Food Ag ISAC

An IT ISAC Community

FARM-TO-TABLE RANSOMWARE REALITIES

Exploring the 2023 Ransomware Landscape and Insights for 2024

APRIL 2024

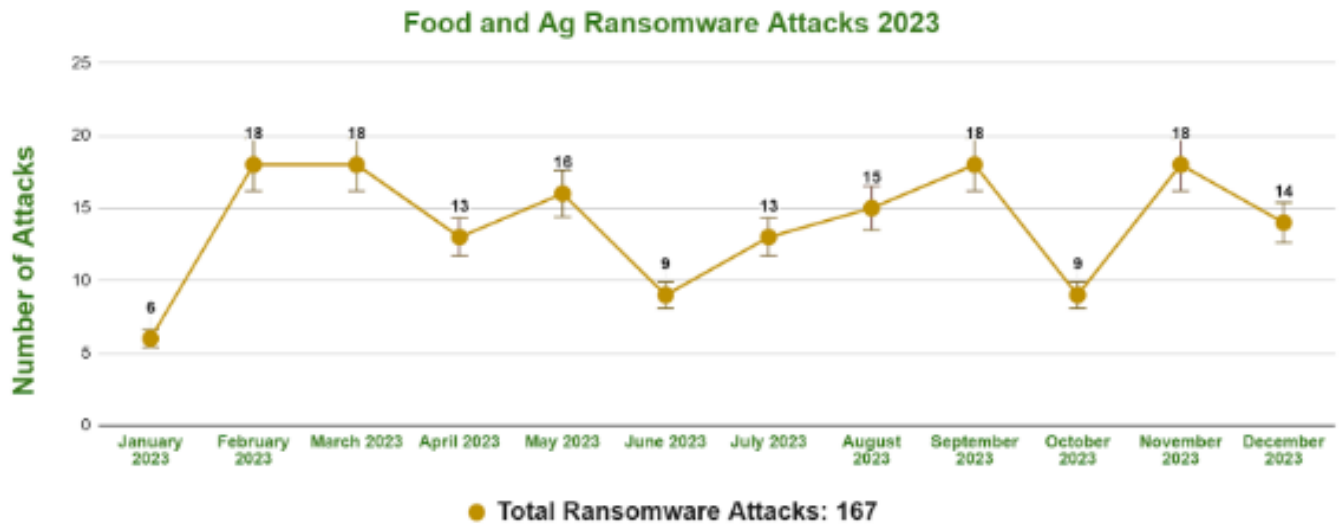
Ransomware is a form of malicious software (malware) often used by financially motivated threat actors to elicit payments from victims. After gaining initial access to a victim's environment, the adversary will use ransomware to encrypt critical data so an organization cannot access files, databases, 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.

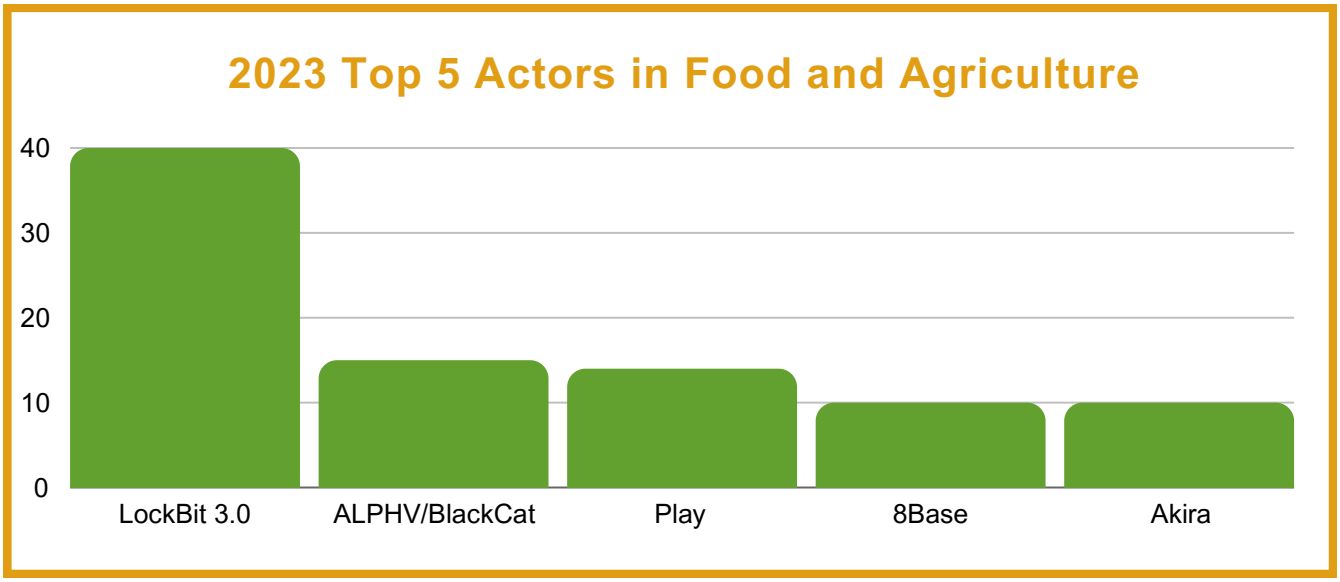
For example, ransomware attacks could impact or disrupt processes along agricultural production lines, such as seed production. Any downtime caused by an attack could lead to a chain reaction of delays, potentially causing late planting or harvesting windows. As a result, crops may need to be palletized 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.

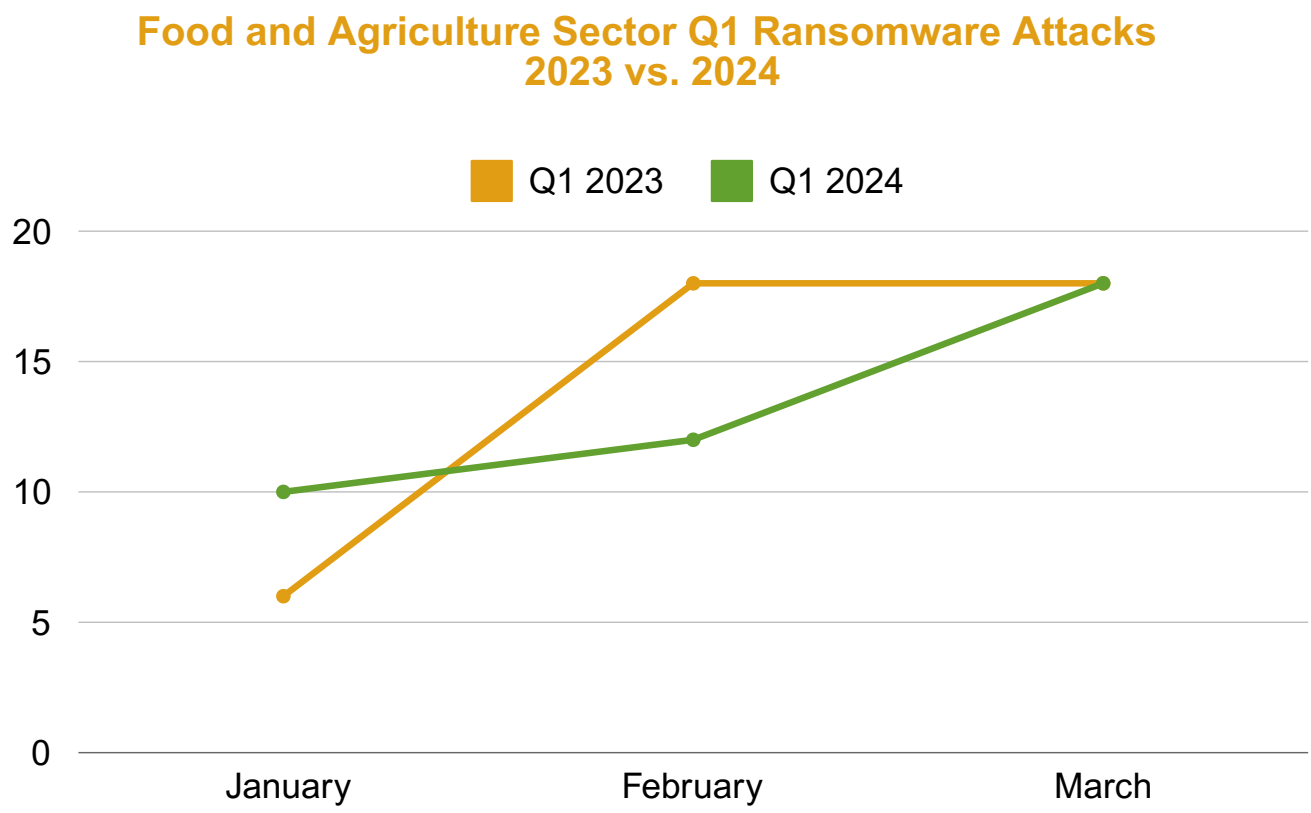
Practice Makes Perfect - Develop and Test a Response Plan
Having a ransomware-specific response plan in place can help you recover and restore operations more quickly. Testing the plan is imperative to find any weak points or flaws.

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.



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.

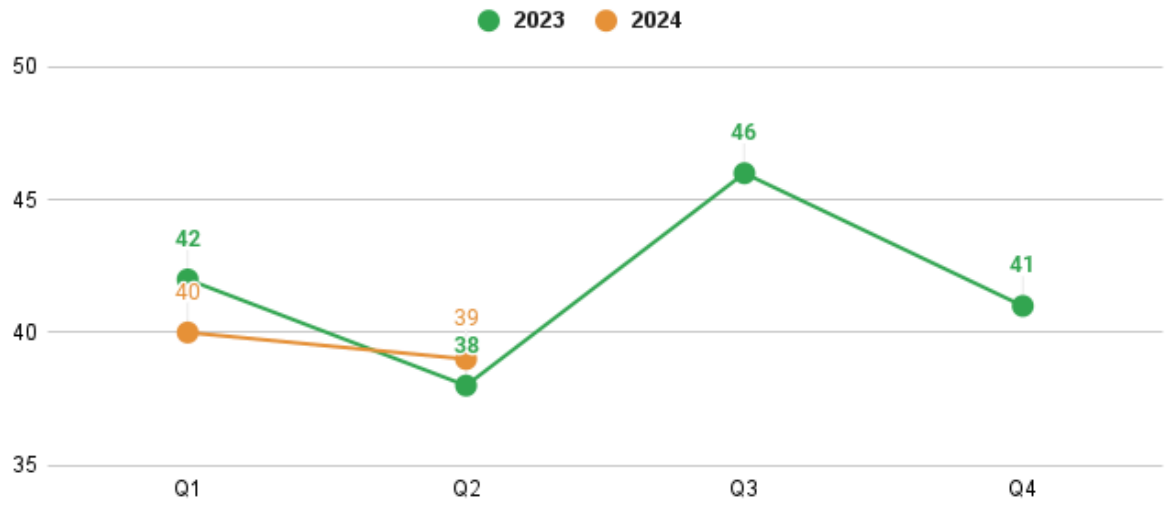
With disruptions to both LockBit and ALPHV/BlackCat, it will be curious to see which other strains will take their spots as affiliates jump ship to the next ransomware-as-a-service (RaaS). ALPHV/BlackCat, which has rebranded several times in the past, will likely go on a hiatus before re-emerging as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

Q2 2024 Analysis
April - June

The Food and Agriculture - Information Sharing and Analysis Center continues to track ransomware attacks and monitor ransomware groups and trends. Based on our findings, ransomware attacks against the food and ag sector remained fairly consistent when comparing Q1 and Q2 of 2023 with the same time periods in 2024. These numbers remained consistent even with law enforcement disruptions to two prominent ransomware groups - ALPHV/BlackCat and LockBit.

Food and Agriculture Sector Ransomware Attacks 2023 vs. 2024

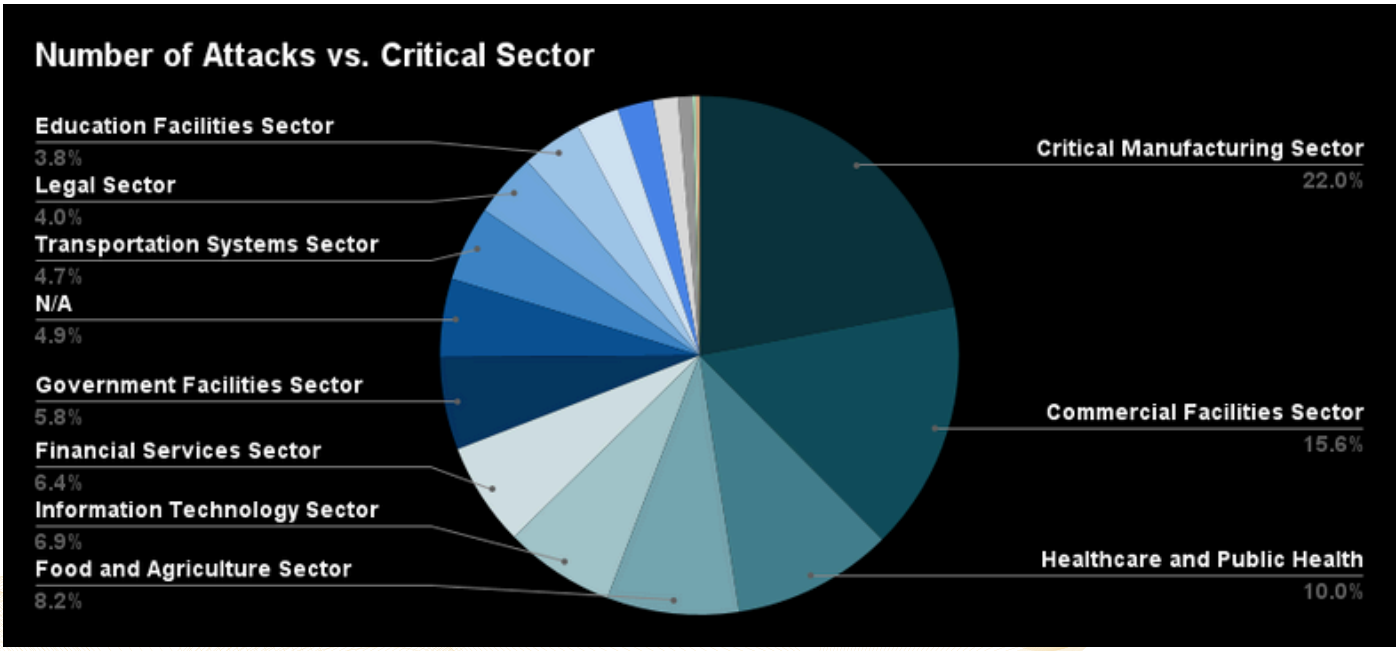


How Does the Food and Agriculture Industry Compare to Other Sectors?

In the second quarter of 2024, the food and ag sector saw a slight increase in percentage of total ransomware attacks at 8.2%, up from 7.0% in the first quarter of 2024. This is a result of decreased observed activity impacting other industries, rather than an increased number of observed attacks against the industry.

We noted 37 attacks against the sector in Q2 of 2024, and 38 in Q2 of 2023. While the food and ag sector ranked fourth in relation to all other sectors we tracked, it was still dwarfed compared to critical manufacturing (22%) and commercial facilities (15.6%). The food and ag sector saw similar attack volumes to healthcare and public health, information technology, financial services, and government facilities sectors.

In 2023, the food and agriculture sector was impacted by 5.5% of all 2,905 ransomware attacks we tracked, while we noted a slight increase in attack volume in Q2 of 2024 (8.2%), the number of attacks remained consistent with 2023.



Q2 2024 Breakdown of Ransomware Attacks
April - June

Law Enforcement Disruptions to ALPHV/BlackCat and LockBit

Global law enforcement operations against the ALPHV/BlackCat and LockBit ransomware strains have caused quite a disruption to the ransomware landscape. LockBit and ALPHV/BlackCat were notably the number one and two most prolific ransomware groups we track in terms of sheer volume of attacks. Law enforcement activity has caused ALPHV/BlackCat to dissolve, and while LockBit was able to become operational again, it has not reached the same level of victimization they saw pre law enforcement seizure.

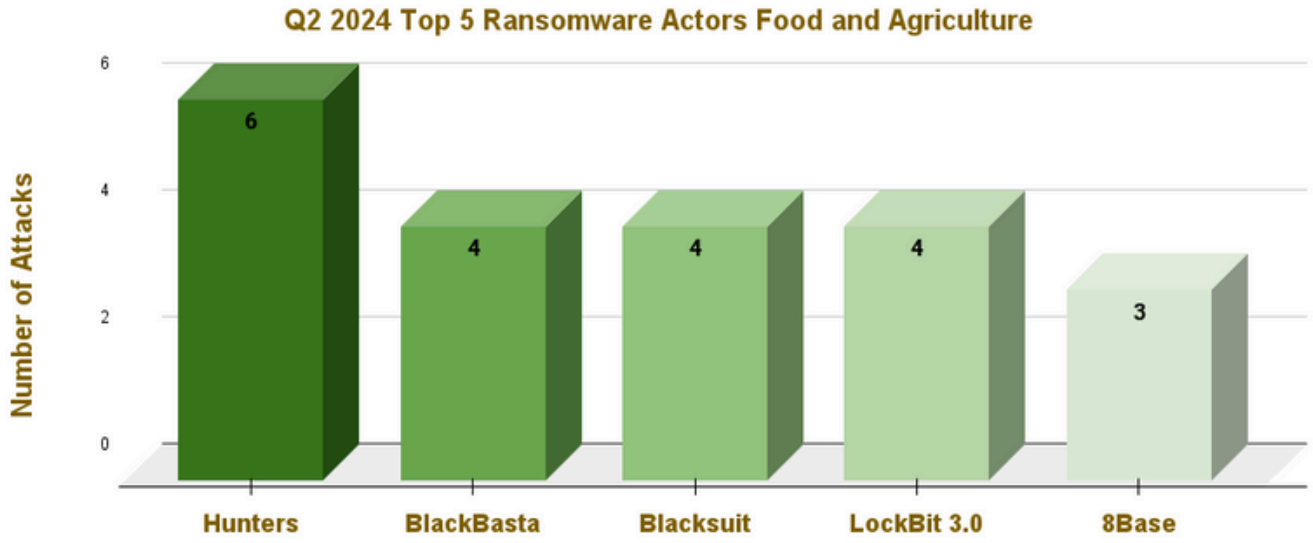
The U.S. Department of Justice (DOJ) publicly announced an operation against the operators of ALPHV/BlackCat on December 19th, 2023. Several websites and TOR services belonging to the actors were seized displaying notices of a seizure by the U.S. Federal Bureau of Investigation. While the group was initially able to restore operations to a backup website, they soon shut down completely around March of this year in an apparent exit scam after a prominent ransom payment was made by Change Healthcare. The actors allegedly posted a fake FBI seizure message to their website, and ran off with the ransom payment leaving affiliates empty handed. While ALPHV/BlackCat has not returned since their exit in March, this group has been known to go silent only to emerge in the future as a newly rebranded entity. The operators of BlackCat have been active since at least 2020, previously appearing as DarkSide which was responsible for the attack on Colonial Pipeline. After DarkSide went silent after law enforcement intervention, they reemerged as BlackMatter in July of 2021. BlackMatter also closed shop in November of 2021 after researchers found a weakness in their encryption methods allowing for a global decryptor. The group soon emerged once again as ALPHV/BlackCat. While we have yet to see a new strain emerge from these actors, past resurrections make it likely they will reappear on the landscape.

In February 2024, law enforcement agencies launched Operation Cronos to disrupt LockBit's infrastructure and take down its command-and-control servers. This operation significantly impacted LockBit's activities, forcing them to resort to misleading claims about their capabilities. In March, as a result of these efforts, law enforcement released decryption keys to help organizations recover their data without paying ransoms. The release of the keys further hindered LockBit's operations and made it harder for them to communicate with affiliates and launch new attacks on industries such as food processing and agriculture. As a consequence, LockBit's activities were significantly impacted, leading to a decline in their effectiveness.

Known Actors Hitting the Food and Agriculture Sector

Regardless of where the sector falls in rank of overall attacks to critical infrastructure sectors, ransomware actors remain active in the food and agriculture sector. We tracked 450 attacks in Q2 of 2024, 37 of those belonging to the food and ag sector. Despite the dismantling of some major ransomware groups, the threat remains, and new ransomware operations continue to fill the void left in their wake.

Below we take a look at the top 5 ransomware actors impacting the industry.



Hunters

Hunters is a new ransomware operation that appeared on the landscape towards the end of 2023. Researchers have noted code similarities between Hunters and the prolific and now-defunct Hive ransomware gang. It is still unclear if the operators behind Hive are running a new operation as Hunters International, or if the new group obtained source code from Hive.

According to Bitdefender, the actors responsible for Hunters International have stated they are independent of the former Hive group, and are simply using Hive malware and infrastructure. Based on current evidence, this seems to be true. While Hunters International is still growing their victim base and recruiting affiliates, they have targeted several high profile targets since their emergence. In the second quarter of 2024, the group was responsible for 6 attacks against the food and agriculture sector.

BlackBasta

In terms of attack volume, BlackBasta is typically near the top of our attack volume list across all critical sectors. The group has already targeted several food and agriculture sector companies in 2024. BlackBasta engages in targeted spear phishing attacks for initial access into victim environments. They are also known to use the following tools: BITSAdmin, PsExec, Windows Management Instrumentation (WMI), RDP, Qakbot, and Cobeacon for lateral movement. For data exfiltration, the group is typically seen using tools like Rclone. Researchers have noted several similarities between BlackBasta and the now-defunct Conti ransomware operation, namely in their malware development, leak site layout, and communications used for negotiation and recovery. The group has also been linked to FIN7, a prominent financially motivated threat actor, based on overlapping IP addresses for their command and control (C2) servers.

SentinelOne noted that BlackBasta used a piece of malware called WindefCheck[.]exe. According to SentinelOne researchers, “Analysis of the tool led to further samples, one of which was packed with an unknown packer. After unpacking, we identified it as the BIRDDOG backdoor, connecting to a C2 server at 45[.]67[.]229[.]148. BIRDDOG, also known as SocksBot, is a backdoor that has been used in multiple operations by the FIN7 group.” Further, SentinelOne noted that the IP address 45[.]67[.]229[.]148 is hosted on “pq[.]hosting”, the bulletproof hosting provider of choice used by FIN7 when targeting victims.

Blacksuit

Blacksuit ransomware was first discovered in early to mid 2023. While the group typically targets the healthcare and education sectors, they have been known to go after other critical sectors. The group uses stolen data for double extortion, and shares several technical similarities with Royal ransomware.

The group has targeted several organizations in the food and agriculture sector, and while their total victim count is low, food and ag targets represented almost 50% of the attacks our team tracked by the group in April of 2024. Blacksuit uses payloads that can impact both Windows and Linux operating systems. Initial access to victim networks is typically obtained via phishing emails and additional frameworks such as Empire, Metasploit, and Cobalt Strike are commonly used. SentinelOne notes that the use of malicious torrent files has also been observed as a delivery vector for BlackSuit ransomware.

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.

Takeaways

Ransomware is and will continue to be an ongoing threat. Regardless of disruptions to some prominent ransomware operations (LockBit and ALPHV/BlackCat), ransomware attacks against the food and ag sector have not slowed down. While the sector has seen fewer attacks than other critical sectors, ransomware remains a persistent threat.

Due to the just-in-time delivery of products and services in the food and agriculture sector, ransomware operators may view sector entities as prime targets for attacks. In addition to financial considerations, the added stress of health and human safety being at risk due to production impacts can add another layer of pressure against companies during a ransomware incident. While the sector continues to experience ransomware attacks, much of the targeting still appears to be opportunistic. Many of the groups targeting the sector have targeted other sectors at an equal or greater rate, and there are no specific patterns seen in the victimology.

Visit the full copy of the Food and Ag-ISAC's Farm-to-Table Ransomware Realities: Exploring the 2023 Ransomware Landscape and Insights for 2024 to access the original report, ransomware mitigation key tactics, and the Q1 2024 analysis.

How We Collect Our Data

Note that metrics for Q2 were obtained via open-source sites, the dark web, member input, and information shared between National Council of ISAC members. Due to outside assistance in monitoring ransomware attacks from partners and third parties, our metrics are likely biased towards the information technology and food and ag sectors.

Food Ag ISAC

An IT ISAC Community

membership@foodandag-isac.org
foodandag-isac.org