



Learn more about how IBM Tivoli Endpoint Manager can help enterprises address their patch and endpoint security needs

SC Magazine > News > Features > Anti-hack: Retaliatory action against digital attacks

FEATURES

Anti-hack: Retaliatory action against digital attacks

Deb Radcliff July 01, 2010

PRINT | EMAIL | REPRINT | PERMISSIONS | TEXT: A | A | A | Tweet 0 | Like Confirm

Has the time come to take retaliatory action against digital attacks? And if so, where is the line drawn? **Deb Radcliff** reports.



At about the time U.S. Cyber Command (USCYBERCOM) was being forged out of the National Security Agency, a startup named Mykonos Software was creating a technology to positively identify and take direct action against website attackers.

What do these events have in common?

USCYBERCOM, charged with coordinating computer-network defense and directing U.S. cyberattack operations, will support the Department of Defense's new cyberwar mission, including offensive actions. There will be some crossover into the private sector in cases under Presidential Order. At the same time, the emergence of offensive tools in the private sector represents a renewed interest in taking action against attackers even without being driven by authorities.

"The ability to react against known attackers is all technically do-able today," says Marcus Sachs, director of government affairs, national security policy, for Verizon Communications. And the private sector will certainly have to be brought into intelligence cyber operations because the internet is almost entirely run by the private sector while the military networks that USCYBERCOM is charged to protect are all run over those public backbones. Sachs has also served a variety of roles in infrastructure security leadership through the Department of Homeland Security and the White House.

The biggest question holding retaliatory measures back has been and will be: Is this type of activity legally do-able, he says, adding, "I don't think those legal and policy roadblocks are going to go away anytime soon."

A call to cyberwar?

Laws and policy were acknowledged as problematic to USCYBERCOM's mission by Lt. Gen. Keith Alexander, NSA director, during his senate confirmation hearing to head USCYBERCOM in May. Senators at the hearing enthusiastically pledged to help overcome some of these legal and policy obstacles for USCYBERCOM's cyber

SC Magazine Video

Find more videos at SC Video

MORE FEATURES

- [Going mobile: Bedford Industries and GroupLogic](#)
- [Case closed: Rausch, Sturm, Israel, Enerson & Hornik, LLC and Vormetric](#)
- [Paying dividends: Financial Services Roundtable](#)
- [The 2012 election & cybercrime](#)
- [Company news: Gerhard Eschelbeck appointed CTO at Sophos, and other corporate happenings](#)

RELATED TOPICS

[Cyber Attacks](#) | [USCYBERCOM](#) | [NSA](#)



MORE IN FEATURES:
[Cybercrime today](#)
[Read More >>](#)

operations.

USCYBERCOM's mission is to integrate the technical capability of military cyber operations and synchronize war-fighting effects to defend the DoD information security environment so as to protect and defend U.S. national security and the lives of men and women in uniform, according to a followup release to the May hearing.

To this end, USCYBERCOM also has authority to aid and assist private sector critical infrastructure organizations when approved by the president, based on Alexander's testimony in May. This includes the sharing of advanced technologies, also mentioned in the Quadrennial Defense Report, released in February. In the report, the DoD officially recognized USCYBERCOM as a new war domain for DoD activities, adding to the other war domains of land, sea, air and space.

Sachs and other experts express worry about the ambiguity of the new USCYBERCOM's mission as the DoD also stands up cyber as a new war command —particularly around its impact on civilian organizations and international relations.

"Whenever the Defense Department has stood up a new command, like NORTHCOM or AFRICOM, they've been clear about their missions and what series of events would have to take place before the capabilities of the command are invoked," Sachs explains. "They're not doing this for cyber and that's worrisome, particularly when U.S. cyber capabilities are already feared internationally."

There's questions about what NSA security technologies will be shared with private sector infrastructure organizations. And if cyberwar policy prevails over the internet, what level of involvement would the private sector have in supporting acts of cyber aggression on behalf of the U.S.?

USCYBERCOM's public affairs officer would not answer what the offensive nature of these acts would be or the potential involvement from private sector in these acts because information like this is classified. And, in his senate testimony, Alexander tread gingerly over invasion-of-privacy questions as they pertain to the private sector organizations that he acknowledged would have to be involved in cyber operations because they essentially support the military networks. There would also be crossover in infrastructure emergencies, he acknowledged.

Fed up enough?

While the Defense Department can't say what the private sector's involvement may be in offensive actions against attackers, market indicators may reveal that some private sector organizations, at least, are fed up enough to take more stringent action against attackers – beyond the passive detection and blocking that they do today.

For example, Rochester, N.Y.-based Synergy Global Solutions, a cloud-based managed security services provider, is installing Mykonos for advanced security services that will be offered at a premium to its customers.

The tool can track back to the real attacker's browser with enough accuracy to launch a counterattack. It does this by sending HTML code containing fake vulnerabilities to the requesting browser. If the browser starts mounting an attack against that vulnerability, the tool runs the attacker through paces to see if it's a skilled attacker or merely a botnet.

Further, the tool can place an encrypted cookie on the offending browser to monitor the attacker, or to send a

iStudy uWin

Get tools to help you study for any (ISC)² exam, and a **FREE iPad2**.

[Click here](#)

(ISC)²

Most Popular

Most Emailed

Most Recent

- [Malicious apps discovered in Android Market](#)
- [Anonymous claims new Monsanto-related hack](#)
- [Four charged with hacking Subway, other retailers](#)
- [Blue Coat acquired by equity firm for \\$1.3 billion](#)
- [Vandals hack checkout terminals at California supermarkets](#)
- [Lockheed Martin hit, but not breached, with Adobe zero-day](#)
- [Three "critical" patches to be in Microsoft security update](#)
- [Thirteen patches from Microsoft, including Duqu fix](#)
- [Cyber crime aftermath: Beyond the indictment](#)
- [Yahoo wins \\$610M spam judgment](#)

PEOPLE

RECENT

POPULAR

Recent Comments



John S The phase "We now have ... the most secure credit card processing [hardware] in the industry," should never be used. This is an open invitation to hackers.

message through a web page showing the attacker that his location and activities are known and being monitored. It also has the capability to send reverse attacks against the offending browser.

"Commercially, customers will be happy with the green light features which are mostly detecting blocking and the deep intelligence it can provide through the HTML lures and browser cookies," says Jeff Thorn, director of information security at Synergy. "The stuff that's in red — let's do this or send that to attacker — represents retribution. I don't know if customers will care so much for the counterattack measures."

Neither does Rob Lee, director of the forensics firm Mandiant. He sees organizations putting additional resources into the "cool" factor of going after attackers.

"Some of these techniques of using poisoned HTML to observe attackers are already happening," says Lee. "Something like this provides good data for forensics purposes. But for organizations not involved in investigations, their dollars would be better spent on website assessment, monitoring and having a really smart team."

Like Sachs and Lee, Winn Schwartau, who in the early 1990s authored a definitive book, *Information Warfare*, questions the legal scenarios under which offensive acts are launched — from hiding an encrypted cookie on the attacking browser to being able to tweak the tool to reverse an attack and intrude deeper into that computer to gather data. Private sector organizations generally have more leeway in terms of putting cookies on visiting browsers, but are limited to what they can do with said cookies. As well, government agencies are restricted by more stringent privacy regulations.

Schwartau, chairman of the smartphone security company Mobile Active Defense, also wrote *Time-Based Security*, which includes a process for HTML poisoning to observe attackers and take necessary actions against them when called for. The intelligence community, he says, would be greatly interested in this type of technology for the information it can provide on advanced techniques, as well as for its offensive capabilities.

David Koretz, president of Mykonos, confirms "strong" interest on the part of intelligence and law enforcement agencies in both the information gathering and the reactive capabilities of the tool. He adds that if such organizations want to open the tool up and program it to do things like reverse attacks and searching offending computers, they could certainly do so. The capability, however, is not operational on the commercial product and won't be until the legal ramifications can be worked out, he adds.

Are we on the cusp of taking more direct action against attackers from a private sector scenario? Experts do believe we're getting closer to that day.

"Seventeen years ago when I brought this capability up in my first Pentagon meeting, the lawyers were all over the reasons why we couldn't do this," says Schwartau. "We've obviously developed the capability since then. The threats are much higher today, and the legal and political arena is softening."

Photo (from left): Navy Adm. Eric Olson, U.S. Army Gen. David Petraeus, unidentified, and Air Force Gen. Duncan McNabb prepare to testify on the creation of a 'Cyber Command' to defend the United States from computer attack.

From the July 2010 Issue of SCMagazine

Like Confirm You like this. · Admin Page · Insights · Error
You like this Sign Up to see what your friends like. · Admin

Ads by Google

Industrial Control Survey

Insight on trends impacting ICS operators worldwide. Free report.

www.industrialdefender.com

Four charged with hacking Subway, other retailers - SC Magazine US · 5 hours ago



David Harley Thanks, Sam. I don't think prognostication is completely useless, but I do think your point is 100% valid. There's not much point in panicking about next year's threats when you're still wide open...

Top of the potshots - SC Magazine US · 6 hours ago



serdheim99 David, I couldn't agree more and full disclosure... I'm in marketing. I recently wrote a blog for my company, AlgoSec, about this very same topic. Marketers and reporters alike love to talk about...

Top of the potshots - SC Magazine US · 8 hours ago

community on DISQUS

Powered by Disqus

www.twitter.com/SCMagazine
SC Magazine



eSecurityP Microsoft's "critical" #security bugs are at their lowest level since 2005. <http://t.co/KCKU7wBm> @scmagazine
7 hours ago · reply · retweet · favorite



Otunba_QT RT @eSecurityP: Microsoft's "critical" #security bugs are at their lowest level since 2005. <http://t.co/KCKU7wBm> @scmagazine
7 hours ago · reply · retweet · favorite



netsecu @SCMagazine: Microsoft to begin silently updating IE in 2012 <http://t.co/OvIPohdS>

twitter

Join the conversation

White Papers

Advanced Persistent Threat, (APT), Detection, Mitigation and Prevention: Advanced Persistent Threats (APT) are a type of customized malware ...

VERDASYS

Cyber threat intelligence: In today's environment, potential attackers have all the time they ...