

CREDIT UNION JOURNAL

CUjournal
.COM

THE NEWSWEEKLY FOR GROWTH-ORIENTED CREDIT UNIONS

March 21, 2011

TECHNOLOGY SPECIAL REPORT

Blacklisting Employee ‘Productivity Wasters’

By Kevin Jepson, *Technology Correspondent*

ANTIGO, Wis.—Some employees at CoVantage CU here apparently love to play Minecraft, the online monsters-meet-construction game.

“Employees could launch Minecraft on the Internet, and it’s a productivity waster,” said Aaron Hurt, information security officer at the \$870-million CU.

CoVantage has an enterprise “blacklist” to ban selected Internet sites, but each popular new game or shady website must be manually added to the list before the blacklist can do its job.

Meanwhile, commercial lending employees, seeking to chat instantly with one another during the workday, took matters into their own hands and installed instant messaging (IM) software on business computers, Hurt continued.

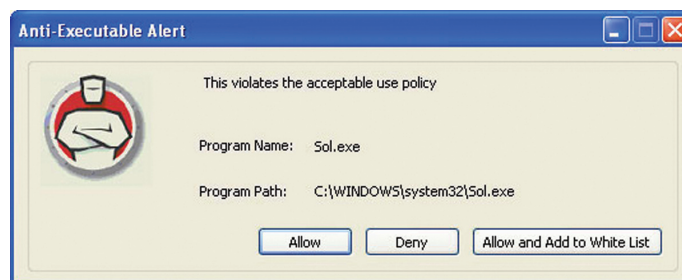
“The IM client not only had a lot of bloat and conflicted with other applications but also had file-sharing capability,” he said. “That was a huge potential security event.”

But the most urgent risk comes from CoVantage’s service kiosks, deployed at each of eight branches, said Hurt. “Members try out our website and Internet banking on a kiosk.



We don’t want someone to put a keylogger on that kiosk that could steal private information.”

CoVantage has alleviated these risks, from Minecraft to keylogger malware and seemingly innocent software updates, with a “whitelist” endpoint security solution called “Anti-Executable,” Hurt said. The solution is part of CoVantage layered security and is provided by San Ramon, Calif.-based Faronics.



Demo of what an employee sees if he tries to log onto a blocked site.

“Anti-Executable popped up four years ago as a good way to control our PCs,” Hurt said. “It’s lightweight and transparent.” Employees work unhindered as Anti-Executable actively monitors their computer—until they try to launch unauthorized files or websites and are blocked.

Anti-Executable takes a somewhat atypical approach, employing a “whitelist” that allows approved applications, rather than using the traditional blacklist to block applications that aren’t. That way, CoVantage can create a whitelist consisting of the limited number of executables permitted rather than trying to build a blacklist of the nearly infinite number of those that aren’t.

“What a fantastic concept,” Hurt said. “You lock down the computer only to allowable executables. Why hasn’t the anti-virus and endpoint security industry gone more in the whitelist direction?”

Anti-Executable is particularly valuable in blocking today’s evolving malware, Hurt suggested. “Malware gets harder and harder to identify. Some programs that look legitimate actually have reporting functions that could send sensitive data outside our network.”

CoVantage Takes Steps To Block Employee ‘Productivity Wasters’

And even if a piece of malware changes its file name or contents, Anti-Executable will block it. That’s because Anti-Executable compares authorized file hashes to rogue file hashes, explained Carlos Santamaria, product manager, Faronics. File hashes always stay the same, even when other changes are made to a file, he said.

Anti-Executable is installed on about 120 machines at the CU, but Hurt said he would like to extend the deployment to any machine that’s in a public area or used in member interactions. “If someone wanted to be malicious, they could infect a computer when a staff member leaves their station.”



Anti-Executable is combined with Faronics “Deep Freeze,” software that can automatically reboot computers to their original settings.



Members can try out online banking at this kiosk.

Hurt said Deep Freeze has made him feel more comfortable about kiosk security. “If malware somehow were to make it past Anti-Executable, Deep Freeze instantly reloads the kiosk system to its original image after 15 minutes of non-use.”

Used alone, anti-virus software is a weak defense against malware for many reasons, Hurt added. “Blacklist anti-virus software can’t keep up with the signature files needed to block malware. And end-users complain that antivirus slows down their computers.”

Faronics provides low-profile anti-virus software that can complement layered security and can be integrated and

FOR MORE INFORMATION

CoVantage CU
www.covantagecu.org
Faronics
www.faronics.com

remotely managed along with all other Faronics products from a central console, said Liliya Apostolova, product marketing manager, Faronics.

