Cybersecurity Law Report
An Acuris company

DOJ Guidance on How Companies Should Pursue Stolen Data on the Dark Web

By Matt Fleischer-Black, *Cybersecurity Law Report*

Large corporations are turning to external surveillance of criminal web forums to defend their networks. This threat intelligence research involves visiting web forums where criminals and black hats solicit and sell malware samples, security vulnerabilities and stolen data. The DOJ's recent guidance, "Legal Considerations When Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources," addresses the growing market for cyber threat intelligence services.

The guidance, issued in February 2020, looks at risky activities for private security practitioners on forums, including posing questions, exchanging information and buying purloined data. The Cybersecurity Law Report spoke to John Carlin, a partner at Morrison & Foerster and former Assistant Attorney General of the DOJ's National Security Division, about the Department's motivations for issuing this guidance, its tips and suggested practices, compliance programs for threat research efforts and shifting expectations around corporate interactions with the dark web.

See "Are Companies Turning a Blind Eye to Their Lost Data on the Dark Web?" (Mar. 25, 2020).

DOJ Encourages Companies to Gather Intelligence

CSLR: What led DOJ to issue this guidance?

Carlin: It was hearing from counsel and from companies that wanted to go into the business of gathering threat intelligence, and from victim companies wondering whether they could hire third parties to search for and collect information on the dark web. DOJ wanted to clarify the permitted practices for the sector, and encourage companies that are committed to compliance to enter this space in a safe way.

CSLR: Why is the DOJ encouraging companies to gather intelligence?

Carlin: Everyone recognizes that this burgeoning dark market of criminal activity is well-funded. It's well-organized. It operates with the sophistication and speed that we see in regular e-commerce. There is a lot of intelligence available to gather, but there's a gap. The government simply doesn't have enough resources to monitor all dark web areas. It is trying to put more resources to monitoring the space and work with partner agencies but, even so, the dark web has exploded and continues to grow.

At the policy level, the Justice Department sees that organizations with good motives and strong compliance programs can be allies in collecting intelligence that can benefit victims and, ultimately, law enforcement. Confusion over what the law allows was acting as a deterrent to such organizations.

CSLR: Who has been contacting the Department about intelligence-gathering concerns, and for how long?

Carlin: There have been one-off questions to DOJ, and also from groups of outside counsel who practice in this space, including our firm.

Questions about this dated back to when I was at Justice, over four years ago. But the questions have increased over the last couple of years, as the sophistication and number of companies entering the threat intelligence space has increased.

[See "Prosecuting Borderless Cyber Crime Through Proactive Law Enforcement and Private Sector Cooperation" (Mar. 2, 2016).]

Companies Have Been Operating in Gray Areas

CSLR: Does the DOJ commonly issue guidance on computer crime?

Carlin: Unlike other divisions, the Computer Crime Intellectual Property Section (CCIPS) has issued other guidance documents in recent years that promote lawful cybersecurity practices. This guidance is an example of DOJ leaning forward to solve a problem outside of prosecutors' usual toolkit of arrests, charging documents and trials. Technology is changing far more quickly than the law can keep up, so it is often unclear how to apply the law to new situations.

On some issues, companies and lawyers would ask for clarity on a statute, or hypotheticals on how it might apply, and DOJ did not want to answer so that organizations would err on the side of caution in interpreting the statute.

DOJ's lack of guidance on intelligence gathering had created perverse incentives. Smaller companies outside the United States are more willing to operate on the edge, and have been jumping into some of the riskiest activities. Bigger cybersecurity vendors that are committed to compliance and legal clarity had been limiting their activities on the dark web – leaving a smoother path for crooks, or some of the nation-states behind the scenes, to victimize innocent consumers and companies.

CSLR: What have the "edgy" companies done that is risky?

Carlin: They have hacked their way to restricted parts of the dark web forum, for example, using their own malware or tools. Or, to prove bona fides to the crooks in charge, they may have committed small criminal acts, or helped facilitate criminal activity. Some will act to disrupt the bad guys, by hacking back, for example.

Maybe nobody prosecutes that. But the DOJ's guidance now calls many of those activities highly risky.

CSLR: What is the impact of the guidance?

Carlin: The language of the statute alone, without the gloss of how it's being interpreted by prosecutors, created uncertainty about whether well-intentioned threat intelligence services might run afoul of the letter of the law. Lawyers could not point to a public document to reassure clients that they were properly interpreting the law. Many security professionals are ex-law enforcement or come from government agencies and want to comply with the law. They're mission oriented. They get frustrated when lack of clarity means they can't look at evidence or information that they know is right there and could help their clients.

Hacking and disruption were things that security people could do lawfully in their prior lives as government actors. You can't when you're operating on your own.

The benefit to the DOJ is that it can now shape the behavior of both victim companies and those consulting companies that have sprung up in this space to help navigate the dark web. Besides giving counsel a solid basis for legal advice, the guidance helps by describing some trends in what the criminal groups are doing.

[See "Goodbye to the Blame Game: Forging the Connection Between Companies and Law Enforcement in Incident Response" (Apr. 19, 2017).]

Gathering Intelligence Becomes Standard Practice

CSLR: Are more large companies gathering cyber threat intelligence?

Carlin: Yes. It's becoming standard practice for large companies to use intelligence to protect their systems. A growing number of companies have, as part of their defensive program, a component for reviewing dark web and other online resources for indications that the company's information had

been compromised. The expectation is not universal. It will depend on a company's sector, the type of information it holds and the digital services it offers.

If a company has an incident and sensitive data has been lost, it will now often take steps to figure out whether that information is for sale online.

You see a range of companies wrestling with whether they should develop their own capability for intelligence gathering or hire someone who has the capability.

CSLR: Is it also standard now for companies to go outside their networks to disrupt adversaries' activities?

Carlin: Because of the legal issues, in part, no, there's not an expectation that you're going to go out and take down the botnet attacking your company. Only some who work in this space, like Microsoft and government actors, have capabilities for that, and legal teams to guide what they do. Other companies are instead expected to develop defense-in-depth and protect their own systems. This includes asking, "How can I look outside my system to see if, unbeknownst to me, I had an incident inside the system?"

[See "ISAO Organization Releases a Roadmap to Cyber Threat Information Sharing" (Oct. 5, 2016).]

DOJ Suggestions and Scenarios

CSLR: Which intelligence-gathering scenarios does the guidance discuss?

Carlin: DOJ issued this guidance in response to the evolution of dark web forums. After law enforcement succeeded with takedowns of a number of dark web forums, the owners of such forums wised up to lurking by law enforcement and threat intelligence researchers. So forum owners created new roadblocks, like requiring payments or proof of bona fides, which created uncertainty around what threat intelligence researchers could do to access such forums.

The DOJ guidance clearly advises that it's okay for companies to use a fake name to access the dark web sites. But they should

not use stolen credentials or assume the identity of a real individual.

CSLR: The DOJ guidance states that passively collecting intelligence in a forum where criminals are discussing crime typically is legal. Is that helpful advice?

Carlin: You used to be able to lurk more easily. You could use a fake name, then watch what's going on and get intelligence. Now some websites don't let you lurk, to deter outsiders.

A harder issue is what you can say on criminal forums. Asking questions about illegal activity or getting advice is generally OK, but longer conversations that discuss technical information are riskier because you might provide assistance that facilitates a criminal act.

DOJ gives some practical tips. One is to deconflict. Don't accidentally end up on the wrong side of the criminal investigation because the government doesn't know who you are. That will eventually get straightened out, but it's a waste of law enforcement resources, and not pleasant for companies to be on the wrong side.

CSLR: Is anything preventing intelligence vendors or client companies from notifying the FBI about their plans to gather dark web intelligence?

Carlin: It feels unusual to seek the attention of law enforcement. If you're in a compliance department, you spend a lot of time thinking it's a bad day to get a call from the FBI.

The FBI and Secret Service have tried to be victim-oriented here. They spell out that it would be beneficial to inform law enforcement before you engage in these activities. Early engagement ensures that you don't unintentionally interfere with an ongoing investigation. And they provide contact information.

CSLR: DOJ includes two broadly-phrased tips: "Be neither a perpetrator nor a victim," and "deliberately assess your risk." Are those difficult for companies to practice?

Carlin: It depends very much on your business model and compliance program. The DOJ made clear that gathering intelligence is ultimately a risk/benefit decision for each company. The document "strongly recommends" that

companies consult with their in-house and outside counsel, someone who practices and advises companies in this space, because the risks are changing fast, and we're going to see the technology and criminal groups evolve in their methods.

[See "DOJ Encourages Cyber Incident Reporting and Advance Planning With Best Practices Guidance" (May 20, 2015).]

Compliance Programs for Gathering Intelligence

Cybersecurity Vendors

CSLR: The guidance's first recommended best practice is creating "rules of engagement." What should those include?

Carlin: The guidance gives companies performing these types of activities as a service a good roadmap. Create a compliance guide that lays out clear, bright lines, specifying activities you cannot do, and lines that cannot be crossed. Make it real – use actual examples in the "Don't" category, and in the "OK" category.

You want to have rules for when staff confront hard situations. Note the instances that require employees to ask for higher-level approval and consult with legal counsel. You want to set rules stating what the investigators need to document and which company tools to use for documentation, so it is auditable.

CSLR: How can companies implement the DOJ guidance's statement that they should "Be Prepared To Be Investigated"?

Carlin: Because the dark web hosts criminals, companies should engage in elaborate work-through with counsel before starting intelligence activities, so they truly can point to their rules of engagement or a compliance program if questioned.

The person investigating might end up communicating with a designated terrorist or sanctioned entity in a dark market, or purchasing data from one, which is a strict liability regime. Government officials who are assessing under a strict liability regime evaluate the conduct of a company just like in other

know-your-customer spaces. They will look at what type of compliance program the company implemented. What were its rules of engagement and what steps did it take to avoid breaking the rules?

Companies definitely want to train their employees. Government intelligence actors train their undercover agents. Government officials examining a company would expect to see a version of that.

[See "Designing, Implementing and Assessing an Effective Employee Cybersecurity Training Program (Part One of Three)" (Feb. 17, 2016); Part Two (Mar. 2, 2016); and Part Three (Mar. 16, 2016).]

Client Corporations

CSLR: What questions must companies ask the cybersecurity vendors they hire for intelligence gathering?

Carlin: Companies should design a vendor questionnaire to make sure that the vendor has a robust compliance system to avoid unlawful activities and a set of guardrails in place for the intelligence gathering, or the data buyback, that it will do for you.

A company does not need to know in detail, depending on its appetite for risk, what the vendor's program looks like. It can, however, use this DOJ guidance to make sure that it covers each of the issues: how to access a forum; the behavior to take once you access the forum; and rules for the purchase of stolen data.

Have language that requires it to comply with the law, which sounds obvious, but in this space some companies engage in activities that are gray to black. They're doing it for a good purpose and motive, but they may be violating the law.

Make sure, as DOJ suggests, that the vendor consults with outside counsel in developing the compliance program, because these are the folks at the tip of the spear, who see how the bad guys' methods are evolving. They see the problems that poses for gaining intelligence.

Explaining the Threats to Upper Management

CSLR: What best practices should companies follow for using the threat intelligence they collect?

Carlin: You're increasingly seeing information security professionals brief relevant corporate committees and the board regarding the threat environment. The guidance provides some questions that management and compliance departments should be asking and the type of information that the information security team should provide to them

It's helpful to provide the board or committees a threat report that offers a sense of the top risks in the company's sector, what the trends are in the activity of criminal and nation-state groups, and describes the company's profile online. These sorts of reports can inform spending decisions, and they can inform how the company phrases its risk factors for investors if it is a public company. There's a real appetite for such reports in upper management.

[See "Report Shows Strategic Buy-In From Executive Leadership Is the Key Driver of Successful Risk Mitigation" (Aug. 07, 2019).]

CSLR: The document discusses buying back data that, it turns out, includes information or assets belonging to another company, which surely makes the entire C-suite nervous. What's the best practice when that happens?

Carlin: This problem is one of the reasons you're seeing victim companies shy away from buying data on the dark web, even if it's their own. Companies are hiring vendors instead, believing it will become the vendor's problem, not theirs.

The guidance suggests that if you didn't know, and you had no reason to know, that the stolen data that you bought belongs to others, "there is little chance" of prosecution. If a company ends up with data that belongs to others, however, it can cause investigative scrutiny. The DOJ encourages companies to sequester data purchased on the dark web, avoid access to it, and immediately contact law enforcement.

[See "FBI Veteran Discusses Using Law Enforcement's Cyber Resources to Improve Security and Obtain Board Buy-In" (Nov. 2, 2016).]

What Remains Uncertain?

CSLR: Are there areas where the DOJ guidance lacks clarity?

Carlin: It just leaves open the question of civil liability if you deal with one of the designated entities. Another one it leaves somewhat open is what are the rules of the road for making ransomware payments. That's a hard question.

We may find a new set of questions that we will require DOJ clarification. You're going to continually have to reevaluate what problems you're encountering in this space. There have been a lot of shifts already, and it's going to keep changing.