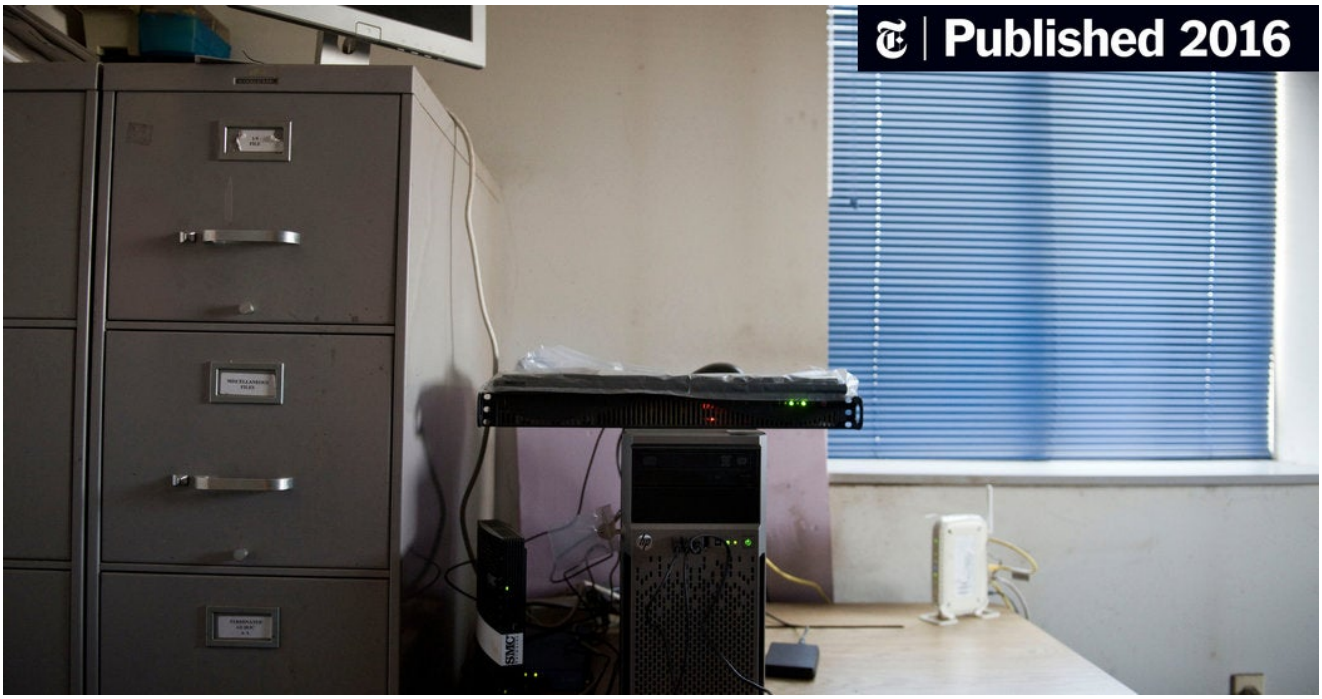
The Chinese Hackers in the Back Office

nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html

Nicole Perlroth June 11, 2016



Continue reading the main story

BELLEVILLE, Wis. — Drive past the dairy farms, cornfields and horse pastures here and you will eventually arrive at Cate Machine & Welding, a small-town business run by Gene and Lori Cate and their sons. For 46 years, the Cates have welded many things — fertilizer tanks, jet-fighter parts, cheese molds, even a farmer's broken glasses.

And like many small businesses, they have a dusty old computer humming away in the back office. On this one, however, an unusual spy-versus-spy battle is playing out: The machine has been taken over by Chinese hackers.

The hackers use it to plan and stage attacks. But unbeknown to them, a Silicon Valley start-up is tracking them here, in real time, watching their every move and, in some cases, blocking their efforts.

"When they first told us, we said, 'No way,'" Mr. Cate said one afternoon recently over pizza and cheese curds, recalling when he first learned the computer server his family used to manage its welding business had been secretly repurposed. "We were totally freaked out," Ms. Cate said. "We had no idea we could be used as an infiltration unit for Chinese attacks."

On a recent Thursday, the hackers' targets appeared to be a Silicon Valley food delivery start-up, a major Manhattan law firm, one of the world's biggest airlines, a prominent Southern university and a smattering of targets across Thailand and Malaysia. The New York Times viewed the action on the Cates' computer on the condition that it not name the targets.

The activity had the hallmarks of Chinese hackers known as the C0d0s0 group, a collection of hackers for hire that the security industry has been tracking for years. Over the years, the group has breached banks, law firms and tech companies, and once hijacked the Forbes website to try to infect visitors' computers with malware.

There is a murky and much hyped emerging industry in selling intelligence about attack groups like the C0d0s0 group. Until recently, companies typically adopted a defensive strategy of trying to make their networks as impermeable as possible in hopes of repelling attacks. Today, so-called threat intelligence providers sell services that promise to go on the offensive. They track hackers, and for annual fees that can climb into the seven figures, they try to spot and thwart attacks before they happen.

These companies have a mixed record of success. Still, after years of highly publicized incidents, Gartner, a market research company, expects the market for threat intelligence to reach $1 billion next year, up from $255 million in 2013.

Remarkably, many attacks rely on a tangled maze of compromised computers including those mom-and-pop shops like Cate Machine & Welding. The hackers aren't after the Cates' data. Rather, they have converted their server, and others like it, into launchpads for their attacks.

These servers offer the perfect cover. They aren't terribly well protected, and rarely, if ever, do the owners discover that their computers have become conduits for spies and digital thieves. And who would suspect the Cate family?

Two years ago, the Cates received a visit from men informing them that their server had become a conduit for Chinese spies. The Cates asked: "Are you from the N.S.A.?"

Image
Cate Machine & Welding, a family-run business in rural Wisconsin, is at the center of a spy-versus-spy battle.Credit...Lauren Justice for The New York Times
One of the men had, in fact, worked at the National Security Agency years before joining a start-up company, Area 1, that focuses on tracking digital attacks against businesses. "It's like being a priest," said Blake Darché, Area 1's chief security officer, of his N.S.A. background. "In other people's minds, you never quite leave the profession."

Mr. Darché wanted to add the Cates' server to Area 1's network of 50 others that had been co-opted by hackers. Area 1 monitors the activity flowing into and out of these computers to glean insights into attackers' methods, tools and websites so that it can block them from

hitting its clients' networks, or give them a heads-up days, weeks or even months before they hit.

The Cates called a family meeting. "People work really hard to make products, and they're getting stolen," Ms. Cate said. "It seemed like the least we could do." Area 1 paid for the installation cost, about $150.

Shortly after installing a sensor on the machine, Mr. Darché said his hunch was confirmed: The sensor lit up with attacks. Area 1 began to make out the patterns of a familiar adversary: the C0d0s0 group.

Area 1 was founded by three former N.S.A. analysts, Mr. Darché, Oren Falkowitz and Phil Syme. The three sat side by side at Fort Meade, tracking and, in some cases, penetrating adversaries' weapons systems for intelligence. A little over two years ago, they decided to start their own company and raised $25.5 million in funding from major venture capitalists and security entrepreneurs in Silicon Valley, including Kleiner Perkins Caulfield & Byers and Cowboy Ventures, and security veterans like Ray Rothrock, the chief executive of RedSeal, and Derek Smith, the chief executive of Shape Security.

Area 1 is a new player in threat intelligence, a nascent subsector of the security business that includes companies like iSight Partners and Recorded Future that track attackers in underground web forums and on social media, gleaning intelligence about them.

Threat intelligence is still more art than science. The jury is still out on whether companies are equipped to use that intelligence to thwart hackers. Area 1 claims that it can head off attacks through the compromised servers it is tracking. It can also use its vantage point to see where attackers are setting up shop on the web and how they plan to target their intended victims.

A handful of Area 1 customers confirmed that its technology had helped head off attackers. One client, a chief information security officer at a large health care provider, said the health care sector had been slammed by digital criminals and governments in recent years. He asked that the company not be named, to avoid becoming a more visible target.

He credited Area 1's sensors with blocking several attacks on his network, helping his company avoid the fates of the health insurer Anthem, which was breached by Chinese hackers last year, and a growing number of hospitals hit by attacks that have forced them to pay a ransom to get important information back.

Mr. Smith, the chief executive of Shape Security, said Area 1 gave his company warning of three attacks before they happened, providing time to block them. Mr. Smith said he was impressed enough that he made a small investment in Area 1.

“Many of these mom-and-pop shops are ambivalent because the attacks don’t directly impact their business and revenue,” he said. “Meanwhile, they unwittingly operate this attack infrastructure.”

But Area 1’s business model can pose ethical dilemmas. What does the company do when it sees attacks against prominent companies and government agencies who are not Area 1 customers?

“We think of ourselves as a bodyguard, not a police force that runs around telling everyone they’re a victim,” said Mr. Falkowitz, Area 1’s chief executive. “We’re in the business of pre-emption.”

Image
Tools used by the Cate family at its welding shop in Belleville, Wis.Credit...Lauren Justice for The New York Times
They do warn some victims, he said. For instance, they tipped off a law firm, a manufacturer, a financial services firm and electronics company that were attacked via the Cates’ server after they saw the C0d0s0 hackers make off with their intellectual property. Some of those victims, including the law firm, later signed up for Area 1 services.

Not all companies heed the warning. A security consultant for one victim, who spoke on the condition of anonymity because of nondisclosure agreements, said that his client chose not to act on a tip from Area 1 last year out of concern that a scandal over a successful online attack against the company would jeopardize its recent acquisition. It figured its acquirer would not have been thrilled to learn that the start-up’s proprietary technology was now in Chinese hacker’s hands.

Posted on the wall of Area 1’s headquarters in a historic house in Redwood City, Calif., is a list titled “45 Things That Are Harder Than Cybersecurity.” It includes flight, solar power, the flu vaccine, brain surgery, the internet, heart transplants, skyscrapers, the Thermos and the Q-tip.

Mr. Falkowitz disagrees with a growing concern that it is too difficult or impossible to stop online attacks. As attackers have grown more sophisticated, many security companies have stopped believing they can block attacks with traditional defenses like antivirus software. Instead, many focus on trying to detect an intrusion “in real time,” to catch hackers before they steal too much.

Eighty percent of the time, victims learn they have been breached only when law enforcement or someone else shows up with their stolen data, according to Verizon, which tracks breach data.

At the N.S.A., Mr. Falkowitz had worked with teams that detected North Korean missile launches. Much of that early work was done with satellites that would look for sudden heat blasts.

Eventually, Mr. Falkowitz's team tried a more proactive approach. If they could hack the computers that controlled the missile launch systems, they could glean launch schedules. Area 1 is now taking a similar approach to digital attacks, tapping into the attackers' launchpads, as it were, rather than waiting for them to attack.

Hackers don't just press a big red "attack" button one day. They do reconnaissance, scout out employees on LinkedIn, draft carefully worded emails to trick unsuspecting employees to open them and click on links or email attachments that will try to launch malicious attacks.

Once they persuade a target to click — and 91 percent of attacks start this way, according to Trend Micro, the security firm — it takes time to crawl through a victim's network to find something worth taking. Then they have to pull that data off the network. The process can take weeks, months, even years and leaves a digital trail.

Area 1 watches for this kind of activity and then teams up with firms like Blue Coat, a web security company, to build what it has learned into security software that can try to block attacks when they come.

The owners of Cate Machine & Welding say that living with Chinese attackers in your office can be a strange feeling. Recently, Area 1 executives visited the shop and showed them some of what they had learned from watching their computer. The C0d0s0 group had used their server to pilfer a law firm's due diligence on an impending acquisition, a financial services firm's confidential trading plans, a mobile payment start-up's proprietary source code, some blueprints and loan applications at a mortgage company.

Hearing that, Mr. Cate expressed pride — and maybe even a hint of schadenfreude. For years, the welding business that is his family's bread and butter has been migrating to China. Now his family is helping American businesses fight back.

"We want to do the right thing for these businesses," Mr. Cate said, "For our country."