PRESS RELEASE

報道関係各位

2014 年 4 月 9 日
ネクスト・イット株式会社

ネクスト・イット株式会社、持続的標的型攻撃の検出と修復能力が著しく向上した、米国 ThreatTrackSecurity 社製、動的マルウエア解析ソフト 『ThreatAnalyzer5.0(スレットアナライザ 5.0)』の出荷を開始

ネクスト・イット株式会社（本社：東京都品川区、代表取締役: 仲西敏雄、以下 NextIT）は、本日、ThreatTrackSecurity 社製（本社：米フロリダ州クリアウォーター、最高経営責任者：Julian Waits 以下 TTS 社）で業界最高峰のマルウエア分析ソリューションである ThreatAnalyzer5.0 の国内出荷を開始しました。ThreatAnalyzer5.0 では、マルウエアが行う振る舞いを分析するための基本機能が向上したことに加え、サンドボックスを認識し回避するようなマルウエアに対するリブートシミュレーション機能、生産性を高める新ユーザインターフェースなど、30 以上もの新しい拡張が加わりました。この最新バージョンを導入することによって、サイバーセキュリティのプロフェッショナルが悪意のあるファイルを特定することだけでなく、そのようなファイルを自社ネットワーク内から迅速に排除することも可能となります。

TTS 社の ThreatAnalyzer は、世界中で 300 もの企業に採用されています。導入企業は、大手企業、金融機関、政府、国防関係機関等です。「脅威は検出だけ行えば良いというものではありません。排除しなければならないのです」、NextIT 代表取締役仲西敏雄は、こう述べます。「ThreatAnalyzer は大企業のみならず政府機関など、現在 300 社以上の企業や団体に導入されています。未知のマルウエア検体が自社のエンドポイント上でどのような振る舞いをするかを把握できるだけでなく、より重要なことは、自社ネットワークからこのような脅威を根絶するために必要なあらゆる情報をこのソリューションでは提供できるという点が挙げられます。ThreatAnalyzer は、APT・標的型攻撃・ゼロデイ攻撃など、企業の事業活動を標的とする巧妙化したマルウエアに対処できるサイバーセキュリティソリューションです。」

自動化、分析、そして対処

ThreatAnalyzer は、監視された環境内でファイルや URL への接続を実行し、ネットワークに与えるリスクを分析、特定します。ユーザは検体のサブミットプロセスを自動化しあらゆる脅威を詳細に分析できるため、機密性の高いデータの保護措置を迅速に講じることができます ThreatAnalyzer は、これまで何日もかかっていたプロセスを数十秒から最大 2 分間(デフォルト)に短縮できます。

①自動化 – 一日に分析するマルウエア検体の数は急増しています。このような中、ヒューマンエラーを招く手動分析のみでは、多大な時間とコストがかかるだけでなく、巧妙化されたサイバー脅威に十分対処できない可能性もあります。

②分析 – 様々な組み合わせのアプリケーション上でマルウエアの振る舞いを分析することで、マルウエアの実行の仕組み、マルウエアがシステムに加えた変更、マルウエアが生成したネットワークトラフィック、不正利用されたアプリケーション、対象となったデータなど、マルウエアに関する詳細レベルの情報を提供できます。

ネクスト・イット株式会社〒140-0004 東京都品川区南品川 2 丁目 4 番7号 アサミビル 電話（03）5783-0702 FAX（03）5783-0734

③対処 – ThreatAnalyzer は、脅威のブロックやチームメンバへの通知を行うだけではありません。ネットワーク内に悪意のあるコードを少しも残さずに除去すると共に、マルウエアによって加えられた変更を修正することもできます。このため、ネットワークに侵入した脅威を完全に排除することが可能となります。

ThreatAnalyzer5.0 の新機能

①リブートシミュレーション機能 – システムがリブートされてから初めて活動を行うような悪意のあるコードを検出します。この独自の検出機能により、他の多くのサンドボックス分析テクノロジでは検出できなかったようなコードも実際に実行させることができます。

②脅威情報ダッシュボード – 検出したマルウエアの情報と現在のリスク状況の把握に役立つ、マルウエア情報と総合脅威レベルを表示します。分析したマルウエアの上位 10 件の IP やドメイン、確認された上位 5 件の悪意のある振る舞い、脅威の地理情報を示したワールドマップなど、様々なデータを提供します。

③ワークフローオプティマイザ – ユーザが日々経験するような標準的なシナリオに基づき、複数のサンドボックスへのサブミットを効率化します。毎日のオペレーションを最適化する機能拡張です。

④API インテグレータ – JSON や XML の形で出力されたデータをサポートします。ユーザは、この ThreatAnalyzer のマルウエア情報を別のサイバーセキュリティソリューションに連携させることができます。

⑤検体保存機能 – マルウエア検体がアクセスまたは生成した JavaScript、Flash、HTML、ネットワークトラフィックなどのデータを保存します。この機能を利用すれば、目的のマルウエア検体をオフラインで後日詳細に分析することが可能となります。

業界トップのマルウエア動的分析ソリューション

ThreatAnalyzer には、SaaS ベースの仮想的な分析エンジンにはない、次のような様々な機能があります。物理環境及び仮想環境でマルウエアを実行させることで、サンドボックスや VM を認識・回避するようなマルウエア検体を分析することもできます。お客様が現在利用している様々なアプリケーションの組み合わせに一致するように動的解析環境を構成、設定しクローンを作成することができ、これによって、悪意のある振る舞いをより深く理解し、標的型攻撃の特定も効率化できます。独立したサンドボックスはオフライン分析が行えるだけでなく、機能を制限することなく安全にマルウエアの分析ができます。

『TTS 社製 ThreatAnalyzer』についての詳細は、こちらのサイトでもご覧戴けます。
http://nextit.jp/product/threatanalyzer/index.html

【報道関係者様のお問い合わせ先】 **ネクスト・イット株式会社** 担当：谷尾 TEL：03-5783-0702 e-mail：press@nextit.jp URL: http://www.nextit.jp/	【ご購入、評価をご検討のお客様のお問い合わせ先】 **ネクスト・イット株式会社** 担当：ソリューション営業部 TEL：03-5783-0702 e-mail：info@nextit.jp URL: http://www.nextit.jp/

【ネクスト・イット株式会社について】

NextIT は 2002 年に創業した、先進の次世代 IT 技術を駆使して企業が抱える様々な IT ソリューションニーズにお応えする総合 IT プロデューサー集団です。『リスクマネージメント・ソリューション』『プロフェッショナルサービス・ソリューション』事業をメインとし、ネットワーク、セキュリティ、ストレージ等のシームレス展開を実現させる「技術とサービスのワンストップ提供」を通して、日本の IT ビジネス業界に新しい価値の創造と変革をもたらす会社を目指しています。詳細は、http://nextit.jp/をご覧ください。

【ThreatTrack Security 社について】

世界各国の大企業には、依然、従来型のサイバー防衛システムが導入されています。しかし、APT 攻撃や標的型攻撃、巧妙化したその他のマルウエアには、従来型のサイバー防衛システムを回避するよう工夫が施されています。このような攻撃やマルウエアを特定しその動きを封じる上で、ThreatTrack Security 社は専門家の立場から企業や組織を支援します。ThreatTrack Security 社は、サンドボックステクノロジを利用したマルウエア動的分析ソリューション「ThreatAnalyzer」、など、最新の脅威を検出・分析・修復する先進のサイバーセキュリティソリューションを開発しています。

ネクスト・イット株式会社〒140-0004 東京都品川区南品川 2 丁目 4 番 7 号 アサミビル 電話(03)5783-0702 FAX(03)5783-0734