ADVISEN FPN
FRONT PAGE NEWS

U.S. companies work under almost perpetual state of cyber siege

Publication Date **08/28/2014**
Source: **USAToday.com**

SAN FRANCISCO - The financial industry indeed, most businesses works within a state of almost perpetual cyber siege at a level few consumers grasp. And the costs and dangers are growing for those who seek to protect their assets and their customers.

"The constant barrage of attacks is real," says J.J. Thompson, CEO of Rook Security, an Indianapolis-based firm.

Tensions are so high, Thompson says, one of his clients has a task force called the SBAN group for "sleep better at night" focused on creating new approaches to solving the threat.

The cyber attack on JPMorgan Chase and at least four other financial institutions first reported on Wednesday highlights the ongoing nature of cyber crime.

The nation's largest bank said it had not seen unusual fraud activity but officials briefed on the attack said there had been multiple, very sophisticated, intrusions.

A federal law enforcement official who was not authorized to comment publicly told USA TODAY that law enforcement officials believe the attacks were carried out by Russian hackers. It's unknown whether the Russian government played a role.

Low-level online attacks are a fact of life for businesses today.

"Look at a company like Comcast," said Scott White, who directs the computing and security technology program at Drexel University in Philadelphia. "Every single business day they get thousands of hits trying to crash their system. Some are just some teenage kids and some are these very well-funded criminal groups."

However some experts see a more sinister hand at work in this week's attacks.

American financial institutions are in the midst of a crime wave unlike any since the 1920s and the age of gangsters, says Tom Kellermann, a professor of cyber security at American University who also sits on the board of the International Cyber Security Protection Alliance.

The attacks seem to be part of an international wave of nationalist cyber crime campaigns against financial institutions which began this spring.

Thus far it has included numerous German and Swiss banks, the International Monetary Fund, the NASDAQ and the European Central Bank, said Kellerman, who is also the chief security officer with the security firm Trend Micro.

Both the FBI and the United States Secret Service are working to determine the scope of the attacks, said Greg Wuthrich, with the FBI's San Francisco Division.

"Combating cyber threats and criminals remains a top priority for the United States government, and we are constantly working with American companies to fight cyber attacks," he said.

What makes this week's attacks stand out is that usually cyber criminals simply steal user account information and credentials so that they can quickly steal money or sell them on the black market.

In this instance "from what I'm hearing, the stolen data is not limited to payment system information," said Kellermann, who declined to go into greater detail.

He believes that while the attacks are not officially the work of the Russian state, they are being done with its blessing.

"The best hackers in the former Soviet block countries have to demonstrate their allegiance once in a while; that's how they maintain their untouchableness."

"Honestly I think this is just unleashing the hounds. It's as if you've got three Rottweilers in the back yard and your neighbors are annoying you, so you open the gate," Kellermann said.

Online attacks have changed over the years. Initially it was just hackers out for notoriety, then those who were financially motivated.

"Those have increased in sophistication and coordination as organized crime began to drive them," said Rob Sadowski at RSA Security, a long-time computer security firm based in Bedford, Mass.

The past few years have also seen a rise in hacktivist groups out to gain notoriety for their causes. For example, a nebulous conglomeration of hackers that calls itself Anonymous recently took down the city government websites in Ferguson, Mo.

Now the rise of "potentially nation-state funded hackers activity, which gets close to espionage," is a major concern, Sadowski said.

"At the end of the day, serious attackers, not just cyber punks who try to steal credit card information, will go to great lengths and spend immense amounts of money in order to reach their target, employing not only lessons learned from online criminals over the last 20 years but also decades worth of espionage and social engineering tactics," said Adam Kujawa, head of Malware Intelligence at Malwarebytes Labs.

Others aren't as convinced.

"I think it is early to be jumping to conclusions about the attribution for an attack like this," said Bob Stratton, a partner at Mach37, which helps launch cyber security startup companies. "The trickiest part of defending networks in the modern age is determining the actual, rather than the apparent source of an attack. It will take time to forensically sort this out."

While Russia has been known to use cyber attacks in the early stages of military action, for example in Georgia and Crimea, "it isn't clear this is relevant here," Stratton said.

However in April Richard Clark, a top counter-terrorism and intelligence official for both the Clinton and George W. Bush administrations, said that Russia could use an attack on American computer systems as a way to seek revenge on the U.S. for supporting Ukraine.

Living in a time of siege is expensive. JPMorgan Chase said in its 2013 annual report that it planned to spend more than $250 million and devote about 1,000 people to cybersecurity in 2014.

According to a report on cyber security and the banking sector released by the New York State Department of Financial Services in May, more than three-quarters of financial institutions expect their IT security budgets to rise over the next three years.

"It's a never-ending battle," says Patrick Peterson is CEO of the security firm Agari.