BLUVECTOR®
A COMCAST COMPANY

Detection of Malicious Content over Encrypted Traffic

Encryption is one of the most powerful tools available for data privacy and security. Modern encryption algorithms are secure enough that it is infeasible to access encrypted data without access to the appropriate secret key.

For this reason, the use of encryption for web traffic has grown significantly in recent years. An estimated 80-90% of all Internet traffic is estimated to be encrypted today. This is a significant increase from the estimated 55% of Internet traffic that was encrypted just five years earlier.

While the growth of encryption on the Internet is good for data privacy and security, it also benefits cybercriminals. Encrypted traffic can be used to conceal malicious communications, making it more difficult for organizations to detect malware or data exfiltration. Without security tools capable of identifying encrypted malicious traffic, organizations can be left blind to many attacks.

How Cyber Threat Actors Use Encrypted Communications

The encryption of network traffic provides significant privacy and security benefits to users, but it can also benefit cyber threat actors. Companies commonly rely upon deep packet inspection and network traffic analysis to detect and investigate attempted attacks against their systems.

Cybercriminals are increasingly using encrypted communications at various stages of the cyberattack lifecycle to make their attacks more difficult to detect and remediate. Common uses of encrypted network traffic by cybercriminals include concealing the delivery of malicious content, command and control communications, and the exfiltration of sensitive data from an organization's systems.

Malware and Malicious Content Delivery

Network monitoring is an essential component of a threat detection and prevention strategy. Sensors deployed at a single location can protect the entire network against inbound threats, and if an organization can identify malware or other malicious content in network traffic, it can potentially block it before it reaches its destination and poses a threat to the organization.

However, detecting malware and malicious content in network traffic can require the ability to see the contents of packets on the network. Network-based threat detection solutions often depend on identifying malware based on known patterns or extracting and analyzing it within a sandboxed environment.

If the data within a network packet is encrypted, an organization's network-based threat detection capabilities may be limited. Cyber threat actors know this and commonly encrypt malicious content when sending it over the network to make it more difficult to detect and block at an organization's network perimeter. In 2020, an estimated 70% of malware campaigns used encrypted communications, and the percentage continues to grow.

Command and Control Traffic

Few types of malware are completely "fire and forget." Often, they are designed to communicate back with their handler to send out information and receive instructions. For example, malware that gains a foothold on a system within an organization's network may use its access to explore and map the corporate environment. This information could then be sent back to the operator, who could use it to plan their next move and send instructions to the malware regarding the next steps.

Visibility into command and control traffic can be invaluable for an organization's security team. Some of the ways in which a SOC can take advantage of visibility into command and control traffic include:

- **Threat Detection.** The presence of command and control communications associated with a particular malware variant indicates that an organization is facing a malware infection. Monitoring for known command and control traffic can be part of a corporate threat detection strategy.
- **Incident Investigation and Response.** Visibility into command and control traffic can provide SOC analysts with information about all of the actions that the malware has taken on their systems and the data accessed by it. This information can dramatically expedite the process of determining the scope of the incident, quarantining it, and remediating it.
- **Control Over Malware.** Command and control protocols are designed to allow an attacker to control malware on a target system remotely. If a SOC analyst can send commands to the malware, it is easier to identify infected systems and potentially use built-in functionality to eradicate the infection. Alternatively, blocking commands from being sent to the malware could prevent undesirable actions, such as data encryption or exfiltration by ransomware.
- **Counter-Intelligence.** If a SOC team can intercept command and control communications, they can potentially modify them. These modifications could be used to send false information to the attacker.

The success of a cyberattack depends on the attacker being able to conceal their command and control communications from a defender. One of the most effective ways of hiding command and control traffic is to encrypt it, making it impossible for defenders to read its contents without the appropriate secret key. For this reason, a growing percentage of malware uses encryption to conceal its command and control traffic.

Data Exfiltration

Data theft is a common objective in cyberattacks. In addition to malware specifically designed to steal organizations' or individuals' sensitive data, other types of malware, such as ransomware, are being expanded with data-stealing capabilities. In the case of ransomware, stealing an organization's sensitive data and threatening to leak it provides additional leverage to the attacker when extorting a ransom from the victim.

Gaining access to an organization's sensitive data is not enough for an attacker. They also need to get that information out of the organization's network for it to be useful. However, this dramatically increases their probability of detection. Data loss prevention (DLP) and other solutions can scan network traffic for sensitive data types, such as credit card information or other customer data. If detected, these solutions can raise the alarm or block the traffic performing the exfiltration. Network traffic encryption is invaluable for an attacker looking to exfiltrate data from an organization as well. For example, consider the case where an attacker is uploading sensitive data to Google Drive or other cloud-based storage via an HTTPS connection. Without visibility into the encrypted traffic, it can be difficult for an organization to differentiate this attempt at data exfiltration from the use of an organization's legitimate cloud-based infrastructure by an employee. Data encryption makes data exfiltration much more challenging to detect and prevent, amplifying the cost of a cyberattack to its victim.

The Future Growth of Encrypted Communications

Encrypted Internet traffic has grown dramatically in recent years. This provides cyber threat actors

with many opportunities to conceal malicious traffic amongst legitimate encrypted traffic.

The Internet is currently in the midst of a transition from unencrypted to encrypted protocols. In the past, many webpages containing only non-sensitive information used HTTP; now, HTTPS is the default. Other protocols containing useful and potentially sensitive information are also moving toward encryption. For example, DNS has historically been an unencrypted protocol, but the emergence of DNS over HTTPS (DoH) and DNS over TLS (DoT) means that a growing percentage of this traffic will be encrypted as well.

As these protocols move toward encryption, a growing percentage of malware command and control traffic will be encrypted as well. DNS is a common command and control mechanism because it is permitted through corporate firewalls. Also, the owner of a DNS record determines where requests for that record are sent, enabling requests for attacker-controlled domains to be sent to attacker-controlled servers. DNS traffic analysis is a common way to identify phishing attacks and malware infections that make requests for known-bad domains. With the emergence of encrypted DNS, network traffic analysis alone will no longer be enough. Achieving crucial DNS visibility will require the ability to access and process logs from a local DNS resolver, a capability that many organizations currently lack.

How to Manage the Threat of Encrypted Communications

Without visibility into the contents of network traffic, detecting and managing the threat of encrypted malicious communications can be complex. One common way companies attempt to address the impacts of encrypted communications on network visibility is by using a proxy to break the encryption of TLS traffic. However, this approach carries significant security risks, including:

- **Lack of Certificate Validation.** With TLS introspection, client computers are configured to accept the proxy's digital certificate for all websites, allowing the proxy to create separate encrypted connections between itself and the client and server. As a result, a client cannot see or validate the digital certificate presented by the webpage that they are visiting.
- **Centralized Security Risks.** TLS introspection proxies decrypt all TLS traffic passing through them for inspection. If an attacker gains access to the proxy, this provides full visibility into all network traffic flowing through the proxy.
- **Limited Encryption Visibility.** TLS introspection assumes that all malware and cyber threat actors will use TLS for traffic encryption, allowing the proxy to break the encryption. However, malware commonly uses baked-in encryption algorithms to protect its command and control traffic, which the proxy lacks the ability to read.
- **Regulatory Compliance.** The data contained within network traffic may be protected under the GDPR and similar data privacy laws. Decrypting and inspecting this traffic not only violates user privacy but may also be grounds for legal action.

The limitations of TLS introspection make it a less-than-ideal solution for detecting encrypted malicious communications on the network. However, it is not the only option available to an organization. Even without visibility into the contents of network traffic, a security team can learn a great deal from the encrypted traffic itself and where it goes.

For example, the traffic patterns within an organization's network can indicate the presence of various threats. Traffic between two hosts that do not normally communicate could be a sign of network scanning or attempted lateral movement. Large volumes of outbound traffic from a particular host could indicate attempted data exfiltration.

The use of machine learning and anomaly detection algorithms can enable an organization to identify unusual traffic flows that could point to a potential threat to the organization. With knowledge of common traffic flows within an organization, network traffic monitoring solutions can identify anomalies that could indicate potential threats and that warrant further investigation.

Detecting Encrypted Communications with BluVector

Encryption of malicious network traffic is designed to deny an organization visibility into potential threats. Data protected by strong encryption algorithms can't be read without access to the corresponding secret key. While this may be good for data privacy and security, it can also make it more difficult for security personnel to identify and respond to threats to the organization. BluVector enables SOC teams to overcome the challenges associated with encrypted malicious communications by providing improved network visibility and context. Capabilities that enable BluVector solutions to identify encrypted malicious traffic include:

- **Supervised Machine Learning.** Supervised machine learning doesn't require labeled training data to learn how to identify potential threats or significant events within network traffic. This allows BluVector solutions to identify novel threats and anomalies of interest in encrypted traffic.
- **Continuous Learning.** BluVector's machine learning algorithms are built based on decades of experience in malware detection and continuously learn and update their models based on new observations. This enables them to accurately identify evolving threats while minimizing false-positive alerts.
- **Entity-Centric Reporting.** Security teams are commonly overwhelmed with massive numbers of alerts. BluVector solutions correlate alerts to associated entities, providing improved context and eliminating alert overload.
- **Automated Triage and Risk Scoring.** BluVector solutions assign risk scores to each entity within an organization's environment and present the highest-risk entities to analysts first. This enables SOC analysts to focus their time and effort and maximizes their impact on corporate cybersecurity.
- **Attack Chain Synthesis.** BluVector solutions automatically correlate related alerts and synthesize network traffic into potential campaigns. This enables analysts to more rapidly identify potential threats without requiring visibility into the contents of encrypted traffic.

Cyber threat actors' use of encrypted communications is designed to leave companies blind to threats entering and present in their networks. BluVector solutions can help organizations detect these attacks without placing the security of their networks at risk. For more information about identifying and protecting your organization against encrypted malicious traffic, schedule a meeting or request a demo of the BluVector platform today.

BluVector
4501 North Fairfax Drive, Arlington, VA 22203
www.bluvector.io