JULY+AUGUST 2015 SecuAvail

SecuAvail NEWS vol.7

特集! NetStare Suite APT SENCER～緊急リリース!

NEWS CONTENTS

CONTENTS 01

新たに検知した３つの脅威

情報セキュリティ通信　脅威動向

2015年５月脅威件数による動向

2015年5月に弊社IPSで検知した脅威件数の集計です。TOP15までの傾向は、上位に関しては、４月に検知した脅威と同様の結果になっています。ただし､5月になって新たに検知した脅威が３つあります。『WinRARのバッファオーバーフローに対して脆弱性を狙った攻撃』、『不正なPDFファイルを使った攻撃』、『不正な形式のUTF-8でエンコードされたHTMLを利用した攻撃』です。『WinRARのバッファオーバーフローに対して脆弱性を狙った攻撃』は、主にWindowsを対象とした攻撃ですが、Linux、MacOSにも影響があるので注意が必要です。『不正なPDFファイルを使った攻撃』はFoxit Readerを利用しているデバイスを狙った攻撃です。不正なPDFファイルを開かせるように仕向け、開かせることでターゲットにリモートで攻撃を実行します。『不正な形式のUTF-8でエンコードされたHTMLを利用した攻撃』はMS IEを利用しているユーザを狙った攻撃です。悪意のあるページにユーザがアクセスすることでユーザのデバイスで任意のコマンドを実行する攻撃です。『不正なPDFファイルを使った攻撃』、『不正な形式のUTF-8でエンコードされたHTMLを利用した攻撃』の２つは昨今流行の標的型攻撃に使われるような手法です。

IPS 脅威検知件数集計 (2015年５月)

※弊社IPS運用サービスにて検知した「High」アラートの集計結果

	検知した脅威の内容	5月
1位	MIME対応電子メールのバッファオーバーフローの脆弱性を狙った攻撃	2,025
2位	Bashの脆弱性(ShellShock)を狙った攻撃	1,859
3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	402
4位	WinRARのバッファオーバーフローに対して脆弱性を狙った攻撃	164
5位	Heartbleedの脆弱性を狙った攻撃	95
6位	PHP include関数を狙った攻撃	61
7位	PHP CGI構成の脆弱性を狙った攻撃	50
8位	HTTP GETリクエストを利用した攻撃	45
9位	MS IISの脆弱性を狙った攻撃	42
10位	URL内のスタックオーバーフローの脆弱性を狙った攻撃	20
11位	不正なPDFファイルを使った攻撃	16
12位	MS Exchangeでリモートでのコードの実行を引き起こす攻撃	15
13位	サーバ上のバッチファイルを不正からリモートで実行する攻撃	15
14位	不正な形式のUTF-8でエンコードされたHTMLを利用した攻撃	10
－	その他	50
	合計	4,869

今後の傾向と対策

今年は年金機構問題で標的型攻撃対策について注目が集まっています。標的型攻撃対策の一環でIPS導入を検討している企業の方は是非、IPS導入前に一度当社にご相談いただくか、当社セミナーの『標的型攻撃対策セミナー』にご参加ください。

特集記事担当：卒区次郎

CONTENTS

02 特集！ NetStare Suite

Security for the Future 未来を見つめる「ログ管理」を実現

ログ分析によるビックデータ管理

数年前より大容量データ「ビックデータ」というキーワードが頻繁に使われるようになった。ビックデータとは何か … 検索、購入、行動、稼働 … 等々、あらゆる履歴を一元的に管理・分析し傾向を導き出し活用するための情報群である。ビッグデータの活用は履歴という「ログ」を活用することに他ならない。つまり、「ログ管理」こそがビッグデータ活用と同義と言える。
創業より「顧客環境に適したセキュリティ維持の実現」をテーマにファイアウォールや IPS などの運用サービスを提供し、自社開発した運用監視基盤とログ分析ツールを駆使し、潜在する問題の抽出や傾向分析からセキュリティマネジメントサービスもまた提供してきた。
「潜在する問題を抽出する」これは、セキュリティ対策をする上で一般的な考えではあるが実効性のある対策へと導くのは容易ではない。問題発生時に通信ログ等から、なぜそうなっているのか仮説を立て、それを検証するべくログ分析を実行しなければならない。

技術者依存のセキュリティーをシステム化

今回、リリースした標的型攻撃検知センサーには、社外の特定のメールアドレスから社内の複数人（例えば 10 人以上）に一定の容量（例えば 1MB 以上）のファイルが添付されているメールが送信されていると不正なメールであろうと仮定し、それをお客様に通知するという機能を有している。
セキュリティ対策における問題認識は、攻撃元や対象、攻撃内容や件数などの事実に基づくが、その判定基準は技術者のスキルや経験に依存する部分が多く、対策へと導く過程と決定に差異が生じる場合がある。NetStare Suite はファイアウォールや UTM などの機器から得られる監視データと通信ログを一元管理しセキュリティログというビックデータを構築、創業より培った運用ノウハウを最新のテクノロジーで実装しシステム化することで俯瞰的かつ客観的な分析結果を導き出す。技術者の経験とスキルに依存することなく、EC サイトのレコメンド機能のように、機器の寿命や障害発生の予兆を検知するなど将来予測を提示します。
NetStare Suite は、今までになかった未来のセキュリティ問題への対策を導くサービスとして、今後も進化します。

期待される NetStare Suite の今後…

2015 年 6 月 1 日にサービスを開始した NetStare Suite（以下、NSS）。
その後、日本年金機構の標的型攻撃による情報漏洩事故などの市況から標的型攻撃検知サービス「NetStare Suite APT SENCER」を緊急リリースした。セキュアヴェイル独自の視点から、メールログを分析し標的型攻撃の疑義がある通信を検知し通知するサービスである。現在はメールログの分析のみだが UTM、proxy サーバなど Internet の出入り口のログを相関分析することでより検知精度を高めたサービスもリリースする予定である。

今後の NSS は …

1）NSS 無料サービス開始（監視とログ分析）→リリース済
2）APT SENCER → リリース済
3）APT SENCER Ver.2.0 →近々リリース予定
4）運用対象機器の障害予防検知（将来予測）
5）自社環境のセキュリティ対策度耐久性評価（将来予測）
6）セキュリティ偏差値診断（相関分析によるスコアリング）
7）セキュリティ対策度順位（相対評価により自社の位置付け）
8）学習機能による自動ログ分析レポート（ビックデータ活用）

NSS はビッグデータ活用による、未来のセキュリティ対策の強化に向け客観的で定量的な指標を提供するサービスへと進化する予定です。乞うご期待。

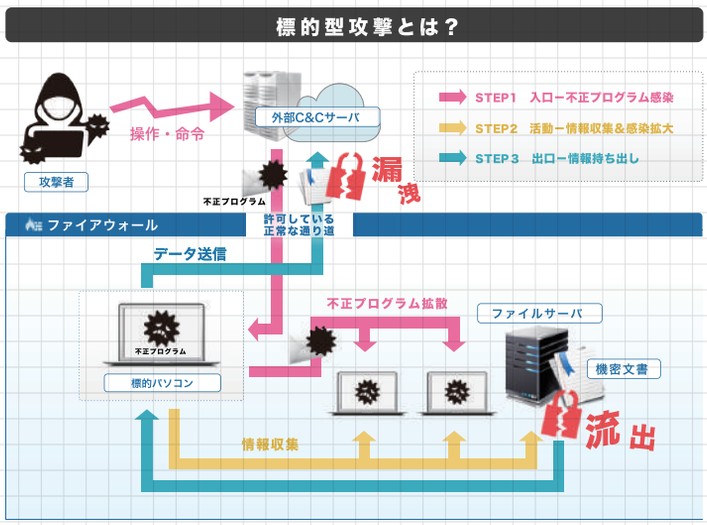
APT SENCER～ 緊急リリース！

ビッグデータ技術が未来のセキュリティリスクの提示へと導く…

検知が難しい「標的型攻撃」

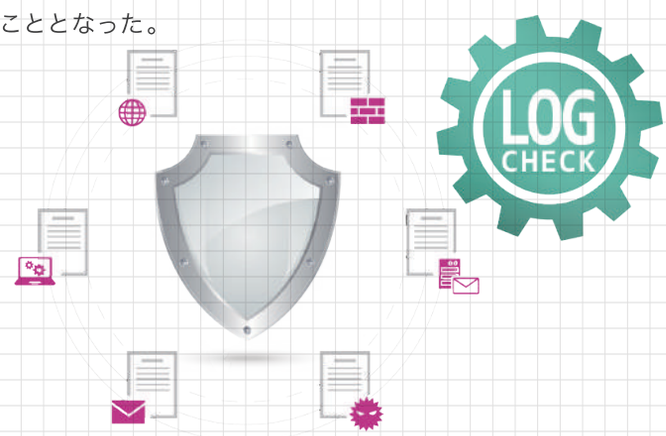
「NetStare」と「LogStare」の 2 本柱のサービス・プロダクトの融合から誕生するのが次期主力製品の「NetStareSuite（NSS）」である。
開発中の現段階ではその全貌はまだ明らかにできないが、先日 NSS の機能を一部切り出すカタチで APT（標的型攻撃）センサーを緊急リリースしたのは前述の通りである。

特定のターゲットにあたかも通常のメールであるかのようになりすまし、不正プログラムを潜伏させ情報漏洩に導くなど、巧妙な手口で知られる「標的型攻撃」は検知が難しいと言われる。



NSS の基盤となるビッグデータ技術

難しいとされる標的型攻撃検知を APT センサーはどのように実現しているのか…
その秘密は NSS の基盤となるビッグデータ技術があるからに他ならない。
従来は RDBMS を利用しログを管理するのが一般的な手法であった。様々な切り口で高度に扱えるという利便性がある一方で、大容量のデータを扱うのは不得意であるという側面もあった。NSS を完成させるためには大容量のデータ（ビッグデータ）を取り扱えるフレームワークが必要であり、約 1 年半以上かけていくつかのフレームワークをベンチマークした。この結果、選択されたフレームワークは現状の製品で課題となっていた大量データの取り扱いを容易にするだけではなく、相関的かつ俯瞰的な視点で迅速に分析結果を導き出してくれることで、新しいセキュリティリスクを発見できる大きな活路を見出すこととなった。



見えないセキュリティリスクを可視化する

監視結果や稼働ログは単に全て過去の事実の積み重ねでしかない。しかしながら、その過去の事実が膨大になり別視点でその事実を見つめると、そこにある一定の法則や傾向が導かれる。本来、従業員が不在である時間帯にメールが送信されているなどの単純な傾向から、業務及び組織構成上においてこのメールの送受信は極めて不自然であるという傾向も浮かび上がってくる。メールの送受信ログの積み重ねから、人の行動（操作）の傾向が可視化され、不正プログラム侵入による情報漏洩などをいち早く検知するという可能性も否定できないのである。
日常のオペレーションログはその多くが定常化されることになり、一般的な傾向として認知されそこにセキュリティリスクがあるとは考え難い。このログの蓄積の先に、日常の傾向とは乖離したログ … つまり、非日常を検知したこの瞬間がセキュリティリスクが高いことを知らしめてくれる。標的型攻撃は巧妙にメールを作文しているため、単純にログを確認しただけでは不正を検知することができない。見えないセキュリティリスクを可視化するのが大容量データ「ビッグデータ」であり、そのデータを様々な角度から分析するモジュールが NSS に実装されている。NSS が有するビックデータ分析技術は数百社以上の顧客へのセキュリティマネジメントサービスで養われた実践的な運用視点（ノウハウ）が存在してこそ実現するシステムである。

記事担当：海女若

CONTENTS 03

ログコレクターは設置するべきか？

なるほど～NetStare

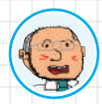
ログコレクター設置
運用にあまり影響ないのでは？


お客様

NetStare に加入するときにログコレクターっていうのも設置しなければいけないって聞いたけど、これっているの？これで初期費用が高くなってしまうならいらないんだけど。


セキュアヴェイル

弊社がカテゴリ 4 以上と定めている機種（例：PaloAlto2000 シリーズ以上、FortiGate310B 以上）ではログコレクターは必須です。なぜかというと、こういった上位機種はお客様の通信量、ログが多いことを想定しているからです。


セキュアヴェイル

ログ送信する際にそのまま送ってしまうと回線を圧迫したり盗聴されてしまう危険性がより高くなってしまいます。ログコレクターはログを 1/10 に圧縮、暗号化処理を施して http で弊社へ送信しますので、回線を圧迫することなく、しかも安全に送信することが可能となります。


お客様

へ～でも安全に送信すると言えば、VPN は？
運用してもらうために VPN を張るんだからそこからログを送ってくれたらいいと思うんだけど。


セキュアヴェイル

もちろん VPN 経由でもある程度安全にログ送信はできます。ただ、その場合 VPN の張り直しのタイミングにログ送信が重なると、ログの欠損が生じる可能性が高いのです。


お客様

そっか～でも、多少欠損が出たとしても運用にはあまり影響がないんじゃないの？


セキュアヴェイル

いえ、私たちは毎時間お客様のログを分析して異常な傾向を発見次第、お客様にご報告しています。もしログの欠損があると、こういった異常にリアルタイムに気づくことができない可能性が高まり、セキュリティレベルが下がってしまいます。


お客様

なるほどね～！色々なことを想定した上で、十分なセキュリティレベルを保つためにはログコレクターを設置するべきなんだね。

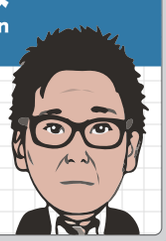
記事担当：ぐりこ

マイナンバーで変わるセキュリティ対策とは？

マイナンバー制度施行に向けてセキュリティ対策はどんな対象を見直す必要があり、何をしなければならないのか？大きな投資が必要なのではなく「最適化」することが最善であるとの視点を検証し、考察します。

担当：卒区次郎

CONTENTS 04 セミナー情報 Seminar information



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

大阪本社
〒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

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 /・特集 !!　McAfee NSP
・情報セキュリティ通信脅威動向・コラム

www.secuavail.com