NEWS RELEASE

エイチ・シー・ネットワークス株式会社

2017 年 6 月 6 日

HCNETのAdapterシリーズ、Damballa Network InsightおよびAPRESIAと連係し、不正通信端末遮断ソリューションを実現

このたび、エイチ・シー・ネットワークス株式会社は、自社が開発・販売している認証ログ管理アプライアンス「LOG@Adapter」（ログアダプター）、および認証・アカウント管理・DHCPアプライアンス「Account@Adapter＋」（アカウントアダプタープラス）を、ネットワンシステムズ株式会社が販売のCore Security社製で標的型攻撃や高度化したランサムウエアなどのマルウエアに感染した端末を迅速に特定する自動感染検知システム「Damballa Network Insight」、およびAPRESIA Systems株式会社製の認証スイッチ「Apresia13200-28GT」と組み合わせた連係検証を実施し、正しく動作することを確認しました。

この連係により、ランサムウエアなどのマルウエア感染が検知された端末をネットワークの末端レベルで遮断することが可能となり、よりセキュアなネットワーク環境が実現します。

■連係動作概要

LOG@Adapterは認証ログの管理に特化したsyslogアプライアンスであるとともに、IPSなどの不正通信を検知する製品や、認証スイッチおよびAccount@Adapter+と連係することで、不正な通信を行った端末をネットワークから遮断します。

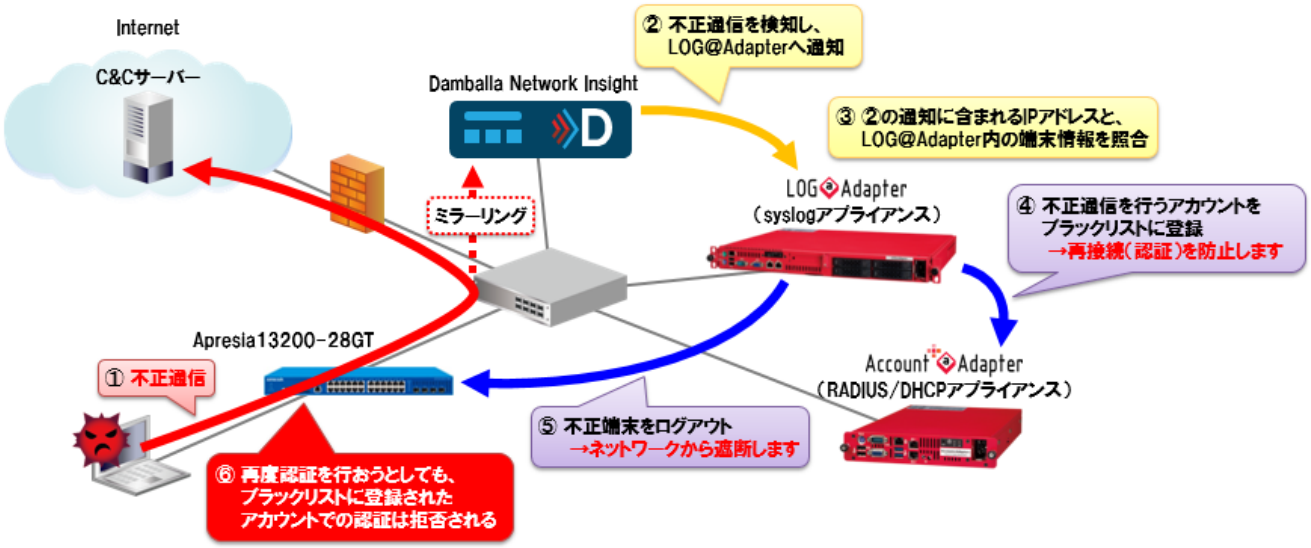
Damballa Network Insightは、全世界のインターネットトラフィック、とりわけ北米インターネットトラフィックの約65%を監視することで、日々得られる1.2兆ものDNSクエリーや20万のランサムウエアなどのマルウエア検体を最先端のセキュリティデータサイエンスに基づく機械学習で分析した膨大なセキュリティビッグデータを基に、これまでのアンチウイルスやファイアウォール、サンドボックスといった防御ツールでは判定が難しかったランサムウエアなどの高度な脅威に感染した端末を迅速に特定します。

Damballa Network Insightが不正な通信から感染検知を断定すると、LOG@Adapterへ通知します。LOG@Adapterは、Apresia13200-28GTから送信された認証ログなどを基に作成された端末のIPアドレスやMACアドレス、端末が接続している認証スイッチや認証に利用したアカウントなどが格納された端末情報データベースと、Damballa Network Insightから送信されたログを照合し、不正な通信を行っている端末を特定します。

さらに、LOG@Adapterは、Apresia13200-28GTに対して不正な通信を行った端末を、ネットワークから遮断するコマンドを発行するとともに、認証時に利用したアカウントをAccount@Adapter+のブラックリストへ登録するよう通知します。

Apresia13200-28GTからログアウトされた不正な通信を行った端末が再度認証を試みても、ブラックリストに登録されたアカウントは認証時に拒否されるため、ネットワークに接続することができません。

■連係動作フロー



① Apresia13200-28GTで認証済みの、ランサムウエアなどのマルウエアに感染した端末がC&Cサーバーと通信
② Damballa Network Insightが①から感染を断定し、LOG@Adapterへ通知
③ LOG@Adapterは、Apresia13200-28GTやAccount@Adapter+から受信したログを基に作成した端末情報と、Damballa Network Insightから受信したログを照合
④ LOG@Adapterは、対象端末がApresia13200-28GTにネットワークログインする際に利用したアカウントをAccount@Adapter+のブラックリストへ登録するよう通知
⑤ LOG@Adapterは、Apresia13200-28GTへ対象端末のログアウトコマンドを発行し対象端末をログアウト
⑥ Apresia13200-28GTからログアウトされた端末が再認証を試みても、Account@Adapter+のブラックリストに登録されたアカウントは拒否されネットワークに接続不可

■LOG@Adapter(エイチ・シー・ネットワークス社製syslogアプライアンス)

LOG@Adapterは、各種機器のsyslog、SNMP Trap情報を一元管理可能なsyslogアプライアンスです。不審なログに対するアラートメールやトラップを管理者に通知する機能などを搭載しています。また、APRESIA、ALAXALA、Aruba、QuOLA@Adapterとの連係機能により、ネットワークの利用状況を把握することが可能となります。

■Account@Adapter+(エイチ・シー・ネットワークス社製RADIUSアプライアンス)

Account@Adapter+は、RADIUS機能、LDAP機能、CA(認証局)機能、DHCP機能を1台に搭載した専用アプライアンスです。ユーザー自身によるアカウント、端末、証明書の申請機能や、MACアドレス自動登録、未使用アカウントの自動削除、一括アカウント申請＆発行機能などを搭載しています。

■Damballa Network Insight

Damballa Network Insightは、ランサムウエアなどのマルウエア感染による機密情報の組織外流出という脅威から、組織におけるサーバーや端末などを確実に保護するためのセキュリティインテリジェンス製品です。感染端末を検出するだけではなく、リスク判定エンジンによって感染端末にリスクスコアを付けることで、人手による判断などの運用負荷を最小化します。アラートの嵐に晒されることなく、貴重なセキュリティアナリストを手間のかかる分析作業から解放し、SOC・CSIRTの作業効率化を実現します。

■Apresia13200-28GT

Apresia13200-28GTは、高性能と優れたコストパフォーマンスを実現したALL Gigaディストリビューションスイッチです。SDカードブートに対応し、SDカードからのファームウェア、config情報の読み込みが可能です。保守手順を簡略化することで保守作業の時間とコストを削減します。

また、Web、MAC、IEEE802.1X、DHCPスヌーピングの4つの認証方式に対応し、利用環境に応じた柔軟なセキュリティポリシーの設計が可能です。

■エイチ・シー・ネットワークス株式会社

エイチ・シー・ネットワークスは、高品質＆信頼ネットワークの提供をビジョンとするネットワークインテグレーション会社です。30年以上のシステム構築実績を生かし、「ネットワーク」、「セキュリティ」、「ビジュアルコミュニケーション」、「トータルマネジメントサービス」のフィールドで、提案から構築・保守までワンストップでトータルネットワークソリューションを提供しています。詳細は以下のURLからご覧いただけます。

http://www.hcnet.co.jp/

■ネットワンシステムズ株式会社

ネットワンシステムズ株式会社は、お客様が利用するビジネスアプリケーションを、プライベートクラウド/パブリッククラウドを包括してセキュアに支える「クラウドシステム」を提供する企業です。そのために、常に世界の最先端技術動向を見極め、その組み合わせを検証して具現化するとともに、実際に自社内で実践することで利活用のノウハウも併せてお届けしています。詳細は以下のURLからご覧いただけます。

http://www.netone.co.jp/

■Core Security社

Core Security社は1996年に設立、セキュリティ脅威に関する卓越した知見に基づくアイデンティティ、アクセスおよび脆弱性管理のためのソリューションの提供を継続しています。2016年7月、ネットワーク脅威検知の専門企業である米Damballa Inc.の戦略的買収を機に、新たなセキュリティプラットフォーム「Actionable Insight & Response（AIR）」の展開を開始。AIRではセキュリティリスクの阻止・緩和、ネットワーク不正アクセスの検知、感染端末の特定、対処、セキュリティコントロールの検証機能を持続的に提供します。詳細は以下のURLからご覧いただけます。

https://www.coresecurity.com/ja

■APRESIA Systems株式会社

APRESIA Systems株式会社は、意思決定の迅速化とさらなる成長をめざして、2016年12月1日付けで日立金属株式会社から独立し、発足いたしました。

日立グループで長年培った技術をさらに磨き、情報システム専業会社として、通信インフラの高度化への対応やネットワーク構築への支援など、全てのお客様のご期待に応えて参ります。詳細は以下のURLからご覧いただけます。

http://www.apresiasystems.co.jp/index.html

■本ニュースリリースに関するお問い合わせ

〒111-0053
東京都台東区浅草橋1-22-16 ヒューリック浅草橋ビル4F
エイチ・シー・ネットワークス株式会社　営業本部　営業企画グループ

お問い合わせURL：http://www.hcnet.co.jp/inquiry/

■登録商標

LOG@Adapter、Account@Adapter、QuOLA@Adapter、HCNETおよびそのロゴは、エイチ・シー・ネットワークス株式会社の商標または登録商標です。

本ニュースリリースに記載されているその他の社名および製品名は、各社の商標または登録商標です。

本ニュースリリース記載の情報（製品・サービスの内容、仕様、価格、発売日、お問い合わせ先、URLなど）は、発表日現在の情報です。予告なしに変更される可能性がありますので、あらかじめご了承ください。

以上