TERILOGY PRESS RELEASE

報道関係者各位

2012 年9月 11 日
株式会社テリロジー
（大証 JASDAQ 市場　証券コード 3356）

テリロジー“次世代標的型マルウエア防御クラウドサービス”開始
企業情報流出をブロックするセキュリティ出口対策の決定版！
―無償センサーソフトを企業ネットワークにインストールするだけで即クラウドサービス加入―

株式会社テリロジー（本社：東京都千代田区、代表取締役社長：津吹憲男、以下：テリロジー）は、国内で急増する標的型マルウエア攻撃による企業機密情報の流出被害を未然に防ぐ強力な対策として米国 Lastline 社（Jens Andreassen,CEO：サンタバーバラ、カリフォルニア州）と同社クラウドサービスの代理店契約を締結いたしました。尚、テリロジーは日本国内だけでなく、香港とシンガポール市場での同社クラウドサービスを展開いたします。

Lastline 社は、標的型マルウエア研究では世界的に有名なカリフォルニア大学サンタバーバラ校の教授および研究者達が 2009 年に設立し、2005 年から同大学でのマルウエア実証検証を含めた最新技術をベースにクラウドサービスの商用化に成功しました。米国では既に 300 サイト以上の利用実績を上げており、幅広い業種分野で同社の標的型マルウエア防御サービス利用で効力を発揮しています。
Lastline 社の創業メンバーは、オーストリアのウイーンに本部を置く“International Secure Systems Lab”設立にも深く関与しています。Lastline 社は、この研究機関とも密接な連携をとり、常に標的型マルウエア分析の分野でのイノベーティブな役割を担っています。Lastline 社は米国だけでなく、今後、日本を含むアジア、さらにはヨーロッパへのセキュリティクラウドビジネス拡大戦略を計画しています。

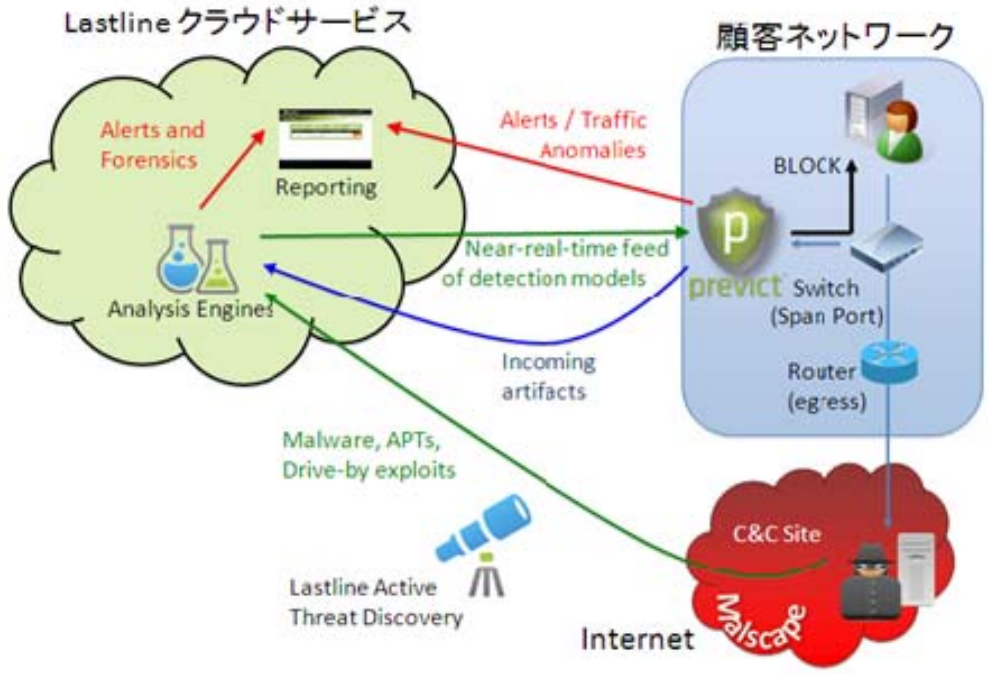
Lastline 社が提供する標的型攻撃防御のクラウドサービス（以下の構成図参照）は、業界レベルを上回る高検知率および低誤検知率を誇る高精度分析エンジンをクラウド上に置き、“Previct（TM）”と呼ぶ無償センサーソフトウエアを企業ネットワークにインストールします。企業ユーザは、自社ネットワークに無償センサーソフトをインストールするだけで、ネットワーク構成を変更せず標的型マルウエア攻撃防御のクラウドサービスを簡単に導入できます。
企業内での標的型攻撃のセキュリティ対策としては、企業ネットワークの入口でセキュリティ防御する「入口対策」と、企業内部の感染ユーザパソコンから外部の悪意なサイトに情報流出するのを防ぐ「出口対策」とがあります。Lastline 社は標的型マルウエアに特化したことで、セキュリティ出口対策を可能にしました。もちろんセキュリティ入口対策は他社同様に対応しています。

昨今、セキュリティ攻撃は広範囲に及んでおり、従来型セキュリティ攻撃はアンチウイルスソフト、ファイアウオール、不正侵入装置（IPS）でも対応が可能であるが、最新の標的型マルウエア攻撃はこれらのツールでは分析・検知・ブロックが困難です。
テリロジーでは、国内の製造、金融、流通の一般企業およびマネージドセキュリティサービス事業者（MSSP）を中心に、Lastline 社クラウドサービスを9月 11 日から本格的受注活動を開始します。
尚、Lastline 社次世代標的型マルウエア防御クラウドサービスの利用料金は年間2百万円（税別）から。初年度は 50 サイト、3年間で 200 サイトのユーザ獲得を目指します。

Lastline 社が提供する次世代標的型マルウエア防御クラウドサービスの主な特長は以下の通りです。

サービス名：次世代標的型マルウエア防御クラウドサービス

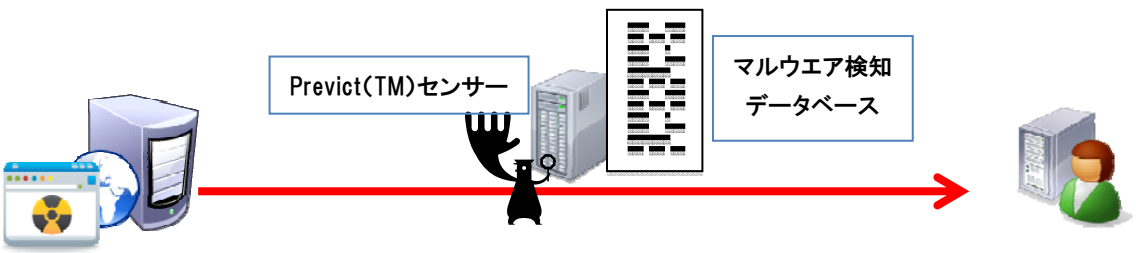
- 標的型攻撃による企業情報流出をブロックするセキュリティ出口対策の決定版。
- 無償 Previct（TM）センサーソフトを企業ネットワークにインストールするだけでクラウドサービスを提供。
- カリフォルニア大学サンタバーバラ校教授および研究者メンバーの長年にわたる研究成果をもとに画期的なマルウエア分析手法を製品化。
- 検知、防衛、対策、可視化をパッケージで提供。



（1）マルウエア検知

膨大でかつ的確な新規マルウエア検知情報を収集

- マルウエア潜伏の可能性あるグローバルの膨大なウエブサイトを独自手法でクローリング。
- 分析・検証したマルウエア検知情報を Previct（TM）センサーにリアルタイムにアップデート。インターネットから侵入するマルウエア攻撃を検知、ブロックします。
- 常に新規マルウエア情報をアップデートし、誤検知を最小限に抑えます。
- 自社情報だけでなく、世界の 40 社におよぶパートナーからも新規情報を収集。



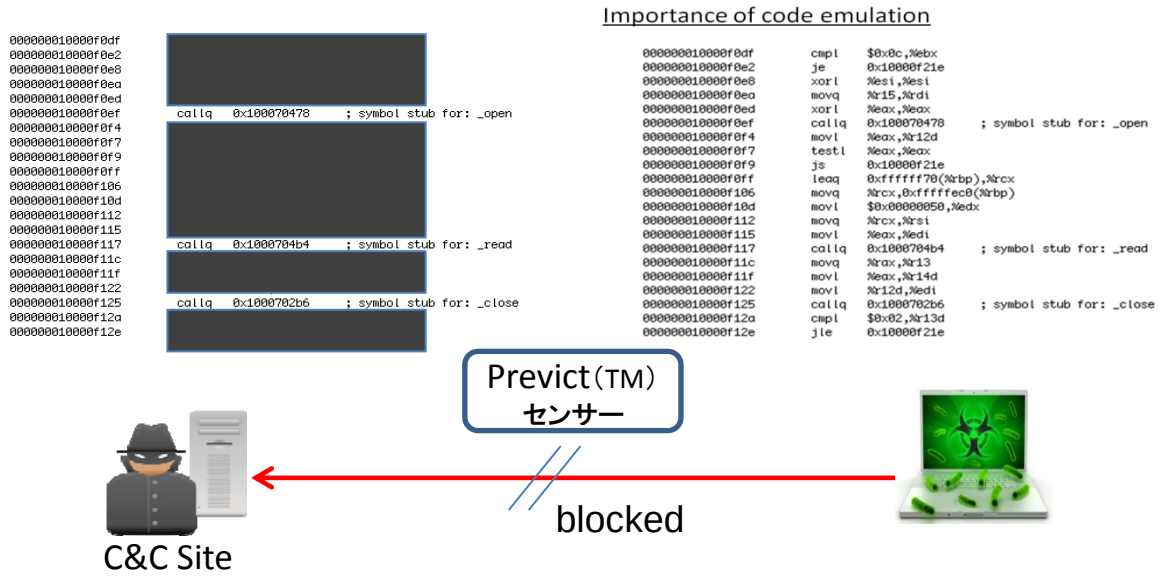
(2) マルウエア分析

業界レベルを上回る高検知率と低誤検知率

高精度マルウエア分析により、他セキュリティ製品ではミスしそうなステルス型マルウエアを見逃さずに検知

- システムコールだけではなくマルウエアによって実行するすべてのインストラクション（命令）を観察し、すみずみに至るまでの可視化と分析を提供。
- 「Exiting や Timeout」の手口で分析ツール検知から逃れようとするマルウエアを高度なエミュレーション技法でシャットアウト。
- 外部インターネットと通信しようとする際のビヘイビア（振る舞い）を独自のプロファイルでモデル化し、C&C（Command and Control）サイトを識別。

（注）下の図で左側の表示は、システムコールの行為だけした観察できない他セキュリティツールのケース。
右側の表示は Lastline 社クラウドの分析エンジンが観察できる攻撃行為すべての実行命令。



(3) マルウエア防御

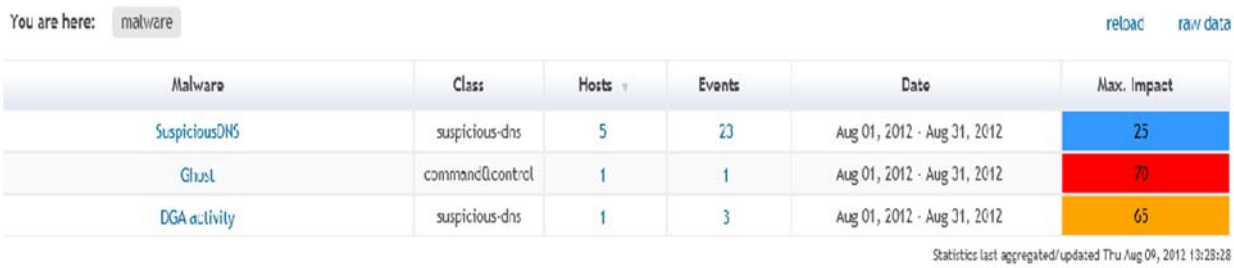
企業ネットワークを流れるトラフィックを分析してすべての脅威を防御

- マルウエアが潜むファイル、メール、ウエブページ、ドキュメントからユーザを保護。
- 幅広い領域をカバーし、モバイルデバイスも含むマルチ OS 環境から外部への機密情報の流出をブロック。

(4) イベント表示

豊富な構成設定機能により具体的なアクション情報をわかりやすく表示

- 各イベントはインシデントに関連付けられ、集約されており、脅威の状況を管理および具体的な対応策を提供。
- インシデントは緊急度別に分類され、それぞれに応じた対応情報を提供。



本リリースに記載されている社名、商品名は、各社の商標または登録商標です。

【Lastline 社について】
Lastline 社はカリフォルニア大学サンタバーバラ校の教授陣、Dr. Engin Kirda, Dr. Christopher Kruegel, Dr. Giovanni Vigna により 2009 年に設立されました。. 創業メンバーはマルウエア分析に関するアカデミックリサーチ界で数々のアワードを受賞しています。また、彼らは世界の研究機関向けに利用されているマルウエア診断オンデマンドツール“Anubis および Wepawet”.の開発者としても世界的に有名です。米国では既に 300 サイト以上の導入実績を上げており、幅広い分野で同社の標的型マルウエア防御サービスが利用されています。
本社はカリフォルニア州サンタバーバラで、アジアではオーストラリア、ヨーロッパでは英国で活動しています。
Lastline 社 URL：http://www.lastline.com/をご覧ください。

【株式会社テリロジーについて】
株式会社テリロジーは、1989 年に会社設立、エンタープライズ LAN/WAN、ブロードバンド・アクセス、セキュリティ、ネットワーク管理の 4 つのソリューションを中核に、市場および顧客ニーズに対応したハードウエアからソフトウエアまでの幅広い製品を取り扱うネットワーク・インテグレータです。顧客は大企業や通信事業者を中心に 300 社を超え、ネットワーク関連ビジネスでは豊富な経験と実績を上げています。テリロジーは“ネットワーク&セキュリティ”カンパニーとして、強力な製品発掘力により常に海外の最先端技術を先取りし、ユーザの皆様に差別化ソリューションを提供しています。テリロジーは設立以来、“In collaboration with customer”をコーポレイトミッションとし、顧客の視点に立ったビジネス戦略をおこなっています。
株式会社テリロジーURL：http://www.terilogy.com/をご覧ください。

【本サービスに関するお問い合わせ先】
株式会社テリロジー
事業本部エンタープライズ営業部
TEL：03-3237-3291、FAX：03-3237-3293
e-mail ：terilogy@terilogy.com

【報道関係者お問い合わせ先】
株式会社テリロジー
経営企画本部 広報宣伝・IR 担当 齋藤清和
TEL：03-3237-3291、FAX：03-3237-3293
e-mail ：ksaito@terilogy.com