untangle

WHY TOP MEAT SUPPLIER JBS WAS TARGETED IN A RANSOMWARE ATTACK

SECURITY BRIEF

Less than a month after the Colonial Pipeline ransomware attack, JBS SA announced that they had experienced a cyberattack. A major, global meat producer headquartered in Brazil, JBS has more than 150 plants in 15 countries. Through a statement released May 31, 2021, the company said it was the target of an organized ransomware attack that affected servers supporting its North American and Australian IT systems. While plants in North America, Australia and Canada were affected, the JBS operations in South America were not disrupted.[1]

Taking immediate action as soon as the breach was discovered, JBS suspended all affected systems and notified the authorities. Because their backup servers were not affected, they began the process to restore all systems. And, by June 3rd most operations were back up and running.

WHO ARE THE ATTACKERS?

With the Colonial Pipeline attack still fresh in memories, this attack is also attributed to an organized cybercrime group based in Russia. REvil, whom the FBI associate with the attack, is known to law enforcement and has recently made some of the largest ransom demands. They are a “ransomware-as-a-service” organization much like DarkSide, the perpetrators behind the Colonial Pipeline attack.

These criminal organizations are far from the old image of lone hackers in a dark room. These syndicates are often large and either conduct the attacks themselves or develop a tool for someone else to execute ransomware attacks and take a portion of the profits. Often based in Russia, these organizations escape the scrutiny of local law enforcement as long as their targets are outside of Russia.

What is interesting about both REvil and DarkSide groups is that they don't try to hide. Both have had a presence on the dark web (DarkSide has since disabled their site) and even release statements, sometimes related to the ransomware attacks attributed to them. In the case of REvil, they even had a representative give an online interview stating what industries they would target. DarkSide had a manifesto posted on its site and declared that it would give a portion of their gains to charities, although it is uncertain if any recipients accepted the gift.

One thing these recent attacks highlight is that cyberattacks have made a significant shift from targeting data and personal information to finding consumer pain points.

RANSOMWARE TARGETS HAVE CHANGED

Previously, hackers would target online IDs, bank information and other sensitive data. However, as technology has become more sophisticated and efficient, so did the attacks and many bad actors have moved their operations to ransomware. In fact, according to Check Point Software, just in the first half of 2021 there has been a 102% increase in ransomware attacks over the same period last year.[2] Once a capable hacker sees the potential to gain millions of dollars, many are willing to take the risk to try and infiltrate multiple businesses in the hopes that one or more will pay up.

With an increase in ransomware exploits, these attacks quickly became top of mind for businesses. In Untangle's 2020 SMB IT Security Report 75% of respondents said that recent security breaches and ransomware attacks in some way affect the way they view their security roadmap.

In addition to the increase in ransomware attacks, malicious actors increasingly are targeting critical entities. Besides the JBS and Colonial Pipeline attacks, local governments, healthcare organizations and universities have also seen a rise in ransomware attacks. And at least 40 food companies have been targeted by ransomware gangs over the last year, including brewer Molson Coors and E & J Gallo Winery.[3] During another attack on critical infrastructure, while not a ransomware attack, in February 2021, a hacker gained access to the water treatment plant in Oldsmar, FL, bumping the sodium hydroxide in the water to a "dangerous" level.

RECENT RANSOMWARE PAYMENTS

Entity	Ransom Payment
The University of Utah	$450,000
City of Florence, FL	$300,000
UCSF School of Medicine	$1,140,000
Hancock Regional Hospital	$55,000

Taking another approach was Michigan State University who, despite threats to release student records and financial documents, refused to pay the ransom. While it may make sense to pay ransom in some events, it can set a bad precedent and encourage further attacks.

WHY ATTACKS ARE INCREASING

Ransomware attacks are increasing for several reasons. First, and foremost, the increase is due to the fact that companies are paying the ransom in order to regain access to their systems or have their data decrypted. It has been reported that JBS paid $11 million in ransom. The Colonial Pipeline also paid a $4.4 million ransom, although a good portion has been returned. Cybercriminals see the large payouts and it encourages them to strike more often and at larger, more lucrative targets.

Critical services and infrastructure are also being targeted at increasing rates because bad actors know they will pay the ransom to get services up and running as soon as possible.

The proliferation of IoT has also contributed to the increase in cyberattacks. With the majority of business systems now running online, coupled with adding mobile devices to networks and distributed workforces, there are numerous entry points for hackers to exploit.

Malicious actors also target industries and companies that may be seen as less “tech savvy,” have restrictive IT budgets and personnel, and are busy focusing on other critical tasks. Companies such as the aforementioned hospitals, universities, meat processing, local government, and water facilities are often targeted for these reasons, as well as for the consequences if their systems are offline. When targeting these businesses, attackers count on patches not being up-to-date, loose employee compliance with security protocols such as password protection and not clicking on unknown or suspicious links.

WHAT THESE ATTACKS MEAN FOR YOU

These attacks are the beginning of a worrisome trend in ransomware. Seeing successful attacks and how lucrative they can be, attackers are targeting essential services in order to disrupt society and hit consumers in the pocket. Businesses don’t want to lose money by being offline, for example shutting down processing plants, as every day not producing is very costly in lost revenue.

But more than harming a company’s bottom line, attackers are now targeting entities where consumers and society will feel the attack. Long gas lines for days followed the Colonial Pipeline attack. And consumers are sure to see a rise in beef and pork prices following the ransomware attack on JBS.

Cybercriminals have learned that they can leverage causing societal disruption to demand larger ransoms delivered faster. To avoid consumer complaints about service interruptions or price hikes, as well as lost revenue from being offline, companies are willing to pay ransoms to get their business back to running smoothly.

Where ransomware attacks once targeted holding data and information hostage, the attacks have become more brazen, impacting large portions of society, and this is the beginning of a new, unwanted and possibly dangerous trend.

WHAT IS BEING DONE

In light of recent high profile cyberattacks, the Biden Administration has released an Executive Order (EO) on improving the nation's cybersecurity.[4] While the EO is directed at US federal departments and agencies, and federal contractors, it would set the bar for protecting not only government agencies but for critical infrastructure as well. With official guidelines, all government agencies will be able to work towards the same robust standards. State and Local Governments will then be able to aspire to these guidelines too and follow them. The influence of this EO reaches further than just government agencies and provides a set of standards that other business corporations can implement.

The Executive Order Will:

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector.
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government.
- Improve Software Supply Chain Security.
- Establish a Cybersecurity Safety Review Board.
- Create a Standard Playbook for Responding to Cyber Incidents.
- Improve Detection of Cybersecurity Incidents on Federal Government Networks.
- Improve Investigative and Remediation Capabilities.

Currently, the U.S. has no cybersecurity requirements for companies outside of the electric, nuclear and banking systems. However, to successfully combat cybercrime and ransomware attacks, the government needs cooperation from private industry. Following the guidelines laid out in the EO will allow businesses to work towards the same robust cybersecurity standards as the government.

In addition to the EO, there is now more pressure on Russia to stop harboring cybercriminals, and the Biden administration is also looking to allies to work together to hold countries who harbor cybercriminals accountable.[2] Cybercrimes will also be a key topic when President Biden and Russian President meet at their first summit.

For businesses to protect against ransomware attacks, the EO has some concrete best practices that most companies can implement and may one day become commonplace standards:

- Auditing trust relationships
- Use of Multi-factor authentication
- Encrypting data
- Maintaining up to date software

SOURCES

[1] https://www.globenewswire.com/news-release/2021/05/31/2239049/17532/en/Media-Statement-JBS-USA-Cybersecurity-Attack.html
[2] https://www.cnn.com/2021/06/03/tech/ransomware-cyberattack-jbs-colonial-pipeline/index.html
[3] https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says
[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

HOW UNTANGLE CAN HELP

Untangle enables organizations to address network concerns and remain vigilant against unauthorized network access. The Untangle Network Security Framework provides IT teams with the ability to ensure protection, monitoring and control for all devices, applications, and events, enforcing a consistent security posture across the entire digital attack surface.

Untangle's cloud based centralized management tool, Command Center, does not rely on customer update schedules. Every update can be pushed within minutes to improve the security posture of the whole network management system.

UNTANGLE NETWORK SECURITY FRAMEWORK

ADVANCED SECURITY

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

INTELLIGENT SD-WAN

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Untangle AI-based Precitive Routing technology for first packet, dynamic path selection
- Manage one or many appliances from Command Center

CLOUD MANAGEMENT AT SCALE

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints

untangle

Untangle, Inc.
25 Metro Drive, Ste. 210
San Jose, CA 95110
www.untangle.com

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.