

Ransomware - Everything You Need to Know

Despite most organizations having cyber defense solutions in place, the attacks data and news cycles show that more effort is needed. Ransomware continues to be a scourge across all economic sectors and businesses of all sizes. A look at the 2023 attack data shows many high-profile organizations have been hit by ransomware attacks - UK Royal Mail, San Francisco BART, and Dole Food Company, to name a few.

It's safe to assume that these and other organizations hit by ransomware attacks in 2023 had cybersecurity defenses in place that didn't prevent them from becoming victims. The focus in 2023 needs to be on the early detection of network anomalies that are indicators of compromise, having good IT system and data handling policies and procedures in place, as well as detailed and tested incident response and recovery plans.

Boards and C-suite leadership teams must ensure that the solutions needed to protect their organizations from ransomware are in place and updated continuously. The risks of not doing this are existential in worst-case scenarios. In this paper, we'll look at the ransomware threat in 2023, how you can minimize the risk, and what technologies can make the task easier to improve your organization's cybersecurity posture.

The Current Threat Landscape

There has been a notable rise in cyberattacks targeting organizations of all sizes in recent years. These attacks encompass a range of threats, Malware, Threats against data, Social Engineering, Disinformation/Misinformation, Ransomware, Threats against availability (Internet and DoS/DDoS), and Supply-chain Attacks. Unfortunately, all signs suggest that the threat level will not decrease in 2023 or beyond.

This rise in attacks doesn't convey the complete picture of the increased threat. A more important factor is the type of threats and the techniques they are using. The attackers are using more sophisticated methods and machine learning to probe defenses and craft more believable Phishing attacks and fake websites. The use of deep fakes to trick people into divulging sensitive data or authentication details is also on the rise.

Organizations should assume that their defenses will be breached and have solutions to detect attacker activity on their networks to enable them to respond rapidly and neutralize attacks before they can do significant damage. Deploying network detection & response (NDR) capabilities will deliver the network monitoring, detection, analysis, and response capabilities needed to defeat modern ransomware attacks.

Flowmon's **The Cybersecurity Outlook for 2023** (see reference 1) covers the current threat landscape. It discusses what's behind the 81% rise in cyberattacks since the start of the COVID pandemic. A threat highlighted in the report is ransomware, as well as how the absence of network detection tools makes it harder to detect and stop ransomware activity when attackers evade other defenses. In this white paper, we'll focus on the ransomware threat. And outline how to mitigate the risks.

What is Ransomware?

Ransomware is a type of malware (**malicious software**). Ransomware is one of the most dangerous forms of malware. The goal of a ransomware attack is to bypass cybersecurity defenses and infect an endpoint device or server. Generally, once a foothold exists on a network, ransomware will look for other hosts it can jump to and infect. After some time, the ransomware infection will activate and perform tasks that steal data and then encrypt data to enable the extortion of money from the attacked organization. Both stealing data before encryption and the ransom part of the attack are common practices in current attacks. There may be a delay post-infection when the ransomware does nothing to avoid detection. It is at this point in a ransomware infection that NDR solution can detect the various indicators of compromise that are apparent in network traffic.



Ransomware attacks have exploded over the last few years. This is due to the success rate and the financial returns that cybercriminals have seen from this cyberattack method. Ransomware works so well that ransomware-as-a-service solutions are now available for criminals without the skills to write malicious code. The SonicWall 2023 Cyber Threat Report (ref 2) has data to show that there were 494 million recorded ransomware attacks seen in the SonicWall data in 2022. This was the second-highest recorded number in any year, but the fact that it was second doesn't signal a decline. The number recorded in the final quarter of 2022 was the highest since 2021 Q3. An upward trend that's likely to be seen in the 2023 figures when available. Plus, the attacks that did occur in 2022 were more damaging and costly to those impacted — as the SonicWall report outlines.

When ransomware has infected devices on a network, it will perform three main activities. Monitoring for these and responding quickly when detected can significantly reduce the damage done by ransomware attacks. We cover how NDR solutions can enable rapid detection later in this white paper.

- **Discover and spread to other systems** - Ransomware uses various network discovery methods to look for other systems on the network. It will then use automated attack methods or leverage known vulnerabilities to try to log in to any discovered systems to spread the ransomware infection and make it harder to eliminate.
- **Copy data from infected systems** - This step has become more common in ransomware attacks. Cybercriminals will identify file stores and databases that may have valuable data. They will then copy the data to servers they control on the Internet. The terms data exfiltration get used to describe this data copying. This data is often sold on the Dark Web. It can also be used to plan further attacks against an organization. For example, by using it to build more complete user background profiles to use in future Phishing attacks. It is often also used as another way to extort money from the attacked organization after the encryption step. In this scenario, the cybercriminals will threaten to release the stolen data unless they are paid not to. Often the stolen data contains sensitive and personal information that will damage the organization's reputation and lead to fines if it is publicly released.
- **Encrypt the data on infected systems** - the primary goal of a ransomware attack. Once the attackers have discovered and infected as many computer systems as they can and possibly copied data for later reuse, they then trigger the encryption phase of the attack. Once devices and servers are encrypted, a message is displayed on-screen demanding a ransom payment to get a code or tool that the organization can use to decrypt the encrypted files.

The ransom demands ask for payment in cryptocurrency. There is an active debate within cybersecurity circles, law enforcement, and Governments about whether anyone should pay ransomware demands. At present, it's up to the affected organizations, but strong voices say that paying the ransom should be made illegal to stop the flow of funds to cybercriminals from ransomware attacks. Irrespective of how this debate is resolved, anecdotal evidence suggests that a significant number of organizations that pay the ransomware extortion fee never receive a working method to unencrypt their files. Additionally, many of those who do pay the ransom demand are victims of additional attacks soon after paying — probably using information gained by the attackers in the primary attack.

Even though the overall number of ransomware attacks during 2022 was down from the 2021 total in various data sets and surveys, as noted above, in the SonicWall report data, the final quarter of 2022 had the highest recorded number of incidents since 2021 Q3, an upward trend that is likely continue into 2023. The sophistication of the ransomware attacks is also changing. New ransomware strains are improving at avoiding detection measures and also using new ways to infect systems. Some try to bypass endpoint device security software, and others dwell entirely in memory and don't write out any information to disk that signature-based anti-malware systems can detect.

Impacts of a Ransomware Attack

A successful ransomware attack can have severe consequences and lasting effects on an organization. In some cases, it can even be terminal, and the organization may never fully recover from the disruption. There are three primary areas where a ransomware attack can cause damage.

Financial damage - The **Sophos State of Ransomware 2023** report (ref 3) shows that organizations who paid the ransom doubled their costs — averaging \$750,000 in recovery costs per incident versus \$375,000 for organizations that used backups to get data back. The mean recovery cost in 2023 is now \$1.82 million (up from \$1.4 million in 2022). Reported mean recovery costs started at \$165,520 for organizations with less than \$10 million in annual revenue, rising to \$4,496,086 in \$5 billion-plus businesses. While these numbers mask a range of recovery costs, there is a clear pattern of recovery costs increasing with revenue. These costs cover all the activities required to recover from a ransomware attack. Including paying the ransom, the costs associated with business

disruption when IT systems are unusable, operational downtime for machinery and other plant devices usually controlled by IT systems, staff overtime payments during the recovery period, and more. The ransom is only a portion of the costs incurred to recover from an attack. So even if an organization decides not to pay the ransom and recovers via other means, the costs will still be high.

Reputation damage - The consequences of a ransomware attack go beyond just financial loss for an organization. The damage to their reputation can be equally devastating, especially if sensitive data is stolen and leaked online. This loss of trust can have ripple effects when potential customers or business partners are considering working with them. The recent Kaseya attack, which spread ransomware to their clients and then on to many third-party organizations, is a cautionary tale of how such an attack can severely impact an organization's reputation.

Operational damage - Ransomware encryption renders IT systems inoperable, causing significant disruption to many businesses. Systems that control essential functions for day-to-day operations are particularly vulnerable. In the event of an attack, these control PCs or other software-based systems and servers may be taken offline, resulting in a complete halt of business activities. Such incidents can lead to severe financial and reputational damage (as discussed above), particularly if services or products cannot be delivered. The resources that are redirected to recover from the attack cannot also be used for new business improvement projects. Recovery can take weeks or months, and this can significantly disrupt business plans.



What is Ransomware as a Service (RaaS)?

Ransomware as a Service (RaaS) is an offering where cybercriminals provide ransomware to other attackers, who then use it to target organizations. These secondary attackers pay a fee to gain access to the ransomware and other necessary tools to conduct successful attacks, such as instructions for distributing the malware and collecting payment from the targeted victim. It is often used by attackers without the skills to create the attack tools themselves.

Many cyber criminals with the skills to create ransomware attack chains prefer to make it available for others to use via RaaS as this approach enables them to profit from offering a service without personally executing the attack. This reduces their chances of getting apprehended by law enforcement and lets them concentrate on developing newer and more sophisticated forms of ransomware.

The popularity of RaaS has increased in recent years due to its accessibility for those without technical skills and the potential for profit. It has enabled less tech-savvy criminals to participate in ransomware attacks, contributing significantly to the rise in attacks. RaaS is an offering that is part of a broader underground marketplace where cybercriminals buy and sell services.

Who are the Attackers?

There are three main groups that use ransomware to achieve their goals. The first are cybercriminals, primarily motivated by financial gain, who target businesses and other organizations. They demand a ransom payment in exchange for decrypting the affected data and also threaten to sell or publicly release any stolen data if an additional payment is not made - in other words, they blackmail those that have been targeted.

The second group is hacktivists with political or ideological motivations to attack organizations. They may target governments, corporations, or other organizations they have ideological differences with.

Thirdly, there are state-sponsored attackers. These groups are affiliated with governments and may use ransomware for espionage or coercion. Their targets may include foreign governments, businesses, or individuals, and the goal is to steal sensitive information, exert political pressure, or disrupt their targets' activities.

Attack groups employ different methods to infect target systems, such as phishing emails, malicious websites, and exploit kits.

In recent years, these groups have been linked to highly publicized ransomware attacks, such as those targeting Colonial Pipeline, JBS Foods, Kaseya, and others.

How to Defend Against Ransomware

To protect against ransomware attacks, it's crucial to adopt a wide-ranging approach. There's no single solution that can guarantee complete protection. However, implementing preventive measures and devising incident response and disaster recovery plans are essential steps for every organization in ransomware prevention and recovery planning.

Most security and IT professionals are already implementing cybersecurity risk management measures. However, not all organizations are doing all that they should. It's worth noting that the threat landscape is continually evolving, and it's crucial to keep abreast of emerging attack methods used by attackers to spread ransomware and other malware types. Here are some brief things organizations should do to prevent successful attacks or to help recovery afterward. Reference 4 has a longer article on these topics.

Backups — Ensure your backups are up to date, tested in proper way and data can be recovered from them. In case of a ransomware attack that renders IT systems unusable and there is no decryption tool available, even after a ransom payment, backups are the ultimate safety net. Recent data backups will be necessary to restore the systems to an up-to-date state from before the attack. To ensure the effectiveness of backup procedures, offline copies of data must be included. Many types of ransomware actively look for and target backup solutions on the network, which means keeping backup copies of recent data that are not connected to the network is essential.

It's a well-known adage in IT system administration, but it rings true: "Untested backups are not backups at all!" Regularly performing test restores is necessary to ensure IT admins can restore data from backups. Losing three months of data due to faulty backups is not something anyone wants to explain to the CTO or CEO.

Deploy Endpoint Protection — It is common for cybercriminals to target the devices used by staff. To prevent these attacks, it is recommended that endpoint security tools are deployed on all devices. It is also essential to ensure that endpoint devices do not automatically run any executable code from external USB drives or other devices when

plugged into a computer. Cyber attackers have been known to drop ransomware and other malware-infected USB drives in the parking lots of businesses they are targeting, hoping that someone will pick it up and plug it into their PC.

Network Detection Tools — To stay ahead of potential ransomware attacks, it's essential to use network monitoring tools that can rapidly detect unusual activity, like adversary/attacker lateral movement between endpoints and inside infrastructure. NDR tools can detect the activity associated with ransomware and other attacks if the attackers have gotten past endpoint protection tools and other edge protection. This proactive approach adds an extra layer of security and can help identify attacks in progress. Flowmon Anomaly Detection System (ADS) is ideal for performing this vital ransomware protection activity. We outline Flowmon ADS in the next section.

Network Deception Technologies — Deception technology solutions set up fake systems, such as servers, applications, and databases, on a network to lure attackers. These decoys look like the real thing but do not have any actual user data. Instead, machine learning algorithms imitate user activity on these systems, such as log-ins, using applications, and submitting database queries. By utilizing these dummy systems in combination with micro-segmentation (see below) on the network, cybersecurity defenders can protect the real infrastructure from attackers while also gaining valuable insights into their attack methods. The dummy systems deceive attackers into thinking they have found systems to attack while also allowing cybersecurity professionals to monitor their actions. This information can then be used to ensure that production systems are not susceptible to the attack methods used.

Use Micro-segmentation — Micro-segmentation divides the network into multiple small parts that are logically isolated, thus preventing the discovery of devices and nodes on different segments by attackers. By doing so, the network becomes opaque, limiting the chances of any network discovery by cybercriminals.

Use Zero Trust — In zero trust, every network connection is viewed as dangerous and hostile, no matter its origin. Whether the request is from a secure desktop PC in a corporate HQ or an unknown IP address over a VPN from an external location, each access request must undergo the same high level of scrutiny. Proper authentication details and responses must be provided before any system access is granted. No connection is given special treatment based on its origin.

Update Network Edge Protection — For years, perimeter defense systems like firewalls, intrusion detection systems, and security-enhanced network devices have been the foundation of cybersecurity. These physical and virtual network infrastructure devices are

still critical components of any comprehensive cybersecurity strategy. It's crucial to keep all connected devices updated with the latest operating systems and security patches. If any devices are no longer supported and not receiving updates, creating a plan to replace them as soon as possible is crucial.

Use Strong Multi-Factor Authentication — It's important to implement Identity and Access Management (IAM) alongside robust password policies. For most organizations, IAM is provided through Active Directory or another directory service. Since applications are often deployed across both cloud and on-premise data centers, there's typically some authentication federation in place to enable logins across hybrid systems. Regardless of how a user connects- whether through a cloud-hosted app, VPN, or on the local network - it's crucial to have strong authentication measures in place. Good IAM systems need to:

- Enforce a solid password policy
- Use multi-factor authentication
- Provide single sign-on capabilities

Add Privileged Access Management — Using IAM as a foundation for login security is a great start. However, implementing Privileged Access Management (PAM) for critical systems takes it to the next level by providing additional protection, accountability, and rollback from any detrimental changes. Accessing a PAM-protected system involves a workflow that requires approval from multiple people. If the request is approved, all session activities are logged in detail and, in some cases, recorded in a video file for future reference. PAM systems can also be configured to prevent the execution of destructive commands on systems. Additionally, many PAM solutions time limit sessions to prevent a single request from being used over an extended period.

Use SIEM — To ensure comprehensive security across all IT devices and applications, it is recommended that endpoint protection and other solutions integrate with a Security Information and Event Management (SIEM) system. A SIEM solution provides a holistic view of the entire IT landscape, including endpoint devices, servers, network equipment, and cloud-deployed applications.

Apply System Patches — IT systems are vulnerable to new threats that frequently emerge, even in systems that have been in use for years. To protect against these vulnerabilities, it is crucial to use systems that are still supported and keep them up to date. However, not all vulnerabilities are detected before cyber criminals find them. When zero-day exploits emerge, there is an urgent need to patch software and resolve the issue. To ensure the best protection, it is important to quickly deploy the latest updates and security patches for operating systems and any software in use. As soon as vulnerabilities are publicly disclosed, cyber criminals will be scanning for unpatched systems to exploit.

Disaster Recovery Plan — To protect against ransomware attacks and ensure overall cybersecurity, it is vital for every member of an organization to be involved in the effort. It is crucial that everyone can identify potential threats and knows the necessary steps to take if something seems suspicious. Clear and concise policies and procedures are vital, outlining specific actions to take in all possible scenarios. Different teams will have different procedures to follow, such as end-users versus IT and security teams. Documented procedures should be frequently reviewed and updated to include new information.

Staff Awareness Training — Cybersecurity training for staff should be frequent, easy to understand, and cover technical and social engineering techniques that attackers use to trick people into making mistakes. Most successful ransomware attacks happen when someone is tricked into following a link, opening a file, or sharing sensitive information. Modern cybersecurity training solutions can simulate Phishing attacks to test users and gather data on who needs further training. These simulated attacks are harmless and pose no risk to the organization but are excellent in preparing staff to deal with real Phishing threats.

Early Detection with Flowmon

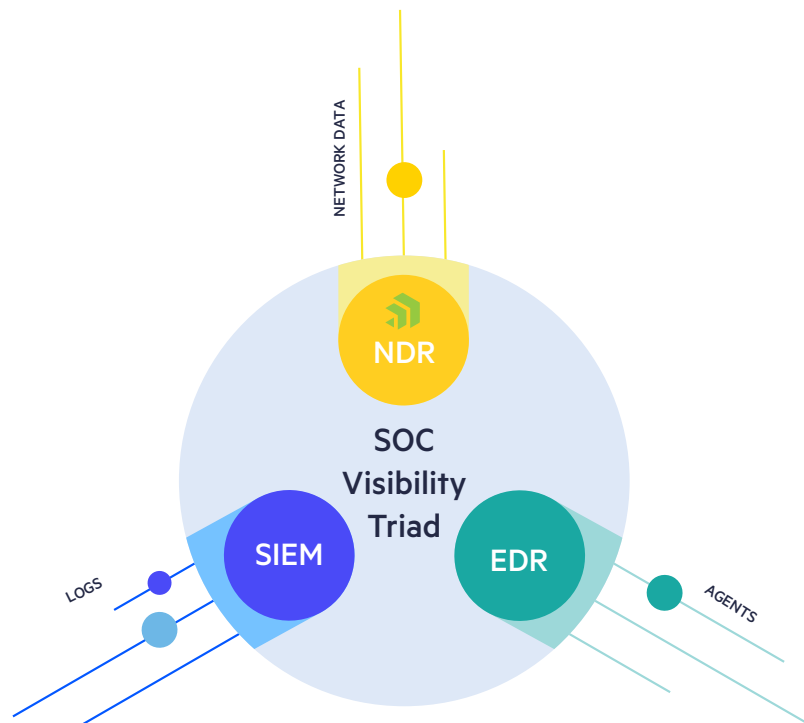
A major requirement for any cybersecurity strategy to prevent ransomware from causing significant financial, reputational, and operational damage is to have network monitoring solutions that can detect anomalies from baseline behavior in real time.

The Flowmon Anomaly Detection System (ADS) is a cutting-edge solution that employs machine learning to monitor networks in real-time. Its primary purpose is to detect any unusual network activity generated by unauthorized users. The system utilizes multiple built-in detectors for various attack activities and methods. It also employs algorithms that use heuristics, machine learning, and other techniques to analyze the data collected. All these methods build up a comprehensive picture that allows Flowmon to inspect the traffic in ways that are not available to simpler solutions.

The SOC Visibility Triad

Gartner created the SOC (Security Operations Center) Visibility Triad as a way to combine and discuss three main pillars needed for robust cybersecurity:

- EDR for endpoint security
- SIEM for processing logs & events and presenting the big picture
- NDR for network monitoring, anomaly detection, and response (Flowmon is an NDR solution that operated in this part of the SOC Triad)



As the diagram above shows, NDR targets the analysis of network data. In contrast, SIEM analyses log data (and other system information), and EDR monitors and protects endpoint devices using agents. NDR solutions have emerged from existing network monitoring solutions to add another layer to defenses by providing SOC teams with real-time metrics about network traffic and behaviors, alerts on suspicious activities, and automated responses to stop potential attack activity before it can do extensive damage. This NDR part of the SOC Visibility Triad is crucial for the early detection and mitigation of ransomware attacks.

How Flowmon ADS Enhances Cybersecurity Defense and Response

Flowmon ADS delivers NDR that works with SIEM, EDR, and other modern technology approaches like XDR engines or SOARs deployed at various layers and locations within the IT infrastructure. Logically ADS fits into overall cybersecurity between perimeter defenses and endpoint security by monitoring network traffic to spot anomalies that could indicate malicious activity not detected by the perimeter and endpoint security tools.

Tools that monitor network traffic and use statistical algorithms to highlight deviations from baseline behavior have been available for some time. Flowmon ADS is an evolution of these analysis tools that goes beyond traditional statistical analysis. As such, it is more sensitive and can help detect the subtle tactics used for modern ransomware.

Flowmon ADS does not rely on signatures of known ransomware and other threats. It also uses detection technologies based on machine learning, adaptive baselining, heuristics, behavior patterns, and reputation data from across the industry to monitor networks and identify anomalous behavior. These multiple detection methods draw on data sources from across the network:

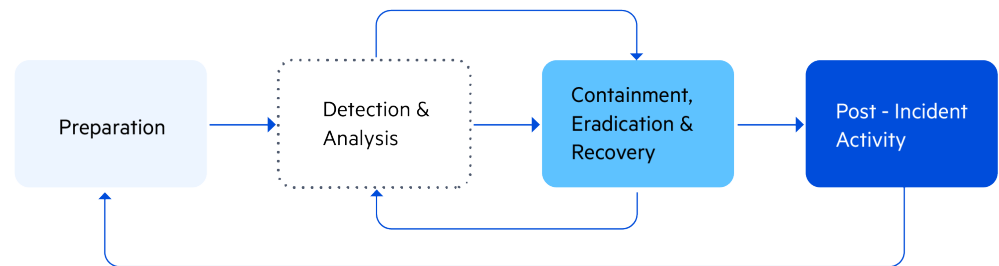
- Propriety Enriched Network Telemetry.
- 3rd-party NetFlow/IPFIX data and compatible standards.
- Raw network packet data (when required).
- User identity information.
- Custom threat intelligence.
- Intrusion Detection System (IDS) signatures.
 - Flowmon does not rely on signature detection but provides it as additional insight for security operations.

These methods and data sources allow Flowmon to detect known and unknown attack vectors that signatures for anti-malware and other protective solutions do not include.

Incident Response using Flowmon

There are many standards and recommendations for Incident Response procedures, and each organization, when creating its Incident Response Plan, will design around their individual needs and the subjective impacts of a potential ransomware incident.

Many organizations use NIST (National Institute of Standards and Technology) standards in cyber security. The NIST Incident Response Cycle is a framework that outlines the key stages involved in responding to and managing cybersecurity incidents. It provides a systematic approach to incident response, helping organizations effectively detect, analyze, contain, eradicate, and recover from security incidents. Flowmon can play a key role in this approach at every point of the cycle shown in the diagram below:



A diagram of a computer system

- 1. Preparation:** This stage involves establishing an incident response capability within an organization. It includes compiling a list of IT assets such as networks, servers, endpoints, and applications, identifying their importance, and highlighting which ones are critical or hold sensitive data. For preparation data gathering, Flowmon helps by understanding what assets are in the network as well as discovering some potentially unknown assets.
- 2. Detection and Analysis:** In this stage, organizations monitor their networks and systems to detect potential security incidents. Flowmon NDR (Network Detection System) is used to identify indicators of compromise (IoCs), unusual activities, or suspicious behaviors. Once detected, the events related to the incident are analyzed autonomously in real-time to determine their nature, impact, and extent. Flowmon highlights anomalies using events categorized according to the character of network traffic that has been evaluated as anomalous. Each event is assigned a priority, and these events are grouped by category. This is done in a two-step process.

- **Step 1**

Identify the originator, context, and analysis of the attack automatically with Flowmon ADS (Anomaly Detection System) with built-in IDS (Intrusion Detection System). When analyzing events, Flowmon uses the severity of events (Critical, High, etc.) and then analyses the individual categories of the events, the originator of the event, and also identifies the device it originated from. Flowmon determines the stage of the attack by MITRE ATT&CK framework classification to the detected event. Detected events allow Flowmon to reconstruct the activity of attackers, identify the targets of the attacks, estimate their intentions, and choose a suitable defense strategy.

- **Step 2**

Threat hunting and analyzing related data flows - An attacker's activities may be wider than the range of events detected by the Flowmon ADS module. All the activity of attackers, any compromised devices, and the general impact of security incidents can be analyzed in Flowmon Monitoring Center (FMC), which records, archives, and visualizes data network traffic in the form of data flows and in Flowmon Packet Investigator (FPI) which provides full packet capturing of events automatically. Using the information obtained in Step 1, Flowmon can identify all the communication on the network related to an attacker, potentially affected systems, the attacker's activity, and any other potentially compromised systems and show it in summary on a chart.

3. Containment, Eradication, and Recovery: Once an incident is confirmed, the focus shifts to containing its impact and preventing further damage. This stage involves taking immediate action to isolate affected systems, disconnect compromised accounts, and mitigate the threat. As part of containment, it is important to identify the attacking host and validate its IP address. This allows the blocking of communication from the attacker and also identifies the threat actor to understand their mode of operation, plus the identification and blocking of any other communication channels they may be using. All that is possible thanks to Flowmon's detection and analysis capabilities.

The next step is eradication, which involves removing the attacker's presence from the affected systems and ensuring the systems are secure. Finally, recovery activities are initiated to restore systems, data, and services to their normal state. This can't be guaranteed without continuous Flowmon monitoring to ensure complete eradication without any potential attacker backdoors being used for

further attacks. Flowmon monitoring at this stage also validates the restoration of systems by comparing the consistency of current network communication between applications and end users with the network data captured in the preparation phase before the incident occurred.

- 4. Post-Incident Activity:** After the incident has been contained and normal operations have been restored, organizations engage in post-incident activities. This includes conducting a thorough post-mortem analysis to understand the incident's root cause, identifying any vulnerabilities or weaknesses in the organization's security posture, and implementing remediation measures to prevent similar incidents in the future. Lessons learned from the incident are documented, and necessary updates are made to incident response plans and procedures. Here, Flowmon provides its greatest added value in network forensics thanks to its long-term data retention - weeks, months, or years. The detail and granularity of the data, the visualization, and the possibilities of contextual analysis make it possible to check any digital trace related to ransomware and other incidents for reporting, learning lessons, increasing the organization's resilience, or for investigations by law enforcement agencies.

Flowmon can be integrated with a configuration management database (CMDB) system that records information about the assets of a given environment with links for information about any given device. This allows the quick identification of devices plus their context when analyzing security incidents.

Flowmon Typical Use Case

From existing deployments of Flowmon ADS across multiple sectors, we see indicators of compromise from ransomware attack activity highlighted, and attacks stopped before they infect too many systems and impact is substantial. In the interests of anonymity, rather than outline a named and detailed case study, we'll use a summary of where in typical ransomware attack activity, ADS can detect, alert, and allow the eradication of ransomware attacks.

When attackers gain access to a network with ransomware, the following activities occur to allow the infection to spread, find interesting data to exfiltrate, and then encrypt vital resources before issuing ransom demands.

Discovery - The initial infection on a device or server on the network performs discovery scans to find other systems that can be targeted. These typically use an ARP scan that looks for devices that are available on the same network, followed by a vertical TCP SYN scan, where the ransomware is looking for services that can be compromised. These scans show up in the network flow data that ADS monitors and are flagged as anomalies.

Credential Attacks - Once other systems have been discovered, ransomware attacks will use brute force login attempts to access them. This is typically done using a password spray attack that uses many typical account and password combinations to find a match that works and grants access. Hopefully, in 2023 the accounts and passwords used on systems will be unique, random, and strong. ADS will highlight this network activity if it occurs.

Vulnerability Exploits - Another common attack vector used is to exploit known vulnerabilities in systems that may not have had patches applied. There are many known and exploitable vulnerabilities in IT systems that attackers can use to get access. And new ones are discovered, patched, and announced regularly. ADS can detect the unusual network activity that frequently results after a vulnerability is exploited and attackers are operating on a network.

Data Exfiltration - Extracting data to see or hold for ransom is part of almost all current ransomware attacks. Attackers attempt to hide that they are copying data from the network to a server they control. One of the ways to do this is by splitting the data into smaller chunks and exfiltrating the data using DNS queries or pinging the data out of the network. Flowmon ADS can detect these events and even capture full network traffic for further forensic analysis. This can be very useful if a Ransomware attack is successful, as it can often be challenging for organizations to tell if and what data has been exfiltrated. Analysis of packets that have left the network will show if data has been hidden in this traffic.

Encryption - The final stage of a ransomware attack is data encryption. If the attackers have not been detected on the network before this starts, then it's crucial that this activity is detected and steps are taken to mitigate the damage. A Flowmon customer recently caught encryption on a network share, and they were able to identify and isolate the infected host quickly. The damage was contained to one data store and only a few files.

Conclusion

Protecting against ransomware attacks requires both technical solutions and the vigilance of people using IT systems. Flowmon's early detection of anomalous network behavior delivers a much lower chance of organizations getting impacted by ransomware.

References

1. **Progress Flowmon: Cybersecurity Outlook for 2023** - <https://www.flowmon.com/en/resources/ebooks/cybersecurity-outlook-2023>
2. **SonicWall: 2023 SonicWall Cyber Threat Report Casts New Light On Shifting Front Lines, Threat Actor Behavior** - <https://www.sonicwall.com/news/2023-sonicwall-cyber-threat-report-casts-new-light-on-shifting-front-lines-threat-actor-behavior/>
3. **Sophos: The State of Ransomware 2023** - <https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/>
4. **Progress Kemp: What is Ransomware, and how do I stop it?** - <https://kemptechnologies.com/blog/what-is-ransomware-attack>
5. **Flowmon: Ransomware Detection** - <https://www.flowmon.com/en/solutions/security-operations/ransomware-detection>








Request Your Trial

www.flowmon.com/en/download-free-trial

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to build the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com

 /progresssw
 /progresssw
 /progresssw
 /progress-software
 /progress_sw_

2023 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved. Rev 2023/08 RITM0211970