The Most Dangerous People On The Internet in 2015

December 30, 2016

The world has never been so safe. In the long view of civilization, no time in history has ever seen so few deaths from disease or violence.

But 2015 didn't feel very safe. And that's in part because the Internet has brought the world's dangers closer than ever before, both in awareness and influence. In 2015, ISIS could broadcast directly into the West to terrorize and recruit new members through Twitter and Facebook. A presidential candidate could spew racist hate-speech directly to his millions of followers on those same networks. And hackers could reach into Americans' most sensitive guts and spill them on the open web.

Every year, WIRED names the individuals who embody the world's dangers in digital form. Our list isn't limited to those who merely threaten public safety, but also those who threaten the status quo and the world's power structures, for better or for worse. These are the dangerous characters we've been watching in 2015.

Donald Trump

No one needs to check their party registration to see that Donald Trump is a demagogue, more interested in inciting backward fears and playing to Americans' worst prejudices than addressing global problems. With more than 5.3 million twitter followers, Trump also has the largest online platform of any presidential candidate. And he's used it to support rhetoric that slanders Mexicans as rapists and bans Muslims from entering the United States. Those inflammatory and carefully engineered remarks only fuel the propaganda of anti-American forces like ISIS, trading Americans' actual security for a cheap boost to a billionaire's ego.

ISIS

Even before the Paris attacks, ISIS had become synonymous with danger. And this ultra-violent, pseudo-religious, apocalyptic cult uses the internet like no jihadist group ever has before, with tens of thousands of social media accounts that are created as fast as Facebook and Twitter can ban them. But when WIRED asked social media extremism expert Humera Khan who she thought was the single person who most represents ISIS online, she corrected us, calling ISIS's online presence an "adaptive swarm" without any permanent face. "It's the ISIS Borg collective that makes it dangerous," she writes, "Not a single individual."

James Comey

Over the last year, FBI director James Comey has become the world's most vocal opponent of encrypted communications. In testimony to Congress, he's warned of a future where encryption causes law enforcement surveillance to "go dark," letting organized crime and terrorism run wild in a lawless digital world. But his arguments against encryption threaten a technology that's long been accepted as a necessary part of a secure internet in an age of ever-increasing data breaches. And despite new encryption tools, surveillance agencies have more data at their fingertips than ever before; even former NSA head Mike McConnell has said that despite rising use of encryption, the internet has made the NSA's surveillance better "than any time in history," and former DHS chief Michael Chertoff has called attempts to oppose encryption "misguided."

Cody Wilson

Cody Wilson, the creator of the world's first fully 3-D printable gun, has made WIRED's "most dangerous" list for years thanks to his efforts to allow anyone to download and print their own working firearm at home. That notion has only become more controversial in a year when gun killings dominated the headlines. And Wilson's non-profit group Defense Distributed advanced his DIY weaponry goal further in 2015 by shipping a computer-controlled milling machine that allows anyone to create a metal body of an AR-15 with no background check or even a serial number. He's also pursuing a lawsuit against the State Department for blocking him from publishing gun files online on the basis that they would represent an illegal weapons export. Wilson's argued that ban represents a first amendment violation—the files are only information, after all, not physical weapons. His case has already won support from the EFF, the Cato Institute, and 16 members of congress.

Verto and Kimble

As 2015 began, a market called Evolution ruled the Dark Web's underground economy, with tens of thousands of listings of drugs for sale alongside weapons and stolen financial information. The site, run by two pseudonymous figures named Verto and Kimble, displayed a darker side of the Dark Web markets, drifting from the Silk Road's ethos of enabling only victimless crime. Then in March, Evolution proved that in a fully anonymous economy, there's no honor even among thieves: The market suddenly went offline, and Verto and Kimble with it. The pair took all the money stored in Evolution's bitcoin accounts, a heist of their own business whose payoff one former employee estimated at $15 million.

Chaouki Bekrar

Hackers have long hired out their intrusion skills to intelligence agencies and sold their techniques to the highest bidder. But no one has brought the digital arms trade into the open like hacker-entrepeneur Chaouki Bekrar. This year, Bekrar founded the zero-day exploit dealer Zerodium, a startup that brokers the sale of those secret software cracking techniques, buying them from independent hackers and reselling them to what Zerodium describes as "government organizations in need of specific and tailored cybersecurity capabilities," as well as private corporations ostensibly using the techniques for defensive purposes. Bekrar has gone so far as to release a public list of prices for exploits, ranging from $50,000 for a technique that breaks Internet Explorer to $500,000 for a tool that cracks the latest version of iOS. Bekrar is hardly

alone in the zero-day exploit industry, an underground economy largely dominated by American defense contractors. But by bringing his business into the open, Bekrar has become the face of that once-secret trade, and may also be opening the zero-day economy to a new crowd of hackers.

Impact Team

There may have been bigger data breaches this year than the one that hit extramarital affairs site Ashley Madison in July. But few, if any, have been quite so damaging to its targets. In August, the hacker or hackers known as Impact Team released a 9.7 gigabyte file containing the personal information of 32 million of Ashley Madison's users. The hackers laid bare the names, email addresses and sexual idiosyncrasies of registered visitors to a site that described itself as "most famous name in infidelity and married dating." The result was an untold number of scandals; two suicides are linked to the breach's revelations. Before releasing the data, Impact Team demanded that Ashley Madison's parent company Avid Life Media shut down due to what it described as fraudulent practices. "We have explained the fraud, deceit, and stupidity of ALM and their members," the group wrote a month later. "Now everyone gets to see their data." Five months after that shocking breach, Impact Team appears to still remain at large.

Phineas Fisher

What's more dangerous than a group of government-sponsored hackers-for-hire? The hacker who hacks them. In July, a pseudonymous figure called Phineas Phisher announced that he'd hacked Hacking Team, the notorious Milan surveillance firm. The resulting 400 gigabytes of leaked data revealed that Hacking Team's customers included regimes with questionable human rights records, including Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Morocco, Nigeria, Oman, Saudi Arabia, and Sudan. But Hacking Team wasn't even Phineas Fisher's first target. Last year he had breached another surveillance firm called Gamma Group, and had even published a DIY guide to other would-be hacktivists. Fisher shows no signs of stopping. "Gamma and HT down," he wrote on twitter in July, "A few more to go. :)"

Julian Assange

This year marked the half-decade anniversaries of many of WikiLeaks' biggest releases, including the Collateral Murder video of a US Apache helicopter firing on civilians in Iraq and the Cablegate database of secret State Department communications. But Julian Assange's secret-spilling group has also experienced a resurgence in 2015, emerging again as one of the web's most prolific providers of contraband information. Starting in June, the group launched a series of NSA leaks revealing the agency's history of spying on allies like France, Brazil, and Japan. It also served as a kind of hacker's clearinghouse, obtaining and publishing searchable files pulled from Hacking Team, Sony, and the email account of CIA director John Brennan. Assange has made clear that WikiLeaks is on the hunt for new digital scandals, too, relaunching its anonymous submission system for leaks after a five-year hiatus and putting a bounty on certain leaked data, like cockpit video of the Kunduz hospital bombing.

Preet Bharara

When a crime takes place online, it's not always easy to determine under whose jurisdiction it falls. But if US Attorney Preet Bharara has any say in the matter, the internet will be policed in

the Southern District of New York. In 2015, Bharara pursued high-profile cybercrime cases as distant as the filesharing don Kim Dotcom in New Zealand and Roger Thomas Clark, the alleged right hand man of the Silk Road, arrested in Thailand. In November, he indicted four individuals for a massive alleged hacking scheme that targeted JP Morgan. But Bharara's biggest feat of the year was the example he made out of Ross Ulbricht, the Silk Road's creator. Ulbricht was convicted on all counts—including a "kingpin" charge usually reserved for mafia dons and drug cartel leaders—and sentenced to life in prison without the possibility of parole.