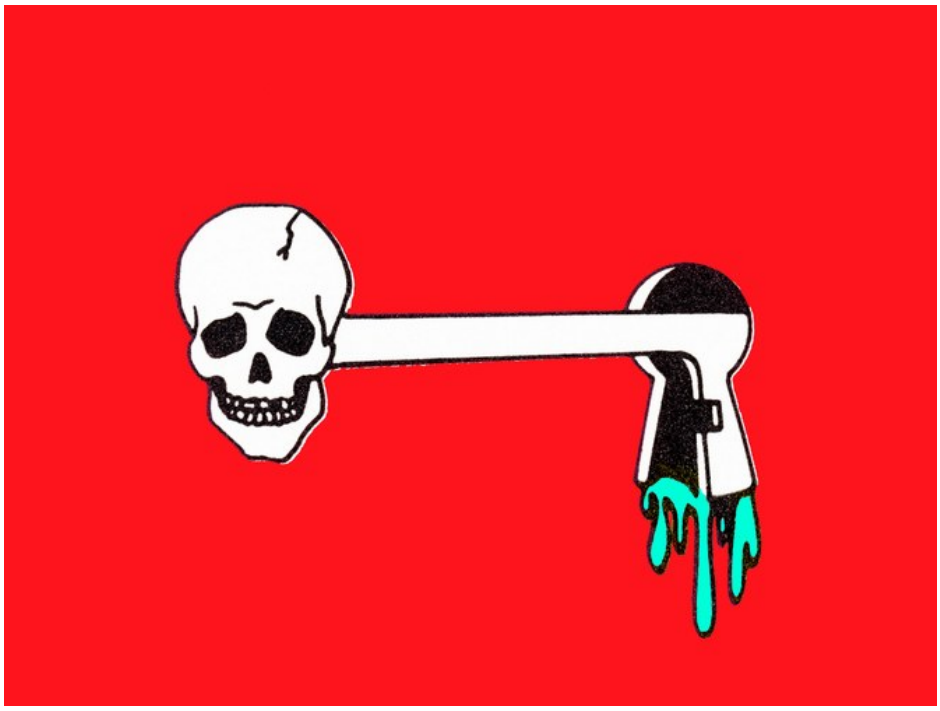
ANDY GREENBERG SECURITY 05.19.17 1:05 PM

HACKERS ARE TRYING TO REIGNITE WANNACRY WITH NONSTOP BOTNET ATTACKS



GETTY IMAGES

OVER THE PAST year, two digital disasters have rocked the internet. The botnet known as Mirai knocked a swath of major sites off the web last September, including Spotify, Reddit, and *The New York Times*. And over the past week, the WannaCry ransomware outbreak crippled systems ranging from health care to transportation in 150 countries before an unlikely "kill-switch" in its code shut it down.

Now a few devious hackers appear to be trying to combine those two internet plagues: They're using their own copycats of the Mirai botnet to attack WannaCry's kill-switch. So far, researchers have managed to fight off the attacks. But in the unlikely event that the hackers succeed, the ransomware could once again start spreading unabated.

Under Siege

Since the WannaCry ransomware worm began to fan out through the internet Friday, security researchers noticed a curious feature. When it infects a computer, it first reaches out to a certain random-looking web address, apparently as part of a check that it's not running in a "sandbox" environment, which security

researchers use to test malware samples safely. If WannaCry connects to a valid server at that specified domain, the ransomware assumes it's under scrutiny, and goes dormant.

Marcus Hutchins, a 22-year-old cybersecurity analyst for the security firm Kryptos Logic, spotted that trait last week, and immediately registered the web domain in WannaCry's code. In doing so, he effectively neutered the malware, cutting short what would have otherwise been a far worse epidemic, and instantly becoming a minor celebrity in cybersecurity circles.

Since then, hackers have directed armies of zombie devices—webcams, modems, and other gadgets caught up in the expansive Mirai botnet—to funnel junk traffic to the kill-switch web address, also called a "sinkhole," a site security researchers direct malware to in order to contain it. The presumed intention? Knock the domain offline, trigger some of WannaCry's dormant infections to reactivate, and end the epidemic's nearly week-long lull.

"Pretty much as soon as it went public what had happened, one of the Mirai botnets started on the sinkhole," says Marcus Hutchins, the British security researcher who registered the WannaCry kill-switch domain. Since then, he says, near-daily attacks from that first botnet and others built with the same Mirai malware have steadily ticked up in size and impact.

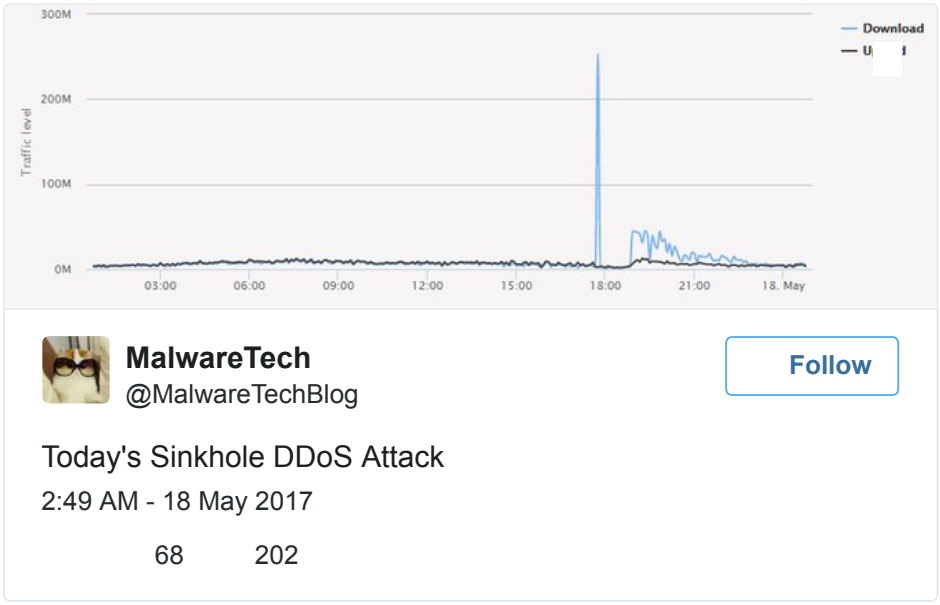
If the DDoS assault did succeed, not all WannaCry infections would immediately reignite. The ransomware stops scanning for new victims 24 hours after installing itself on a computer, says Matt Olney, a security researcher with Cisco's Talos team. But anytime one of those infected machines reboots, it starts scanning again. "The ones that were successfully encrypted are in this zombie state, where they're waiting to be reactivated if that domain goes away," says Olney.

Hutchins says he doesn't believe the source of the botnet attacks are the original malware authors but, rather, other groups of hackers hoping to kickstart WannaCry again just for the amusement of watching it spread. "They've obviously got no financial incentive. They're not the ransomware developers," Hutchins says. "They're just doing it to cause pain."

Mirai Image

The first DDoS attack, Hutchins says, was so small he barely noticed it. "It was sort of a love-tap from a botnet," he says. But since then, he's seen five attacks, trending upward. On Wednesday, Mirai hit the sinkhole domain with its worst flood yet, 20 gigabits per second of traffic. For comparison, that's less than a fiftieth of the size

of the Mirai DDoS that hit the DNS provider Dyn in September and knocked major websites offline, but 20 times the gigabit-per-second that DDoS-tracking firm Arbor Networks measured as an average attack in 2016.



Hutchins says he has no doubt that he and his colleagues at Kryptos Logic can still keep the attackers at bay. They've now enlisted the services of a DDoS mitigation firm that he declines to name—he says identifying it might help the attackers make their attacks more efficient. The service should help absorb any future attacks, and even take over the domain from Kryptos Logic if necessary. But before Hutchins fully engaged that protection service, he says the pressure to keep the sinkhole online and safe from attack was intense. He pulled an all-nighter after registering it to make sure it stayed up, and didn't sleep more than three consecutive hours until Tuesday.

Even though Hutchins' domain has protection, it's not the only one that's key to preventing WannaCry's spread. Over the weekend, another variant of the worm appeared, designed to connect to a different web address. Researcher Matt Suiche, the Dubai-based founder of security firm Comae Technologies, quickly registered it to enable a new kill-switch. Suiche says that he's also experienced at least one DDoS attack against his domain, but declined to say more, or comment on how he's protecting it.

It's not clear exactly who's behind the sinkhole attacks. But Hutchins says he's fairly sure it's not the original authors of the WannaCry malware itself. He says the attacks appear to be coming instead from known knockoffs of the original Mirai

botnet that began to pop up when Mirai's creator released the code for the internet-of-things-hijacking tool.

"Now any idiot and their dog can set up a Mirai botnet," Hutchins says. He believes the attackers are likely nihilistic, low-skilled hackers using public tools to cause mayhem for their own entertainment.

In this case, however, the Mirai attacks are more than a nuisance or a temporary disruption. The WannaCry malware that those attacks seek to reactivate has caused untold thousands of victims to lose data—in some cases, permanently—and even paralyzed life-saving health care systems. That makes the repeated attacks on Hutchins' sinkhole especially sadistic, perhaps even more so than the creation of the ransomware in the first place, Hutchins argues. "The initial developers were doing it for money," he says. "These people are doing it just of the fun of hurting people. Which I guess is worse."