radware
Every second counts

Issue 1

Protecting from a Growing Attack Vector: Encrypted Attacks

1
SSL and Encrypted Attacks on the Rise

3
Research from Gartner: Security Leaders Must Address Threats From Rising SSLTraffic

8
Understanding Performance Impacts on Security Infrastructure from Encrypted Attacks

9
Radware's SSL/Encrypted Threat Solutions

10
ProtonMail Overcomes Back-to-Back Attacks: Highly Sophisticated DDoS Attack Targets Encrypted Email Provider

12
SSL Encrypted Traffic Creates New Security Challenges for the Enterprise

14
About Radware

SSL and Encrypted Attacks on the Rise

New Research Highlights Gaps in Protection

It is a common situation that the mass adoption of certain technologies is followed closely by efforts to exploit their wide use through any number of security threats. SSL is no exception to this rule, and has experienced a large number of highly publicized vulnerabilities forcing users to move to new, more secure versions, and ultimately towards a replacement protocol (Transport Layer Security).

However, exploits of newly identified vulnerabilities are not the only way that SSL adoption is being used as a weapon in the hands of malicious actors and adversaries behind cyber threats. Increasingly, SSL is being used to mask and further complicate attack traffic detection in both network and application level threats.

This year's Global Application & Network Security Report from Radware indicated that 35% of respondents have been the target of an SSL or TLS-based attack, representing nearly a 50% increase from the prior year. What is also clear from the Radware survey is that many security professionals are unsure of the ability of their current security architecture to protect from these attacks. Only 31% said they currently have the ability to defend against an SSL flood attack, while 48% said they were unsure.

Other research similarly supports the need for focus on encrypted attack vectors. In its report entitled "Security Leaders Must Address Threats From Rising SSL Traffic," Gartner Research noted that encrypted and encapsulated traffic "weakens defense-in-depth efficiency, exposing endpoints and DMZ servers to threats from outbound and inbound traffic."

One of the reasons SSL attacks are becoming more popular among attackers is that they require only a small number of packets to cause denial of service for even a fairly large server. Attackers launch attacks that use SSL because each SSL session handshake consumes 15 times more resources from the server side than from the client side, meaning their attack is exponentially increased in size without requiring them to tap into additional bots or bandwidth. As a result of these amplification effects, a single standard home PC can take down an entire SSL-based web server, while several computers can take down a complete farm of large, secured online services.

Gartner

SSL-based attacks take many forms, including:

SSL Renegotiation: these attacks work by initiating a regular SSL handshake, and then immediately requesting for the renegotiation of the encryption key. The tool constantly repeats this renegotiation request until all server resources have been exhausted.

HTTPS Floods: these attacks generate floods of encrypted HTTP traffic, often as part of multi-vector attack campaigns. Compounding the impact of "normal" HTTP Floods, encrypted HTTP attacks add several other challenges, such as the burden of encryption and decryption mechanisms.

Encrypted Web Application Attacks: Multi-vector attack campaigns also increasingly leverage non-DoS, web application logic attacks. By encrypting the traffic masking these advanced attacks, they often pass through both DDoS and web application protections undetected.

Encrypted Outbound Traffic: As usage of SSL/TLS encrypted traffic increases, organizations are losing visibility into outbound traffic going through encrypted sessions. Security solutions such as data leakage prevention lose their visibility into the growing portion of traffic that is encrypted.

Fixing a Flawed Protocol

Another important factor related to SSL attacks is the high frequency of serious vulnerabilities related to the protocol, itself. The significant portions of the Information Technology universe leveraging SSL got a major wake-up call in April 2014 with the disclosure of the Heartbleed vulnerability associated with OpenSSL implementations. While far from the first, Heartlbleed was arguably the SSL vulnerability with the widest potential reach and impact, as an estimated 17% of SSL implementations were using the vulnerable instance of OpenSSL software. Some other major SSL vulnerabilities have emerged over the years, including the long standing (and sill impactful) RC4 vulnerability originally discovered in 2002, and the more recent POODLE vulnerability that exploits some software logic to failback to SSL 3.0 (exposing other known vulnerabilities).

The Payment Card Industry, which manages the Data Security Standard required for merchants, is requiring in version 3.1 of the standard a move off of SSL (or the corresponding early versions of TLS) to version 1.1 of TLS by June 2018. This represents a two-year delay from the original deadline of June 2016, which should give organizations sufficient time to take a holistic look at how they're dealing with encryption within the environments and address significant blind spots.

One likely result of the shift towards TLS 1.1 is the increased use of longer keys. The most commonly used level of encryption currently is 2048 bit keys, as the lower level 1024 bit keys have been shown to be 'hackable.' But many are starting to call for and move towards the use of 4096 bit keys. As key length increases, so too do the CPUs required for systems processing the encrypted transactions. This increase will put additional strain on security solutions that need to inspect encrypted traffic to eliminate the common blind spot to encrypted attacks that many solutions suffer from.

A Problem Poised to Get Worse

Despite some high profile security issues, SSL (and TLS) remain the standards for ensuring secure communications and commerce and the web, and have seen dramatic growth in recent years. According to Netcraft, the use of SSL by the top one million websites has increased by 48% over the past two years. As more and more sites add SSL or TLS capabilities, user adoption in turn will also increase. For many years, the thought was that you needed to implement SSL to support security if you had an ecommerce site or were otherwise supporting credit card transactions on your site. Those limitations have gone any with the growth of other purposes for secure communications.

The technology industry has actively been pushing broader adoption of SSL/TLS. Initiatives such as the "Let's Encrypt" project that is launching a new, free certificate authority in an effort to move more users over to encrypted online communication and commerce.

For more on the challenges posed by encrypted attacks, and critical capabilities for protection, read "Understanding Performance Impacts on Security Infrastructure from Encrypted Attacks."

Source: Radware

Research from Gartner:

Security Leaders Must Address Threats From Rising SSL Traffic

SSL encryption provides confidentiality for the encapsulated traffic but weakens enterprise defense-in-depth efficiency, exposing endpoints and DMZ servers to threats from outbound and inbound traffic. This research will help enterprise security leaders to create a traffic decryption strategy.

Impacts

An increasing share of enterprise network traffic is encrypted, creating gaps in defense-in-depth effectiveness that security leaders should not ignore.

Complex sets of laws and regulations on privacy, along with a high risk of conflict with employees, kill most security leaders' outbound Web traffic decryption projects.

Security leaders face limited technology choices for enterprise network traffic decryption, and these solutions often induce high costs and poor user experience.

Recommendations

Evaluate the security risks coming from uninspected encrypted network traffic. Update relevant risk indicators accordingly, and request a sign-off from key stakeholders for acknowledged risks.

Prepare for a legal assessment of traffic decryption with network diagrams, types of decryption to occur, whitelists and data logged, in addition to the safeguards being taken.

Review existing privacy and network usage policy to determine if decrypting the traffic requires a policy update. Engage with HR and worker representatives throughout the entire decision and implementation life cycle.

Leverage existing network security solutions to enforce the outbound Web policy on SSL traffic, based on server reputation or the information available from the SSL certificate. Then, establish a prioritized list of the traffic profiles you need to decrypt.

Analysis

The inspection of network traffic is a core component of a network security policy strategy and often involves more than one technology. In the interests of enterprise security, communications to internal and external servers are encrypted. Paradoxically, this Secure Sockets Layer (SSL) traffic "blinds" other network security mechanisms from inspecting this traffic. Full coverage of the enterprise network with best-of-breed traffic inspections is beyond the capabilities of many enterprises. Oftentimes, security solution architects have to make compromises — one of these compromises is decrypting traffic because of an insufficient awareness of related threats and the inherent complexity of decryption projects.

Gartner conducted an industry survey of network security vendors and enterprises this year to find out how organizations are tackling the challenge of traffic decryption (see Note 1). The survey revealed that less than 50% of enterprises with dedicated secure Web gateways decrypt outbound Web traffic. Less than 20% of organizations with a firewall, an intrusion prevention system (IPS) or a unified threat management (UTM) appliance decrypt inbound or outbound SSL traffic. However, more than 90% of organizations with a public website and a Web application firewall (WAF) decrypt inbound Web traffic.

In response to attacks and compromises, many major public Web services have already switched to HTTPS by default (Google, Yahoo, Twitter, Facebook and Wikipedia).[1] Mobile application toolkits and HTML5 frameworks remove most of the complexity of enabling SSL communication by default. As a consequence, the amount of encrypted traffic represents an increasing share of enterprise network traffic, with steady growth every year. Web traffic encrypted using SSL (HTTPS) accounts for 15% to 25% of total outbound Web traffic and often carries sensitive or personal data.[2]

Already, malware is using SSL to remain under the radar of network security solutions. For example, the pervasive Zeus botnet uses SSL communication to upgrade after the initial email infection. Following the Boston Marathon bombing, a malware attached to a spam message was also using SSL to communicate with its command and control server.[3] With more and more encrypted traffic, this trend is likely to expand rapidly. Gartner believes that, in 2017, more than half of the network attacks targeting enterprises will use encrypted traffic to bypass controls, up from less than 5% today.

FIGURE 1

Figure 1. Impacts and Top Recommendations for Building a Traffic Decryption Strategy

Impacts	Top Recommendations
An increasing share of enterprise network traffic is encrypted, creating gaps in defense-in-depth effectiveness that security leaders should not ignore.	• Evaluate the security risks from uninspected encrypted network traffic, and update relevant risk indicators. • Quantify your current encrypted traffic mix, and anticipate a 10% to 20% yearly growth.
Complex sets of laws and regulations on privacy, along with a high risk of conflict with employees, kill most security leaders' outbound Web traffic decryption projects.	• Prepare for a legal assessment of traffic decryption, in addition to the safeguards being taken.
Security leaders face limited technology choices for enterprise network traffic decryption, and these solutions often induce high costs and poor user experience.	• Leverage existing network security solutions to enforce the outbound Web policy on SSL traffic. Then, establish a prioritized list of the traffic profiles you need to decrypt.

Source: Gartner (December 2013)

Organizations without traffic decryption plans are blind not only to these new sophisticated attacks but also to any attacks that take place over encrypted connections. These enterprises will suffer or may already have suffered from undetected malware activity. Security leaders who seek to include encrypted traffic in their global network security strategies face numerous technical, organizational and human challenges.

Impacts and Recommendations

An increasing share of enterprise network traffic is encrypted, creating gaps in defense-in-depth effectiveness that security leaders should not ignore

For most organizations, SSL traffic is already a significant portion of their outbound Web traffic and is increasing. It represents on average 15% to 25% of the total Web traffic, with strong variations based on the vertical market.[2] The amount of Web inbound traffic that is encrypted varies highly among enterprises, mainly depending on the availability of a secure client Web area or an e-commerce component. Internal traffic for business applications might also be encrypted.

Internal, inbound and outbound traffic each carries different risks and creates different challenges (see Table 1). Even if Web SSL represents a majority of the encrypted traffic, a recent report from Palo Alto Networks, based on real enterprise traffic, shows that 23.8% of the applications using SSL were not using the standard SSL ports.[4] Enterprises with non-standard-encrypted traffic need to ensure that this is explicitly authorized.

According to a Gartner survey of network security vendors, less than 20% of firewalls, UTM and IPS deployments include network traffic decryption (see Note 1). This means the encrypted traffic often is not protected with intrusion prevention technology. Defense in-depth is reduced to what dedicated solutions can provide.

For inbound traffic, decryption is often part of a performance optimization project with an application delivery controller (ADC) performing SSL offloading and, therefore, enabling the inspection of traffic. Ninety percent of enterprises with an ADC or a WAF decrypt inbound traffic.

However, the situation is not so good for outbound Web traffic: Gartner estimates that less than 50% of enterprises with secure Web gateways (SWGs) use them to decrypt and inspect SSL traffic. Along with the lack of coverage from firewalls and network IPSs, a majority of outbound SSL traffic is not inspected by any network security technology. Many network security solutions can decrypt only HTTPS and are unable to decrypt other protocols (such as SMTPS, IMAPS, SFTP or SSH), which could prevent an organization from achieving its expected coverage for encrypted traffic inspection. Enterprise data loss prevention and endpoint protection are alternate solutions that can compensate in some situations for the lack of network protection.

Organizations that leverage a man in the middle (MITM) approach to intercept and decrypt SSL traffic make themselves attractive targets to attackers (see Note 3). Decrypting the traffic exposes data that would be otherwise unavailable on the organization's network (credit card numbers, personal information and so on). Even when traffic is immediately re-encrypted on network security devices, this information might leak through the log files or be stored locally in temporary files.

Recommendations:

- Weigh the risks coming from uninspected encrypted network traffic, and update the key risk indicators accordingly. Raise awareness among key stakeholders.
- Initiate a multiyear plan to improve your organization's coverage of encrypted traffic, and start with inbound and outbound Web traffic.
- Quantify your current encrypted traffic mix, and anticipate a 10% to 20% yearly growth when evaluating future network security purchases.

Complex sets of laws and regulations on privacy, along with a high risk of conflict with employees, kill most security leaders' outbound Web traffic decryption projects

Gartner clients cite organizational complexity as the first reason why they would not tackle a decryption project before dealing with the technical issues. Local privacy laws could prevent or restrict an organization from decrypting traffic that is considered private communications (see Note 2). Enterprises should charge their legal departments to validate that they comply with local laws and regulations for:

1 Decrypting traffic

2 Intercepting communications that were not monitored due to encryption

3 Storing data ("data retention") previously unavailable due to encryption

Multinational enterprises could face additional challenges with regulations that vary based on the location of the employees. "Hub and spoke" architectures might create even more complex situations, with remote employees being in one country and the decryption being performed in another country.

Decrypting Traffic

The act of decrypting should not fall under any specific regulation. However, intercepting outbound SSL traffic requires replacing the public server certificate with a certificate created by the surveillance device (see Note 3). Stringent legal interpretation of MITM interception could tie interception to the network security device, viewing traffic interception as usurpation of the website's identity.

Employee Surveillance

Monitoring employees' communications and storing communications data are often restricted by law. In the U.S., the Electronic Communications Privacy Act (ECPA) and several state laws impact how enterprises can monitor their employees. Similar laws exist in certain European nations and in other countries (see Note 2). Adding encrypted

communications to an existing surveillance program expands the scope of the program and might require updating the privacy policy and employee notifications for these reasons:

- Employees expect encrypted communications to be private.
- Data carried over the encrypted channel is more likely to include personal or confidential data, such as personally identifiable information (PII) and electronic personal health information (ePHI).

Enterprises should re-examine policies for Internet, social media and email usage to ensure they cover encrypted traffic, update the policies if need be, and inform employees if required or advised by the HR department.

Whitelisting categories of websites is a complementary compliance tactic. Gartner clients often put banking and health websites on a whitelist and do not decrypt this traffic. Webmail requires specific attention, since it is a vector for threats, but also carries private communications.

To reassure key stakeholders from the legal department, HR and worker councils, security teams should explain the level of automation for network traffic decryption and subsequent re-encryption, the amount of logged information, and the approval workflow for monitoring or changing security policy.

Data Retention

Network security appliances that perform traffic decryption can log connection metadata (IP and port, time stamp, and protocol headers). In the case of a dedicated decryption appliance forwarding decrypted traffic to a full-packet capture device, the whole data is stored. An enterprise firewall with application and user control features might also store additional application data and user identities in its log.

To improve the organization's compliance with local data retention laws (see Note 2), security teams in charge of the decryption project should check the amount of information logged on decrypted traffic for different protocols and reduce the amount of logged traffic when possible. It is also important to assess the right duration for data retention since minimum and maximum data retention durations might apply from distinct regulatory constraints.

Prepare for Environment Changes

Recent leaks about state-level access to encrypted communications increase the uncertainty around encryption technologies and regulations. As a safety measure, it is important to get ready for important changes around the legitimacy of existing encryption algorithms or the obligation to use new mechanisms. Organizations should prepare for such an eventuality with a privacy continuity plan, similar in nature to a business continuity plan. The privacy continuity plan would cover the impacts and action plan across the entire organization, in case an encryption algorithm (such as AES) or a protocol implementation (such as SSL or IPsec) suddenly becomes deprecated or vulnerable, such as what happened with RC4.5 It should also prepare the organization for situations where changes in the software implementation or encryption algorithm prevent the inspection of traffic for security reasons.

Recommendations:

- Prepare for a legal assessment of traffic decryption with network diagrams, types of decryption to occur, whitelists and data logged, in addition to the safeguards being taken.
- Review the existing privacy and network usage policy to determine if decrypting the traffic requires a policy update. Engage with HR and worker representatives throughout the entire decision or implementation life cycle.
- Make available to employees the elements that demonstrate how privacy issues are handled, including a list of whitelisted domains, sample log data and access restrictions for sensitive data.

Draft a privacy continuity plan to anticipate situations where a flaw is found in an encryption algorithm or software implementation.

Security leaders face limited technology choices for enterprise network traffic decryption, and these solutions often induce high costs and poor user experience

Setting up outbound traffic decryption is complex, relying on MITM interception that impacts the enterprise network and user experience (see Note 3). A network security solution intercepting outbound HTTPS traffic analyzes a minimum of three connections for each SSL connection intercepted: (1) decrypting the client's SSL connection; (2) inspecting the decrypted HTTP; and (3) encrypting the SSL connection to the server.

Decrypting Traffic Has Multiple Effects on the Enterprise Network

Embedded hardware acceleration, when available on network security platforms, often provides limited value. A recent study from NSS Labs reported that decrypting SSL traffic on a firewall implies a loss of 74% for throughput and 87.8% for transactions per second.6 The network latency also suffers, especially during the initial steps of the SSL connection. By the end of 2013, 1024-bit RSA keys will be deprecated by certificate authorities in favor of 2048-bit keys.7 Longer keys will increase the workload needed by the SSL decryption engine, and worsen the existing situation.

Enabling traffic decryption or re-encryption on a firewall, SWG or an IPS will reduce the overall performance of the appliance, often by more than 80%, which, depending on the traffic mix for the organization, often means effectively doubling the network traffic inspection spend. It impacts also the overall cost of the network security solution. It forces security buyers to purchase significantly more expensive appliances to handle the additional workload. This reflects on initial hardware purchase costs, as well as on every support and software option since they are often priced as a percentage of the initial appliance cost.

This performance degradation reflects on user experience, and can prove unacceptable from an employee productivity standpoint. Gartner clients who have initiated SSL decryption projects report that the performance impact is noticeable and is not limited to encrypted traffic when decryption is being performed on the network security platform. Users complain about it, which leads to some projects being halted quickly after the production launch.

Some protocols and applications cannot be proxied, which could create disruptions for business-critical applications that were previously "untouched," thanks to SSL encryption. Before enabling traffic decryption, organizations should seek from their network security vendors a list of known applications that need to be whitelisted.

The performance impact might be lower for inbound traffic, especially in a setup where incoming SSL is decrypted but not re-encrypted ("SSL offloading").

Mitigation Techniques Exist but Are Not Yet Mature

Enterprises can use dedicated decryption appliances that decrypt the traffic once and make decrypted traffic available to multiple stand-alone security protections. This improves the overall performance and simplifies the encryption key management, but could create an environment that is more complex to manage, maintain and audit. It also adds another potential point of failure to the infrastructure. Unfortunately, there are only a few vendors in this space, which limits the available choices.

One more direct way to limit the impact of traffic decryption while improving the overall security coverage is to minimize the amount of traffic to be decrypted. Blocking unwanted servers based on their reputation scores or on specific certificate information is an example of such a work-around. Alternatively, reputation can be used to not inspect "known good" destinations and sources. Most decryption features and products have yet to optimize decryption well and instead opt for a full or nearly full proxying, even for categories where administrators set up a decryption bypass. Organizations using ADCs do SSL termination for inbound traffic. Traffic inspection can be performed by the ADC, or another network security solution can be positioned on the network segment where the traffic is already decrypted.

In addition, content delivery networks (CDNs), vendors offering security cloud services for inbound Web traffic and cloud-based SWGs can decrypt the traffic off-premises. While this relieves the internal network from the burden of traffic decryption, delegating the decryption implies having to share the Web server's secret keys. It allows access to the decrypted data to the cloud service provider, which needs to ensure that it complies with the organization's requirements on privacy.

Recommendations:

- Leverage existing network security solutions to enforce outbound Web policy on SSL traffic, based on server reputation or the information available from the SSL certificate. Then, establish a prioritized list of the traffic profiles you need to decrypt.
- Ensure that network traffic will be decrypted only once. Then, decide whether you will decrypt with your existing network security appliances or with dedicated decryption appliances.
- Ensure that the impact of decrypting traffic based on today's traffic and future growth is reflected in network security budgets.

Evidence

[1] Yahoo will switch to HTTPS by default. A. Peterson, B. Gellman and A. Soltani, "Yahoo to Make SSL Encryption the Default for Webmail Users. Finally." The Washington Post, The Switch blog, 14 October 2013.

Wikipedia plans to progressively switch to HTTPS by default. R. Lane, "The Future of HTTPS on Wikimedia Projects," Tech blog, Wikimedia Foundation, 1 August 2013.

[2] There is no independent organization that gives definitive statistics on global HTTPS usage. Therefore, Gartner has conducted secondary research to consolidate data from several sources, including reports from clients. The share of SSL traffic might vary greatly among different verticals, with financial institutions getting up to 40% of SSL traffic, whereas retailers get a lower than average share of SSL traffic.

[3] Zeus trojan downloads malware using HTTPS. B. Stone-Gross and R. Dickerson, "Upatre: Another Day Another Downloader," Dell SecureWorks, 4 October 2013.

Malware attached to a spam message about the Boston Marathon bombing uses SSL to communicate with its command and control server. N. Villeneuve, "Targeted Attack Campaign Hides Behind SSL Communication," TrendLabs Security Intelligence blog, Trend Micro, 25 April 2013.

Attackers using HTTPS in a drive-by attack. A. Makhnutin, "HTTPS Working for Malicious Users," Securelist blog, Kaspersky Lab, 8 October 2013.

Malware using public online services with HTTPS — Evernote and Google Docs. B. Donohue, "Cybercriminals Use Evernote as C&C," Threatpost blog, Kaspersky Lab Security News Service, 28 March 2013.

L. Constantin, "Malware Uses Google Docs as Proxy to Command and Control Server," Computerworld, 19 November 2012.

[4] "The Application Usage and Threat Report: An Analysis of Application Usage and Related Threats Within the Enterprise," Palo Alto Networks, February 2013. Page 16: "85 of the 356 applications that use SSL never use port 443, nor do they use SSL defined ports (37 hop ports, 28 use port 80, 20 use other ports)."

[5] Recommendation to stop using RC4. Swiat, "Security Advisory 2868725: Recommendation to Disable RC4," Microsoft TechNet blogs, 12 November 2013.

Threats to SSL security. M. Green, "How Does NSA Break SSL?" A Few Thoughts on Cryptographic Engineering blog, 2 December 2103.

[6] J. W. Pirc, "SSL Performance Problems: Significant SSL Performance Loss Leaves Much Room for Improvement," NSS Labs, June 2013.

7 D. Dulay, "Out With the Old: Stronger Certificates With Google Internet Authority G2," Google Online Security blog, 18 November 2013.

Note 1. Gartner's SSL Decryption Survey

During the second half of 2013, Gartner sent a survey to 56 major network security vendors providing enterprise firewalls, SWGs, UTM, IPSs, WAFs and dedicated SSL decryption appliances to understand how their clients were tackling traffic decryption, and 12 vendors responded. The study examined the technologies for traffic decryption and obtained market data about decryption technology usage.

A team of Gartner analysts who follow network security developed the survey and conducted several client inquiries about the current state of their decryption strategies. Both data sources contributed to the estimates provided in this research.

Note 2. Sample Laws Related to Cryptography, Employee Surveillance and Data Retention

Bert-Jaap Koops, "Crypto Law Survey."

U.S. — Electronic Communications Privacy Act of 1986.

U.S. — State laws related to Internet privacy, from the National Conference of State Legislatures.

Canada — The Personal Information Protection and Electronic Documents Act (PIPEDA), Office of the Privacy Commissioner of Canada, 1 April 2011.

Europe — Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Australia — Workplace Surveillance Act, 2005. Part 2, Section 10 requires 14 days' prior notification. Section 12 gives additional requirements for computer surveillance.

Note 3. Intercepting Encrypted Traffic

Decrypting SSL must be done in-line for outbound Web traffic, using an MITM approach. The appliance performing traffic decryption replaces the public Web server certificate with its own custom certificate. To avoid any warning on the endpoint, the client browser must trust the certificate authority that signs these ad hoc certificates. This implies that the network security appliance signs SSL certificates with a certificate authority already trusted in the enterprise, or deploys a certificate on every corporate endpoint, which adds to the burden of SSL decryption projects. A careful user who looks at the certificate will likely notice the interception.

For inbound traffic, this can be done in-line with an ADC or a WAF. This could also be done on a copy of the traffic, since the enterprise owns the server certificates and can provide them to the decryption solution. Working on a copy of the traffic avoids any impact on performance, but does not permit threats to be blocked. Security architects often choose SSL offloading in these situations, especially when an ADC or a WAF is present.

Technical implementations, such as certificate pinning, could prevent MITM interception. Some applications also use SSL encryption as a way to free them from the protocol standard. Once traffic decryption is in use, this often generates false alerts (false positives) and blocks "legitimate" traffic. For example, Microsoft Windows updates would need to be whitelisted.

Source: Gartner Research Note G00258176, Jeremy D'Hoinne, Adam Hils, 9 December 2013

Understanding Performance Impacts on Security Infrastructure from Encrypted Attacks

The Radware 2015-2016 Global Application & Network Security Report highlights as a key trend in cyber security the increased use of encrypted attacks, such as HTTPS floods. Specifically, respondents to the Radware survey indicated that 35% has been the target of an SSL or TLS-based attack, representing nearly a 50% increase from the prior year when 24% of respondents claimed to have been targeted. What is also clear from the Radware survey is that many security professionals are unsure of the ability of their current security architecture to protect from these attacks. Only 31% said they currently have the ability to defend against an SSL flood attack, while 48% said they were unsure.

One of the major advantages that SSL attacks offer to attackers is the ability to put significant computing stress on network and application infrastructures they target. The process of decrypting and re-encrypting SSL traffic increases the requirements of processing the traffic. In many cases, the impact goes beyond the functional performance of security devices used for attack mitigation. Many products or services being used for cyber-attack protection are inline and stateful and cannot handle SSL encrypted attacks, making them vulnerable to SSL flood attacks. Fewer still of these solutions can be deployed out-of-path, which is a necessity for providing protection while limiting impact on legitimate users.

The potential of encrypted attacks also goes beyond basic throughput performance. In the same way SSL and encryption protect the integrity of legitimate communications, they equally effectively obfuscate many attributes of traffic used to determine if it malicious versus legitimate. Some of the solutions being evaluated were using a passive engine for SSL attack protection, meaning they cannot effectively differentiate encrypted attack traffic from encrypted legitimate traffic and can only rate limit the rate of request.

Finally, another complicating factor for managing encrypted attacks is certificate management to enable attack mitigation products and services to inspect encrypted traffic. If the attack mitigation solution requires the use of the actual certificates used on the server hosting the application, this creates significant operational challenges that will not scale, especially in environments where there are a large number of tenants being supported. Imagine having to coordinate changes between network operations and application teams each time a certificate being used to authenticate users against an application is updated. The certificate challenge only grows when organizations look to cloud-based security resources to help with large flood attacks. Often, cloud-only security solutions will require end customers to share their private keys and certificates in order to support decryption and inspection of potentially malicious traffic. This seriously compromises the overall security posture of the customer and in many cases will violate compliance with certain security standards.

Given all of these challenges for maintaining performance, accuracy and integrity what are the key elements that organizations should seek out when looking for effective protection from encrypted attacks?

Here are three attributes that should be investigated by organizations that are including encrypted attack protection in their requirements.

Isolation of Encrypted Attack Traffic from Non-Attack Traffic

Organizations should look for the use of behavioral analysis technologies enable isolation of suspicious encrypted traffic to limit legitimate user impact. By isolating the malicious traffic, it can be routed to separate hardware, allowing SSL attack mitigation to scale more effectively without impacting the throughput of the primary mitigation engine. This will ensure that when a customer is under an SSL attack any non-SSL traffic or any SSL traffic that is not related to the attack experiences zero latency.

This also guarantees no interruption to other mitigations that occur at the same time as part of a multi-vector attack on the same application, or parallel attacks occurring at the same time against other applications.

Independent Security Key Management

Organizations wanting to avoid the operational challenges of managing coordination of keys should look for encrypted attack solutions that work with any certificate signed by the network security team simplifying operations and minimizing overall number of managed certificates. Additionally, to avoid the need to share private keys with a cloud-based service provider, organizations should look for solutions that use an "ingress-only" process. These solutions can be easily expanded to run in the cloud as part of any volumetric mitigation and since they are using different certificates than the server certificates, organizations aren't required to share private keys of their server certificates to extent protection to the cloud.

Source IP Agnostic Mitigation

In the Internet's earlier years, the Internet Protocol (IP) address was the primary means initiating and completing transactions. In time, IP address became a foundational element of user identification and association with certain behaviors or reputational information. But more recently IP addresses have become a much less reliable resource for security, such as attack detection and mitigation. This is especially true for protecting assets sitting behind a Content Delivery Network (CDN). Many attack mitigation solutions utilize rate limiting or blocking by source IP. If attack traffic starts coming through the IPs of one or more CDN nodes all traffic, including legitimate being served up by the CDN, will be blocked. Organizations should seek out an IP address agnostic solution that leverages behavioral analysis that can differentiate between legitimate and malicious traffic coming through the CDN nodes.

Source: Radware

Radware's SSL/Encrypted Threat Solutions

It is clear from the increase in encrypted attacks protection from this growing vector must now be part of an assessment of cyber security solutions. As organizations move down this path they will likely find that many of today's security solutions claim to be able to handle SSL or encrypted attacks, but often put a heavy burden on the user to manage the solution or suffer major performance impacts during encrypted attacks.

Radware offers the industry's most complete SSL or encrypted attack mitigation solution. The solution meets the needs of high capacity mitigation solutions, supports all common versions of SSL and TLS, and isolates suspicious encrypted traffic using behavioral analysis to limit legitimate user impact.

The core elements of Radware's encrypted attack solution include:

- Encrypted DDoS and Flood attack protection: Radware's DefensePro coupled with DefenseSSL provides a highly scalable solution for precise attack detection and mitigation within encrypted traffic
- Cloud-based encrypted attack protection: in response to volumetric encrypted attacks that threaten to overwhelm network capacity, they can be redirect to Radware's DefensePipe which features streamlined certificate management for inspecting encrypted traffic
- Encrypted application layer attack protection: Radware's Appwall and Cloud WAF can decrypt SSL and TLS traffic to detect advanced application threats such as the OWASP Top 10 and encrypted bot traffic
- Outbound encrypted traffic inspection: Radware's Alteon Outbound SSL Inspection Solution intercepts and decrypts SSL sessions to to enforce the outbound Web policy on SSL traffic

One major advantage to the Radware solution is that some components can be deployed out-of-path so that when a customer is under an SSL attack any non-SSL traffic or any SSL traffic that is not related to the attack experiences zero latency. The Radware solution guarantees no interruption to other mitigations that occur at the same time as part of a multi-vector attack on the same application, or parallel attacks occurring at the same time against other applications. Because the Radware solution is designed to use separate hardware, SSL attack mitigation can scale more effectively without impacting the throughput of the primary mitigation engine.

Radware's solution for encrypted attacks works with any certificate signed by the network security team simplifying operations and minimizing overall number of managed certificates. The SSL mitigation process is an "ingress-only" process and can be easily expanded to run in the cloud as part of any volumetric mitigation. Since the Radware DefensePro is using different certificates than the server certificates, customers aren't required to share private keys of their server certificates to extent protection to the cloud.

For organizations with critical assets behind a CDN, Radware provides an IP address agnostic solution that leverages behavioral analysis in conjunction with deep signature based blocking. As a result, it can provide protection behind a CDN and differentiate between legitimate and malicious traffic coming through the CDN nodes. This eliminates the need to do extensive manual whitelisting to allow legitimate traffic through from the CDN while still profiling and blocking attackers floods from bad actors behind the same CDN IP address.

Radware's Alteon Outbound SSL Inspection Solution offers a unified solution that uniquely addresses the challenges and requirements of inspecting encrypted outbound traffic. Based on its advanced URL and Layer 4-7 classification capabilities, Alteon NG seamlessly intercepts and decrypts SSL sessions. The decrypted traffic is then steered to any content inspection security solution such as firewalls, anti-malware, data leakage protection, etc. Alteon NG can be programmed with different security policies for different groups of end users and different application classifications. Each security policy can include any combination of the following actions:

- Intercept and decrypt/re-sign the SSL session
- Pass the traffic untouched
- Service chain multiple security elements based on customer policies and traffic classification
- Only send a copy of the traffic to a predefined destination

It is clear from the dramatic rise in encrypted traffic, both legitimate and illegitimate, that organizations need to eliminate encryption blind spots within security infrastructure. The combination of attack coverage, unique deployment options and coordination across components makes the Radware SSL/Encrypted Attacks solution a strong option for all organizations. Customers can operate with confidence that as encrypted attacks scale in frequency and size, as more online transactions move to encryption, and as new versions of encryption standards emerge, the Radware solution will provide comprehensive, scalable protection.

To learn more about Radware's SSL/encrypted attack solutions, visit www.radware.com.

Source: Radware

ProtonMail Overcomes Back-to-Back Attacks: Highly Sophisticated DDoS Attack Targets Encrypted Email Provider

It is clear that both businesses and consumers are driving an increase in encrypted traffic. According to a recent report from Dell, there was a 109% increase in the volume of HTTPS web connections from January 2014 to January 2015 (2015 Dell Annual Security Report). For many years, the thought was that you needed to implement SSL to support security if you had an ecommerce site or were otherwise supporting credit card transactions on your site. Those limitations have gone any with the growth of other purposes for secure communications. One area of dramatic growth is around encrypted email services.

A recent series of attacks highlighted how providers of encrypted service can become targets for encrypted attacks. ProtonMail is a leading provider of encrypted email services, providing a secure means of communication to over 500,000 users. ProtonMail was created to provide privacy to activists, journalists, whistleblowers and other at-risk groups. In November 2015, the Swiss-based encrypted email provider experienced back-to-back attacks from two different sources—one seeking financial gain and another aiming to undercut ProtonMail's central mission. These advanced DDoS attacks included volumetric attacks over 100 Gbps as well as application layer attacks. The attacks also included multiple encrypted attack vectors including SSL SYN flood attacks that required advanced behavioral analysis to identify malicious traffic and maintain legitimate encrypted traffic flows.

Here is a recap of the series of events and guidance for how any organization can prepare for similar attacks.

- November 3, 2015 – Slightly before midnight, ProtonMail received a blackmail email from The Armada Collective. Like DD4BC, The Armada Collective blackmails companies for Bitcoin under the guise of a DDoS attack.7 In keeping with The Armada Collective's standard modus operandi, following this threat was a DDOS attack that took ProtonMail offline for about 15 minutes.

- November 4, 2015

  – 11 a.m. – The next DDoS attacks hit ProtonMail's datacenter, and its upstream provider begins taking steps to mitigate the attack. However, within a few hours, the attacks take on an unprecedented level of sophistication.

  – 2 p.m. – The attackers directly assault the infrastructure of ProtonMail's upstream providers and the datacenter itself. The attack on the company's ISP exceeded 100Gbps targeting not only the datacenter, but also routers in Zurich, Frankfurt and other locations where the ISP has nodes. The coordinated assault on key infrastructures successfully brings down both the datacenter and the ISP, affecting not only ProtonMail but also hundreds of other companies.

  – 3:30 p.m. – Under intense third-party pressure, ProtonMail grudgingly pays the ransom o the Bitcoin address 1FxHcZzW3z9NRSUnQ9Pcp58ddYaSuN1T2y. As ProtonMail later noted on its company blog, "We hoped that by paying, we could spare the other companies impacted by the attack against us, but the attacks continued nevertheless. This was clearly a wrong decision so let us be clear to all future attackers – ProtonMail will NEVER pay another ransom."

- November 5 – 7, 2015 – ProtonMail suffers from ongoing, high-volume, complex attacks from a second, unknown source.

- November 8, 2015 – ProtonMail begins working with Radware's Emergency Response Team and implements its attack mitigation solution. Service is restored shortly after. "In Radware, we found a solution that was capable of protecting ProtonMail without compromising email privacy," noted Andy Yen, CEO of ProtonMail. "With Radware DefensePipe, we were finally able to mitigate the attack on ProtonMail."

- November 9 – 15, 2015 – Attacks continue at a high volume, reaching at much as 30Gbps to 50 Gbps at peaks throughout these days. These attacks are successfully mitigated by Radware.

Assessing the Attacks

Following the attacks, ProtonMail worked with MELANI, a division of the Swiss federal government, to exchange information with other companies also attacked. It became clear that the attack against ProtonMail occurred in two stages and was arguably two separate campaigns. The first was the volumetric attack targeting only the company's IP addresses. The second was the more complex attack targeting weak points in the infrastructure of ProtonMail's ISPs.

As noted on the ProtonMail blog, "This second phase has not been observed in any other recent attacks on Swiss companies and was technically much more sophisticated. This means that ProtonMail is likely under attack by two separate groups, with the second attackers exhibiting capabilities more commonly possessed by state-sponsored actors. It also shows that the second attackers were not afraid of causing massive collateral damage in order to get at us."

Lessons Learned

While it is impossible to predict the next target of a ransom group, organizations need to proactively prepare networks and have an emergency plan in place for such an incident. If faced with a threat from a blackmail group, it is important to take the proper steps to mitigate the attack. As ProtonMail's experiences underscore, organizations under attack should consider:

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe.
- A hybrid solution that includes on-premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A cyber-security emergency response plan that includes an emergency response team and process. Identify areas where helped is needed from a third party.
- A solution that can maintain the integrity of encrypted communications while still inspecting these traffic flows for anomalous activity that requires deeper investigation for potentially malicious intent.

Source: Radware

SSL Encrypted Traffic Creates New Security Challenges for the Enterprise

Most web applications used for private, commercial or business purposes encrypt the transactions based on SSL/HTTPS protocol to ensure the privacy of data transfer between the user and server. Recent surveys show that enterprise communication sent through its LAN and WAN infrastructure contains 25%-35% of SSL encrypted traffic on average. Certain vertical segments (such as finance or medical) can reach 70% of SSL encrypted traffic in the network due to the information communicated. SSL technology continues to improve the security it provides, with more complex and longer keys used to encrypt data.

SSL has solved the privacy problem and secures the communication of sensitive information in and out of the enterprise. However, it has created new blind spots in the visibility of traffic that goes in and out of the enterprise. SSL has also become a vehicle to carry malicious programs into the enterprise IT infrastructure and allows sensitive information to leak out of the enterprise unnoticed.

The use of cloud applications has exacerbated matters even more. Many enterprises have clear security policies on what information is allowed to be stored in the cloud and what information must remain inside the enterprise's private datacenter. SSL encrypted traffic makes the enforcement of these policies impossible as data leakage prevention solutions can't analyze the SSL encrypted traffic sent out to the cloud application and storage.

Even private emails or innocent collaboration tools have become a security hazard as malicious programs can cross through the enterprises' advanced, anti-virus solution unchecked, hide in the SSL connection established between the two ends and infect the end user's computer with malicious programs. This can lead to an infection with Trojan horses that sends sensitive information outside the organization over other SSL connections. As a result, it's impossible for the enterprise's data leakage prevention (DLP) solution to identify and block this data leakage.

Things to Consider When Addressing the Visibility of SSL Traffic Challenges

A solution that enables visibility into SSL encrypted traffic should consider several things to ensure a long lasting, cost effective and efficient solution.

- **Visibility:** Decryption/re-encryption of SSL sessions to enable inspection of both clear and encrypted traffic for security purposes while keeping the privacy of the traffic content in its journey to its destination.
- **Service chaining:** Any SSL inspection solution needs to be able to selectively forward traffic to one or more security solutions.
- **Flexible traffic inspection:** In order to make the solution as efficient as possible and provide the ability to inspect encrypted traffic masquerading as clear traffic, the solution must dynamically define filters that intercept and open traffic for inspection even if it flows through non-standard TCP ports (such as HTTPS port 443).
- **Security:** To avoid turning the SSL traffic inspection solution into a target itself, the solution needs to not perform like a proxy or have its own IP address.
- **Scalability:** As the amount of traffic/SSL traffic continuously grows, SSL traffic inspection solutions must seamlessly scale and eliminate forklift upgrades as much as possible.
- **High availability:** To avoid downtime due to outages in the security solution, the SSL traffic inspection solution should always ensure traffic is forwarded to the fastest responding available security servers, and automatically bypass out of service servers.

Benefits of Using an Outbound SSL Traffic Inspection Solution

Application Delivery Controllers (ADC) are an ideal platform to deliver SSL inspection solutions because of their SSL termination capabilities and traffic steering technologies. The use of an ADC architecture enables significant benefits for the enterprise.

- **Enable visibility to all SSL traffic:** Decrypt the SSL traffic on the fly, and forward the traffic for inspection in real time, to one or more DPI security solutions and logging solutions.
- **Enable regulatory compliance:** Enable organizations to meet various types of regulatory compliance requirements such as logging details of encrypted transactions, while ensuring and maintaining data exchange privacy.
- **Flexible security policies:** IT security can define flexible security policies and filters, per types of users or applications, and pass them through a corresponding set of DPI security services.
- **Simple architectural solution:** Provide a holistic solution for both inbound (SSL offload) and outbound (SSL inspection) transaction analysis, security solutions, load balancing and scalability – supporting multiple security value added services.

- **Seamless scalability:** Utilize the ADC as a load balancer to scale security services.

- **Selective traffic inspection:** Treat different traffic with different policies based on URI and content classification models.

- **Reduced latency:** An SSL inspection solution that can service chain multiple security solutions means that an organization will only need to decrypt and reencrypt traffic once. Transparent traffic steering and service chaining means that only relevant traffic per security service is passed to each of the services in a row.

Summary

As SSL traffic continuously gains momentum and increases in volume, so is the amount of security threats that take advantage of this new "invisibility" tunnel into the organization's network and datacenters. Security and network administrators need scalable solutions that will regain visibility into potential threats that may "hide" in SSL sessions.

The ideal SSL traffic inspection solution enables transparent high capacity SSL traffic interception and decryption, with a strong traffic steering engine that can flexibly steer the unencrypted traffic to several relevant security solutions for deep packet inspection. An ADC's integrated capabilities can offer a simple one box solution that is easy to deploy and eliminates the need to reconfigure end user clients' network configuration or reengineer the network to steer the traffic.

The ability to perform SSL/TLS traffic inspection with transparent traffic steering and load balancing technologies benefits enterprises through uncompromised visibility into encrypted content, data security and regulatory compliance, all while maintaining high resource utilization efficiency and seamless scalability.

Source: Radware

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.