Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Litigation Options For Post-Cyberattack 'Active Defense'

By **Alexander Berengaut and Tarek Austin**
(October 29, 2018, 2:03 PM EDT)

Alexander Berengaut

Tarek Austin

In March 2017, Rep. Tom Graves, R-Ga., introduced a draft bill titled the Active Cyber Defense Certainty Act. The bill would amend the Computer Fraud and Abuse Act to enable victims of cyberattacks to employ "limited defensive measures that exceed the boundaries of one's network in order to monitor, identify and stop attackers."[1] More specifically, the ACDC would empower individuals and companies to leave their own network to ascertain the perpetrator (i.e., establish attribution), disrupt cyberattacks without damaging others' computers, retrieve and destroy stolen files, monitor the behavior of an attacker, and utilize beaconing technology.[2] An updated, bipartisan version of the bill was introduced by Rep. Graves and Rep. Kyrsten Sinema, D-Ariz., in October 2017.[3]

There has been significant debate on whether the types of "self-help" measures that the ACDC expressly authorizes — sometimes referred to as "active defense" — are currently prohibited by the CFAA. While no court has yet ruled on the issue, several commentators (and the U.S. Department of Justice) have long argued that because the CFAA prohibits accessing computers without "authorization," cyberattack victims expose themselves to criminal liability if they venture outside their network to unmask an attacker and disrupt, disable or destroy the attacker's system.[4] The purpose of the ACDC is to reduce legal uncertainty by, in effect, providing a statutory safe harbor for victims of cyberattacks to "hack back" — under the right circumstances, and subject to limitations.

In addition to the legal question of whether active defense is currently barred by the CFAA, the desirability of active defense as a policy matter has also been debated. Advocates of the ACDC have argued that companies, no matter how sophisticated their preventive cyber defenses, continue to suffer major breaches, and that the number of cyberattacks far exceeds the government's ability to identify and prosecute criminals. They argue that in a lopsided cyber battlefield, victims need additional tools to actively respond to ongoing attacks. In critics' view, however, the bill will promote cyber-vigilantism by victims who are overeager to aggressively strike back at cyber intruders and thieves — thereby creating tit-for-tat patterns of retribution and a significant risk of collateral damage to innocent third-party computer systems.

While the legal and policy debates raised by the ACDC are important, they often overlook the fact that victims of hostile cyber activity may already be able to avail themselves of the judicial process to lawfully engage in the types of "active defense" measures that the ACDC would expressly authorize. Several such techniques of "active defense through litigation" are relatively well-established; others are untested. Because active defense through litigation necessarily involves the judicial process, moreover, it can be relatively time-consuming (particularly in comparison with the more immediate responsive measures contemplated by the ACDC). Although courts can provide certain forms of expedited relief in a matter of days or even less, this time frame may be prohibitive in some cases. Nevertheless, for victims of cyberattacks that are weighing an active response, it may be worth considering one or more of these options.

The most established and typical form of active defense through litigation is using third-party discovery to obtain information about the perpetrators of a cyber-intrusion and, potentially, establishing "attribution" of the culprit. In Liberty Media Holdings LLC v. Does 1-59, for example, hackers unlawfully accessed copyrighted materials on a company's protected website.[5] The company brought suit against the unknown culprits — named "John Does" in the complaint — for violating the CFAA, the Electronic Communications Privacy Act and the Copyright Act.[6] It then provided the court with the internet protocol addresses of each defendant.[7] The court granted the company's motion that it be allowed to serve subpoenas on the defendants' internet service providers and cable providers to compel them to "produce all documents and/or information sufficient to identify the users of the IP addresses."[8]

A more sophisticated form of active defense through litigation involves victims obtaining injunctions and restraining orders to combat ongoing cyberthreats. In Luxottica Group SpA. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," an owner of eyewear brands brought a Lanham Act action against hundreds of defendants alleged to infringe on its trademarks via a thousand domains and 50 online marketplaces.[9] Just over a week later, Luxottica obtained from the court an order mandating that domain-name registries transfer the defendants' domain names to Luxottica.[10] The order further instructed a host of third parties who serviced defendants — marketplaces, web hosts, search engines, banks, third-party processors, etc. — to immediately cease all interactions with them and provide Luxottica expedited discovery as to the defendant's identities, locations and operations.[11]

Through similar mechanisms, technology companies have invoked the courts' equitable powers to craft injunctive relief enabling them to disrupt large-scale cybercrime. In 2010, for example, Microsoft Corp. brought suit in federal court in the Eastern District of Virginia against 27 John Doe defendants registered as the owners of domain names used for botnet communications.[12] Charging that defendants utilized a global illegal network of millions of computers infected with malware — a botnet named "Waledac" — to send spam email and steal information, account credentials, and funds, the complaint asserted violations of the CFAA, the CAN-SPAM Act, the ECPA, false designation of origin and trademark dilution under the Lanham Act, trespass to chattels, conversion, and unjust enrichment.[13] Microsoft obtained from the court a sealed temporary restraining order that ordered the defendants' domain registry, VeriSign, to "lock" their domains, hold them in escrow, and preserve evidence of misconduct.[14] In subsequent years, Microsoft pursued similar actions against other botnets and malicious actors.[15]

Because both Microsoft and the Luxottica plaintiffs alleged trademark infringement, they were able to take advantage of a powerful tool in the Lanham Act: a provision that empowers courts to grant ex parte orders for the seizure of equipment involved in the production of counterfeit trademarks.[16] The Lanham Act is not the only statute that contains this remedy, however. Notably, the recently enacted Defend Trade Secrets Act permits a party to seek, on an ex parte basis, an order providing for the seizure

of property "necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[17] The DTSA's ex parte seizure procedure sets a high bar for obtaining the remedy, and few motions for ex parte seizure thus far have been successful.[18] But for cyber-victims that have lost trade secrets as part of a cyber-intrusion, the DTSA is an additional potential tool to consider as part of an active defense strategy.

Even outside the statutory contexts of the Lanham Act and the DTSA, there are potential vehicles to enlist the courts' assistance in undertaking an active defense strategy. Courts have broad powers to grant equitable relief in connection with other statutory or common-law causes of action. As the U.S. Supreme Court has explained, "once a right and a violation have been shown, the scope of a district court's equitable powers to remedy past wrongs is broad, for breadth and flexibility are inherent in equitable remedies."[19] Indeed, the CFAA — in play whenever a computer has been accessed without authorization — expressly contemplates "injunctive relief or other equitable relief."[20] Such relief is also available to plaintiffs who assert claims under state computer-crime laws or common law claims for computer trespass and conversion.

One such equitable remedy is the writ of replevin, a traditional prejudgment process involving the seizure by U.S. marshals of property alleged to have been illegally taken or wrongfully withheld. This historic common-law writ, now often governed by state statutes, has been commonly used to take property from an individual wrongfully in possession of it and return it to its rightful owner. Subject to variations in state statutory law, plaintiffs invoking the writ generally must establish that they are the owner of the property, that they have a right to immediate possession of it, and that the defendant wrongfully took or detained the property.[21] In some states, a plaintiff who can show an urgent risk that the defendant will destroy or conceal the property is eligible to obtain an ex parte seizure order without prior notice to the defendant.[22]

Although historically the writ of replevin has been used to recover only tangible goods and chattels, some courts have recently held that plaintiffs can invoke replevin statutes to recover stolen or wrongfully withheld electronic data. For instance, in SEIU Healthcare v. Evergreen, the court held that a nonprofit organization could obtain seizure via replevin of electronic spreadsheets that it alleged another nonprofit had illegally purchased from a former employee.[23] The court reasoned that Washington's replevin statute "does not distinguish between tangible and intangible property," and that what matters instead is "whether the property can be taken back from the defendant and returned to the plaintiff."[24]

To be sure, in many cases of cyber theft the replevin remedy would likely be unavailable, insofar as data stolen via a cyberattack may be difficult to trace and locate and may not qualify as a "specific, identifiable item of personal property," as required by some replevin statutes.[25] But even then, this traditional, well-established mechanism for seizure of wrongfully taken property could still prove a useful reference point for courts assessing the scope and types of injunctive relief that they have authority to issue pursuant to their broad equitable powers.

Ultimately, the writ of replevin, like the ex parte seizure provisions of the Lanham Act and DTSA, illustrate the diversity of mechanisms through which plaintiffs may enlist the assistance of the courts in engaging in the type of active defense measures contemplated by the ACDC.

Alexander A. Berengaut is a partner and Tarek J. Austin is an associate at Covington & Burling LLP.

[1] Active Cyber Defense Certainty Act: Bipartisan Bill Empowers Americans to Develop New Defenses Against Cyber Attacks, https://tomgraves.house.gov/uploadedfiles/acdc_expaliner.pdf

[2] Id.

[3] H.R. 4036, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/4036

[4] Office of Legal Education, Department of Justice, Prosecuting Computer Crimes (2010), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

[5] Liberty Media Holdings, LLC v. Does 1-59, No. 10-1823, 2011 WL 292128 (S.D. Cal. 2011).

[6] Id. at *1.

[7] Id. at *2.

[8] Id. at *1.

[9] Amended Complaint, Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Aug. 25, 2016), 2016 WL 8577031.

[10] Sealed Temporary Restraining Order, Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322, at 12 (N.D. Ill. Sept. 1, 2016), ECF No. 30.

[11] Id. at 12-15.

[12] Complaint, Microsoft Corp. v. John Does 1-27, No. 1:10-CV-00156 (E.D. Va. Feb. 22, 2010), ECF No. 1.

[13] Id. at 1, 7-10, 14.

[14] Ex Parte Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, Microsoft Corp. v. John Does 1-27, No. 1:10-CV-00156, at 5 (E.D. Va. Feb. 22, 2010), ECF No. 13.

[15] E.g., Complaint, Microsoft Corp v. John Does 1-11, No. 2:11-cv-00222 (W.D. Wash. Feb. 9, 2011) (Rustock botnet); Complaint, Microsoft Corp. v. John Does 1-39, 1:12-cv-01335 (E.D.N.Y. March 19, 2012) (Zeus botnet); Complaint, Microsoft Corp. v. John Does 1-18, 1:13-cv-00139 (E.D. Va. Jan. 31, 2013) (Bamital botnet).

[16] 15 U.S.C. § 1116(d)(1)(A).

[17] 18 U.S.C. § 1836(b)(2)(A)(i).

[18] 18 U.S.C. § 1836(b)(2)(A)(ii); Beusse Wolter Sanks & Maire, PLLC, How Has the Defend Trade Secrets Act Fared Two Years After Enactment? (July 9, 2018), http://www.bwsmiplaw.com/blog/2018/07/09/how-has-the-defend-trade-secrets-act-fared-two-years-after-enactment/

[19] Hills v. Gautreaux, 425 U.S. 284, 297 (1976).

[20] 18 U.S.C. § 1030(g).

[21] E.g., Cornelio v. Stamford Hosp., 717 A.2d 140, 143 (Conn. 1998).

[22] E.g., Conn. Gen. Stat. Ann. § 52-278e; Kan. Stat. Ann. § 60-1005.

[23] SEIU Healthcare Nw. Training P'ship v. Evergreen Freedom Found., No. 76220-6-I, 2018 WL 4691593 (Wash. Ct. App. Oct. 1, 2018).

[24] Id. at *7; see also Chefs Diet Acquisition Corp. v. Lean Chefs, LLC, No. 14-cv-8467, 2016 WL 5416498, at *7 (S.D.N.Y. Sept. 28, 2016) (replevin of electronic customer lists).

[25] Chefs Diet, 2016 WL 5416498 at *7.