Food Ag ISAC

An IT ISAC Community

FARM-TO-TABLE RANSOMWARE REALITIES

Exploring the 2023 Ransomware Landscape and Insights for 2024

APRIL 2024

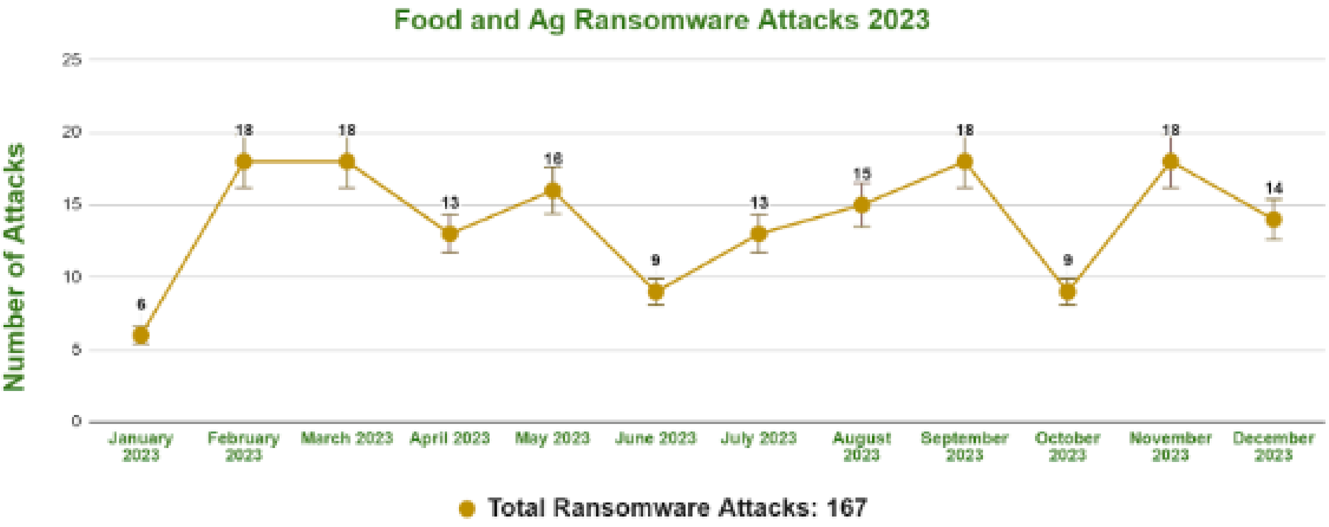
Ransomware is a form of malicious software (malware) often used by financially motivated threat actors to elicit payments from victims. After gaining initial access to a victim’s environment, the adversary will use ransomware to encrypt critical data so an organization cannot access files, databases, or applications, rendering systems unusable. The attacker will demand a ransom payment from the victim to release the files. Ransomware payments are typically requested in the form of cryptocurrency, which allows threat actors to move large amounts of money with a lessened risk of being detected by law enforcement or to circumvent protections in place at traditional financial institutions. Cryptocurrency tumbling services may also be used to further obscure the final delivery to specific wallets. While global law enforcement efforts have disrupted prominent ransomware activities, many of these actors reside in countries where extradition is not common, even when indictments are made. These adversaries tend to go on hiatus when law enforcement intervenes, only to reemerge as a rebranded strain at a later time.

As companies have improved their defenses against ransomware events and improved processes to restore critical systems via back-ups, ransomware actors have turned towards other forms of extortion to convince victims to pay. Ransomware attacks have expanded from only encrypting files to additional threats such as distributed denial-of-service (DDoS) attacks, intellectual property theft, data leaks, public shaming, and more. In some cases, even an organization’s customers may be contacted in an attempt to force a ransom payment through public pressure. Stealing data for extortion has become the norm for many ransomware groups, and double extortion is extremely common. Some groups have chosen to forgo encrypting files, instead only stealing sensitive data for extortion purposes.

Ransomware attacks are typically opportunistic. These attacks are spread out across all critical sectors, and specific ransomware groups show a level of variability in their targeting. For initial access, threat actors will search for organizations with publicly exposed and vulnerable systems, leverage phishing and social engineering attacks, or employ initial access brokers: cybercriminals and insiders who sell access to vulnerable networks.

Many ransomware groups offer their malware and negotiation services through a ransomware-as-a-service (RaaS) model, meaning individuals or groups of cybercriminals can breach their target(s) and then pay to use the ransomware malware infrastructure - giving a cut of ransom payments to the developers. This model has proliferated ransomware attacks by allowing ransomware developers to pair their skills with other adversaries more specialized in breaching organizations.

Ransomware attacks plague organizations globally across all industries. The IT-ISAC and the Food and Ag-ISAC jointly maintain a ransomware tracker that tracks attacks across 11 known critical sectors. The data is sourced from open-source intelligence and active monitoring of the dark web and data leak websites; it is also shared with us via our partners and members. This data is then distributed in a Monthly Ransomware Report, highlighting emerging trends and specific increases across critical sector targeting. The report helps our membership stay on top of ransomware trends by highlighting specific actors and new tactics, techniques, and procedures, as well as commonly exploited vulnerabilities.



How Does the Food and Agriculture Sector Compare to Others

In 2023, the IT-ISAC and the Food and Ag-ISAC tracked 2,905 total ransomware incidents. 167 of these were against the food and agriculture sector, which accounted for 5.5% by volume of total attacks. In comparison, critical manufacturing (15.5%) and financial services (12.4%) are the two sectors that saw the greatest number of attacks in 2023. Food and agriculture ranks number 7 out of the 11 sectors we monitor with the most attacks.

One challenge with ransomware attacks is that they can cause consequences for suppliers or partners of the victim company, in addition to the direct impact on the victim company itself. Considering the integrated and interconnected nature of the food and agriculture industry, a disruption in one company likely will have cascading impact. Previous ransomware incidents in the industry have demonstrated this interconnectedness, but also demonstrated the sectors’ resilience as companies adjust operations in response to the disruptions.

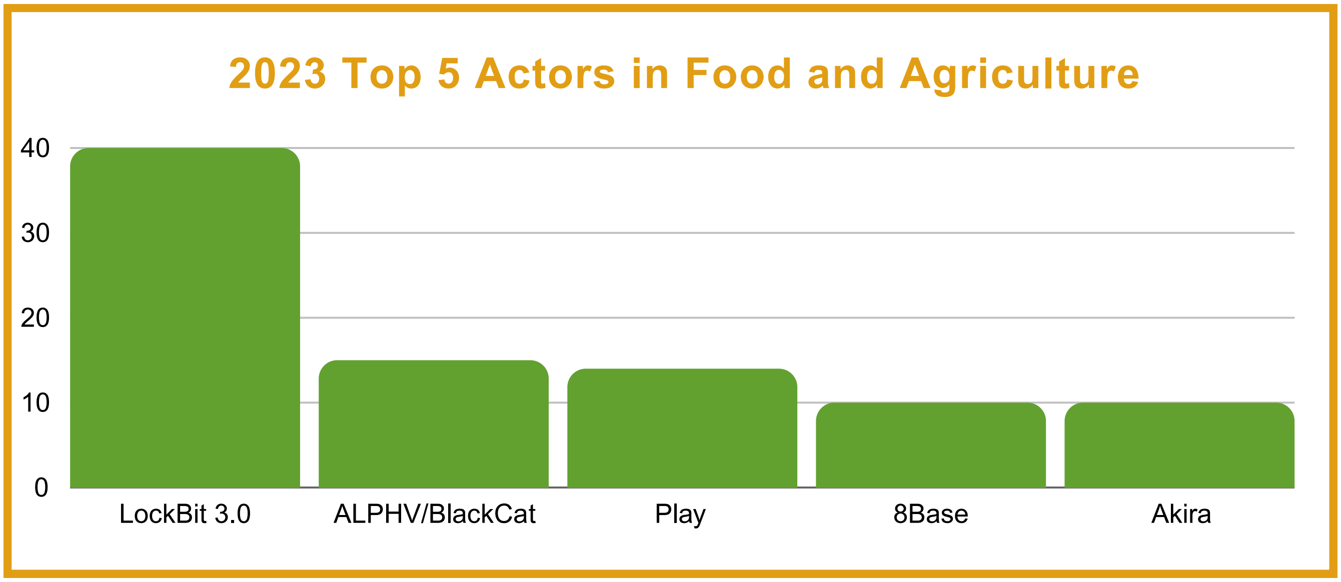
For example, ransomware attacks could impact or disrupt processes along agricultural production lines, such as seed production. Any downtime caused by an attack could lead to a chain reaction of delays, potentially causing late planting or harvesting windows. As a result, crops may need to be palletized and moved to other regions with an active growing season, which is done in cases of severe weather such as droughts or flooding. This is an expensive and taxing process that puts strain on organizations, costing them already-limited time and resources.

Ransomware poses other perils as well, such as the theft of intellectual property. It can take many years to develop a product from inception to sale. If information gets stolen somewhere along this timeline, that amounts to years of lost work and value. The impact on genetic work can be particularly costly, as this field requires expensive equipment, laboratories, and employees.

As noted above, ransomware attacks against the sector appear to be opportunistic. Ease of access is important to cybercriminals, who will often go after low-hanging fruit, or organizations that have notable security lapses. Ransomware operators will often scan the internet for publicly exposed and vulnerable systems, leverage initial access brokers, or offer their malware to other criminals through a RaaS model.

However, financial gain is the primary motivation of ransomware actors. While specific ransomware groups carry out multiple attacks against food and agriculture sector companies, they often target other sectors with similar or higher frequency.

Known Actors Hitting the Food and Agriculture Sector



LockBit

LockBit is a prolific ransomware actor, known to target organizations across various industries and verticals. In 2023, our metrics showed LockBit was responsible for nearly 25% of all attacks. In terms of volume of attacks, no other group came close. The only instance in which LockBit was surpassed last year was when the Cl0p ransomware group took advantage of a vulnerability in Progress's MoveIT product. That campaign by Cl0p impacted thousands of customers, creating an anomaly in our data.

LockBit was recently the target of "Operation Cronos," a global law enforcement operation which seized 34 servers critical to the group's operations. While it appeared the group was initially impacted by these takedowns, they were unfortunately able to restore systems and have once again begun targeting victims. The group has already carried out hundreds of attacks in 2024, nearly doubling its closest competition.

LockBit operates as a Ransomware-as-a-Service (RaaS), meaning affiliate cybercriminals can use the malware in their own attacks, giving a cut of the ransom payments to LockBit operatives. The group leverages double extortion tactics to steal data from victims to post on their public data leak website should they refuse to pay.

ALPHV/BlackCat

While the developers and affiliates refer to themselves as ALPHV, researchers have commonly referred to this group as BlackCat due to an image of a black cat on the group's ransom payment site. The group is likely a rebrand of several now-defunct ransomware strains including GandCrab, REvil, BlackMatter, and DarkSide.

In September 2023, the FBI reported that ALPHV had compromised over 1,000 victims and collected nearly $300 million in ransom payments. The group has been known to target critical infrastructure, primarily the health sector, despite claiming: "We do not attack state medical institutions, ambulances, [and] hospitals." In 2023, the U.S. Health Sector Cybersecurity Coordination Center (HC3) called ALPHV/BlackCat one of the most aggressive and sophisticated threats to the health sector. The continued targeting of critical infrastructure has placed the group in the crosshairs of law enforcement entities.

The group is known to carry out triple extortion attacks, using ransomware to encrypt systems, threats of data leaks on public shame websites, and distributed denial-of-service (DDoS) attacks against victims unwilling to pay.

In December of 2023, the group saw its infrastructure seized by law enforcement but was able to regain control of their servers and restart operations. However, after a prominent attack on UnitedHealth's Change Healthcare unit (Optum) which resulted in a $22 million dollar payment, the group shut down servers again in a likely exit scam to avoid paying affiliates involved in the attack. The ransomware's source code is allegedly for sale for $5 million.

Play

The Play ransomware (Playcrypt) emerged in the middle of 2022 and has carried out attacks across various sectors, including businesses and critical infrastructure in North America, South America, and Europe. The group leverages double extortion to not only encrypt systems but also exfiltrate data to use as additional leverage during ransom negotiations.

The group is known to exploit vulnerable public-facing applications (FortiOS, Microsoft Exchange), but also uses legitimate account access, especially that of remote desktop protocol (RDP) and Virtual Private Networks (VPN) for initial access.

Play was responsible for 14 attacks against the food and agriculture sector in 2023, and we have seen 5 more already in the first quarter of 2024. They should be regarded as a considerable threat to the sector, though their targeting appears to spread fairly widely across many industries and verticals.

8Base

8Base is a relatively unknown ransomware group that started ramping up attacks in the middle of 2023. In total, we saw 163 attacks during that year, with 10 of those being attributed to the food and ag sector. The group's targeting appears to be spread out across various sectors in industries, with Commercial Facilities (18.4%) and Critical Manufacturing (17.2%) being the top two.

Like most ransomware groups, 8Base participates in double extortion tactics, stealing data on top of encrypting systems. The ransomware itself appears to be related to Phobos and is often seen paired with SmokeLoader, which is distributed via phishing campaigns.

Akira

Akira ransomware takes our fifth spot. While tied with 8Base in terms of food and ag sector targeting in 2023, the group’s total attack volume was lower. Akira appears to be focused primarily on Critical Manufacturing (16.8%) and Information Technology (12.4%) victims, but did attack the Food and Ag sector in about 10% of their attacks.

The group emerged in early 2023 and uses double extortion tactics to convince victims to pay their ransom demands. Interestingly, researchers have noted the group begins ransomware negotiations with unconventional ransom demands of hundreds of millions of dollars. The group is known to exploit vulnerable public-facing systems and to target known vulnerabilities in Virtual Private Networks (VPNs), especially those lacking multi-factor authentication. Sophos researchers say they have seen Akira actors performing extortion-only operations, foregoing the encryption of systems via ransomware deployment – a tactic several other ransomware groups have adopted. As companies have increased their resiliency to ransomware attacks via security defenses and backup, the theft of sensitive data and threats of data leaks have proven a greater incentive for ransomware payments.

While we have yet to attribute any attacks by this group to the food and agriculture sector in 2024, their opportunistic targeting and historical impacts necessitate further monitoring.

Takeaways

Ransomware is a threat that doesn't hold back; it targets all critical infrastructure. The food and ag industry is not alone in experiencing these attacks. However, it sees fewer attacks than many other critical infrastructure sectors.

We expect ransomware attacks to continue to increase across all industries. Financially-motivated attackers will continue to seek financial gain; as long as the risk of getting caught is low and the potential for a large payday is high, ransomware will continue. In 2023, Chainalysis said ransomware payments surpassed $1 billion in extorted cryptocurrency payments from victims for the first time.

Indeed, the data for the first two months of 2024 bears this out. Despite some great work by law enforcement to disrupt ransomware groups, we have cataloged 386 ransomware incidents from January 1 through February 29th, 2024. For January, this was a 54% increase from the same period in 2023.

What You Can Do to Protect Yourself

Protecting yourself or your company from ransomware isn't accomplished in one step or one security practice, but through a combination of preventative measures and security practices. The following steps should help most enterprises defend against ransomware attacks and help organizations recover if an attack does occur. The IT-ISAC also explores general ransomware mitigation in their *Exploring the Depths* ransomware report.

Update! Update! Update!
Much like armies look for vulnerabilities in opposing forces, attackers look for vulnerabilities in a target's network. It is common for vendors to issue "patches" or updates to plug vulnerabilities in their hardware or software as they are discovered. Regularly updating your software can help protect your data and devices from threats.

Be Unique (Stay Weird) with Passwords, or Better Yet - Passphrases
Reusing the same password(s) for multiple accounts can jeopardize all accounts, even if only one account is compromised. The National Institute of Standards and Technology (NIST) recommends that unique passwords contain a combination of at least 8 letters, numbers, and special characters. Another option is a passphrase, which are made up of multiple words, numbers, and special characters - making them longer and more complex than passwords.

Add an Extra Layer of Protection with Multi-Factor Authentication (MFA)

Using MFA increases your security by providing bad actors additional hurdles, requiring two or more distinct types of identification before granting access. MFA works by requesting something you have (phone) with something you know (password) - this serves as an extra layer of protection.

Don’t Forget to Backup Your Files (and do it often!)

If you were to be a victim of a ransomware attack, you will want to recover as quickly and efficiently as possible. Having a backup of your files and data that you can restore will help you to continue operations as you respond to the incident. But remember your backups will only be as good as your backup process.

Encrypt Sensitive Files

Remember: not all information is equal. Some information is more important or sensitive than others. Deploy encryption to protect your most sensitive information and documents, including customer information, Personally Identifiable Information (PII), and emails.

Keep it Separate - Segment Your Networks

Ensuring your networks are segmented will limit and minimize operational risk should there be disruption. To the extent possible, limit internet connections to your operational technologies. If they must be connected, ensure operational networks such as manufacturing and production are segmented from business networks.

Don’t Take the Bait

Phishing remains one of the most common initial access points for cyberattacks, including ransomware attacks. Employees should be trained to avoid common phishing scams.

Practice Makes Perfect - Develop and Test a Response Plan

Having a ransomware-specific response plan in place can help you recover and restore operations more quickly. Testing the plan is imperative to find any weak points or flaws.

Sharing is Caring - Engage with Others

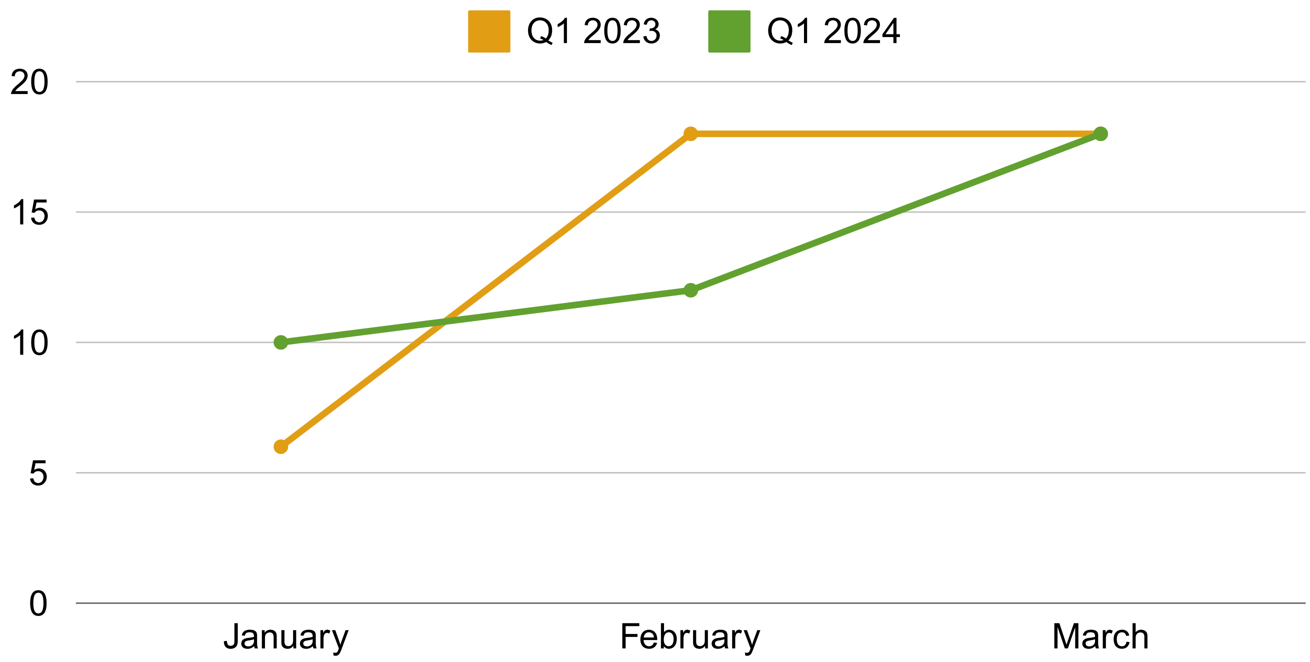
Ransomware groups and actors share with one another - we must share with each other to help protect. Engaging with peer companies can help you stay informed of this changing landscape so you can better defend.

To read more on security practices, the Food and Ag-ISAC has developed a cybersecurity guide for small and medium-sized businesses that companies can use or implement to improve their cybersecurity posture.

Q1 2024 Update

Ransomware attacks started strong in 2024, up 54% from January 2023. This initial spike was short-lived, however, as ransomware attacks were down in February (- 42%) and March (- 55%). The decrease in ransomware attack volume can likely be attributed to law enforcement disruptions against the LockBit and ALPHV/BlackCat ransomware groups, which commonly ranked 1 and 2 in terms of total attack volume.

Food and Agriculture Sector Q1 Ransomware Attacks 2023 vs. 2024



While LockBit and ALPHV/BlackCat were able to reclaim control of their infrastructure, neither have recovered to their previous victim output. LockBit remains a consistent threat, but has not been as prolific as it once was. The group has likely lost affiliates as a result of law enforcement disruptions, and has been seen actively recruiting on various cybercriminal forums. ALPHV/BlackCat has since shut down, citing law enforcement action, but many experts have hinted at a possible exit scam by the operators. After initially recovering their servers and carrying out a high-profile attack against Change Healthcare and several other health sector targets, the group claimed to have been seized again – a claim Europol has refuted.

With disruptions to both LockBit and ALPHV/BlackCat, it will be curious to see which other strains will take their spots as affiliates jump ship to the next ransomware-as-a-service (RaaS). ALPHV/BlackCat, which has rebranded several times in the past, will likely go on a hiatus before re-emerging as a new operation.

The Play ransomware group has been steadily increasing their attack volume in 2024, taking the top spot and accounting for 15% of all attacks in March. Notably, this group has already attacked the food and ag sector five times in 2024. While the group's targeting appears highly variable, they should still be seen as a threat to the sector due to their successful targeting and increasing attack volume.

Food Ag ISAC

An IT ISAC Community

MEMBERSHIP@IT-ISAC.ORG

IT-ISAC.ORG