The

Broadcasters' Desktop Resource

www.theBDR.net

... edited by Barry Mishkind – the Eclectic Engineer

Doing IT

The Heimdal Anti-Ransomware Suite

By Ron Castro

[November 2019] It is not a matter of a couple of computers, most stations have dozens of interconnected computers and departments.

For that reason, as more and more instances of ransomware happen, stations are giving more attention to ways to harden security on the LAN.

Any broadcast engineer or IT person who does not live in mortal fear of a ransomware attack is either living in a bubble of bliss – or truly is in a coma!

Everything in the modern broadcast facility, from the small market standalone to the nationwide corporate chain, is dependent on workstations, servers, mobile devices, routers, phone systems, automation systems, access points and more – all of which ultimately connect to the Internet.

As a consequence, every day you and your fellow employees and managers are exposed to a barrage of emails, websites, and downloads that can result in disaster with a single click of a mouse.

Not what you ever want to see

NO LONGER UNCOMMON

In recent times, we have all heard about some of the ransomware attacks on municipalities, entities large and small, and broadcasters, too.

Major facilities like San Francisco's KQED, Radio One, and Entercom's national network system as well as single station computer networks have been crippled, with the perpetrators demanding thousands, and in some cases, millions of dollars in ransom to unencrypt the compromised files.

For radio stations, loss of music and commercial libraries, archived programs, traffic, and financial databases, including payroll records, can be an unmitigated disaster.

ENOUGH IS ENOUGH

My small company was hit by two ransomware attacks back some years ago before the hackers had developed software with the ability to spread itself to the far corners of a network, so only two computers were compromised.

Fortunately, we had installed CrashPlan, an offsite automatic backup system that allowed me to restore all of the files and thwart both attacks.

Backup programs are absolutely essential, but they are like airbags in your car: it is good to know they are there, but you really do want to avoid situations that can make them deploy.

HEIMDAL SECURITY

Both of the computers that I saw infected had a well-known anti-virus program installed, but it did no good against the attacks.

This led me on a search for a protection protocol that was specifically designed to ferret out and stop ransomware. After scouring the Internet, I found Heimdal Security.

Heimdal is a small company based in the Netherlands that claims a completely different approach to malware that does not rely on the traditional signature-based scan method used by the vast majority of anti-virus programs. (The newest batch of malware programs use "polymerphic" code, which exhibits a different signature every time it installs itself.)

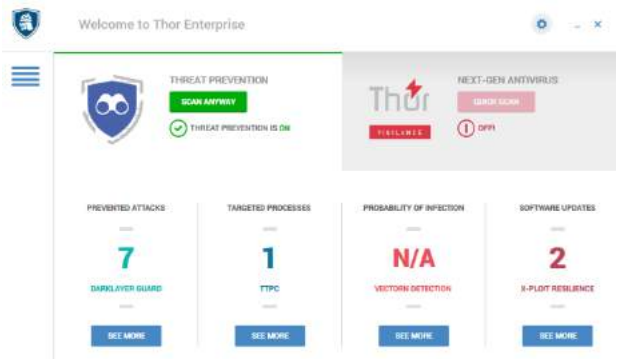
HOW IT WORKS

In addition to code scanning, the Heimdal product uses several additional methods to prevent a successful attack.

First, it looks for unusual processes, such as mass file encryptions or calls to known hacker "command and control" servers, and reports suspicious events to Heimdal's technicians for review. Heimdal also works to block nefarious websites by substituting your computer's designnated DNS server with theirs.

Finally, the enterprise version "pushes the latest updates and security patches for many of the common programs that are typically exploited to become malware entry vectors, such as Chrome, QuickTime, Java, and dozens of others.

Network administrators have a web-based console to control policies and to view individual user's activities and they get daily email updates alerting them to potentially compromised computers in their networks.



The Heimdal Security Thor Agent client on a typical workstation

IT IS WORKING OUT WELL

Does it work? We have now had the product installed on some 80 workstations and servers in our company for four years and we have not had a single successful attack.

That does not mean we can let our guard down. In addition to an effective anti-ransomware like Heimdal, here is the laundry list of additional safeguards we recommend:

1. An automatic, off-site backup program that saves files on at least a daily basis and *does not overwrite them* so that files can be restored from an earlier time.
2. Each Windows workstation should be protected by either Microsoft Security Essentials, Windows Defender, or some other signature-based anti-virus.
3. Use a strong router, such as a SonicWall appliance, that employs subscription-based filters and Stateful Packet Inspection for both HTTP and HTTPS traffic.
4. Regularly remind employees about the dangers of clicking on email links and/or falling for phishing attempts.
5. Do not allow any unprotected devices to connect to your network. Use a guest WiFi so that guest users can get to the internet but are isolated from your LAN.

While you can spend a bundle on Internet security, the measures I have outlined represent only a modest expense, especially when weighed against the potential cost of full-scale ransomware attack.

Be safe out there!

- - -

Ron Castro is the Chief Technical Officer for Results Radio, LLC, in Santa Rosa, California. You can contact him at ronc@sonic.net

- - -

If articles like this are useful to you, please feel free to subscribe to our one-time-a-week BDR Newsletter. It takes just 30 seconds here.

- - -

Return to The BDR Menu