FUTURE TENSE | WHAT'S TO COME? | NOV. 12 2014 1:37 PM

The Mercenaries

Ex-NSA hackers and their corporate clients are stretching legal boundaries and shaping the future of cyberwar.

By Shane Harris

Illustration by Charlie Powell

Excerpted from **@War: The Rise of the Military-Internet Complex** *by Shane Harris. Out now from Houghton Mifflin Harcourt.*

Bright twenty- and thirtysomethings clad in polo shirts and jeans perch on red Herman Miller chairs in front of silver Apple laptops and sleek, flat-screen monitors. They might be munching on catered lunch—brought in once a week—or scrounging the fully stocked kitchen for snacks, or making plans for the company softball game later that night. Their office is faux-loft industrial chic: open floor plan, high ceilings, strategically exposed ductwork and plumbing. To all outward appearances, Endgame Inc. looks like the typical young tech startup.

It is anything but. Endgame is one of the leading players in the global cyber arms business. Among other things, it compiles and sells zero day information to governments and corporations. "**Zero days**," as they're known in the security business, are flaws in computer software that have never been disclosed and can be secretly exploited by an attacker. And judging by the prices Endgame has charged, business has been good. Marketing documents show that Endgame has charged up to $2.5 million for a zero day subscription package, which promises 25 exploits per year. For $1.5 million, customers have access to a database that shows the physical location and Internet addresses of hundreds of millions of vulnerable computers around the world. Armed with this intelligence, an Endgame customer could see where its own systems are vulnerable to attack and set up defenses. But it could also find computers to exploit. Those machines could be mined for data—such as government documents or corporate trade secrets—or attacked using malware. Endgame can decide whom it wants to do business with, but it doesn't dictate how its customers use the information it sells, nor can it stop them from using it for illegal purposes, any more than Smith & Wesson can stop a gun buyer from using a firearm to commit a crime.

Advertisement

Endgame is one of a small but growing number of boutique cyber mercenaries that specialize in what security professionals euphemistically call "active defense." It's a somewhat misleading term, since this kind of defense doesn't entail just erecting firewalls or installing antivirus software. It can also mean launching a **pre-emptive or retaliatory strike**. Endgame doesn't conduct the attack, but the intelligence it provides can give clients the information they need to carry out their own strikes. It's illegal for a company to launch a cyberattack, but not for a government agency. According to three sources familiar with Endgame's business, nearly all of its customers are U.S. government agencies. According to security researchers and former government officials, one of Endgame's biggest customers is the National Security Agency. The company is also known to sell to the CIA, Cyber Command, and the British intelligence services. But since 2013, executives have sought to grow the company's commercial business and have struck deals with marquee technology companies and banks.

Endgame was founded in 2008 by Chris Rouland, a top-notch hacker who first came on the Defense Department's radar in 1990—after he hacked into a Pentagon computer. Reportedly the United States declined to prosecute him in exchange for his working for the government. He started Endgame with a group of fellow hackers who worked as white-hat researchers for a company called Internet Security Systems, which was bought by IBM in 2006 for $1.3 billion. Technically, they were supposed to be defending their customers' computers and networks. But the skills they learned and developed were interchangeable from offense.

Rouland, described by former colleagues as domineering and hot-tempered, has become a vocal proponent for letting companies launch counterattacks on individuals, groups, or even countries that attack them. "Eventually we need to enable corporations in this country to be able to fight back," Rouland said during a panel discussion at a conference on ethics and international affairs in New York in September 2013.

Rouland stepped down as the CEO of Endgame in 2012, following embarrassing disclosures of the company's internal marketing documents by the hacker group Anonymous. Endgame had tried to stay quiet and keep its name out of the press, and went so far as to take down its website. But Rouland provocatively resurfaced at the conference and, while emphasizing that he was speaking in his personal capacity, said American companies would never be free from cyberattack unless they retaliated. "There is no concept of deterrence today in cyber. It's a global free-fire zone." One of Rouland's fellow panelists seemed to agree. Robert Clark, a professor of law at the Naval Academy Center of Cyber Security Studies, told the audience that it would be illegal for a company that had been hacked to break in to the thief 's computer and delete its own purloined information. "This is the most asinine thing I can think of," Clark said. "It's my data, it's here, I should be able to delete it."

To date, no American company has been willing to say that it engages in offensive cyber operations designed to steal information or destroy an adversary's system. But former intelligence officials say "hack-backs"—that is, breaking into the intruder's computer, which is illegal in the United States—are occurring, even if they're not advertised. "It is illegal. It is going on," says a former senior NSA official, now a corporate consultant. "It's happening with very good legal advice. But I would not advise a client to try it."

A former military intelligence officer said the most active hack-backs are coming from the banking industry. In the past several years banks have lost billions of dollars to cybercriminals, primarily those based in Eastern Europe and Russia who use sophisticated malware to steal usernames and passwords from customers and then clean out their accounts.

In June 2013, Microsoft joined forces with some of the world's biggest financial institutions, including Bank of America, American Express, JPMorgan Chase, Citigroup, Wells Fargo, Credit Suisse, HSBC, the Royal Bank of Canada, and PayPal, to disable a huge cluster of hijacked computers being used for online crime. Their target was a notorious outfit called Citadel, which had infected thousands of machines around the world and, without their owners' knowledge, conscripted them into armies of "botnets," or clusters of infected computers under the remote control of a hacker, which the criminals used to steal account credentials, and thus money, from millions of people. In a counterstrike that Microsoft code-named Operation b54, the company's Digital Crimes Unit severed the lines of communication between Citadel's more than 1,400 botnets and an estimated 5 million personal computers that Citadel had infected with malware. Microsoft also took over servers that Citadel was using to conduct its operations.

Microsoft hacked Citadel. That would have been illegal had the company not obtained a civil court order blessing the operation. Effectively now in control of Citadel's victims—who had no idea that their machines had ever been infected—Microsoft could alert them to install patches to their vulnerable software. In effect, Microsoft had hacked the users in order to save them. (And to save itself, since the machines had been infected in the first place owing to flaws in Microsoft's products, which are probably the most frequently exploited in the world.)

It was the first time that Microsoft had teamed up with the FBI. But it was the seventh time it had knocked down botnets since 2010. The company's lawyers had used novel legal arguments, such as accusing criminals who had attacked Microsoft products of violating its trademark. This was a new legal frontier. Even Microsoft's lawyers, who included a former U.S. attorney, acknowledged that they'd never considered using alleged violations of common law to obtain permission for a cyberattack. For Operation b54, Microsoft and the banks had spied on Citadel for six months before talking to the FBI. The sleuths from Microsoft's counter-hacking group eventually went to two Internet hosting facilities, in Pennsylvania and New Jersey, where, accompanied by U.S. marshals, they gathered forensic evidence to attack Citadel's network of botnets. The military would call that collecting targeting data. And in many respects, Operation b54 looked like a military cyberstrike. Technically speaking, it was not so different from the attack that U.S. cyber forces launched on the Obelisk network used by al-Qaida in Iraq.

Microsoft also worked with law enforcement agencies in 80 countries to strike at Citadel. The head of cybercrime investigations for Europol, the European Union's law enforcement organization, declared that Operation b54 had succeeded in wiping out Citadel from nearly all its infected hosts. And a lawyer with Microsoft's Digital Crimes Unit declared, "The bad guys will feel the punch in the gut."

Microsoft has continued to attack botnets, and its success has encouraged government officials and company executives, who see partnerships between cops and corporate hackers as a viable way to fight cybercriminals. But coordinated counterstrikes like the one against Citadel take time to plan, and teams of lawyers to approve them. What happens when a company doesn't want to wait six months to hack back, or would just as soon not have federal law enforcement officers looking over its shoulder?

NEWS & POLITICS

POLITICS

NOV. 12 2014 8:02 PM

Less Firing, More Hiring

The VA shouldn't focus on cleaning house. What the agency needs is truckloads of doctors and nurses.

Josh Voorhees

No, Republicans Aren't Going to Impeach Obama

Why China Is Finally Shouldering (Some of) the Burden

An Auction in Pennsylvania Where the Items up for Bid Are Guns Used in Suicides

The FBI Might Have Mistaken Me for a Terrorist. I Was Just a Teenager.

SLATE PLUS

SLATE ARCHIVES

NOV. 11 2014 12:25 PM

Slate Voice: "Stop Dressing Like a Slob When You're Traveling"

J. Bryan Lowder defends looking nice on a flight or train.

J. Bryan Lowder

***Walking Dead* Podcast: Listen to Slate-sters Recap Episode 5**

***Doctor Who* Podcast: Recapping the Finale Episode**

***Slate*'s Working Podcast, Episode 5 Transcript: How Perfumers Work**