National DEFENSE
NDIA
NDIA's Business and Technology Magazine

Defense Companies Facing Array of New Cyberthreats (UPDATED)

March 2014

By Stew Magnuson

Waterholes, crypto-lockers and Shodan.

These three terms are just a few of the new pitfalls out there for defense companies large and small that face a dizzying array of threats against their networks.

Criminals and spies remain unrelenting in their pursuit of what firms have, whether it is intellectual property or financial data, cybersecurity professionals said in interviews.

The waterhole scheme is a twist on an old tactic, in which an adversary through an email tricks a company or government employee into clicking on a website that contains malware.

In this case, like a gazelle lured to the promise of a cool drink, the lion, or in this case the hacker, is in the bushes waiting to pounce.

The email contains a link to a website that appears to be perfectly legitimate, explained Paul Christman, public sector vice president at Dell Software.

"It looks like a legitimate link, but then they hijack you to another site that injects malware. ... It is a sophisticated way of getting to users who are getting smarter about links. The first one looks clean, the second is not," he said.

Crypto-lockers, also known as ransomware, is another troubling trend that can affect any company with valuable but perishable data, said Curt Aubley, chief technology officer and North American vice president at McAfee.

It begins again with an employee clicking on an attachment or linking to a website that allows a hacker into the network. The intruder searches for important data and then places encryption on it.

Next comes a message, Aubley said, "Look, we didn't steal your data. But we have encrypted it and you can't get to it, so if you pay us this amount of money, we will give you the key to unlock the data."

If the victim doesn't comply, the hacker has the power to let the perishable data expire or leave the encryption on, he said.

Individuals have been extorted for amounts as small as $250, but large companies have lost much more, he said.

The best defense is understanding where the important data is kept, ensuring that it is backed up and having an incident response plan in place, he said.

The new mantra in the cybersecurity world is: "No more free bugs," said Allen Harper, chief hacker and executive vice president at Tangible Security and lead author of Gray Hat Hacking: The Ethical Hacker's Handbook.

The bugs are better known as zero-day vulnerabilities. These are previously unknown holes in software programs that hackers can use to penetrate systems almost undetected. Since they are unknown, firewalls cannot pick up the signatures of an attempted infiltration.

Only a few years ago, computer experts exposed them willingly so patches could be released as soon as possible, but that isn't happening as frequently anymore, Harper said.

Discovering the bugs and trading them is now a lucrative endeavor. There are legal businesses offering subscriptions to anyone who can pay for the most recent zero-day discoveries. Who are their customers? Spy agencies and criminals are certainly among them, Harper said. The Washington Post reported recently that the National Security Agency spent $25 million last year to purchase these vulnerabilities.

"I guarantee you if they are doing that, other governments are doing that as well," he said. A bug can be purchased for anywhere from $25,000 to $250,000, and some have gone for as much as $1 million, he said.

The average zero-day — once discovered — remains unknown for 151 days. During that time, the software manufacturer either isn't aware of it, or hasn't produced a patch, he said.

The legal companies buying and selling zero-days through subscriptions are "leaving the rest of us vulnerable to cyber-espionage," Harper said.

"That is how bold this underground economy has become. And that is just what we know about. You can imagine that the true black market with organized crime and such is probably 10 times" the amount of what is being traded in the open, he said.

About 95 percent of network defenses are focused on signature-based detection, he added. Zero-days by definition don't have signatures because the software manufacturers don't know about them. Since there is no patch for a zero-day, the signature detecting tools are blind, he said.

"It is a real clear and present danger to individuals, corporations and governments alike," Harper said.

That leads to a website called Shodan.

Harper described it as a "Google site for hackers."

"The only reason you would go there is to find vulnerable systems on the Internet," he said.

The website's intention is actually good, he said. The purpose is to expose vulnerabilities and shame companies into fixing the problems. The result is that the bugs are sitting there for everyone to see and potentially exploit for a cyber-attack.

One Russian security company posted 100 vulnerabilities within supervisory control and data (scada) systems that ultimately affected 60,000 devices reachable through the Internet.

While the company's intentions may have been good, or it was just trying to call attention to itself, "it just made life easier for hackers," Harper said.

"The dangerous part here is that the people who own these devices don't know they are on Shodan. It is being used by cyber-espionage players," he added.

Companies and consumers should regularly check the site to ensure "that their dirty laundry isn't being aired," he said.

The proliferation of new, popular applications only provides hackers with more opportunities, said Dan Barber, cybersecurity business unit director at Engility.

"Our attackers are getting more and more sophisticated and so they are targeting things like healthcare IT systems, which is obviously a hot button issue this year," he said. "Our adversaries blow me away sometimes with how creative they are."

Twitter stores GPS coordinates, for example, and that can be used to build trust. A hacker may learn that someone works in the Pentagon, too. The hacker can in turn trick someone into believing he works in the Pentagon. It is one more stepping stone to goading someone into clicking on an attachment or link that contains malware.

Christman predicted that the theft of healthcare data is going to be on the rise. Medical files contain lots of useful information for hackers and criminals. Credit card data accumulates there, along with personal information that can be sold for the purpose of identity theft.

Barber said zero-day vulnerabilities are found in new applications.

"This is where our adversaries gain the most ground — paying attention to the new hot things and trying to exploit their software," Barber said.

Along with new applications, there are thousands of devices being connected to the Internet and almost no attention is paid to securing them, said Harper. Firmware security promises to get more attention in the coming year.

"It is similar to where we were with the Internet in mid-1990s. It was like the Wild, Wild West — there were systems everywhere with vulnerabilities," he said.

Nuclear power plants, scada systems, medical devices, cameras, photocopiers, thermostats, vehicles, printers, routers, baby monitors — they are all increasingly part of the "Internet of things."

"What we have is billions of small computers running outdated operating systems and applications full of vulnerabilities," Harper said. And they are in homes, businesses and government offices.

He recently went to Office Depot and bought three consumer Wi-Fi enabled devices. Within a week he was able to break into all three — two of them "right off the bat," he said.

A hacker could take control of someone's insulin pump through a BlueTooth device and send him into a sugar coma, he said. Wi-Fi enabled cameras are sometimes used to monitor sensitive places, he added.

"Not a lot of security focus has been given to these devices and they are everywhere. We as experts are starting to assert that if we don't do something about this problem … the attackers are going to start to recognize it. We are already starting to see malware and worms written just for the purpose of attacking firmware," Harper said.

"We don't have a good way to find the [bugs] and fix them at this point," he added.

Christman said a new approach to cybersecurity that is going to get under way in earnest this year is continuous diagnostics and monitoring, or CDM. It is a "predictive" rather than a "reactive" strategy.

Instead of trying to reinforce a network's perimeter with firewalls, it looks at users' behavior on their computers.

CDM will try to anticipate security violations before they happen.

Organizations have a lot more data available to them on the internal workings of their networks than what or who is trying to penetrate their defenses from the outside, he explained.

"They [the employees] haven't necessarily done anything wrong, but they are doing something strange," he said. For example, why is someone changing his password five times in a month rather than only once as required? Or maybe an employee clicks on a lot of attachments.

Looking for user anomalies may help security professionals react to the unknown before it happens, Christman said.

Otherwise, "you're always a cycle behind, if not several cycles behind. You've got to patch and keep up to date on the newest threats, but if you just do that, you are ignoring the potential threats," he said.

Correction: The original article misstated Allen Harper's title and misidentified the nationality of the security firm that posted vulnerabilities on Shodan.

Photo Credit: Thinkstock

http://www.nationaldefensemagazine.org/archive/2014/March/Pages/DefenseCompaniesFacingArrayofNewCyberthreats.aspx