Surge in Ransomware Attacks Exposes U.S. Cyber Vulnerabilities

By: Sarah Gleim | Jun 8, 2021

In the first half of 2021, the number of organizations impacted by ransomware across the globe has more than doubled compared with 2020, according to research by Check Point Software Technologies. SYNTHEX/SHUTTERSTOCK

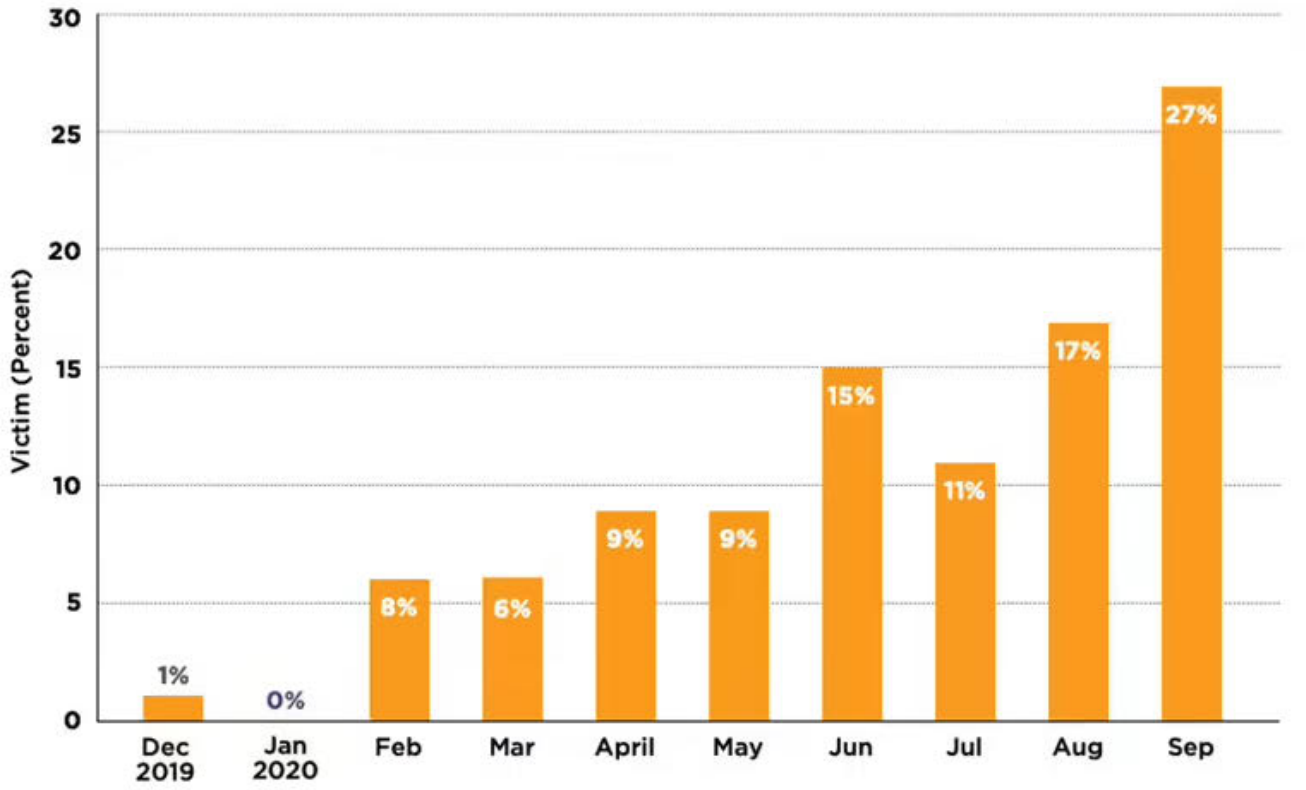
In March 2018, Atlanta was hit with a ransomware attack that infected nearly 3,800 government computers belonging to the city of Atlanta, including servers. After the virus was deployed, the ransomware essentially locked all

the infected computers, rendering them impossible to access. Atlanta's court system went down; police were unable check license plates; residents couldn't pay bills online.

Just three weeks before Atlanta was hit, the small city of Leeds, Alabama, also experienced an identical cyberattack. And before Leeds in January, it was Hancock Regional Hospital in the suburbs of Indianapolis.

What these three attacks have in common is they were all hit by SamSam ransomware, also known as MSIL/Samas.A. Each attack demanded around the same amount — about $50,000 in cryptocurrency. Hancock Regional Hospital and Leeds, Alabama, paid the ransom. However, the city of Atlanta did not. Instead, it chose to pay millions to get its systems back online.

At that time, the city of Atlanta was one of the most prominent to be attacked by ransomware, which according to John Hulquist, is when a cybercriminal accesses a network of computers, encrypts all the data and extorts the company to unlock it. Hulquist is vice president of analysis, Mandiant Threat Intelligence at FireEye, an intelligence-led security company.



FireEye's Mandiant M-Trends 2021 report shows a dramatic increase in ransomware attacks from December 2019 to September 2020.
FIREEYE MANDIANT

Ransomware Is Nothing New

Hulquist says ransomware attacks, which essentially hold a company network "hostage" until the demanded ransom is paid, are nothing new. They've been going on for several years (as these three cases indicate).

In the first half of 2021, the number of organizations impacted by ransomware across the globe has more than doubled compared with 2020, according to research by Check Point Software Technologies. FireEye's Mandiant M-Trends 2021 report also identified more than 800 extortion attempts that likely had data stolen. These numbers are based on Mandiant investigations of targeted attack activity conducted from Oct. 1, 2019, through Sept. 30, 2020.

The targets now are becoming much more high-profile. In the U.S. alone since April, prominent companies like Colonial Pipeline, JBS Foods, the NBA and Cox Media Group have all been hit.

Hackers typically access networks through phishing attacks, which are emails sent to employees tricking them into giving up passwords or clicking on malicious links that will download the malware onto the company network. Ransomware also looks for other entries into company networks via passwords that are easily cracked, like 123qwe for instance.

Fears of a gasoline shortage from the shutdown of the Colonial Pipeline in May led to panic buying and hoarding among U.S. drivers along the East Coast. Colonial paid $4.4 million in bitcoin to get the pipeline back online.
ANDREW CABALLERO-REYNOLDS/AFP VIA GETTY IMAGES

Why So Many and Why Now?

Hulquist explains it like this: Originally ransomware was mostly automated and targeted small systems. He calls it "spray and pray."

"The ransomware would go out and hit whatever system it could get," he explains. It looked for vulnerable passwords, open networks, easy entryways. "[The attackers] were known to be quite friendly; they would unlock the data — even offer discounts sometimes — and move on with their life." Bitcoin, he says, offered a good platform for transferring that money. That's exactly what happened in Leeds. The attackers demanded $60,000; the town paid $8,000.

But then things changed, Hulquist says. The ransomware went from automated "spray and prays" to large, directed attacks on bigger companies with more money. And ransoms skyrocketed. In 2020, companies paid more than $406 million in cryptocurrency in ransom to attackers, according to the latest report from Chainanalysis, which analyses blockchain and cryptocurrency.

"These new targets have to pay out because often they are critical infrastructure," Hulquist says. "They have to get back online. Consumers are actually a factor because they are forcing these companies to make hasty decisions as far as paying."

To Pay or Not to Pay?

That was the case in the Colonial Pipeline attack. The hack took down the largest fuel pipeline in the U.S. April 29 and prompted mass fuel hoarding across the East Coast. Colonial Pipeline CEO Joseph Blount told The Wall Street Journal the company paid the ransom — $4.4 million in bitcoin — to

bring the pipeline back online. But the decryption key the adversaries provided didn't immediately restore all the pipeline's systems.

And that's just one of the issues with paying ransom. The other major question is whether paying ransoms just encourages more problems. "I think paying ransoms clearly leads to more targeted attacks," Hulquist says, "but if you're a company in an impossible situation you have to do the right thing for your organization."

The good news for Colonial is the U.S. Department of Justice announced June 7 it recovered 63.7 bitcoins, valued at about $2.3 million Colonial paid to its hackers. "The move by the Department of Justice to recover ransom payments from the operators who disrupted U.S. critical infrastructure is a welcome development," Hulquist says. "It has become clear that we need to use several tools to stem the tide of this serious problem."

Of course not paying the ransom can be just as problematic. "Some of these companies don't want to pay, so they force them to pay by leaking their data publicly," Hulquist says. "That's a proposition that a lot of organizations do not want a part of." Leaked emails and other proprietary information, he says, can be far more damaging to some companies than simply paying up. It can open them up to legal trouble or end up hurting their brand.

Other hackers simply demand payment without even installing ransomware. That's what happened during the attack on the Houston Rockets in April. No ransomware was installed on the NBA team's network, but the hacking group Babuk threatened to publish contracts and nondisclosure agreements it claims it stole from the team's system if it didn't pay up.

JBS Foods, which is one of the world's largest food companies, was also attacked by ransomware May 31. The malware affected some of its servers supporting its North American and Australian IT systems, forcing the company to suspend operations June 1.
CHET STRANGE/GETTY IMAGES

What Is the Government Doing?

Hulquist says there's a lot more the government can be doing. "We've known this problem was growing for some time now and they're finally just now taking it seriously and stepping up their efforts," he says.

He's, of course, referring to several new initiatives laid out by the Biden administration in response to the surge in ransomware attacks. On May 12, President Biden signed an executive order designed to improve the cybersecurity in the federal government networks. Among its executive actions, it will establish a Cybersecurity Safety Review Board modeled after the National Transportation Safety Board (NTSB). The panel will likely include

public and private experts who will examine cyber incidents similar to how the NTSB investigates accidents.

Anne Neuberger, Biden's deputy assistant and the deputy national security adviser for cyber and emerging technology, also released an open letter June 2 addressed to "Corporate Executives and Business Leaders."

In it she says the private sector has a responsibility to protect against cyber threats and that organizations "must recognize that no company is safe from being targeted by ransomware, regardless of size or location ... We urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat."

How to Protect Your Company

What can you do to ensure your network is safe? Cybersecurity and Information Security Agency (CISA) and the FBI May 11 released best practices for preventing business disruption from ransomware attacks. In it they list six mitigations companies can do now to reduce the risk of being compromised by ransomware:

1. Require multifactor authentication for remote access to operational technology (OT) and IT networks.
2. Enable strong spam filters to prevent phishing emails from reaching end users. Filter emails containing executable files from reaching end users.
3. Implement a user training program and simulated attacks for spearphishing to discourage users from visiting malicious websites or opening malicious attachments and reenforce the appropriate user responses to spearphishing emails.

4. Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL blocklists and/or allowlists.

5. Update software, including operating systems, applications and firmware on IT network assets, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program.

6. Limit access to resources over networks, especially by restricting remote desktop protocol (RDP), which is a secure network communications protocol for remote management. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require multifactor authentication.

Hulquist says the entire purpose of the game now is to hit a huge target who is likely to pay — and one that *has* to pay. And taking critical infrastructure offline is not out of the question. That, he says, the U.S. is not prepared for.

"Our sophistication is our Achilles' heel in this space," he says. "It makes us more vulnerable to incidents. One of the lessons we should be taking from all of this is we are not prepared for cyberwar. We do know that they've targeted health care and other critical capabilities. Everybody is learning from this."

Now That's Crazy

So who's behind all of these ransomware attacks? Remember SamSam, the ransomware that took down Atlanta? In 2018, a grand jury indicted two Iranians who were in it for the money. Three other

ransomwares — NETWALKER, REvil and Darkside — are what's known as RaaS (Ransomware-as-a-Service), which means they offer anyone who spread their malware 10 to 25 percent of the payout. Darkside is said to have been behind the Colonial Pipeline attack. These operations appear to be based in Russia.

Frequently Answered Questions

Is ransomware a threat?

Ransomware is a serious threat to businesses and individuals. It can result in the loss of important data and the inability to access systems and data. Ransomware can also lead to financial loss and damage to reputation.

Can you remove ransomware?

It is possible to remove some types of ransomware, but it is not possible to remove all types. Some ransomware is designed to be difficult or impossible to remove, and some types of ransomware encrypt files in a way that makes them impossible to decrypt.