Source : www.thehindu.com Date : 2021-03-27

NEW WAVE OF ‘HACKTIVISM’ ADDS TWIST TO CYBERSECURITY WOES

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

A different kind of cyber threat is re-emerging: activist hackers looking to make a political point. | Photo Credit: Reuters

(Subscribe to our Today's Cache newsletter for a quick snapshot of top 5 tech stories. Click here to subscribe for free.)

At a time when U.S. agencies and thousands of companies are fighting off major hacking campaigns originating in Russia and China, a different kind of cyber threat is re-emerging: activist hackers looking to make a political point.

Three major hacks show the power of this new wave of "hacktivism" - the exposure of AI-driven video surveillance being conducted by the startup Verkada, a collection of Jan. 6 riot videos from the right-wing social network Parler, and disclosure of the Myanmar military junta's high-tech surveillance apparatus.

And the U.S. government’s response shows that officials regard the return of hacktivism with alarm. An indictment last week accused 21-year-old Tillie Kottmann, a Swiss hacker who took credit for the Verkada breach, of a broad conspiracy.

Also Read | Hackers breach cameras at banks, jails, Tesla and more

"Wrapping oneself in an allegedly altruistic motive does not remove the criminal stench from such intrusion, theft and fraud," Seattle-based Acting U.S. Attorney Tessa Gorman said.

According to a U.S. counter-intelligence strategy released a year ago, "ideologically motivated entities such as hacktivists, leaktivists, and public disclosure organizations," are now viewed as "significant threats," alongside five countries, three terrorist groups, and "transnational criminal organizations."

Earlier waves of hacktivism, notably by the amorphous collective known as Anonymous in the early 2010s, largely faded away under law enforcement pressure. But now a new generation of youthful hackers, many angry about how the cybersecurity world operates and upset about the role of tech companies in spreading propaganda, are joining the fray.

And some former Anonymous members are returning to the field, including Aubrey Cottle, who helped revive the group’s Twitter presence last year in support of the Black Lives Matter protests.

Anonymous followers drew attention for disrupting an app that the Dallas police department was using to field complaints about protesters by flooding it with nonsense traffic. They also wrested control of Twitter hashtags promoted by police supporters.

"What’s interesting about the current wave of the Parler archive and Gab hack and leak is that the hacktivism is supporting anti racist politics or anti fascism politics,” said Gabriella Coleman, an anthropologist at McGill University,Montreal, who wrote a book on Anonymous.

Gab, a social network favored by white nationalists and other right-wing extremists, has also been hurt by the hacktivist campaign and had to shut down for brief periods after breaches.

DISRUPTING QANON

Most recently, Cottle has been focused on QAnon and hategroups.

"QAnon trying to adopt Anonymous and merge itself into Anonymous proper, that was the straw that broke the camel's back," said Cottle, who has held a number of web development and engineering jobs, including a stint at Ericsson.

He found email data showing that people in charge of the 8kun image board, where the persona known as Q posted, were in steady contact with major promoters of QAnon conspiracies.

The new-wave hacktivists also have a preferred place for putting materials they want to make public - Distributed Denial of Secrets, a transparency site that took up the mantle ofWiki Leaks with less geopolitical bias. The site's collective isled by Emma Best, an American known for filing prolific freedom of information requests.

Best's two-year-old site coordinating access by researchers and media to a hoard of posts taken from Gab by unidentified hackers. In an essay this week, Best praised Kottmann and said leaks would keep coming, not just from hacktivists but insiders and the ransomware operators who publish files when companies don't pay them off.

"Indictments like Tillie's show just how scared the government is, and just how many corporations consider embarrassment a greater threat than insecurity," Best wrote.

The events covered by the Kottmann indictment took place from November 2019 through January 2021. The core allegation is that the Lucerne software developer and associates broke into a number of companies, removed computer code and published it. The indictment also said Kottmann spoke to the media about poor security practices by the victims and stood to profit, if only by selling shirts saying things like "venture anti capitalist" and "catgirl hacker."

But it was only after Kottmann publicly took credit for breaching Verkada and posted alarming videos from inside big companies, medical facilities and a jail that Swiss authorities raided their home at the behest of the U.S. government. Kottmann uses non-binary pronouns.

"This move by the U.S. government is clearly not only an attempt to disrupt the freedom of information, but also primarily to intimidate and silence this newly emerging wave of hacktivists and leaktivists," Kottmann said in an interview with Reuters.

Kottmann and their lawyer declined to discuss the U.S. charges of wire fraud for some of Kottmann's online statements, aggravated identity theft for using employee credentials, and conspiracy, which together are enough for a lengthy prison sentence.

The FBI declined an interview request. If it seeks extradition, the Swiss would determine whether Kottmann's purported actions would have violated that country's laws.

DISDAIN

Kottmann was open about their disdain for the law and corporate powers-that-be. "Like many people, I've always been opposed to intellectual property as a concept and specifically how it's used to limit our understanding of the systems that run our daily lives," Kottmann said.

A European friend of Kottmann’s known as "donk_enby," a reference to being non-binary in gender, is another major figure in the hacktivism revival. Donk grew angry about conspiracy theories spread by QAnon followers on the social media app Parler that drove protests against COVID-19 health measures.

Following a Cottle post about a leak from Parler in November, Donk dissected the iOS version of Parler’s app and found a poor design choice. Each post bore an assigned number,and she could use a program to keep adding 1 to that number and download every single post in sequence.

After the Jan. 6 U.S. Capitol riots, Donk shared links to the web addresses of a million Parler video posts and asked her Twitter followers to download them before rioters who recorded themselves inside the building deleted the evidence. The trove included not just footage but exact locations and timestamps,allowing members of Congress to catalogue the violence and the FBI to identify more suspects.

Popular with far-right figures, Parler has struggled to stay online after being dropped by Google and Amazon. Donk's actions alarmed users who thought some videos would remain private,hindering the its attempt at a comeback.

In the meantime, protesters in Myanmar asked Donk for help,leading to file dumps that prompted Google to pull its blogging platform and email accounts from leaders of the Feb. 1 coup. Donk's identification of numerous other military contractors helped fuel sanctions that continue to pile up.

One big change from the earlier era of hacktivisim is that hackers can now make money legally by reporting the security weaknesses they find to the companies involved, or taking jobs with cybersecurity firms.

But some view so-called bug bounty programs, and the hiring of hackers to break into systems to find weaknesses, as mechanisms for protecting companies who should be exposed.

"We're not going to hack and help secure anyone we think is doing something extremely unethical," said John Jackson, an American researcher who works with Cottle on above-groundprojects. "We're not going to hack surveillance companies and help them secure their infrastructure."

Please enter a valid email address.

Data from research firm IDC showed Apple's shipments surged 22% to a record 90.1 million phones in the quarter, giving it global market share of 23.4%.

A contest among Wyoming schoolchildren will decide the new supercomputer's name.

END