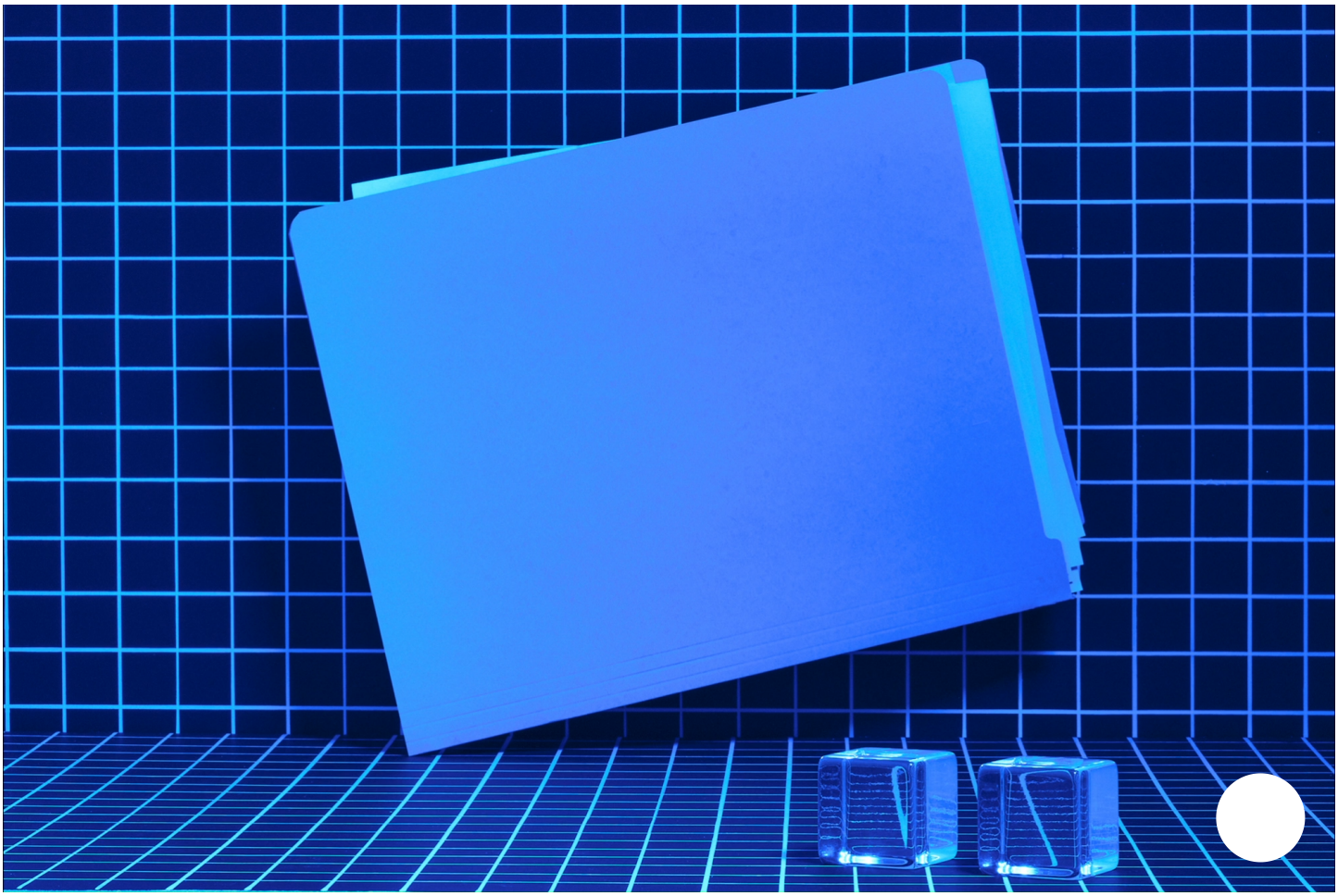


Video: Andrew Williams

SONNER KEHRT BACKCHANNEL SEP 29, 2020 7:00 AM

The Cyber-Avengers Protecting Hospitals From Ransomware

As medical facilities strain amid the pandemic, they're especially vulnerable to cyberattacks. A global coalition of volunteer experts has stepped into the breach.

SAVE

IT WAS EARLY February when Ohad Zaidenberg first started noticing malicious emails and files disguised as information about Covid. He's a cyber intelligence researcher based in Israel, and they were the sort of schemes he encountered all the time—benign-looking messages that trick people into giving someone network access. But more and more of them seemed to be using fear of the new virus as leverage to get people to click a link or download a file. "This little measure can save you," read one email he flagged, before prompting the reader to open a PDF called "Safety Measures." Zaidenberg didn't think too much of it at the time. Coronavirus cases were still mostly confined to China, and it wasn't yet clear the virus would become a global pandemic.

Just over a month later, Zaidenberg went out to dinner. It was his last night out before Israel shut down. Infections were starting to climb, and as he drove back to his home in Tel Aviv, he was thinking about how dangerous everything suddenly seemed. A former intelligence officer with dark hair and a closely cropped beard, Zaidenberg had left the Israeli army with a deep belief in working for peace. Coronavirus is a war, he thought. Then he remembered the malicious documents he'd been seeing. For the most part, they'd seemed benign enough—someone trying to get into a system to spy, for instance. But now something new jolted his mind: What if the malware was instead used to compromise hospital security?

It had already happened three years earlier. In May 2017, computers at National Health Service hospitals all across the UK started displaying a pop-up message demanding users pay $300 in bitcoin to restore access to their files. The ransomware attack, called WannaCry, didn't specifically target hospitals in the UK. In fact, it infected more than 200,000 computers worldwide. But many British hospitals had been running older, more vulnerable Windows operating systems, and once the worm got in, it quickly jumped from computer to computer, encrypting files as it went. Email systems went offline. Doctors couldn't access patient records. Blood test analysis devices and MRI scanners became inoperable, and staff scrambled to cancel surgeries and other appointments—19,000 in all. The attack cost the National Health Service well over $100 million.

As Israel shut down during the pandemic, cyber intelligence researcher Ohad Zaidenberg decided to apply his skills to defending hospitals around the world. PHOTOGRAPH: DUDI HASSON

Zaidenberg could barely bring himself to think what an attack like that would do to hospitals around the world already buckling under a surge of Covid cases. Even a smaller attack could be devastating. Locking doctors out of patient records could easily have life-or-death consequences. If a hospital had to pay a ransom to unlock its systems, perhaps it couldn't buy additional ventilators. People could die.

The next day, Zaidenberg saw the news. The second-largest hospital in the Czech Republic had been attacked. In the early morning hours, an announcement blared over the hospital's PA system, instructing workers to shut down their computers immediately. A few hours later, surgeries were canceled. Luckily, there were fewer than 300 coronaviruses cases in the country at the time, so the hospital wasn't already overburdened. It was, however, one of the Czech Republic's biggest Covid testing centers, and the attack delayed results for a few days.

The Czech incident made it clear to Zaidenberg that his fears were justified. Israel was in the process of locking down, and he knew he would soon have a lot of time on his hands. He also knew his cybersecurity skills could help prevent

attacks like the one in the Czech Republic. After all, he was already monitoring virus-related threats for work. What if there were a way to scale that up globally, a way to alert hospitals—any hospital, anywhere—that they might be vulnerable, *before* an attack happened?

THAT SAME DAY Zaidenberg noticed that Nate Warfield, a Microsoft security manager he'd recently met, was tweeting about the exact same thing. "We as infosec professionals have skills and tools our colleagues supporting the medical field may not," Warfield wrote. "I encourage all of you to do what you can in your communities and regions to help defend them." Zaidenberg messaged him right away. He floated the idea of recruiting a group of cyber threat researchers to work, pro bono, assessing threats related to the virus.

Warfield wrote back less than a minute later: "I would absolutely participate."

WARFIELD, WHO HAS thick, tattooed forearms and an enormous red beard, had traveled to Tel Aviv from his home in Seattle in February. There, he'd given a talk about a recently discovered vulnerability in a piece of hardware called a Netscaler, which helps distribute web traffic across multiple servers. The vulnerability left tens of thousands of companies exposed to remote attackers. After seeing the news from the Czech Republic, he wondered whether any unpatched Netscalers were running on hospital networks. He opened Shodan, a search engine for internet-connected devices, and ran a query for Netscalers, paired with the keyword "health." Six different health care network names popped up.

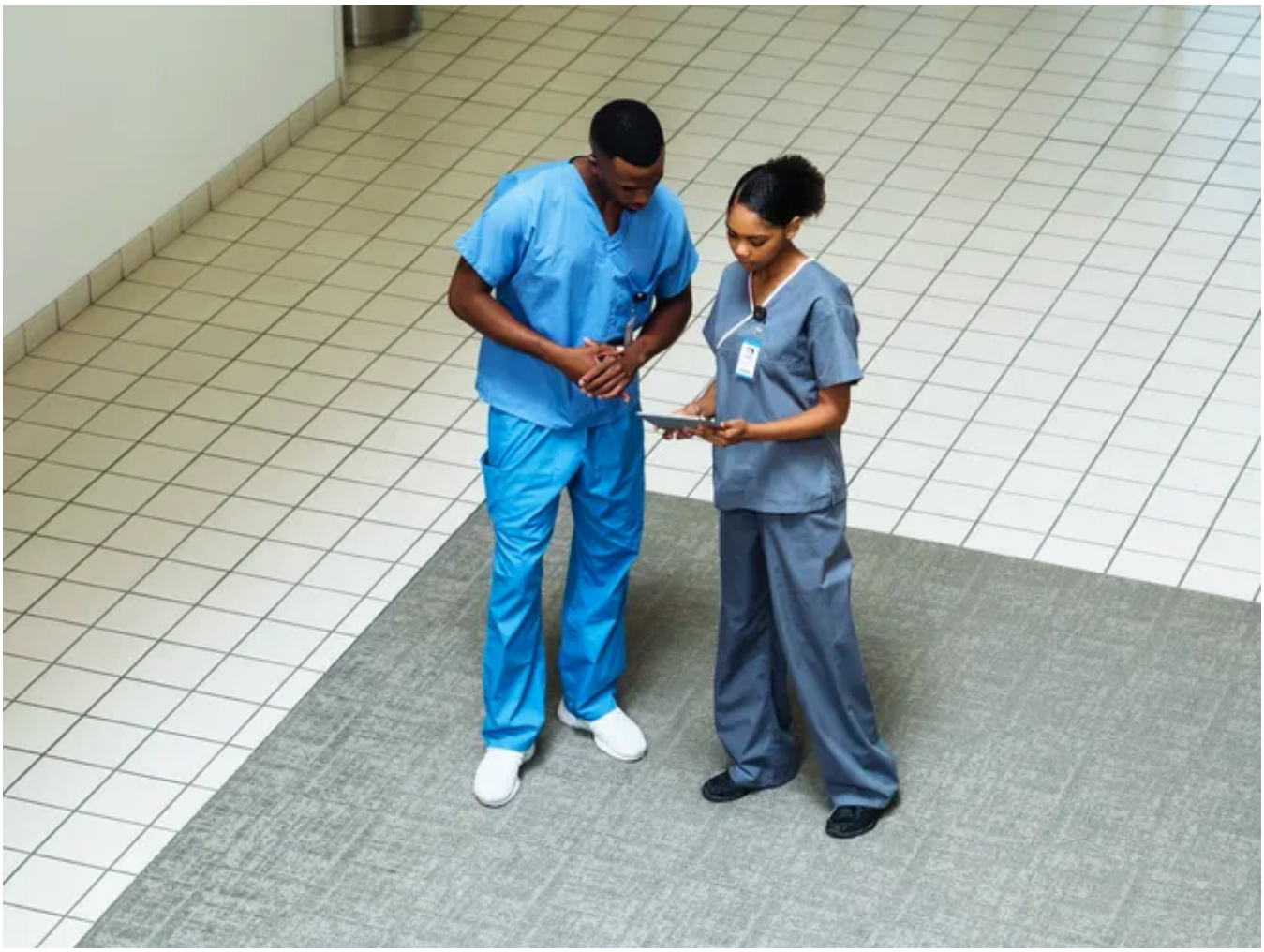
"Oh no," he thought.

That night, he did a more focused search, looking for additional unpatched Netscalers, working through every health-care-related keyword he could think of: "medical," "doctor," "hospital." He also hunted for other vulnerabilities, including one discovered just days before that could travel from machine to machine, letting attackers set their own code loose on computers running Windows 10. By the next day, he'd found 76 unpatched Netscalers and more than 100 other vulnerabilities in health care facilities all across the US. He recognized the names of some of the biggest hospitals in the country. One in particular seemed to jump off the screen —his own doctor's network was running an exposed Netscaler. "When it's your own doctor that's at risk, that's scary," Warfield says. "That's when it really hit home."

Warfield spent almost 45 minutes trying to figure out how to contact his doctor's network IT security team. Finally, he found his way to the LinkedIn page of someone who seemed to work there and sent a message, cramming who he was and the problem he'd found into the 1,900-character limit and hoping he didn't sound like a scammer. As he expected, he never heard back.

"This is not an efficient way to do this," Warfield realized. "I'm never going to be able to contact all these people."

Just before Zaidenberg messaged him, Warfield sent his list of vulnerabilities to Chris Mills, a colleague of his at Microsoft. He hoped Mills would have a better idea of how to get in touch with the hospitals. As it happened, Mills knew people at the Healthcare Information Sharing and Analysis Center, or ISAC. An ISAC is an independent nonprofit that monitors and shares threats specific to particular sectors of the economy—the result of a push two decades ago by the federal government for major industries to better understand the risks they face. Today there are ISACs for everything from the entertainment world to the retail sector to the maritime industry.



A Ransomware Attack Has Struck a Major US Hospital Chain

BY LILY HAY NEWMAN

Mills figured the ISAC would know how to contact the right people at the right hospitals. As he passed the list along, Zaidenberg set up a Slack group for what he'd decided to name the Cyber Threat Intelligence League. A few days later, Warfield sent a message to a group of trusted security researchers he belonged to called the Roadhouse Miscreant Punchers to see if anybody else wanted to join their effort. Mills and Zaidenberg were also spreading the word, and they quickly brought on Marc Rogers, a British expat who oversees cybersecurity at the cloud-based identity management company Okta. Rogers had run security operations at Defcon, one of the world's biggest hacker conventions, for the past decade and seemed to know just about everyone in the cybersecurity world.

Before long, people from around the world were contacting the league, wanting to know if they could get involved. Like so many of us, cybersecurity researchers and threat experts were sitting behind their computers, watching the pandemic

unfold, wondering if there was a way they could help the doctors and nurses working on the front lines. One person, in a message to Zaidenberg, wrote, “I’m feeling useless. I don’t know what to do. I know how to run scripts. I know how to run Java. I know how to analyze malware. In Idaho. I need to do something.”

Cybersecurity experts Marc Rogers (left) and Nate Warfield cofounded the CTI League with Zaidenberg, helping to quickly expand the group's membership and contacts to a global scale. PHOTOGRAPH: DAVID JAEWON OH

IN JUST A few days, Zaidenberg had assembled a team of cybersecurity researchers to look for vulnerabilities in the medical sector. But to expand on what they'd done with Warfield's list of vulnerable Netscalers, they would need hospitals to know who they were and to trust them. "If a hacker goes and knocks on the door of a hospital, especially one that's under stress because of the pandemic and says, 'Hey, I found a vulnerability,' you know, companies historically have not responded well to that," Rogers says. If the league's work was going to be taken seriously, they needed to partner with established organizations that could serve as conduits to would-be victims.

So the league asked the health care and other ISACs for on-going, official support in helping push out information to medical facilities. "People know us and trust us," says Stacey Wright, who works for the Center for Internet Security, which runs two ISACs—one dedicated to threats against state and local governments, the other to threats against election infrastructure. ISAC representatives like Wright brought all of the connections from their day jobs, from law enforcement agencies to local officials across the country, which were now available to help the league spread the word about cyberthreats.

Just a week after Zaidenberg had messaged Warfield, the league was fielding dozens of membership requests a day, taking a Wild West-like approach to building up an infrastructure as new volunteers tossed out ideas. "If you want to donate your time, we're not going to tell you what that looks like," Warfield says. One member developed a bot that pulled data from the Shodan search engine in real time, scanning the internet for vulnerable hardware running on medical networks and automatically posting geolocation and network data to a dedicated Slack channel. Someone else built a bot to monitor BGP changes—BGP is the primary routing protocol for traffic on the internet, and big changes can indicate that someone's hijacked a bunch of IP addresses.

Within a month, the group had well over a thousand members, each vetted for their identities and the skills they could contribute: Were they already members of a trusted cybersecurity group? Could anyone in the league vouch for them? Hospital administrators were joining. Federal-level Computer Emergency Readiness Teams, or CERTs, asked to partner up. When a number of European

CERTs wanted to know if there was a way to see only information on threats in their own countries, a developer in the league built a program to automatically create and send out weekly country-specific bulletins.

Each morning, Warfield would lie in bed and watch messages come in on his phone confirming that patches had been applied. Eventually he got a message from a volunteer who happened to do security consulting for the network that included Warfield's doctor. The hospital had patched its Netscaler vulnerability over the weekend.

IN EARLY JUNE, a member of the Russian dark web forum Exploit posted a message. "Selling access to a large hospital in the EU," the post read. The hospital had 5,000 employees and hundreds of servers. A few days later, the same user, who went by the handle TrueFighter, posted a second, similar message—this time offering administrator access for a hospital in the US. The price was $3,000.

Cyber threats related to Covid aren't limited to vulnerable hardware at hospitals or malicious emails with attachments claiming to list cures. The dark web was exploding with hospital network administrator credentials—both real and fake—for sale. There were piles of stolen patient data. People were selling hydroxychloroquine pills and supposed Covid vaccines. "They shift their business tactic to whatever is the hot item at the moment," says Sean O'Connor, an Atlanta-based league member who specializes in dark web infiltration. "And the hot item at the moment is Covid."

While the initial idea was to help protect hospitals, by this point the league had experts in everything from advanced persistent threats to malware analysis to dark web tracking. It also had raw manpower—members were spread across nearly every time zone. Rather than just searching for vulnerabilities in health care systems, they'd also analyze malware, hunt down malicious websites, pore through repositories of phishing scams, and comb the dark web for compromised medical facility credentials and virus-related scams. "The deeper we go, the more areas we find where we're like, Hey, we can help here, we can help there," Warfield says.

League members organized themselves into teams and fanned out to hunt down Covid-related threats before they could wreak havoc. "We're seeing attacks from every country, going to every country, phishing emails in almost every language known to man," Rogers says. "I've been calling it almost like a world cyberwar."

FROM THE START, Rogers knew that he wanted to involve law enforcement in the league. While working with police as head of security at the Defcon hacker convention, he'd developed a strong conviction that hackers and law enforcement should work with, not against, each other. He knew that the league would eventually run into threats that were also being investigated by law enforcement.

Rogers reached out to FBI agents he knew from Defcon, as well as some contacts at the Department of Homeland Security. Both agencies got on board right away. Then the league put out an invitation to law enforcement through various official and unofficial channels. Today, the group has members from law enforcement worldwide, from the FBI and Interpol to local officers in places as far flung as the Faroe Islands. "We can reach the law enforcement of a large chunk of the planet if we need to," Warfield says.

An Israeli member of the CTI League was searching dark web forums for threats when he saw the posts on Exploit offering hospital access in the EU. Pretending to be an interested buyer, he messaged TrueFighter, asking where the hospital was located. When the answer—Poland—came back, he posted the information to a league Slack channel monitored by law enforcement, where Polish authorities saw it and could respond.

With international law enforcement, CERTs and ISACs, hospital IT teams, and cyber security experts from 80 different countries, the group's Slack channels quickly became a global hub for information about all sorts of malicious activities and threats popping up during the pandemic. The dark web team found scammers selling vials of a virus "cure" for $25,000. One police lieutenant from a township in western Pennsylvania found threats against a 911 call center and a local prosecutor's office. When a vulnerability in a device similar to a Netscaler was discovered in early July, league members spent an entire weekend tracking down devices and alerting vulnerable hospitals.

"It's really an information exchange," said Christopher Krebs, director of DHS's Cybersecurity and Infrastructure Security Agency. In ordinary times, using ordinary channels, it can take a while to reach the person with the right expertise, or the correct organization in the relevant country. But CTI League is like standing in the middle of a crowded room or a town square, Wright tells me. "You just holler out, and chances are somebody's going to pop up and go, 'Yep. I can help.'"

Within the first month alone, they'd found more than 2,000 health care software vulnerabilities in 80 countries. They identified nearly 400 malicious files that were unlikely to be stopped by common antivirus software—things like trojans disguised as instructions on donating to coronavirus relief, which would allow someone to get inside a system, disable protections, and install even more dangerous malware. They also flagged almost 3,000 web domains for takedown. Those websites ranged from slick operations impersonating entities like the World Health Organization and the UN to bottom-of-the-barrel hack jobs cobbled together by opportunists hoping to cash in on the crisis, even if just a little. One website demanded a bitcoin payment without any actual malware or other threat to back up the demand—its creator was apparently just banking on people's fear being enough to scare them into paying.

FEAR IS A powerful motivator. During a time of global panic, it's not difficult for a hacker to find a target, Rogers says. Choosing to click on a link promising to show Covid case numbers in your state isn't a completely irrational decision. But the campaigns he and other league members were seeing capitalized on any number of tall tales circulating on the internet—shelter-in-place orders as a ploy to install 5G towers, certain home remedies as a cure for the disease. You'll never click on a link offering an effective coronavirus vaccine unless you already believe a vaccine exists and for some reason it's not being made available. So Rogers pinged a data scientist he'd been working with over the past couple years. "Hey," he wrote. "How busy are you?"

Sara-Jayne Terp was, in fact, quite busy. She was holed up in Bellingham, Washington, for the pandemic. She'd landed there after spending the previous nine months criss-crossing the US on a one-woman quest to better understand how misinformation affects middle America. At the same time, she was working to adapt the tools of cybersecurity to track such misinformation. By the time Rogers reached out to her, Terp was already running two other groups pursuing that mission.

But Rogers' request was a huge opportunity; he wanted Terp to join the league and head up a team dedicated to misinformation. Terp, who has a background in AI and crisis mapping—using real-time sources in the aftermath of disasters to create a holistic picture of what's happening on the ground—had spent the previous three years arguing that misinfo operations should be viewed as cyberattacks, and that "the infosec crowd," as Terp puts it, is particularly well-positioned to combat the threat. The league offered the chance to set up shop

right in the middle of the community she was trying to get to take on misinformation, so she came aboard and built a team.

One of the first things they began tracking was a yellow poster that appeared on social media in early April, calling for protests against the lockdowns. Terp and her team analyzed the campaign like they would a piece of malware: How did it work? How did it move? What vulnerabilities was it targeting, and what would be the consequences if it were successful? They mined the poster for artifacts—images, associated hashtags, the curious use of the phrase "village piazza"—all of which helped them track the campaign from user to user, and back and forth between websites and social media. The team traced the poster from the US to Canada to a dead end in England, then to Australia, and ultimately, although it made no mention of 5G, to a 5G conspiracy site.

The global uprising the poster called for on April 12 didn't materialize; gatherings were small and sparsely attended. But over the next few weeks, protests against lockdowns grew, spurred on by new social media posts and slightly different hashtags. Terp called the yellow poster an early test case. "It's like somebody is trying something, and it hasn't made it out there yet," she says. Understanding what works and what doesn't, and how that might influence other campaigns, is critical in the fight against misinformation.

When Terp had worked in crisis mapping, she'd seen how the people most affected by disasters were often treated as objects, rather than as a part of the solution. Given the distributed nature of misinformation campaigns, with so many nodes (read: human beings), involving people who might otherwise be victims is critical. "They're not victims," says Terp. "They have agency. They have their own minds." The more people you get involved, she says, the better.

ON A SWELTERING day in early June, I meet Marc Rogers in a park near his home in Moraga, California. A middle-aged former club bouncer from England who's been a hacker since the '80s, he has snake tattoos running down each forearm and a graying goatee that's partly obscured by a sparkly, light-blue mask. We sit down at opposite ends of a picnic table. In Oakland, about 10 miles to the west, protests against police brutality were continuing for the sixth straight day. I ask him about the notion of viewing misinformation as a cyber threat.

All of these bad actors are trying to do the same thing, Rogers says. "You find a vulnerability or weakness—whether that's an absence of information or it's a fear

of something, or it's a natural fault line in society—and then you exploit it. You build a piece of software, you put together a command-and-control infrastructure." Then you push it at the vulnerability and watch things break.

Like Terp, Rogers takes a holistic approach to cybersecurity. First there's physical security, like stealing data from a computer onto a USB drive. Then there's what we typically think of as cybersecurity—securing networks and devices from unwanted intrusions. And finally, you have what Rogers and Terp call cognitive security, which essentially is hacking people, using information, or more often, misinformation. Once, large-scale information campaigns were the sole province of nation-states and perhaps the church. But the tools of influence are now available to anyone with an internet connection.

Rogers tells me the league's misinformation team had recently started tracking campaigns targeting the George Floyd protestors. They'd seen posts saying that antifa was causing riots and that were trying to bait Black Lives Matter supporters to attend protests intentionally scheduled to conflict with second amendment rallies. It was a bit far afield from the league's original mission, but the volume of misinformation was so great and the potential for harm—both viral and violent—so high. "You have sophisticated groups who are doing this, who have great attention to detail," he says. "Protests can create life-threatening situations."

He was thinking about the future of the league. The everyday reality of the virus is shifting from emergency response to a sustained state of being. There's a question of what comes next. Over the summer, the league has become more formalized. Teams run regular trainings. They've written procedure manuals, which they're translating, hoping to make connections in areas of the world where they have less of a presence. Members who just seem to lurk without contributing much are asked to leave. In July, Zaidenberg headed up a CTI League hackathon to develop better info-sharing feeds and new bots, and to think through what the group will look like as the virus wears on—and beyond.

Rogers and his cofounders believe that what they've built can persist, perhaps in a scaled-back form, monitoring threats against the lifesaving sector, and then roaring back to full strength when the next crisis hits. While some league members have eased back on their participation as some normalcy returns to life in their corner of the world, many others continue to contribute as their day jobs have picked back up. Health care infrastructure will still need security support, even after the pandemic has passed. Other events looming on the horizon, like

the election and, someday, the Olympics will inevitably usher in an onslaught of cyberthreats. “Someone needs to be in the gate, ready to go,” Zaidenberg says.

Warfield tells me that for many league members, what they do in their day jobs is somewhat intangible. “I joke sometimes that if a solar flare wipes out all the computers in the world, I will have nothing to show for what I've done with my life,” he says. That’s not just a function of the work being online. When your mission is prevention, there’s not much to show for a job well done. But when the world looks the way it does right now, the absence of one more bad thing feels almost tangible.

More From WIRED on Covid-19

- Want the latest on tech, science, and more? Sign up for our newsletters!
- If you've just had Covid, exercise might not be good for you
- Colds nearly vanished under lockdown. Now they’re coming back
- Covid-19 vaccines could end up with bias built right in
- What teaching online classes taught me about remote learning
- Hey students! Here's how to deal with school in a pandemic
- Read all of our coronavirus coverage here

TOPICS LONGREADS CYBERSECURITY RANSOMWARE HACKING COVID-19

MORE FROM WIRED

Internet Expert Debunks Cybersecurity Myths

Cybersecurity expert Eva Galperin helps debunk (and confirm!) some common myths about cybersecurity. Is the government watching you through your computer camera? Does Google read all...

The Mirai Confessions: Three Young Hackers Who Built a Web-Killing Monster Finally Tell Their Story

Netflix, Spotify, Twitter, PayPal, Slack. All down for millions of people. How a group of teen friends plunged into an underworld of cybercrime and broke the internet—then went to work for the FBI.

ANDY GREENBERG

Satoshi Is Black

For some people of color, crypto isn't in crisis. In the midst of the FTX trial, I went to the Black Blockchain Summit to talk to the movement's biggest believers.

BRANDI COLLINS-DEXTER

The Spy Who Dumped the CIA, Went to Therapy, and Now Makes Incredible Television

Joe Weisberg—the geopolitically entangled, heavily therapized creator of *The Americans* and *The Patient*—is the trickiest character he's written (so far).

LAURA KIPNIS

Twitter's Former Head of Trust and Safety Finally Breaks Her Silence

From Israel vs. Hamas threats to Donald Trump's "wild" posts, Del Harvey helped make the platform's hardest content moderation calls for 13 years. Then she left in 2021 … and disappeared.

LAUREN GOODE

Rebel Moon Director Zack Snyder on Violence, Loss, and Extreme Fandom

The director manages to game the system and keep his soul while doing pretty much whatever he wants. Right now that means trying to make his *Rebel Moon* space opera into a Netflix mega-franchise.

HEMAL JHAVERI