Thu, Jul 08, 2021
Newsweek

WORLD

Launching a Ransomware Attack Against a Nation Is Far Easier Than You Think

BY **NAVEED JAMALI , TOM O'CONNOR AND ALEX J. ROUHANDEH** ON 7/8/21 AT 4:54 PM EDT

As ransomware attacks surge to unprecedented levels, the intricacies of mounting such a potentially destructive and deceptive operation would seem to be far beyond the reach of the average netizen.

But the power to paralyze a company or a nation with malicious intent may be more readily available than is commonly thought—although it is illegal, especially for users in the United States.

A U.S. military cyberwarfare officer who spoke to *Newsweek* on the condition of anonymity described a very simple process for doing a great deal of damage.

"All you need is a Tor Browser and the links to the right underground markets," the officer said. "There's forums, and you can Google them."

Tor, also known as The Onion Router, is a popular free and open-source software that enables anonymous communication and browsing. It provides a door into a virtual bazaar in which points of access, exploits and even entire ransomware toolkits are available on the dark web—essentially, the entire supply chain for a cyberattack.

It's not unlike buying a third-party smartphone application, a pre-packaged bundle of code that enables a device to perform a large range of functions with convenience. And just as consumers can download apps from leading social media companies such as Facebook, Twitter and TikTok, prospective hackers can buy the tools used by top collectives such as REvil.

The suspected Russia-linked group has been behind a slew of ransomware attacks, including an operation that paralyzed the U.S. operations of the world's biggest beef producer, JBS, in March, and a more recent and larger intrusion against the Kaseya software company that appears to have affected more than 1,000 companies.

The JBS operation netted the group $11 million in cryptocurrency ransom. In order to unleash its grip on Kaseya, REvil is demanding some $70 million.

Even for the everyday user, getting access to the very same infrastructure built by such shadowy organizations is far cheaper. Essentially, prospective customers pay these organizations to use these insider methods and networks to launch an attack on their behalf.

Now, this black market is more accessible than ever.

"I think this is not a new phenomenon," the cyberwarfare officer told *Newsweek*. "It's happened for a while now where they can do all the work for you, they gain access, and they sell the passwords, they do the hacking, they identify the vulnerability, and they create the exploits, and then they sell access to them."

The officer said the ransomware industry has become increasingly user-friendly.

"What's interesting now is that it has gotten to the point of commercialization where it is all just multiple friendly user interfaces that you just have to stitch together," he said.

But setting up the hacker infrastructure takes another, far more advanced skill set, one that also helps cover their tracks so that it difficult to trace the hack back to them, the initial point of origin.

And now these sophisticated hackers are utilizing a consumer class seeking to cause mayhem of their own to increase their profits.

"I think what most people think about when they think of a stereotypical hacker is somebody that's in-depth into coding," the officer said. "It has changed now in that it used to be that you had to be very technically adept to be a hacker, but the way the cyber market

or cyber underground has evolved is a lot of those things have become services now."

The industry has diversified, he said.

"Those network attackers, instead of profiting themselves, are now renting out their services and their expertise to others and that's where we see this amplification," the officer said. "It's others renting out the services now. It unlocks another class of folks that can be opportunistic and take advantage of bad cyber hygiene."

*A graphic imitates the screen initiated by a ransomware attack such as the WannaCry worm that infected hundreds of thousands of computers after hackers gained access to tools used by U.S. National Security Agency in 2017.*ISTOCK/GETTY IMAGES

"Cyber hygiene" refers to the overall level of precautionary measures taken by all tiers of users to prevent malicious attacks. While both experts and officials have raised the alarm on the need to increase awareness of better online cybersecurity practices, the gap remains woefully large, leaving an ample pool of unsuspecting victims.

These victims aren't only the targets of the attack, but the unwitting facilitators as well. Armies of unknowingly infected devices serve as so-called "zombie networks" or "botnets" that launch the malware salvo in lieu of the attacker's own computer.

And while being a victim isn't a crime, being an attacker is, even via transaction.

The U.S. hosts a trove of prospective paying customers for ransomware attacks, and the opportunity is tempting knowing that the internet is propped up by commercial entities without the same degree of intervention seen in other countries like China and Russia.

At the same time, most of these providers have peering contracts that necessitate resolving security incidents, including cooperation with federal agencies when criminal activities are identified.

The close relationship between public and private sectors in China and Russia has led U.S. officials to suspect that many of the attacks originating in these countries have been, at least, tacitly, tolerated by their respective governments.

"We actually have a solid system in place, we have a strong system in place for law enforcement and investigation in partnership with the private sector," the officer said.

READ MORE

- Russia's Little Cyber Green Men Versus the U.S. Digital Army
- Will Putin's Hackers Launch a Cyber Pearl Harbor—and a Shooting War?
- U.S. Cyber Tools Turned Against Americans, Limiting Biden's Russia Options

One of the key topics haunting U.S.-Russia relations right now is a request from President Joe Biden that his Russian counterpart Vladimir Putin institute similar crackdowns in his own country. Tentatively, both sides have signaled in public statements that they were willing to stamp out any malicious cyber behavior within one another's respective territories.

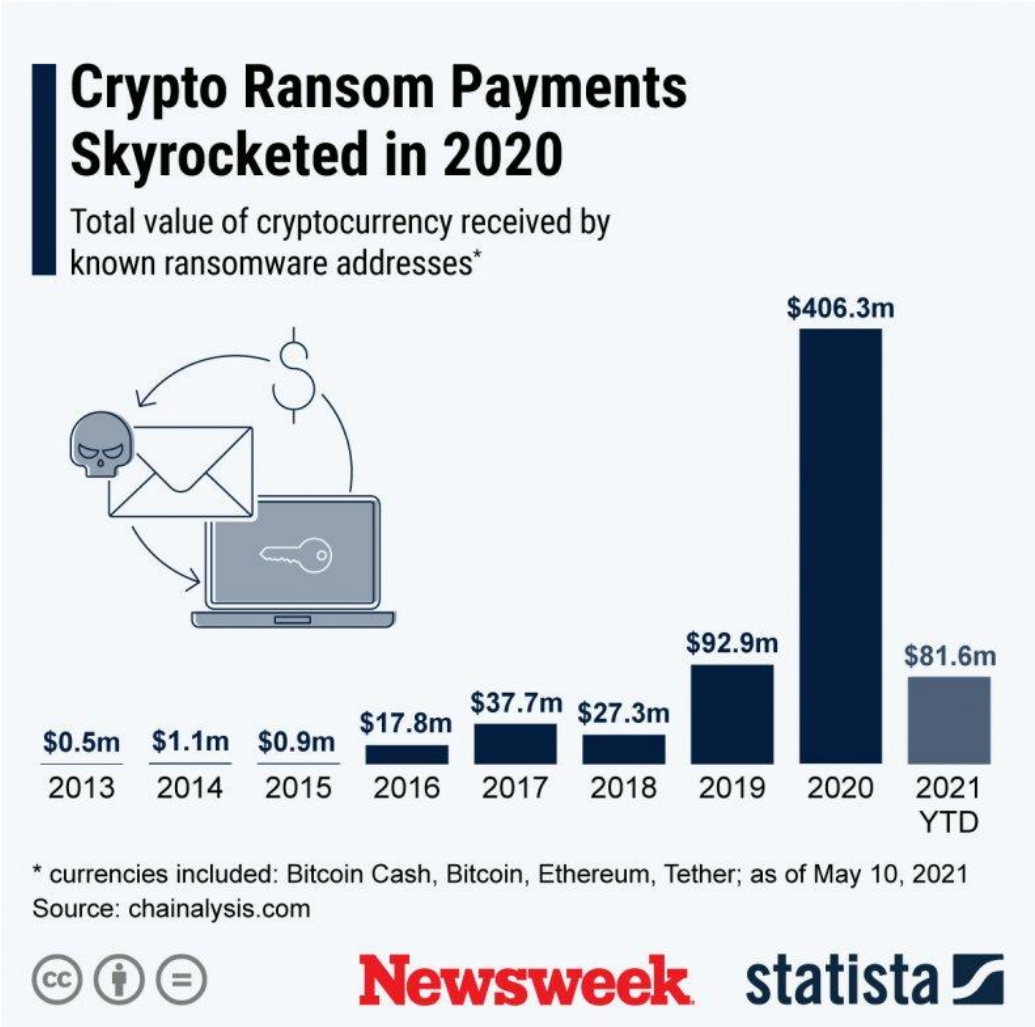
For the U.S. side, the Federal Bureau of Investigation plays a leading role in this field.

"Deterrence is one of the primary objectives of criminal law, and the FBI works closely with our U.S. and foreign partners, U.S. Attorneys, and the Department of Justice to make it clear that the United States is an inhospitable environment for cyber criminals," the FBI said in a statement sent to *Newsweek*.

The Bureau outlined how it takes on threats posed to the U.S. by both criminals and governments in the cyber realm.

"Our strategy is to impose risk and consequences on cyber adversaries—to change the behavior of criminals and nation-states who believe they can compromise U.S. networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves," the FBI said. "Through the FBI's unique authorities, capabilities, and partnerships, we are able to impose consequences both domestically and internationally. We are committed to investigating, disrupting, and pursuing malicious actors who compromise U.S. networks, no matter where they or their infrastructure may be."

But the true extent to which ransomware and other cyberattacks are escalating is unclear, as so many incidents go unreported.



A Statista graphic shows the amount of known cryptocurrency payments made in Bitcoin Cash, Bitcoin, Ethereum and Tether from 2013 through May 10, 2021 as compiled by chainalysis.com.STATISTA

The above graphic was provided by Statista.

Stuart Madnick, a professor of information technology at the Massachusetts Institute of Technology, told *Newsweek* that there are many reasons why ransomware events go unreported, but an unwillingness to admit a breach is a major one. Such an admission breeds bad publicity, legal implications and even possible copycats, he explained.

"So if something happens, if it's a ransomware attack, you pay a few bucks and no one knows that it ever happened," Madnick said.

The potential involvement of governments only further obfuscates efforts for global accountability. While direct links between groups like REvil and the Kremlin have never been established, there are many real-world precedents for commercial opportunities aligning with those of the state.

Madnick points to the historical role businessmen attached to the U.S. sugar and fruit industry played in the overthrow of the Kingdom of Hawaii toward the end of the 19th century. Cyber entrepreneurs also find opportunity in serving their country through malicious means.

"Sometimes your corporate interest and government interests align," Madnick said, "and so the government says, 'Well, we're not pushing it, but we shouldn't interfere with it either.'"

And with the proliferation of these tools in the dark web, he noted the emergence of a new class of hacker, which he calls "the cyber businessman."

Madnick likens the more advanced hacker collectives to weapons manufacturers and arms dealers, and the burgeoning cybercriminal hopefuls as the bank-robbers. He noted, for a robber, there's no bigger bank than the world's leading economy, the U.S.

"They just go to the local gun shops so to speak, pick up the weaponry they need," he said, "and off they go."