SecuAvail
WINTER 2016

SecuAvail NEWS vol.9

ついに NetStare Ver.8 リリース！

NEWS CONTENTS

CONTENTS 01

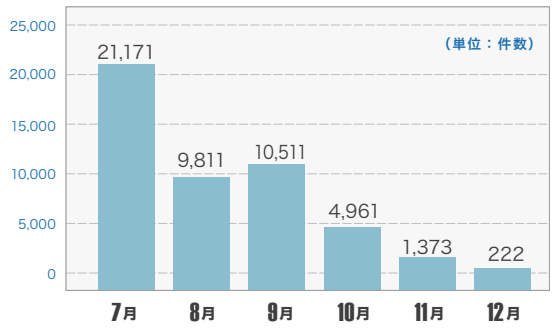
Bash（ShellShock）の脆弱性を狙った攻撃傾向

情報セキュリティ通信

2015年７月~12月の 脅威件数による動向

攻撃件数は、7月の21,171件をピークに減少しており、12月には222件と7月の検知件数の10分の1となっている。その要因としては先にあげたBashシェルの脆弱性とHeartbeatの脆弱性を狙った攻撃が急激に減ったためである。攻撃内容をサービス別に見ていくとDB関連への攻撃が断続的に観測されている。また、Exploit.Kit関連については、件数自体は少ないものの少しづつ増加している。

月別検知件数の推移



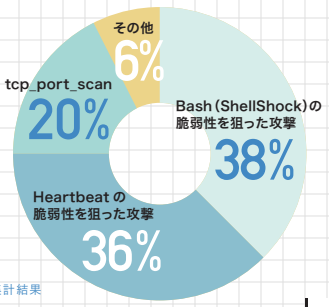
IPS 脅威検知件数集計（2015年7月~12月）

※弊社 UTM 運用サービスにて検知した「Critical」の検知件数集計結果

	検知した脅威の内容	
1位	Bash（ShellShock）の脆弱性を狙った攻撃	18,529
2位	Heartbeat の脆弱性を狙った攻撃	17,541
3位	tcp_port_scan	9,583
4位	udp_scan	1,003
5位	Adobe Flash Player のメモリ破損の脆弱性を悪用する攻撃	178
6位	MS.GDIPlus の BO 脆弱性	159
7位	tcp_syn_flood	153
8位	udp_flood	115
9位	Ruby on Rails の脆弱性を利用する Linux サーバへの攻撃	96
10位	icmp_sweep	69
11位	Angler.Exploit.Kit の検出	33
12位	Apache.Struts2.OGNL.Script.Injection	33
13位	Apache.Struts2 に脆弱性 (DefaultActionMapper の処理に問題が存在)	31
14位	Adobe ColdFusion で任意のファイルのアップロードの脆弱性	28
15位	Wordpress の N- メディアウェブサイトお問い合わせフォームのアップロードの脆弱性	28
–	その他	612
	合計	48,191

今後の傾向と対策

昨年度に引続き Bash シェルの脆弱性と Heartbeat の脆弱性を狙った攻撃が多いものの、日々脆弱性を狙った新しい攻撃が行われている。攻撃を防ぐためには IPS 製品の導入だけでなく、検知後の対策が重要である。NetStare では攻撃検知の連絡だけでなく、攻撃内容及びその攻撃がお客様環境へ影響を及ぼす可能性があるのかを判断し、適切な対策を提案している。IPS 導入時は導入後の運用も含め検討することを推奨する。



※弊社 UTM 運用サービスにて
検知した「Critical」の検知件数集計結果

特集記事担当：卒区次郎

CONTENTS

02 特集！NetStare Ver.8 McAfee NSP 運用サービスリリース！

アラートだけでは見えない兆候を捉えるログ分析ロジック搭載！

ログ分析こそが運用の本質的な実働

インターネットの出入口に IPS が設置されているとセキュリティ対策という意味では心強い。ただ、専門用語と言うか聞き慣れてない言葉（英語）の羅列で何を表示していてそれが何を意味をするのか理解・把握して運用することは難しい。たとえ意味が解っていたとしても導入後に運用することは難しいと言われる IPS。IPS を運用するとは何をすることなのか?何をするべきなのか?セキュアヴェイルは「運用」=「可視化」と定義し、その考えをもとにサービスを構成し提供している。可視化に必須となるのは通信及び稼働状況を視認させる「ログ」である。

長期に渡り分析し、潜在する危険を可視化

つまり、ログ分析こそが運用の本質的な実働ということになる。攻撃を含む不正な通信を検知すると、アラート機能で通知し設定によっては遮断までしてくれる。アラートは危険度に応じて 4 段階ほどに分かれている。危険度が高いアラートを受信すると適切な対処をするが、低いアラートについては問題がないとの判断で放置されることがほとんどである。IPSが教えてくれなければ危険を認識しなくなるため、脅威については無頓着になってしまう。これでは全くの機器依存であり運用しているとは言い難い ....。NetStare は危険度の低いアラートもその頻度や傾向を長期に渡り独自のロジックにて分析し、潜在する危険を可視化する唯一の IPS 運用サービスである。

記事担当：海女若

定期セミナーを開催してます！見て ... 触れて ... 体験してください！

貴社にとって必要な選択肢と判断基準を導く。

「IPS 入門編」など導入するにあたって、何をどのような視点で検討し判断するべきかなのか? IPS ベンダーではなく IPS を運用する専門のベンダーとして貴社にとって必要な選択肢と判断基準を導きます。

導入済の方にも「実践!ログ分析」というタイトルにて、実際の運用現場から取得したログを題材に、どこに着目し、何を調査し、その結果をどう認識することが適切なのか ...。IPS の売り込みや、サービス説明をする営業セミナーとは違う、運用者にとって必要な情報と知識を惜しむことなく公開する実践的なセミナーです。少人数制のセミナーを定期的に開催していますので、是非足をお運びください。

特集記事担当：海女若

定期セミナーの詳しい情報は
公式ホームページよりご覧いただけます

セキュアヴェイル　定期セミナー

IPS の進化系…「McAfee NSP」が持つ視点

入口,出口の両方向の通信に応じた検知エンジン

劇的に変化するインターネット環境に順応すべく進化、強化した IPS。それが McAfee NSP である。
クラウドサービスの普及によりネットワーク環境は変貌を遂げた。これまで社内で完結していた通信が外部へと拡散し、従来の IPS で精査していなかった通信をも精査する必要が出てきたのである。
また、サイバー攻撃については、不正に侵入してくる攻撃だけでなく、標的型攻撃によりボット感染した端末からの通信が外部に出ることを止める必要性が出てきた。
つまり、現代のセキュリティ対策システムには入口 / 出口の両方向の通信に応じた検知エンジンが必要不可欠となっているのである。

従来の IPS を進化させた次世代 IPS

これまでの IPS はシステムの脆弱性を突く攻撃をメインに対応してきたが、マルウェアに感染したノードから外部の C&C サーバとの通信を遮断し被害を最小限に抑えるなど、要求される機能が日々増加している。従来の機能だけではセキュアな環境を維持することが困難な状況になってきたのである。McAfee NSP は入口対策として従来の IPS 機能に加え、標的型攻撃メールに使われる不審なファイルの検知防御機能を実装している。出口対策としてはマルウェア感染やボット化した通信の検知機能である。通信内容だけでなく、通信する先（C&C サーバ等の IP、URL）の情報を含めて通信制御をしている。更に、利用されるアプリケーションの制御機能を実装した McAfee NSP は従来の IPS を進化させた次世代 IPS と言えるのである。

記事担当：卒区次郎

セキュリティログ分析で集中攻撃や内部漏洩を検知！

集中して攻撃されている可能性や、特定の送信者から狙われている脅威を素早く検知

NetStare で提供している「セキュリティログ分析」は、1 時間に 1 回ログを分析し、事前に設定している条件と合致した場合にアラートを出す。
アラート条件は従来、ファイアウォールログを分析し通知を行っていたが、今回、McAfee NSP を NetStare の運用対象機器としてサービス提供を開始するにあたり、アラート条件の見直しを行った。
IPS ログのうち、重要度が低い（info や low）ログをもとに、IPS アラートや 1 行のログだけでは気がつくことができない不正通信を検知可能としている。（右図）

上記アラートから、お客様環境が集中して攻撃されている可能性や、特定の送信者から狙われている脅威を素早く検知し、対策をとることを可能としている。

ログ監視名	アラート条件
お客様環境が狙われている可能性検知	info/low/Inbound のログのうち、1 日にユニークなアラートを 70 件以上検知した場合
特定攻撃者から狙われている可能性検知	info/low/Inbound のログのうち、1 日にユニークな送信元 IP アドレスを 100 件以上検知した場合
特定保護対象を狙われている可能性検知	info/low/Inbound のログのうち、特定の保護対象サーバに対し、合計攻撃回数が 30 回以上の場合
マルウェアの疑いがある通信検知	マルウェアの危険度が 4 以上であるものの、重要度が「high」以外の通信を検知した場合

特集まとめ

高額で運用が難しいと言われる「IPS」。数百台を超える運用実績より、貴社に最適なチューニングを行い IPS 導入効果を発揮するサービスを提供します。

記事担当：甲斐

CONTENTS 04

IPS イベント対応アドバイスとは？

なるほど～NetStare

IPS イベント検知
検知から 2 時間かかる理由


お客様

IPS のイベント検知って、2 時間以内に連絡してくれるということだけどこれって遅くない？
IPS が攻撃検知したら機器からすぐにメールが届くのに・・


セキュアヴェイル

確かに検知メールをすぐに送るのであれば時間はかかりません。
しかし検知メールをそのまま送るとお客様は何をすべきか判断が難しいのです。


お客様

そんなことはないよ。すぐに攻撃がきたことを知らせてくれるほうがこちらも何かできるかもしれないし。


セキュアヴェイル

実際に機器から直接送られてくるメールってみたことありますか？


セキュアヴェイル

subtype:vulnerability config_ver:1 time_generated:2015/05/25 15:31:38.....
(中略)
cpadding:0 threatid:PHP Functions CRLF Injection Vulnerability(31898)category:any contenttype:.....


お客様

うわあああああ・・・全部英語だし何て書いてあるのか理解できないよ。


セキュアヴェイル

しかも、攻撃は一度に複数件同じものが来ることが多く、
その度にこのようなメールが矢継ぎ早に送られてきます。


お客様

一度に大量のメールが届いたらどのメールからどう見ればいいか・・


セキュアヴェイル

NetStare ではこういった複数の検知メールを 1 つにまとめつつ、攻撃内容の解析と各お客様環境に沿った推奨対応方法を考慮した上でセキュリティエンジニアが日本語で分かり易くお知らせしています。
そのため、検知後すぐに連絡するのではなく 2 時間以内の連絡とさせていただいています。


お客様

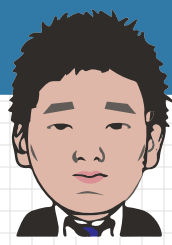
なるほどね～！一番効率的でスピーディな対応を NetStare では提供してくれているんだね。

記事担当：ぐりこ

実践！ログ分析～顧客事例から学ぶこと～

なぜログ分析は難しいと言われるのか？ そもそもログ分析とは何か？
高度な専門スキルがなくても容易に扱える方法は？
弊社統合ログ管理システム「LogStare」の操作を交え実践的に解説します。

セミナー情報
Monthly column



予定講師：Mr.160

SecuAvail 株式会社セキュアヴェイル (SecuAvail Inc.)

大阪本社
〒533-0044　大阪府大阪市北区東天満1-1-19
アーバンエース東天満ビル
TEL:06-6136-0020　FAX:06-6136-0018

東京ブランチ
〒103-0025　東京都中央区日本橋茅場町1-6-17
トラッドビル 6F
TEL:03-5643-0208　FAX:03-5643-0207

次号予告 / SecuAvail NEWS リニューアル！！