PRESS RELEASE

2012 年 9 月 21 日

報道関係各位

株式会社セキュアブレイン

セキュアブレイン、感染原因や経路を特定し、標的型攻撃を防ぐ
セキュリティソリューション「FireAMP」 の販売を開始

株式会社セキュアブレイン(本社：東京都千代田区、代表取締役社長 兼 CEO：成田 明彦、以下「セキュアブレイン」)は、Sourcefire 社（本社：米国、メリーランド州）のセキュリティソリューション「FireAMP™（ファイアアンプ）」（以下、FireAMP™）の販売を本日より開始したことを発表します。

近年増加傾向にある標的型攻撃は、特定の企業や組織のユーザに狙いを定め、脆弱性を悪用した不正メールを使って侵入を試みます。メールに添付されるマルウェアは、従来の攻撃のように不特定多数に対してばらまくマルウェアとは異なり、標的となった企業や組織にのみ使われるため、マルウェアの検体の入手が非常に困難です。このため従来のウイルス対策製品では検出することができず、長期間発見されない傾向にあります。

感染した PC の動作異常や異常なネットワークアクセスなどに気付き、原因となるファイルを特定できた場合、ウイルス対策ベンダーに提供し、シグネチャの更新を依頼することでマルウェアを駆除することができます。しかし、標的型攻撃の多くは単一のファイルではなく、複数のファイルで構成されているため、全ての関連するファイルを自力で見つけだし対応することは不可能です。また、アプリケーションの脆弱性を利用して侵入する攻撃の場合、原因となった脆弱なアプリケーションも特定できないので、根本的な対策ができず、再感染を繰り返してしまいます。

FireAMP™は以下 5 つの新機能により、標的型攻撃に対する防御を大幅に向上します。

- Cloud Analytics （クラウドアナリティックス）- ビッグデータの分析により、他のセキュリティレイヤで見逃された脅威の特定と評価を行う高度な検出機能を搭載したクラウドベースのインフラストラクチャです。
- File Trajectory（ファイルトラジェクトリー） ー企業ネットワーク内のファイルイベントを記録することで、企業・組織へのマルウェアの侵入経路と感染被害状況を特定することが可能です。
- File Analysis（ファイルアナリシス） ー Sourcefire の研究チーム Vulnerability Research Team (VRT™)により構築された解析システムが、マルウェアの詳細な挙動情報を提供します。
- Outbreak Control（アウトブレークコントロール） ーウイルス対策ベンダーから更新（アップデート）を入手する必要なく、ユーザが独自にマルウェアを検知するためのシグネチャ作成機能です。
- Cloud Recall™ （クラウドリコール）- クラウド内に保存した過去のファイルイベントの分析を繰り返す事により、見逃されていた脅威を検出し、駆除する機能です。

FireAMP™ は、企業・組織のネットワークにおけるマルウェア感染の状態について必要な情報を提供する強力なレポートを提供します。これらのレポートでは、ハイリスクコンピュータ、脅威の根本的原因（マルウェアの感染原因となったアプリケーションを示すもの)、そして高度で長期に及ぶ脅威（ユーザの環境で標的型攻撃に利用されたと考えられるマルウェア）が詳細に示されます。

FireAMP™ は、標的型攻撃対策に必要となる情報を収集し分析することで、感染原因や経路を特定し、マルウェアの感染拡大を防止するセキュリティソリューションです。

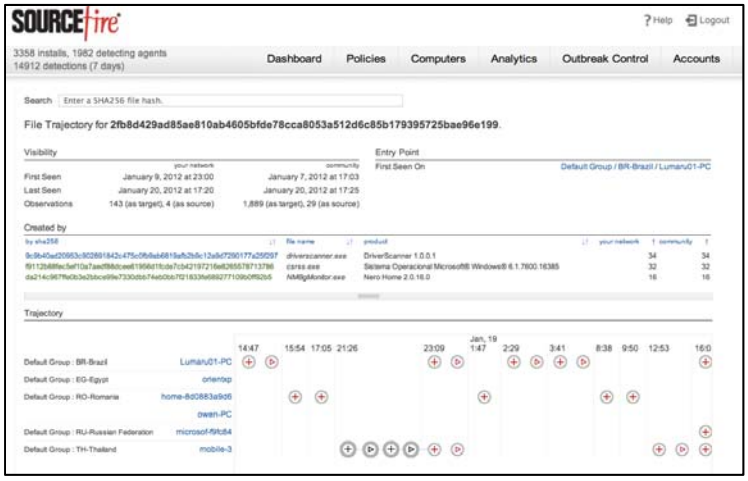
セキュアブレインは、FireAMP™を初年度に年間 100 社への販売を目標とします。

機能詳細については、以下をご覧ください。
http://www.securebrain.co.jp/products/fireamp/index.html

■FireAMP™の主なユーザインタフェース

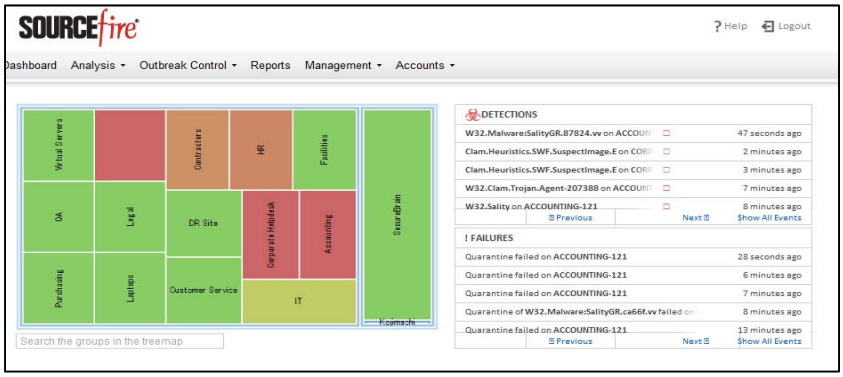
・File Trajectory 機能

マルウェアの侵入経路や企業・組織内の感染状況を把握



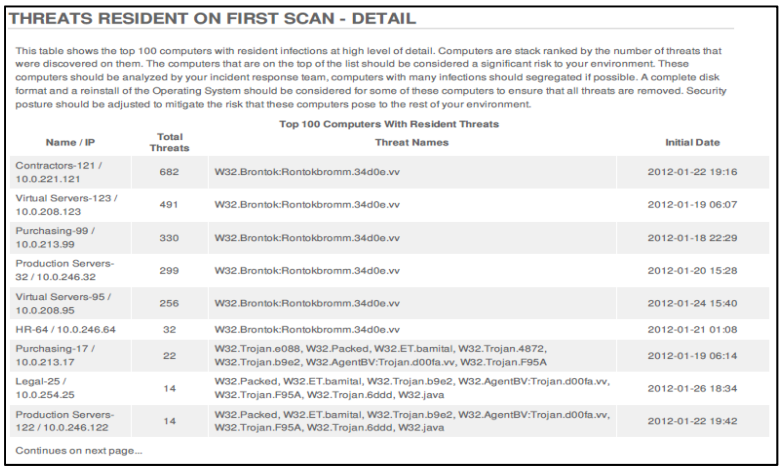
・Heat Chart 機能

部署や拠点ごとの感染状況を一目で把握



・High Risk Computer 機能

感染頻度の高い PC や検知回数の多い PC を特定



THREATS RESIDENT ON FIRST SCAN - DETAIL

This table shows the top 100 computers with resident infections at high level of detail. Computers are stack ranked by the number of threats that were discovered on them. The computers that are on the top of the list should be considered a significant risk to your environment. These computers should be analyzed by your incident response team, computers with many infections should segregated if possible. A complete disk format and a reinstall of the Operating System should be considered for some of these computers to ensure that all threats are removed. Security posture should be adjusted to mitigate the risk that these computers pose to the rest of your environment.

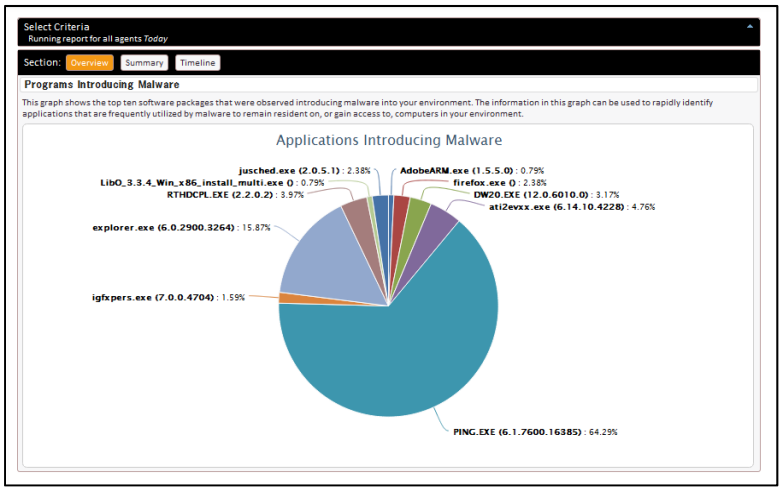
Top 100 Computers With Resident Threats

Name / IP	Total Threats	Threat Names	Initial Date
Contractors-121 / 10.0.221.121	682	W32.Brontok:Rontokbromm.34d0e.vv	2012-01-22 19:16
Virtual Servers-123 / 10.0.208.123	491	W32.Brontok:Rontokbromm.34d0e.vv	2012-01-19 06:07
Purchasing-99 / 10.0.213.99	330	W32.Brontok:Rontokbromm.34d0e.vv	2012-01-18 22:29
Production Servers-32 / 10.0.246.32	299	W32.Brontok:Rontokbromm.34d0e.vv	2012-01-20 15:28
Virtual Servers-95 / 10.0.208.95	256	W32.Brontok:Rontokbromm.34d0e.vv	2012-01-24 15:40
HR-64 / 10.0.246.64	32	W32.Brontok:Rontokbromm.34d0e.vv	2012-01-21 01:08
Purchasing-17 / 10.0.213.17	22	W32.Trojan.e088, W32.Packed, W32.ET.bamital, W32.Trojan.4872, W32.Trojan.b9e2, W32.AgentBV:Trojan.d00fa.vv, W32.Trojan.F95A	2012-01-19 06:14
Legal-25 / 10.0.254.25	14	W32.Packed, W32.ET.bamital, W32.Trojan.b9e2, W32.AgentBV:Trojan.d00fa.vv, W32.Trojan.F95A, W32.Trojan.6ddd, W32.java	2012-01-26 18:34
Production Servers-122 / 10.0.246.122	14	W32.Packed, W32.ET.bamital, W32.Trojan.b9e2, W32.AgentBV:Trojan.d00fa.vv, W32.Trojan.F95A, W32.Trojan.6ddd, W32.java	2012-01-22 19:42

Continues on next page...

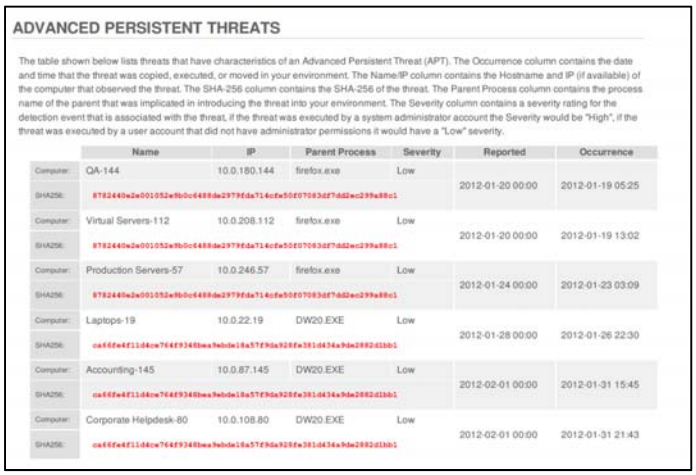
・Threat Root Cause 機能

マルウェアの侵入経路になっているアプリケーションとその割合をグラフ化



・Advanced Persistent Threats 機能

標的型攻撃に利用された可能性のあるマルウェアを表示



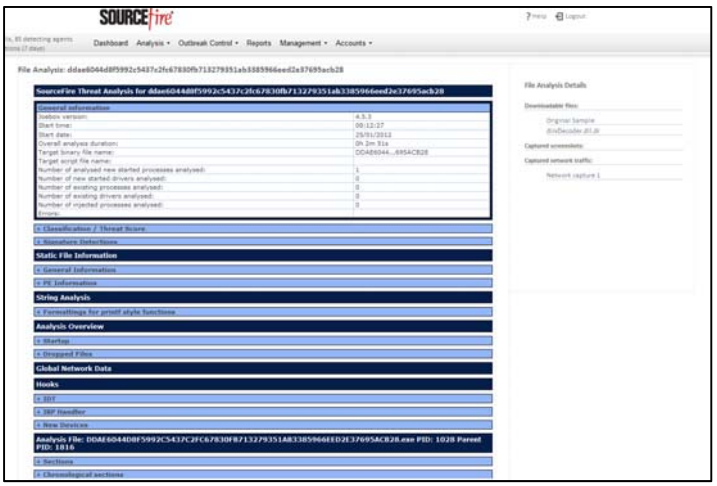
ADVANCED PERSISTENT THREATS

The table shown below lists threats that have characteristics of an Advanced Persistent Threat (APT). The Occurrence column contains the date and time that the threat was copied, executed, or moved in your environment. The Name/IP column contains the Hostname and IP (if available) of the computer that observed the threat. The SHA-256 column contains the SHA-256 of the threat. The Parent Process column contains the process name of the parent that was implicated in introducing the threat into your environment. The Severity column contains a severity rating for the detection event that is associated with the threat, if the threat was executed by a system administrator account the Severity would be "High", if the threat was executed by a user account that did not have administrator permissions it would have a "Low" severity.

	Name	IP	Parent Process	Severity	Reported	Occurrence
Computer:	QA-144	10.0.180.144	firefox.exe	Low	2012-01-20 00:00	2012-01-19 05:25
SHA256:	8782440e2e001052e8b0c4488de2979fda714cfe50f07083df7dd2ec299a88c1					
Computer:	Virtual Servers-112	10.0.208.112	firefox.exe	Low	2012-01-20 00:00	2012-01-19 13:02
SHA256:	8782440e2e001052e8b0c4488de2979fda714cfe50f07083df7dd2ec299a88c1					
Computer:	Production Servers-57	10.0.246.57	firefox.exe	Low	2012-01-24 00:00	2012-01-23 03:09
SHA256:	8782440e2e001052e8b0c4488de2979fda714cfe50f07083df7dd2ec299a88c1					
Computer:	Laptops-19	10.0.22.19	DW20.EXE	Low	2012-01-28 00:00	2012-01-26 22:30
SHA256:	ca66fe4f11d4ce764f9348bea9ebde18a57f9da928fe381d434a9de2882d1bb1					
Computer:	Accounting-145	10.0.87.145	DW20.EXE	Low	2012-02-01 00:00	2012-01-31 15:45
SHA256:	ca66fe4f11d4ce764f9348bea9ebde18a57f9da928fe381d434a9de2882d1bb1					
Computer:	Corporate Helpdesk-80	10.0.108.80	DW20.EXE	Low	2012-02-01 00:00	2012-01-31 21:43
SHA256:	ca66fe4f11d4ce764f9348bea9ebde18a57f9da928fe381d434a9de2882d1bb1					

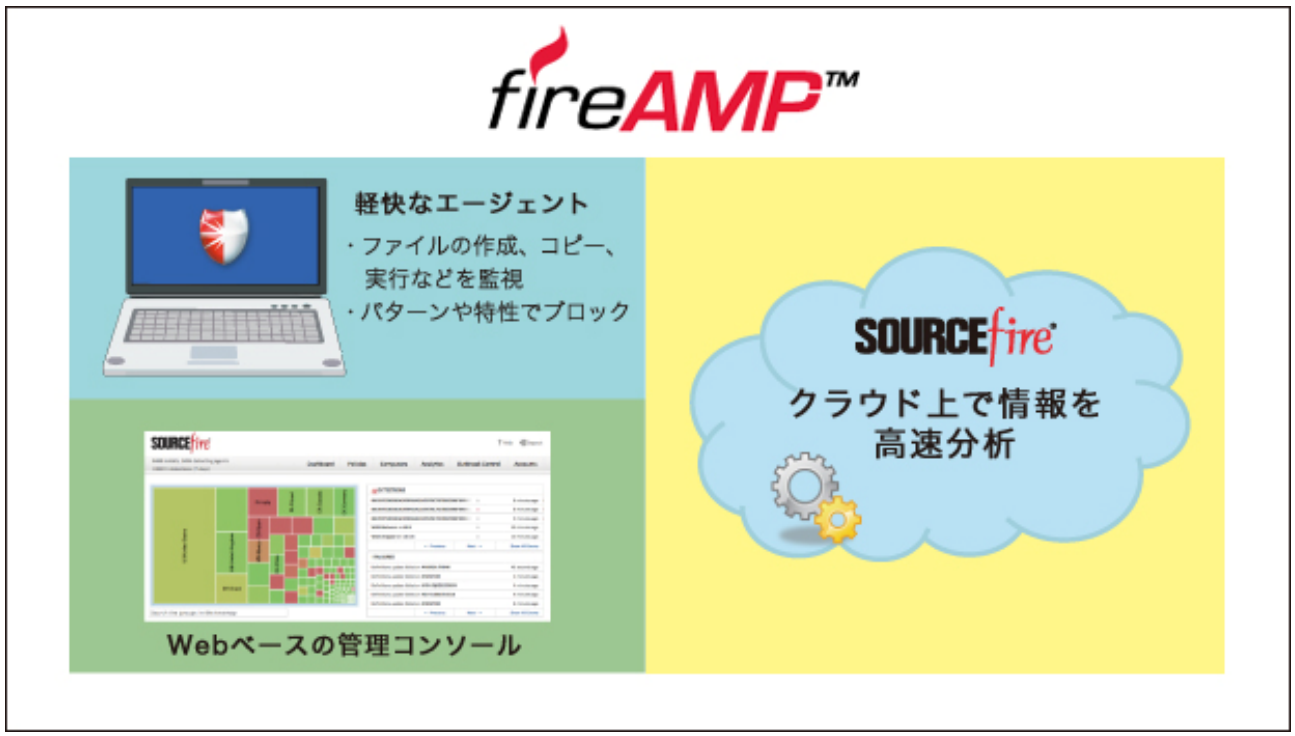
・File Analysis 機能

マルウェアをアップロードすると、マルウェアの特徴に関する情報をレポート



■FireAMPの製品構成

FireAMP は、クライアント PC にエージェントをインストールする必要があります。各エージェントから送られてきた膨大な情報をクラウド上で高速に分析します。管理者は、詳細情報を Web 上の管理コンソールから閲覧することができます。



エージェントは既に使用している他社ウイルス対策ソフトと一緒に使用することができます。

管理コンソールでエージェントの配布、ポリシーの管理、レポート機能など集中管理が行えます。

■システム要件

対応 OS：Windows XP SP2 以上、Windows Vista SP2 以上、Windows 7、Window Server 2008
FireAMP は、Active Directory と LDAP に対応しています。

■価格（年間ライセンス費）

25 ユーザ、245,000 円（税別）より
※年間サポート費が含まれています

※「FireAMP」は、米国 Sourcefire 社の製品です。

以上

セキュアブレインについて

株式会社セキュアブレインは、インターネット上の脅威が多様化する中、全てのインターネットユーザに安心を届ける、セキュリティのスペシャリストチームです。「より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する」というビジョンのもと、信頼性の高いセキュリティ情報と高品質なセキュリティ製品・サービスを提供する日本発のセキュリティの専門企業です。

◆ 本件に関する報道関係者さまからのお問い合わせ先 ◆

株式会社セキュアブレイン 広報担当：丸山 芳生（まるやま よしお）
電子メール：info@securebrain.co.jp
電話：03-3234-3001、FAX：03-3234-3002 〒102-0083 東京都千代田区麹町 2-6-7 麹町 RK ビル 4F