Let hackers in: Experts say traps might be better than walls

February 10 2015, byYoukyung Lee

in this Jan. 20, 2015, Kwon Seok-chul, CEO at computer security firm Cuvepia Inc., presents "Kwon-ga," a real-time monitoring solution that detects hackers during an interview at his office in Seongnam, South Korea. Ever since the Internet blossomed in the 1990s, cybersecurity was built on the idea that computers could be protected by a digital quarantine. Now, as hackers routinely overwhelm such defenses, experts say cybersecurity is beyond due an overhaul. Their message: Neutralize attackers once they're inside networks rather than fixating on trying to keep them out. In South Korea, where government agencies and businesses have come under repeated attacks from hackers traced by Seoul to North Korea, several security firms have jumped on the growing global trend

to develop systems that analyze activity to detect potentially suspicious patterns rather than scanning for known threats. Kwon said it has been tough to convince executives that it's more effective to catch bad guys after they've infiltrated a network instead of trying to keep them out, which he believes is impossible anyway. (AP Photo/Ahn Young-joon)

Ever since the Internet blossomed in the 1990s, cybersecurity was built on the idea that computers could be protected by a digital quarantine. Now, as hackers routinely overwhelm such defenses, experts say cybersecurity is beyond due an overhaul.

Their message: Neutralize attackers once they're inside networks rather than fixating on trying to keep them out.

First they need to convince a conservative business world to gamble on a different approach. And having sold generations of defensive systems that consistently lagged the capabilities of the most advanced hackers, the industry itself must overcome skepticism it's flogging another illusion of security.

According to U.S. cybersecurity company FireEye, 229 days is the median length of time attackers lurk inside their victim's computers before being detected or revealing themselves, underscoring the weakness of conventional tools in identifying sophisticated intruders.

The traditional defenses must "have a description of the bad guys before they can help you find them," said Dave Merkel, chief technology officer at FireEye Inc. "That's just old and outmoded. And just doesn't work anymore," he said.

"There's no way to guarantee that you never are the victim of

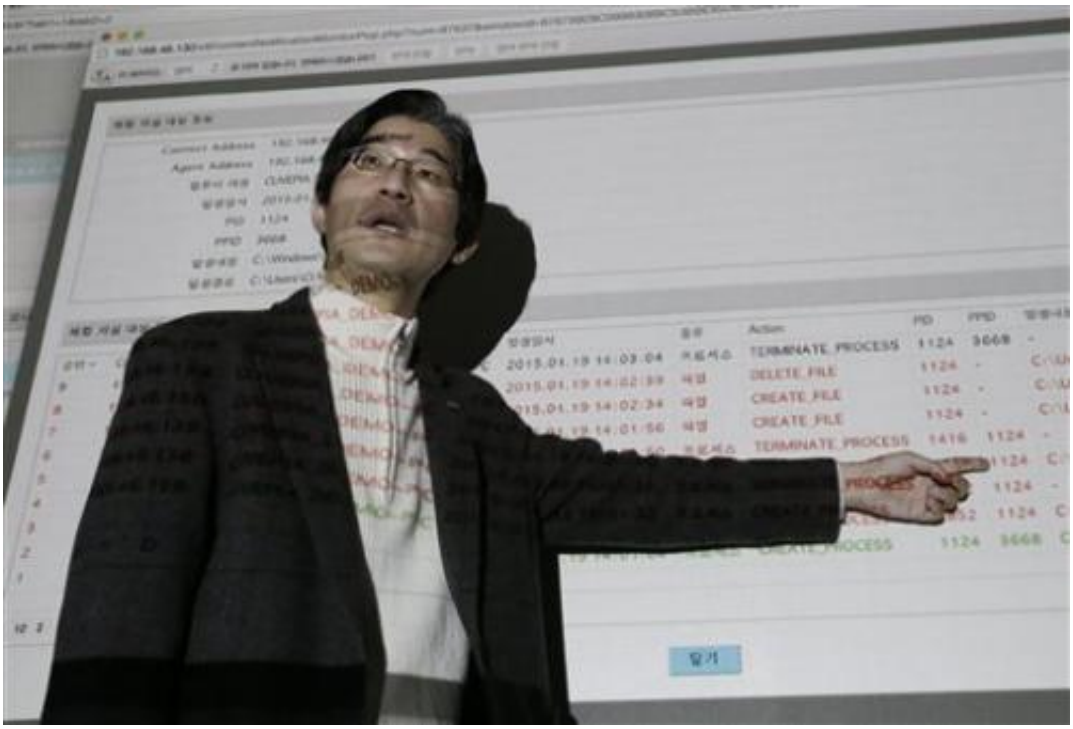
cyberattack."

Merkel said in the worst case he knows of, attackers hid themselves for years.

Experts aren't recommending organizations stop deploying perimeter defenses such as antivirus software or firewalls that weed out vanilla threats. But they say a strategy that could be likened to laying traps is needed to counter the sophisticated hacks that can cause huge losses.

The weakness of relying on a firewall is that it's like building a fence around a housing complex but not hiring a guard to patrol the interior streets, said Ed Amoroso, chief security officer at AT&T.

The hackers who targeted Anthem, the second biggest U.S. health insurer, and accessed personal information of 80 million customers, may have been inside its system for more than a month before being detected, according to the company.



In this Jan. 20, 2015, Kwon Seok-chul, CEO at computer security firm Cuvepia Inc., speaks as he presents "Kwon-ga," a real-time monitoring solution that detects hackers during an interview at his office in Seongnam, South Korea. Ever since the Internet blossomed in the 1990s, cybersecurity was built on the idea that computers could be protected by a digital quarantine. Now, as hackers routinely overwhelm such defenses, experts say cybersecurity is beyond due an overhaul. Their message: Neutralize attackers once they're inside networks rather than fixating on trying to keep them out. In South Korea, where government agencies and businesses have come under repeated attacks from hackers traced by Seoul to North Korea, several security firms have jumped on the growing global trend to develop systems that analyze activity to detect potentially suspicious patterns rather than scanning for known threats. Kwon said it has been tough to convince executives that it's more effective to catch bad guys after they've infiltrated a network instead of trying to keep them out, which he believes is impossible anyway. (AP Photo/Ahn Young-joon)

In the famous Sony Pictures hack, the attackers who breached the Hollywood studio's network went unnoticed until computers were

paralyzed and a mountain of data was dumped on the Internet.

The amount of data copied and removed from Sony's systems should have set off internal alarms long before Sony workers found their PCs taken over by malware, said Mike Potts, CEO of Lancope, a network security company based in Alpharetta, Georgia.

The cybersecurity industry characterizes such long-term intrusions as advanced persistent threats or APT. They are often sponsored by states and target valuable commercial and military information.

In South Korea, where government agencies and businesses have come under repeated attacks from hackers traced by Seoul to North Korea, several security firms have jumped on the growing global trend to develop systems that analyze activity to detect potentially suspicious patterns rather than scanning for known threats.

Kwon Seok-chul, CEO at computer security firm Cuvepia Inc., said it has been tough to convince executives that it's more effective to catch bad guys after they've infiltrated a network instead of trying to keep them out, which he believes is impossible anyway.

Kwon said his company's latest monitoring product keeps a log of all activity, dividing it into authorized users and possible attackers. When certain conditions are met, the program sounds an alarm. A response team, he said, can sit back and watch what hackers copy and respond before damage is done. The security team can cut the hacker's connection or trick the intruder into stealing empty files.

"Because hackers are in your palm, you can enforce any measures that you want," said Kwon, member of an advisory board for South Korea's cyberwarfare command.

In one case, the security team at one of Kwon's clients "enjoyed" watching for about an hour as a hacker scanned its network and installed tools to unlock passwords and counter antivirus programs.

He said that for skilled hackers, it usually takes about 20 minutes to lay out the initial steps of the attack that allow them to stealthily roam a network. Normally the security team would counterattack within a few minutes after gathering intelligence about the hacker's tools. But in this case, the hacker was not sophisticated and employed well-known programs mostly made in China.

In this Jan. 20, 2015, Kwon Seok-chul, CEO at computer security firm Cuvepia Inc., poses after presenting "Kwon-ga," a real-time monitoring solution that detects hackers during an interview at his office in Seongnam, South Korea. Ever since the Internet blossomed in the 1990s, cybersecurity was built on the idea that computers could be protected by a digital quarantine. Now, as hackers routinely overwhelm such defenses, experts say cybersecurity is beyond due an overhaul. Their message: Neutralize attackers once they're inside networks rather

than fixating on trying to keep them out. In South Korea, where government agencies and businesses have come under repeated attacks from hackers traced by Seoul to North Korea, several security firms have jumped on the growing global trend to develop systems that analyze activity to detect potentially suspicious patterns rather than scanning for known threats. Kwon said it has been tough to convince executives that it's more effective to catch bad guys after they've infiltrated a network instead of trying to keep them out, which he believes is impossible anyway. (AP Photo/Ahn Young-joon)

Eventually, the security team severed the hacker's connection to the victim's computer based on the unique ID of the program that Cuvepia's software showed the hacker was using.

According to FireEye's Merkel, there is a rise in awareness in the U.S. and growing interest in Asia in modern approaches to information security that include using automated programs to scan for unusual network activity, encryption and segregating sensitive data in special "domains" that require additional credentials to access.

But many companies are in denial about their vulnerability or are reluctant to spend more on cybersecurity, he said.

In the financial industry at least, part of the reason is greater concern with meeting regulatory requirements for security than improving security itself.

When encryption is used, South Korean courts have limited the liability of companies that faced lawsuits from customers over stolen data, said Hwang Weoncheol, a former chief information security officer at a South Korean financial institution. That reinforces the security strategy centered on compliance with regulation, he said.

Protecting high value information often comes with a high price tag.

Installing Cuvepia's cheapest monitoring product on 1,000 computers for a year costs 450 million won ($410,000). That is many times the cost of installing antivirus software though the cost drops significantly after the first year.

The answer for executives, said Kwon, is to see cybersecurity as an investment not a cost.