In case you missed it

Some of the interesting reports from this week you may have missed. Read more at washingtonpost.com.

Pentagon reverses rules on black hairstyles

A number of popular black hairstyles, including twists and bigger braids, will be allowed across most branches of the military after the relaxation of restrictions that sparked criticism from black service members and lawmakers when they were announced in April.

washingtonpost.com/national

Rights group sees crimes in Egyptian crackdown

Egyptian security forces likely committed crimes against humanity by carrying out mass killings of anti-government demonstrators last summer, Human Rights Watch said in a report. The group called for former military chief Abdel Fatah al-Sissi, now Egypt's president, to be investigated.

washingtonpost.com/world

Manassas principal resigns after fake-résumé claims

Robin Anthony Toogood II, principal of Jennie Dean Elementary School since 2009, resigned at the end of June and forfeited his Virginia teaching and administrative license. Officials said he claimed to have a doctorate in education but in fact had never received even an undergraduate degree.

washingtonpost.com/local

L.A. Clippers' sale to Ballmer finalized

After 33 years under Donald Sterling, the NBA team changed hands this week. On Tuesday, the league announced that Steve Ballmer, the former Microsoft chief executive, had closed the deal on his record $2 billion purchase.

washingtonpost.com/sports

CORRECTIONS

• An article about global trekker Karl Bushby in this weekend's Washington Post Magazine, which was printed in advance, misstates Zach Guglin's job. Guglin is a producer at Westward Productions, a company founded by Beau Willimon and Jordan Tappis.

• An Aug. 14 Sports article about a dispute between the Washington Nationals and the Baltimore Orioles over their television-rights fees misspelled the last name of Joseph Leccese, the chairman of the Proskauer Rose law firm.

The Washington Post is committed to correcting errors that appear in the newspaper. Those interested in contacting the paper for that purpose can:
E-mail: *corrections@washpost.com*.
Call: 202-334-6000, and ask to be connected to the desk involved — National, Foreign, Metro, Style, Sports, Business or any of the weekly sections. Comments can be directed to The Post's reader advocate, who can be reached at 202-334-7582 or *readers@washpost.com*.

The Washington Post

NEWSPAPER DELIVERY
For home delivery comments or concerns contact us at *washingtonpost.com/subscriberservices* or send us an email at *homedelivery@washpost.com* or call 202-334-6100 or 800-477-4679

TO SUBSCRIBE
800-753-POST (7678)

TO ADVERTISE
washingtonpostads.com
Classified: 202-334-6200
Display: 202-334-7642

MAIN PHONE NUMBER
202-334-6000

TO REACH THE NEWSROOM
Metro: 202-334-7300; *metro@washpost.com*
National: 202-334-7410; *national@washpost.com*
Business: 202-334-7320; *business@washpost.com*
Sports: 202-334-7350; *sports@washpost.com*
Reader Advocate: 202-334-7582; *readers@washpost.com*

TO REACH THE OPINION PAGES
Letters to the editor: *letters@washpost.com*

Published daily (ISSN 0190-8286).
POSTMASTER: Send address changes to The Washington Post, 1150 15th St. NW, Washington, DC. 20071.
Periodicals postage paid in Washington, D.C., and additional mailing office.

Foreign security services buy spyware tool

SPYWARE FROM A1

specialized, high-speed network hardware. Until then CloudShield had sold its CS-2000 device, a multipurpose network and content processing product, primarily to the Air Force and other Pentagon customers, who used it to manage and defend their networks, not to attack others.

CloudShield's central role in Gamma's controversial work — fraught with legal risk under U.S. export restrictions — was first uncovered by Morgan Marquis-Boire, author of a new report released Friday by the Citizen Lab at the University of Toronto's Munk School of Global Affairs. He shared advance drafts with The Post, which conducted its own month-long investigation.

The prototype that CloudShield built was never brought to market, and the company parted ways with Gamma in 2010. But Marquis-Boire said CloudShield's work helped pioneer a new generation of "network injection appliances" sold by Gamma and its Italian rival, Hacking Team. Those devices harness malicious software to specialized equipment attached directly to the central switching points of a foreign government's national Internet grid.

The result: Merely by playing a YouTube video or visiting a Microsoft Live service page, for instance, an unknown number of computers around the world have been implanted with Trojan horses by government security services that siphon their communications and files. Google, which owns YouTube, and Microsoft are racing to close the vulnerability.

Citizen Lab's report, based on leaked technical documents, is the first to document that commercial spyware companies are making active use of this technology. Network injection allows products built by Gamma and Hacking Team to insert themselves into an Internet data flow and change it undetectably in transit.

The report calls that "hacking on easy mode," in which "compromising a target becomes as simple as waiting for the user to view unencrypted content on the Internet."

Attacks of that kind were the stuff of hacker imaginings until this year, when news accounts based on documents provided by former National Security Agency contractor Edward Snowden described a somewhat similar NSA program code-named QUANTUMINSERT.

"It has been generally assumed that the best funded spy agency in the world would possess advanced capability," the Citizen Lab report says. "What is perhaps more surprising is that this capability is being developed by Western vendors for sale on the commercial market."

Hacking Team and the company that now owns CloudShield denied any wrongdoing. Messages left with Gamma went unreturned.

The "custom payload" that Hacking Team uses to compromise YouTube injects malicious code into the video stream when a visitor clicks the play button. The user sees the "cute animal videos" he expects, according to Citizen Lab, but the malicious code exploits a flaw in Adobe's Flash video player to take control of the computer.

Another attack, custom-built for use on Microsoft pages, uses Oracle's Java technology, another common browser component, to insert a back door into a victim's computer.

Security and privacy advocates have identified those vulnerabilities before, but the two companies regarded them as hypothetical. In response to a bug report in September 2012, which warned of a potential YouTube attack, Google's security team responded that the use of unencrypted links to send video "is expected behavior." Google closed the discussion with the tag "WontFix."

> ***"What is perhaps more surprising is that this capability is being developed by Western vendors for sale on the commercial market."***
>
> Citizen Lab report

'Against our will'

After Marquis-Boire disclosed to them confidentially last month that their services are under active attack, Google and Microsoft began racing to close security holes in networks used by hundreds of millions of users.

"I want to be sure there's no technical means for people to take a user's data against our will," Eric Grosse, Google's vice president for security engineering, said in an interview. "If they want to do that, they need to use legal means and we pursue that."

Google and Microsoft executives said they are accelerating previous plans to encrypt their links to users across a wider range of their services. Encryption scrambles e-mail, stored files, video and other content as it travels from their servers to a user's computer or mobile device. That step, as far as security engineers know, effectively prevents most attacks in current use.

Since learning of Marquis-Boire's findings in mid-July, Google has encrypted a majority of YouTube video links, and Microsoft has changed default settings to prevent unencrypted log-ins on most live.com services.

"There's a lot of products to update so we're not at 100 percent yet but we're actively engaged with all the teams," Grosse said, acknowledging that Google Maps, Google Earth and other services still connect to users in ways that can easily be intercepted.

Grosse said comprehensive use of encryption should now be regarded as a basic responsibility of Internet services to their users.

"We're probably already [encrypted] to a sufficiently high level that I would guess our adversaries are already having to scramble and shift to some other widely-used service that has not gone to SSL," he said, referring to a form of encryption called the secure socket layer, which is indicated by a padlock icon on some browsers.

Matt Thomlinson, Microsoft's vice president of security, said in a statement that his company "would have significant concerns if the allegations of an exploit being deployed are true."

"We have been rolling out advanced security across our web properties to continue to help protect our customers," he added.

In computer circles, any unencrypted data is known as "cleartext." Marquis-Boire, expanding on a theme that other security researchers have emphasized since disclosures of National Security Agency programs began 14 months ago, said "the big take-away is that cleartext is just dead."

"Unencrypted traffic is untrustworthy," he said. "I would describe this as a sad reality of today's Internet. The techno-Utopian, libertarian ideology of the '90s didn't foresee that the Internet would be as militarized as it is now. People with authority and power have decided to reserve the right to 'own' Internet users at the core. So in order to be safe you need to walk around everywhere wrapped in encryption."

'Lawful intercept'

The computer exploitation industry markets itself to foreign government customers in muscular terms. One Gamma brochure made public by WikiLeaks described its malware injection system, called FinFly ISP, as a "strategic, countrywide" solution with nearly unlimited "scalability," or capacity for expansion. Hacking Team, similarly, says it provides "effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities."

In rare comments to the general public, the companies use the term "lawful intercept" to describe their products and say they do not sell to customers on U.S., European or U.N. black lists.

"Our software is designed to be used and is used to target specific subjects of investigation," said Eric Rabe, a U.S.-based spokesman for Hacking Team, in an extended e-mail interview. "It is not designed or used to collect data from a general population of a city or nation."

He declined to discuss details of the Citizen Lab report, which is based in part on internal company documents leaked to Marquis-Boire, but he appeared to acknowledge indirectly that the material was authentic.

"We believe the ongoing Citizen Lab efforts to disclose proprietary Hacking Team information is misguided, because, if successful for Citizen Lab, it not only harms our business but also gives the advantage to criminals and terrorists," he said.

CloudShield's founder, Peder Jungck, who oversaw the company's relationship with Gamma before departing for a job with the British defense giant BAE Systems, did not respond to requests for comment.

Confidants of the CloudShield engineer, who has since left the company after becoming disillusioned with its surveillance work, identified him as Eddy Deegan, a British citizen. Deegan's LinkedIn profile says he worked for the company as a professional services engineer during the period in question. Reached by telephone in France, Deegan declined to confirm or deny the identity of his external customer in late 2009.

"Nothing came of the work I was involved in at the time," he said. "I asked, and was assured that nothing illegal was undertaken. I have no further comment."

U.S. export restrictions, enforced by the Commerce Department, require a license for any foreign sale of technology described in the relevant statute as "primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications."

Jennifer Gephart, the media relations director for Leidos, which now owns CloudShield, declined to say whether the company had applied for an export license for the Gamma project. The transactions in question took place "prior to our company's acquisition of CloudShield," she said, but "to our knowledge" they were "handled in accordance with applicable regulations."

Gephart confined her statement to the sale of CloudShield's CS-2000 hardware. When asked about the company's development of custom software to turn the device into a spyware delivery system, she declined to respond.

Robert Clifton Burns, who specializes in export controls at the law firm Bryan Cave, said that "surreptitious listening devices are covered and the software for that is also covered on the Commerce Control List."

The regulations are complex and inconsistent, he said, and an authoritative legal judgment would require more facts. CloudShield might argue, he said, that malware injection is not "primarily useful" for surreptitious eavesdropping because it can also be used to track a target's location, take photographs or steal electronic files. Although more intrusive, those attacks were not covered under the rules that applied in 2009.

The Gamma Group lists no e-mail address or telephone number on its Web site. No one responded to a lengthy note left on the company's "Contact" page.

Muench, who has left his old job for a new position in France, read a LinkedIn message requesting an interview. He did not respond. In the past he has dismissed human rights concerns as unproven and defended Gamma's products as vital for saving innocent lives. "The most frequent fields of use are against pedophiles, terrorists, organized crime, kidnapping and human trafficking," he told the New York Times two years ago.

Security researchers have documented clandestine sales of Gamma and Hacking Team products to "some of the world's most notorious abusers of human rights," said Ron Deibert, the director of Citizen Lab, a list that includes Turkmenistan, Egypt, Bahrain and Ethiopia.

At CloudShield, executives knew the identity of at least one prospective customer for the system Deegan built. A former manager told The Post, with support from records obtained elsewhere, that CloudShield sent Deegan to Oman to plan a deployment for one of the country's internal security services. The sale did not go through.

In its annual assessment of human rights that year, the State Department reported that Oman "monitored private communications" without legal process in order to "suppress criticism of government figures and politically objectionable views."

'A push market'

CloudShield did not see itself as a cloak-and-dagger company. It made its name for high-end hardware that could peer deeply into Internet traffic and pull out and analyze "packets" of data as they flew by.

The flagship product five years ago, the CS-2000, could not only look inside the data flow, but select parts of it to copy or reroute. That made it a good tool for filtering out unwanted data or blocking certain forms of cyberattack.

But hardware that could block data selectively could also rewrite innocent traffic to include malicious code. That meant the CloudShield product could be used for attack as well as defense, a former executive said.

CloudShield began pitching its product for offensive use, focusing on U.S. customers because of export controls.

"The basic motivations are pretty straightforward," said one former senior manager there. "It was a push market. We were trying to sell boxes. It was a very conscious effort to target lawful intercept as a space where you could legitimately apply these kinds of technologies."

Two former employees said that Muench, the Gamma executive, traveled to Sunnyvale, Calif., in 2009 in hopes of striking a business relationship. Jungck, CloudShield's founder and chief technology officer, said he could not export that kind of technology and sent Muench home.

But the leadership team reconsidered, and hit upon a plan. They believed that Deegan could do the work for Gamma without triggering U.S. export controls as long as CloudShield's U.S. operations had nothing to do with it.

"I think we all had qualms in the beginning," said one former executive who took part in the deliberations. "I think we rationalized a way in which we felt comfortable with it. Part of that rationalization was to keep it outside the U.S., limit it to that environment where that project was."

What first appeared as an absorbing technical challenge for Deegan began to take a darker cast. His prototype system could inject any of "254 trojans," or all of them, into a targeted computer. If it failed once, it would keep trying, up to 65,000 times.

He was proud of his technical accomplishments, he told confidants, but was no longer sure he had done the right thing. After meeting prospective customers in Oman, his qualms grew worse.

In the end, the Oman deal fell through, and other efforts, with other partners failed, too. CloudShield and Gamma parted ways, and Gamma found another hardware supplier. Deegan's prototype, according to Marquis-Boire and a CloudShield insider, may have sped development of the flagship surveillance product that Gamma brought to market the following year.

bart.gellman@washpost.com

Julie Tate contributed to this report.