なるほど～ NetStare

IPS イベント検知の対象は Critical だけで大丈夫？？

お客様

「リアルタイム IPS イベント検知」では、危険度「Critical」（最も危険度の高いもの）、かつ、遮断を行っていない不正アクセスが通知の対象になっているけれど、Medium や Low などについては通知ってしてもらえないの？

SA

NetStare では全顧客、「Critical」かつ遮断を行っていない不正アクセスを通知対象として統一しています。

お客様

見る人によってどこまで通知して欲しいのかという基準が異なると思うけど、本当に Critical だけで大丈夫なの？

SA

確かに、どの危険度レベルまで確認するかは、お客様の運用ポリシーによっても変わってきますね。Critical はあくまでも「リアルタイム」での通知を行う対象であり、緊急性が高いという判断から 2 時間以内の通知を行っています。全てを通知対象としてしまうと、本当に重要なアラートを見逃してしまうことにもなってしまうことから仕様を決めているのです。

お客様

でもやっぱりそれだけじゃ不安だな・・Critical 以外のイベントを検知した場合はどうしたらいいの？

SA

検知したイベントは危険度に関わらずセキュリティログレポートとして、お客様専用のポータル画面から確認していただけるようになっています。

お客様

でもレポートを見ても何に注意してみるべきか分からないかもしれないし・・

SA

セキュリティログレポートは単なる統計ではなく、運用者の視点から攻撃や通信を分析した結果を表示しています。
例えば、お客様の利用しているアプリケーションに対する攻撃かどうかや、危険度に関わらず攻撃回数が多いイベント等も確認できるようになっています。
もちろん、検知した内容についてはお問合せ頂きましたら攻撃内容や推奨の対策について解説も致します。

お客様

なるほど！これならどんな時に注意してレポートを見るべきかも分かるし、危険度が高い攻撃を見逃すこともないから安心できるね。

（甲斐）

コラム

「不足するセキュリティ人材」

IPA の報告書によると、情報セキュリティに従事する技術者は約 23 万人で、不足人材が約 2.2 万人だそうです。
この 23 万人のうち、必要なスキルと満たしている人材は 9 万人強、残りの 14 万人は実はスキルの向上が必要だそうです。スキル不足のなか、セキュリティ業務を遂行している恐ろしい現実が明らかになりました。
公表されている報告書によると、情報セキュリティの業務を「セキュリティ戦略・統括」「企画・設計」「開発・構築」「運用・管理」「監査・検査」「コンサルティング・教育」という分類に分けたうえでの調査結果であり、ナルホド、と思わせるものでした。

いま、企業を守るセキュリティ人材の不足がコンサルティングや製品導入、SOC の必要性に繋がっており、我々の製品やサービスに対してお客様より日々お問い合わせをいただいていることも納得できました。
社会に必要とされていると感じるとともに、より良い製品・サービスを提供できるよう人材育成等の企業努力を惜しんではならないと改めて思い知りました。

・・セキュリティの人材は足りていますか？

（いっちゃん）

出展元　IPA
http://www.ipa.go.jp/security/fy23/reports/jinzai/

次号予定

情報セキュリティ通信
セキュリティニュースを斬る！
セキュリティレポート解説！
顧客を知る　事例紹介
なるほど～ NetStare

SecuAvail
http://www.secuavail.com
株式会社セキュアヴェイル

本社
〒530-0044　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
E-mail:sales@secuavail.com

東京ブランチ
〒130-0025　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

SecuAvail NEWS

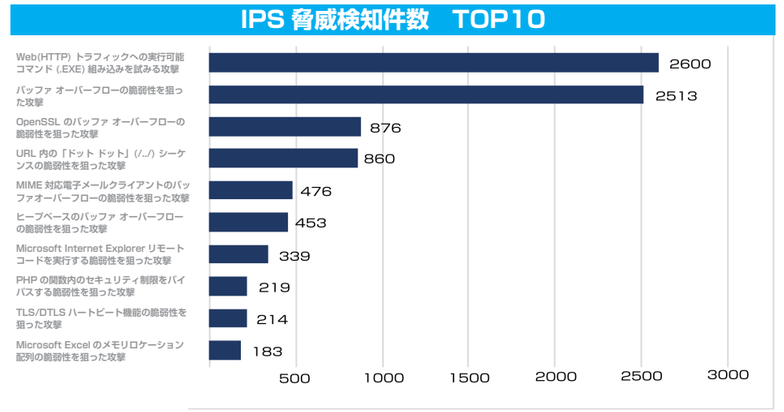
SecuAvail
2014/11
Vol.1

Contents

情報セキュリティ通信

IPS が捉えた真実

今年 9 月に弊社 IPS で検知した脅威のランキングです。
検知件数上位の 1 位と 2 位は 10 年前からある攻撃で、全体の 5 割を占めています。9 位には OpenSSL のハートビート機能の脆弱性がランクイン。影響範囲が広く対策は必須です。検知のピークはゴールデンウィーク頃でしたが、依然として多い状況です。9 月の集計では TOP10 にはランキングされていませんが、9 月 29 日以降は断続的に Bash の脆弱性をつく攻撃が観測されています。
攻撃の 4 割近くが MS Windows を標的としたものです。
攻撃手法としては、リモートでのコード実行を試みる攻撃が 8 割近くとなっています。
弊社では、IPS での防御だけではなく、このような攻撃統計からブラックリストを作成し、FW ポリシーで攻撃先からの通信を遮断するブラックリストブロックを実施しています。
是非セキュアヴェイル NetStare サービスをご利用ください。



	検知した脅威 TOP10 の内容	影響を受けるシステム	検知数
1 位	Web(HTTP) トラフィックへの実行可能コマンド (.EXE) 組み込みを試みる攻撃	Windows 2000、Windows NT	2600
2 位	バッファ オーバーフローの脆弱性を狙った攻撃	Zom-Mail: 1.0.9	2513
3 位	OpenSSL のバッファ オーバーフローの脆弱性を狙った攻撃	全般	876
4 位	URL 内の「ドット ドット」(/../) シーケンスの脆弱性を狙った攻撃	すべての Web サーバー	860
5 位	MIME 対応電子メールクライアントのバッファオーバーフローの脆弱性を狙った攻撃	Windows 95、98、NT4.0、UNIX	476
6 位	ヒープベースのバッファ オーバーフローの脆弱性を狙った攻撃	Sendmail	453
7 位	Microsoft Internet Explorer リモートコードを実行する脆弱性を狙った攻撃	Microsoft Internet Explorer	339
8 位	PHP の関数内のセキュリティ制限をバイパスする脆弱性を狙った攻撃	PHP	219
9 位	TLS/DTLS ハートビート機能の脆弱性を狙った攻撃	全般	214
10 位	Microsoft Excel のメモリロケーション配列の脆弱性を狙った攻撃	Microsoft Office	183

Security Operation Center 裏話

今年は製品 / バージョンのサポート終了が多く、リプレイス / バージョンアップ作業が多いです。Security Operation Center（以下 SOC）では検証作業で大変です。
今月の SOC 裏話は、ある UTM 製品のバージョンアップにまつわるお話です。最新バージョンで利用できる機能が減っているという恐ろしい現象が発生しました。
（実際は GUI からの設定が出来なくなり、CLI での設定は可能です。※一部機器対象）一例として、SSL-VPN のポータル画面が従来は 3 つまで使用可能でしたが、バージョンアップすると 1 つしか使えなくなり、残りの 2 つは勝手に消されるという事態に。幸い弊社のお客様に影響はありませんでしたが、SOC では引き続きバージョンアップ検証作業を続けてまいります。皆さんもバージョンアップは慎重に行いましょう。（卒区次郎）

Security News を斬る！　セキュリティ対策の本質に迫る

セキュリティベンダーの提案？に乗っかってはいけない！

大規模な個人情報漏洩事件から活況となっている情報漏洩対策…
ツールの機能不全が引き起こした問題だと短絡的な分析によるセキュリティ対策強化は一過性のものなる。
原点に返りリスクアセスメントから的確な現状分析…その後、冷静かつ客観的な視点で対策を施すべき！

セキュリティ対策の”提案”とは何なのか？

必要性は誰もが認識するセキュリティ対策。しかし、今すぐ導入する理由が見つからない。今回のような大規模事件または事故があると、「明日は我が身…？」... 具体的な検討をすることになる。セキュリティ対策ツールベンダーも同様「今がビジネスチャンス！」とばかりに販売攻勢をかけてくる。

ただ残念なことにホントに顧客視点からセキュリティ対策強化を提案しているのか？という疑問を禁じ得ない。

ここぞとばかりに売り込みたい製品があたかも今回の事件を防止できたかのような論調で売り込み攻勢をかける。

そこに“提案”など無い。提案とは本来実施すべきセキュリティ対策のガイドラインと現状の施行状態の差分の発生要因を分析し解決手法を提示することである。

未導入のセキュリティ対策製品のヒアリングをして、それだったらうちで扱えるので見積もりをしましょうか。という営業は提案ではないし全く現状を捉えていない。現象への対処である。

提案時におけるベンダーと顧客の視点のずれ

セキュリティベンダーの視点	顧客の視点
1 売りたい物を提案する	1 投資額を抑えて効果的な対策
2 利益率の高いものを良い製品と見せる	2 製品導入がゴールではない
3 導入していない製品を探す	3 自社の絶対評価と相対的な観点から提案が欲しい

客観的、定量的に可視化できるセキュリティ対策の実施を

今ここで本当に実施すべきことは「的確な現状把握」であり、現象把握であってはいけない。現状把握とは客観的かつ定量的に状況を可視化すること。その役割を担うのが“ログ”である。ログは嘘をつかない。セキュリティ対策を強化するための問題を見いだし、対策後の効果を検証するためにもログは必要不可欠。

統合ログ管理ツール、クライアント管理ツール、セキュリティ対策機器に付随するログ収集ツールなど各種ログ管理製品はあるが、先ずはここからスタートするべき。ログ管理製品を導入済みなら活用すべきである。何かあった時のためのログ…その“何か”が今まさに目の前で起こっているのだから…。（海女若）

セキュリティ対策で本当に必要なこと

現状把握 ≠ 現象把握

○ 現状把握　× 現象把握

顧客を知る　事例紹介　LogStare 事例 ～化学メーカー様（従業員数 約 1000 名）～

機密ファイルへのアクセスログを収集。現状の見える化と PDCA の運営に不可欠な定期チェックを実現。

導入前の課題・導入の経緯

あるとき、サーバの機密情報が削除される事態が発生。誰が削除したのか追及することになったが、証跡管理をしていなかったために該当者の特定にひと苦労した。このとき削除された機密情報は、万が一他社に技術を盗まれて模倣されると、自社製品の価値が下がり売上に大きく影響するほどの情報だった。

社内で発生した機密情報の削除をきっかけに、証跡管理に対する課題が浮上した。そこで、ファイル共有で使用している LotusNotes と、機密ファイルを保管している Windows サーバへのアクセス状況を可視化して管理することを決定。何社かの製品を検討の結果、LogStare で可視化することになった。

セキュリティレポート解説！　公開サーバが乗っ取られた？編

公開サーバ乗っ取りの可能性を探る

DMZ 上のサーバから発信されるサービスの通信を解析することにより、乗っ取られた可能性のあるサーバを検知することができます。

DMZ は本来、外部からのアクセスもしくは内部から外部へ向かうサービスを扱うゾーンであり、DMZ から外部への直接のアクセスは、プロキシサーバからの http/https/ftp や dns/smtp/ntp を除きほとんど発生しません。もし、上記以外の通信が発生している場合には、サーバが不正に利用されている、もしくは乗っ取られた可能性があります。

（ウイルス、マルウェア、bot 感染の疑い）

※運用のために ssh 等のサービスを許可している場合も見受けられますが、公開サーバのサービス以外は宛先を限定する、もしくはサービスそのものをブロックすべきです。

公開サーバ乗っ取りによって起こりうるリスク

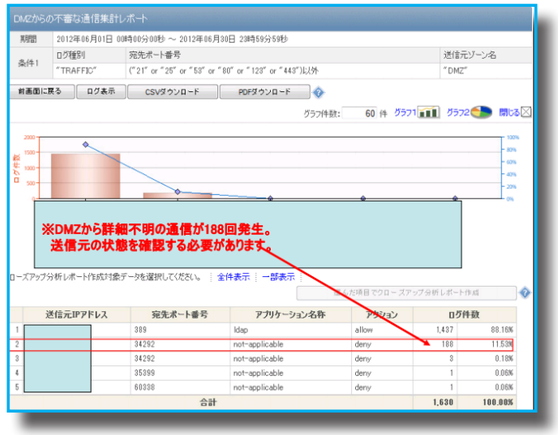
ウイルス、マルウェア、bot 感染による情報漏洩

データ破壊、サーバ障害

公開サーバが乗っ取られる要因

公開サーバの設定や整備の不備

DMZ からの不審な通信集計レポート



公開サーバの安全基準とそれを維持するための対応策

解析の結果、１件も検知がない状態が安全の基準といえます。

検知されない安全な状態を維持するには、公開サーバの OS、ミドルウェア、アプリケーションのパッチ、バージョン管理を行うとともに、IPS、AntiVirus のプログラムも最新の状態にしておきましょう！（ぐり子）

製品決定の決め手

・Notes、Windows のどちらのログも解析実績があり、導入時に作成したいレポートの作成方法も相談ができた点。

・操作が分かりやすく、マニュアルなしで使えると感じた点。

以上を評価いただき、LogStare を導入。

主な運用方法

・機密情報ファイルについて、適切な人物（営業マン、開発員）のみがアクセスしている状態で運用できているか、月に 1 回営業部長にて確認。

・「ログ管理を実施しているので、不用意なことはしないように」と年に 1 回全社員への勉強会を実施し、抑止効果を狙った活動を継続。

	No	レポート名
定期的にチェックするレポート	1	深夜帯のアクセスランキング
	2	土日のファイルアクセスランキング
	3	機密情報アクセス者ランキング
	4	ファイル削除者ランキング
	5	ファイルコピー者ランキング

（ひき氏・ぐり子）

導入製品

製品		導入数
LogStare	基本ライセンス（5 ノード）	1Set
	分析レポート拡張モジュール（2 アプリケーション）	1Set
	Windows ログオプション（1 台分）	2Set

ライセンス費用：￥3,136,000　保守費用：￥627,200

構成図