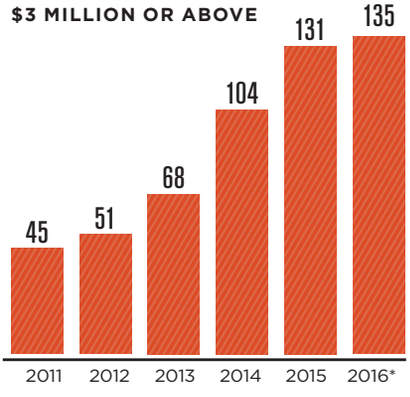
Short of applying thumbscrews to the offending party, it's a pretty satisfying response to a growing problem. SB

STATSHOT

# $3 Million Is the New $1 Million

IF YOU REQUIRE MORE EVIDENCE THAT HOME PRICES IN SEATTLE are back in a big way, look no further than the announcement that Windermere Real Estate, the largest real estate company in the western United States, has launched an "ultra luxury" brand known as the W Collection to showcase homes selling for $3 million or more.

**NUMBER OF KING COUNTY HOMES SELLING FOR $3 MILLION OR ABOVE**




*THROUGH OCTOBER 2016

**165,000**

*Number of King County households with annual incomes above $150,000*

**52%**

*From 2010 to 2016, the increase in the number of King County households with incomes above $150,000*

**18.4%**

*Proportion of all King County households with incomes above $150,000*

**$8.48M**

*Listing price of this 8,579-square-foot, 4-bedroom home on Mercer Island*

SOURCE: WINDERMERE REAL ESTATE