AhnLab Smart Defense:

サイバー攻撃に対抗する成長型ソリューション

AhnLab, Inc.

目次

はじめに

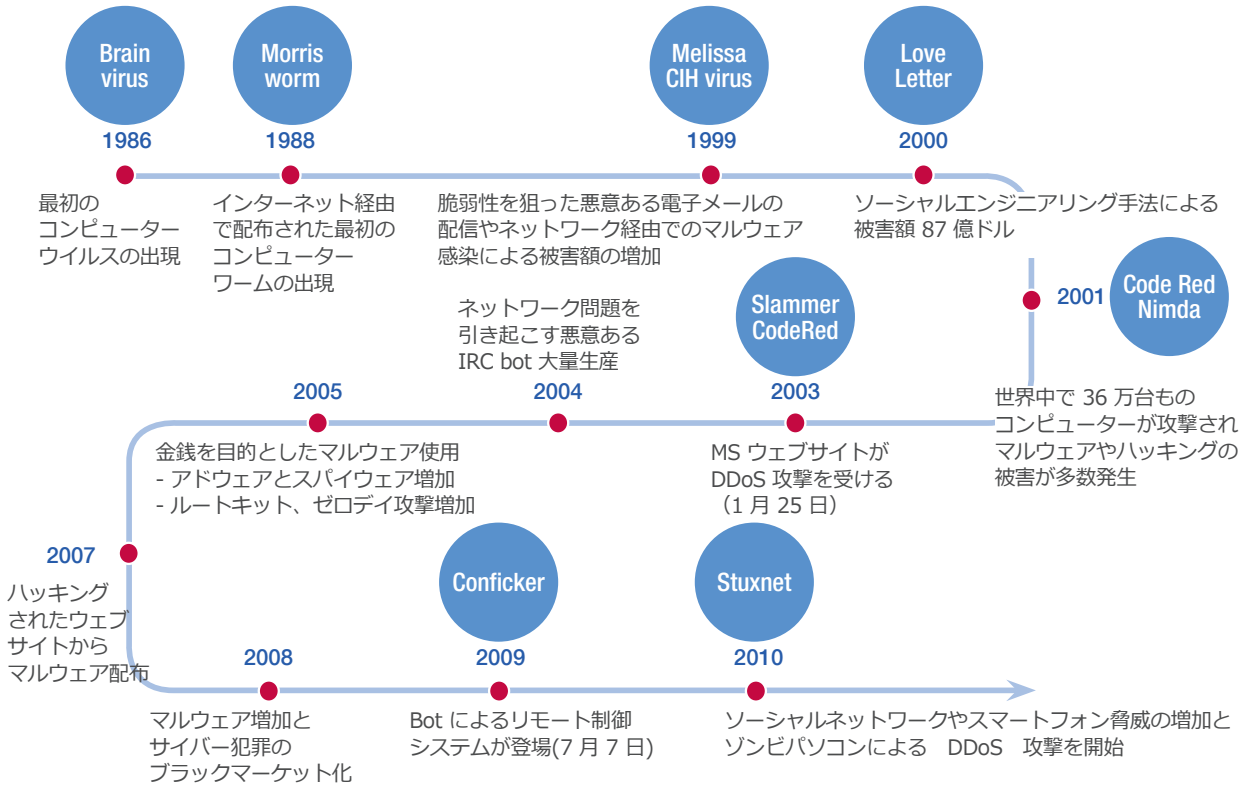
1980 年代後半にウイルスやワームが登場して以来、攻撃と防御は互いに牽制しつつ技術を発展させてきました。攻撃者が新たな手法で攻撃を仕掛けると、セキュリティ企業ではこれらを阻止するための新たな手法で防御する、という攻防戦が繰り返されており、この戦いは今後も続くものと予想されます。この対立構図が続く要因として、おびただしい数のマルウェアの亜種をすべて検知し対応するためのシグネチャを作成するには、膨大なリソースと時間が必要なことがあげられます。サイバーセキュリティ業界では、オンラインビジネスや個人データの取扱いの増加に比例して増え続ける「脅威」に対応するため、より積極的なアプローチを必要としています。

本ドキュメントでは、アンラボが提供するクラウド技術を基盤とする脅威自動分析と約 5 億個に達するサンプルデータベースから、マルウェアの種類を特定するマルウェア DNA マップについてご紹介します。

0ptAhnLab Smart Defense (以下「ASD」)はシグネチャのアップデートに必要な時間とリソースを節減すると同時に、事前対策としてスピーディなマルウェア検出および防御を実現します。

セキュリティ脅威の変遷

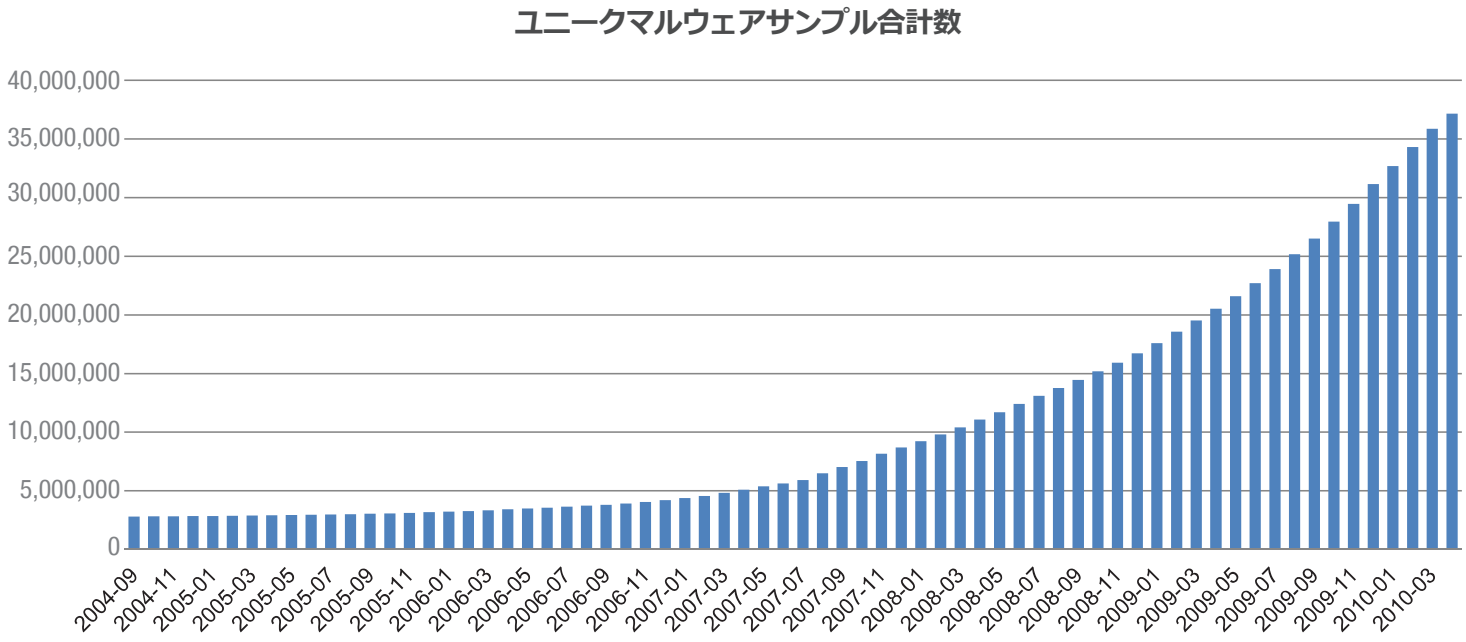
従来、ハッカーは自らの好奇心を満たす事、そして彼らのコーディング技術を広く知らしめる事を目的として、悪意あるスクリプトを作成していました。しかし最近では、攻撃とリモート制御は広範囲にわたり企てられるようになり、利益をもたらす犯罪へと変化しています。



マルウェアの進化

2005 年から台頭した新たなサイバー攻撃手法では、銀行口座番号やクレジットカード情報の売買など不正取得された個人情報がまるで商品のように取引きされるようになりました。こうした不正行為がブラックマーケットをさらに活気づかせています。これらの犯罪の収益増加の勢いに比例して、マルウェアの数も爆発的に増加しています。サイバー犯罪のブラックマーケットでは、多様なマルウェアを生成するために特別な経験や技術力なく簡単にマルウェアを作成できるオーサリングツールが登場した事により、脅威の拡散はさらに加速しています。

世界的に著名なドイツのウイルス対策ソフトの評価機関Av-Test.orgのデータによると、検出したユニークマルウェア数は2004 年には約 300 万でしたが、2010 年には約 3,700 万へと爆発的に増加しました。
アンラボの Security Emergency Response Center (以下「ASEC」) では、2011 年の1年間に全世界で配布されたマルウェア数として 1 億 7,000 万以上を超える報告を受けました。



マルウェア生産の上昇傾向 (資料: AV-Test.org)

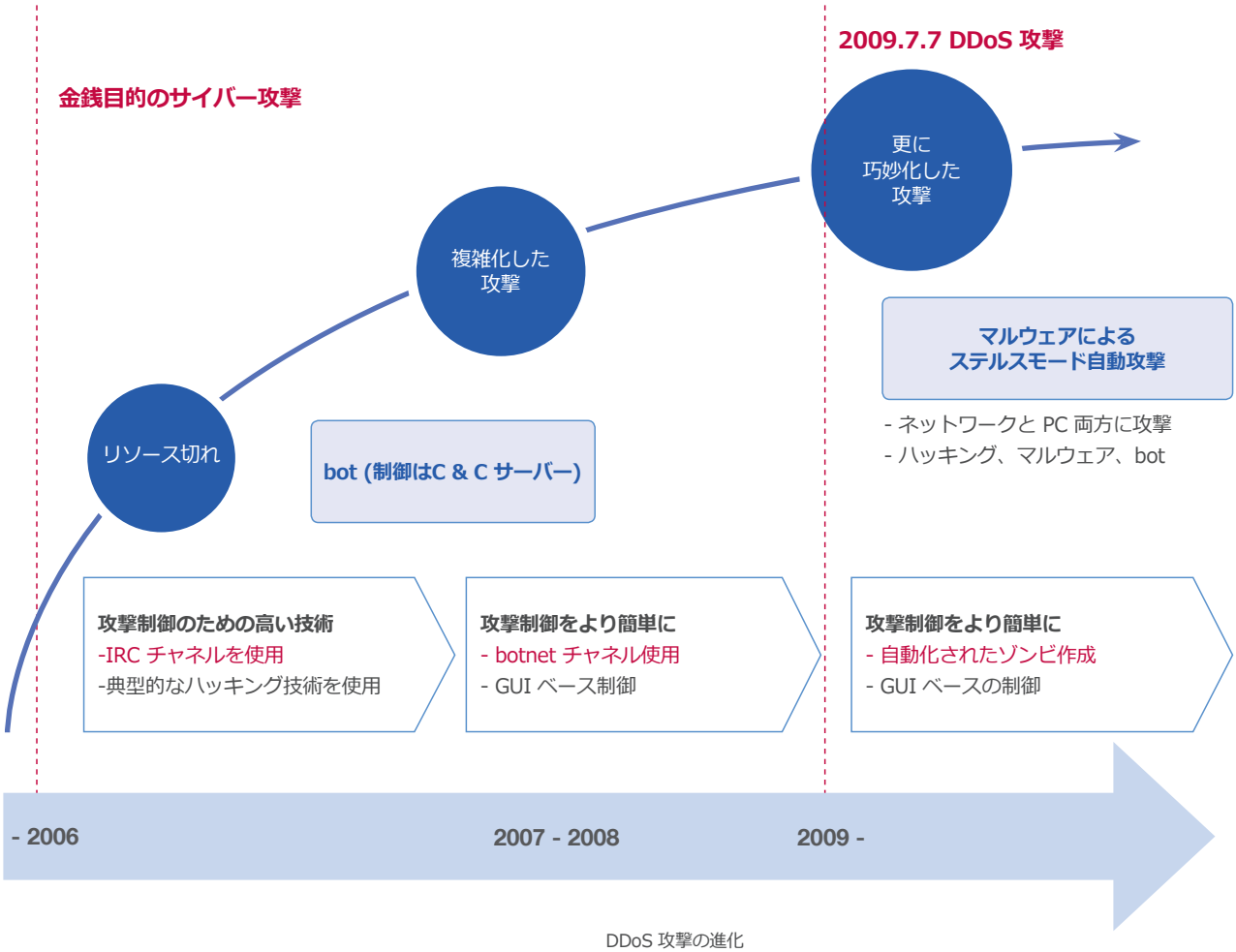
新たな脅威の登場

サイバー犯罪による収益増加に伴い、DDoS 攻撃の形態は大きく変化しています。

初期の DDoS 攻撃は、1～3 Gbps のトラフィックを発生させて TCP プロトコルの SYN フラッド攻撃または UDP/ICMP フラッド攻撃を仕掛けてシステムリソースを使い果たすことを主な目的としていました。

2007 年以降に発生した DDoS 攻撃はコマンドコントロール (C&C) サーバーの制御下にある bot により実行されました。この頃から、マルウェアのオーサリングツールがブラックマーケットで入手可能になりはじめ、ハッカーが簡単にマルウェアを製作できるようになり、マルウェアがサイバー攻撃のツールとして悪用されるようになりました。

続いて 2009 年 7 月 7 日、米国と韓国政府のウェブサイトを標的とした大規模な DDoS 攻撃が発生しました。攻撃当時のパターンシナリオは、事前に指定した時刻になると複数のゾンビパソコンから標的ウェブサイトに集中攻撃を仕掛ける、というものでした。このように高度化した攻撃手法により、bot を隠れ蓑にした攻撃が可能になりました。



DDoS 攻撃の進化

現在のセキュリティソリューション

セキュリティ企業では、マルウェアが爆発的に増加した事を受け、新たな問題に直面することになりました。
業界では 2009 年に韓国で発生したサイバー攻撃以降、エンドポイントとネットワーク両方への攻撃が今後も増加すると予想しています。主に単一機能のソリューションを提供してきたセキュリティ企業では、このような包括的な脅威に対応するための方法について頭を悩ませています。
Av-Test.org が公表したデータによると、セキュリティ企業が新種のマルウェアに対応してシグネチャをアップデートするスピードよりも、マルウェアが発生するスピードが上回っていることが分かります。その数は 2005 年に比べ、 2010 年には平均 150 を上回っており、シグネチャ/プログラムアップデート数は 5 倍に増加しました。

単位	2005	2010
シグネチャ/プログラムアップデート (回数)		
毎日	110	574
毎月	3,400 以上	17,000 以上
毎年	Over 40,000	200,000 以上
新種のマルウェア (個)		
毎日	360	50,000 以上
毎月	10,000 以上	1,500,000 以上
毎年	約 130,000	約 20,000,000

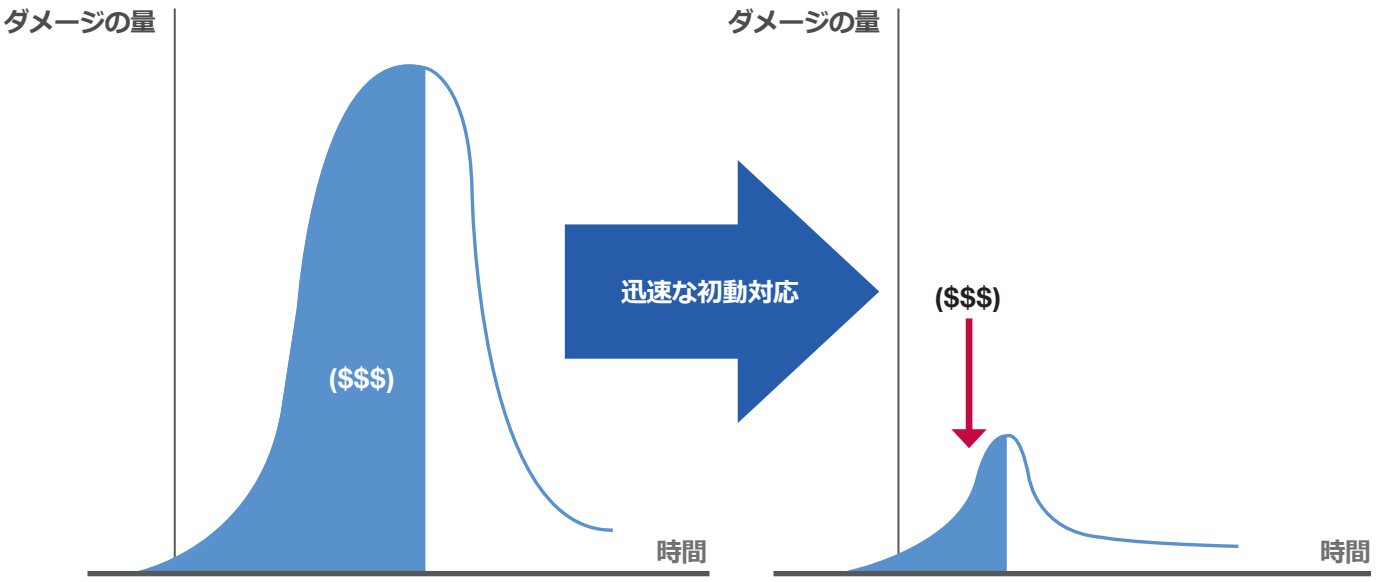
マルウェア増加によるシグネチャアップデートの増加 (資料: AV-Test.org)

既存のアンチマルウェア製品は限界を迎え、主なセキュリティベンダーでは従来のシグネチャベース検出ソリューションに加えてヒューリスティック検出、積極的な予防、サンドボックスなどの技術を次々と追加しました。しかし、これらはコンピューター環境の多様性、ひんぱんなプログラムアップデートのリリース管理の難しさ、そして偽陽性判定リスクに起因するセキュリティ上の問題すべてを完全にはカバーできていない状況です。

対応の遅さがコスト増大を招く

急増するマルウェアに対応するには、タイムリーな対応が要になってきます。企業側でシグネチャの持続的なアップデートサイクルを短縮するには、マルウェアのサンプルを収集/分析し、新しいシグネチャを開発/アップデート版を配布するまでの何段階ものプロセスを短縮する必要があります。

このターンアラウンドサイクルにおいて、ゼロデイ攻撃に対して脆弱性を露出させてしまった穴をすばやく埋めて対処しない限り、その被害コストは膨大なものになりかねません。以下の図のように初動対応が速ければ速いほど、マルウェアによる被害コストを削減することができます。



迅速な初動対応は、被害を軽減する

その他、必要なリソース

現存するソリューションに存在するもう一つの制約事項は、アンチマルウェアソフトに搭載されるエンジンサイズの巨大化です。新種のマルウェアに対応するため、より多くのシグネチャをアップデートするには追加のリソースが必要になります。

Av-Test.org の調査によると、ほとんどのアンチマルウェアプログラムで必要なリソースは 2005 年から 2010 年にかけて平均 15 倍ずつ増加しています。 5 年間で 15 倍増加している状況を考慮すると、急速に増大するリソース量をカバーするには、ハードウェアに負担をかけることになるのは明らかです。

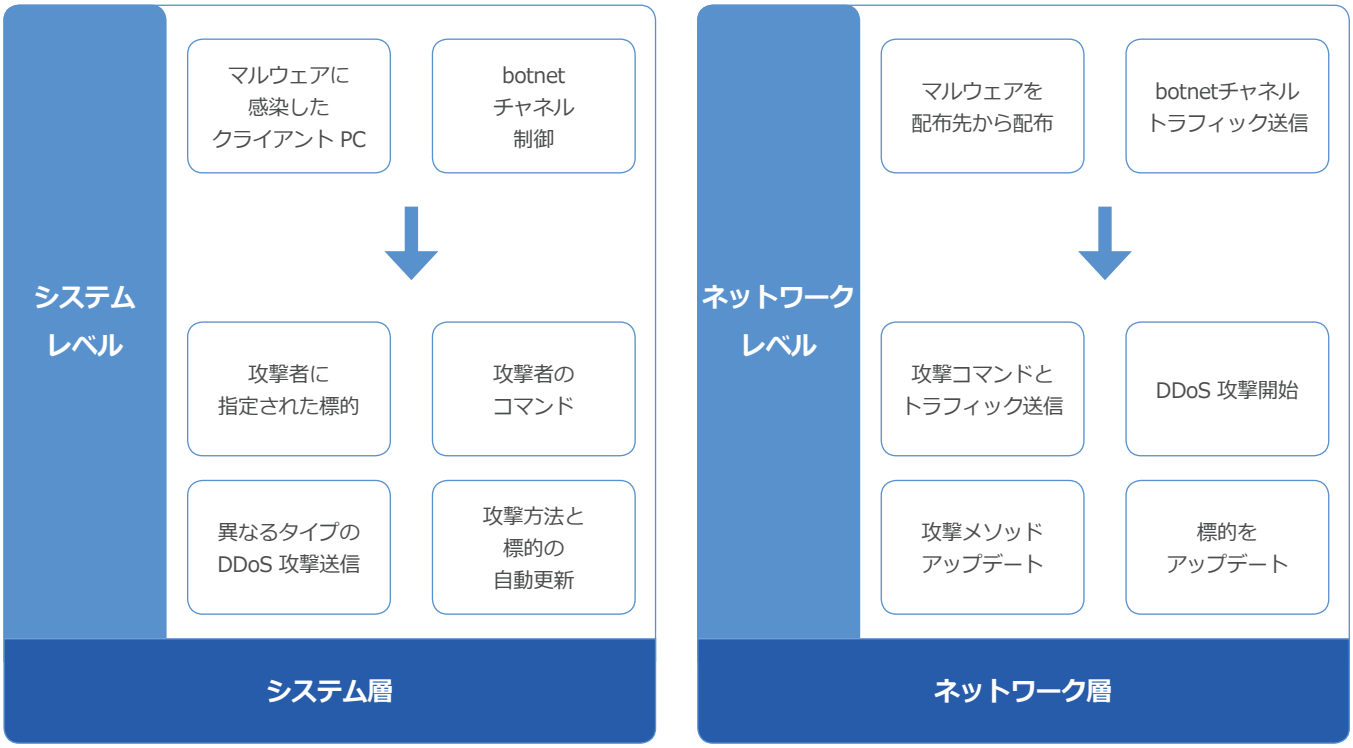
単位	2005	2010
アップデートサイズ		
毎日	1.2GB	17GB
毎月	30GB 以上	500GB 以上
毎年	400GB 以上	500GB 以上

アップデートサイズ増加 (資料: AV-Test.org)

ネットワークセキュリティソリューションの不完全性

ネットワークセキュリティ製品は、不正アクセスや悪意あるトラフィックの侵入をブロックすることでネットワークとサービスの整合性を保ちます。しかし、これらのソリューションでは感染コンピューターをネットワークから隔離することができません。これはネットワーク上の感染拡散を完全には防ぐ事ができないことを示しています。

最近の DDoS 攻撃は、システム層とネットワーク層の両方の脆弱性を突いてきます。システム層の攻撃に対応する性能を有していなければ、ネットワークセキュリティ製品として執拗に実行される攻撃を防ぐことはできません。

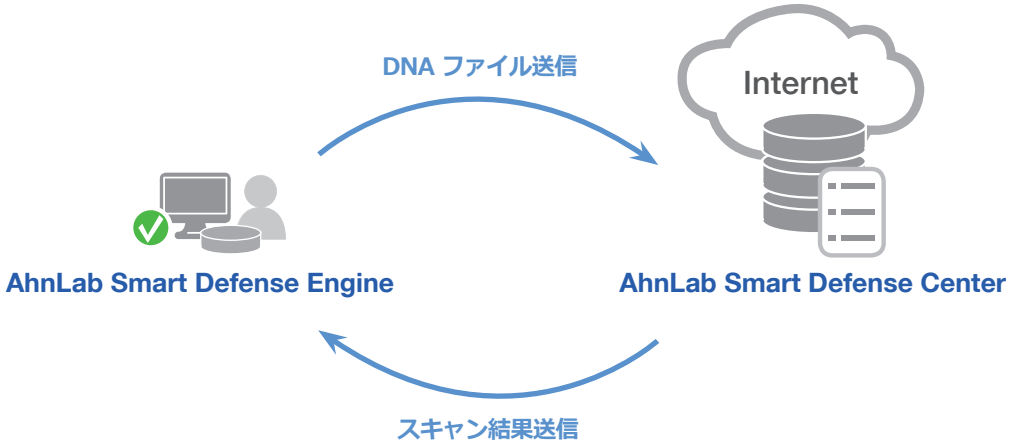


DDoS 攻撃の特性 (システム/ネットワークレベル)

AhnLab Smart Defense（ASD）

ASD は、新しいセキュリティ脅威と新種のマルウェアに迅速に対応するために開発された新しい概念のクラウド技術を基盤とするセキュリティソリューション（2009 年リリース）です。ASD は最新のセキュリティ環境に適した効果的なソリューションであり、採用しているクラウドベースシステムはレスポンスタイムを劇的に改善、システムリソースの占有率を削減すると共に DDoS 攻撃から守るためにネットワークセキュリティの間隙をカバーします。

ASD は、アンラボサーバー上の ASD センターにインストールされているエンジンとローカルコンピューターから構成されている独立型プラットフォームで、サーバー側に搭載されたデータベースがハードウェアに対し広範囲にわたる保護を提供します。従来のローカルコンピューター上に必要とされていた物理的なストレージ部分も省かれ、軽量化されています。



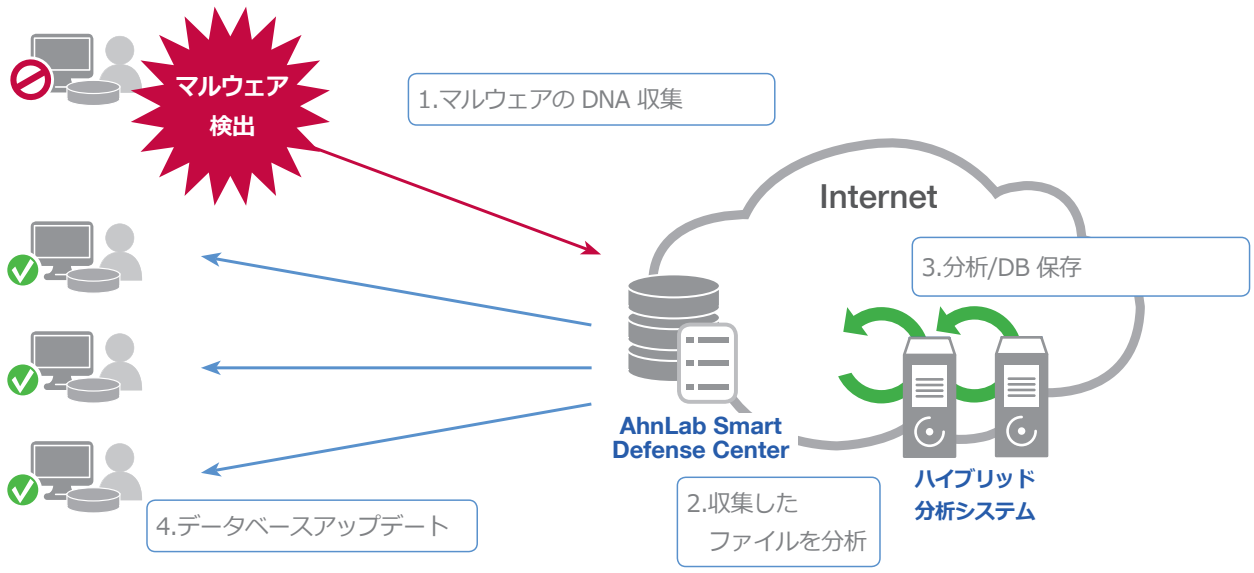
ASD コンポーネント

カスタマイズされた自動対応システム

本ソリューションは、ASD センターとの通信を介してローカルコンピューター上のファイルをスキャンして高度なセキュリティレベルを提供します。その後、レスポンスパフォーマンスを高めるため、ローカルデバイスやリソースの占有率を低減し、脅威分析用にカスタマイズされた自動保護を実行します。

1. スキャンを実行すると、まずローカルファイル用にカスタマイズされたシグネチャデータベースを呼び出し、ローカルコンピューター上にキャッシュを保存します。その後、保存されたシグネチャと新規または変更されたファイルを比較確認します。変更のないファイルはスキャンをスキップして時間短縮します。
2. 上記 1 のプロセスで不明なファイルを検出した場合、ファイルの DNA 情報（ファイル固有のデジタル指紋）を分析するために ASD センターに送信します。
3. ASD センターでは、現時点のデータベースとファイルを比較して DNA を確認します。DNA が一致した場合、安全/マルウェアファイル判定を行い、その結果を ASD エンジンに通知してローカルコンピューター上に存在するシグネチャデータベースをアップデートします。

4. データベース上で DNA が一致するファイルが見つからない場合、その情報は自動分析システムに送信します。送信した情報には実行可能なデータ情報のみが含まれており、いかなる個人情報も含まれません。
5. 自動分析システムは、基本的なファイル情報の分析からプログラムのデジタルシグネチャ、レピュテーションベース分析、ビヘイビア分析、相関分析などのさまざまな分析技術を駆使して、ファイルの安全/マルウェア判定を行います。
6. 分析結果は再度 ASD センターに送信し、データベースをアップデートします。この新規アップデートはすべての ASD ユーザーに配布した後に利用可能になります。



ASD フロー

迅速な対応と効果

ASD は他のセキュリティソリューションとは異なり、未知のマルウェアに対しリアルタイムに対応できます。毎日数十万から数百万人のユーザーからコードサンプルの報告が届き、これらの分析結果はすぐにデータベースに反映されます。
本システムで採用した「Hybrid Analysis System (以下「HAS」)」は、自動ファイル分析技術の導入によりマルウェア分析に要する時間を短縮し、新たに発見されたシグネチャを分析/配布でき、わずかな時間で対応することが可能になりました。
サーバーのデータベースを利用してスピーディにデータファイルを識別することで、従来存在したアップデートサイクルによる時間の浪費を克服して新たな脅威に対応します。
そして、ローカルコンピューター上に個別化されたシグネチャベースを作成するASDの能力は、既知の良性ファイルに対するマルウェア判定に時間を費やしません。
ASD はネットワークトラフィックやネットワークリソースに対する急激な使用の増加を検出した場合、該当するファイルがマルウェアか否かについて判定し、マルウェアによる影響の場合には被害を最小限に抑えるための適切な措置を取ることができます。

DDoS 攻撃が発生した場合、ASD は DDoS 攻撃を効果的に防ぐために、マルウェアの配布経路と他のセキュリティデバイスやファイアウォールへの中継 bot IP 情報を追跡します。

Date	Filename	Size	ASD Detection	Score	ASDP	Count
2010-08-20 10:17:27	maychi.exe	96,256	Backdoor/Win32.Bredolab	100	100	1
2010-08-20 10:14:57	1620040ee1fc903af62debd...	187,904	Trojan/Win32.Hiloti	100	100	
2010-08-20 10:14:55	nabi[1].exe	141,824	Downloader/Win32.Forbid	100	100	8
2010-08-20 10:14:30	zaimpactstrength.exe	766,464	Trojan/Win32.Sadenav	100	100	
2010-08-20 10:13:27	cqldrllkl.exe	768,000	Trojan/Win32.Sadenav	100	100	
2010-08-20 10:11:43	exe.exe	85,504	Trojan/Win32.FakeAV	100	100	
2010-08-20 10:11:40	ddf437b511ec25d4a5e5c56...	98,304	Trojan/Win32.FakeAV	100	100	
2010-08-20 10:11:06	d23dcd17811ea7eae84fc4b...	94,720	Backdoor/Win32.Bredolab	100	100	
2010-08-20 10:10:10	63f74d72e676435b6b22b91...	61,440	Trojan/Win32.FakeAV	100	100	
2010-08-20 10:08:01	CDROM.SYS	84,800	Trojan/Win32.Patched	100	100	1
2010-08-20 10:06:29	sample.exe	35,840	Trojan/Win32.CSon	100	100	
2010-08-20 10:06:04	apr.exe	3,858,432	Dropper/Win32.AdrenaPatched	100	100	3
2010-08-20 10:06:04	kgh.dll	48,012	Trojan/Win32.FraudPack	100	100	
2010-08-20 10:05:38	kgh.dll	48,012	Trojan/Win32.FraudPack	100	100	
2010-08-20 10:05:06	A057RE18.dll	643,584	Trojan/Win32.Overtls	100	100	1
2010-08-20 10:02:10	C_WINDOWS_apsesf.dllx	77,312	Trojan/Win32.Hiloti	100	100	
2010-08-20 10:01:47	C_WINDOWS_system32_a...	20,480	Trojan/Win32.Bredavi	100	100	
2010-08-20 09:59:30	qney.exe	194,048	Trojan/Win32.OnlineGameHack	100	100	1
2010-08-20 09:59:29	14a38041e080a3cf22b6c4c...	96,768	Backdoor/Win32.Bredolab	100	100	
2010-08-20 09:58:01	C_WINDOWS_help.dllx	94,208	Backdoor/Win32.Cindyc	100	100	

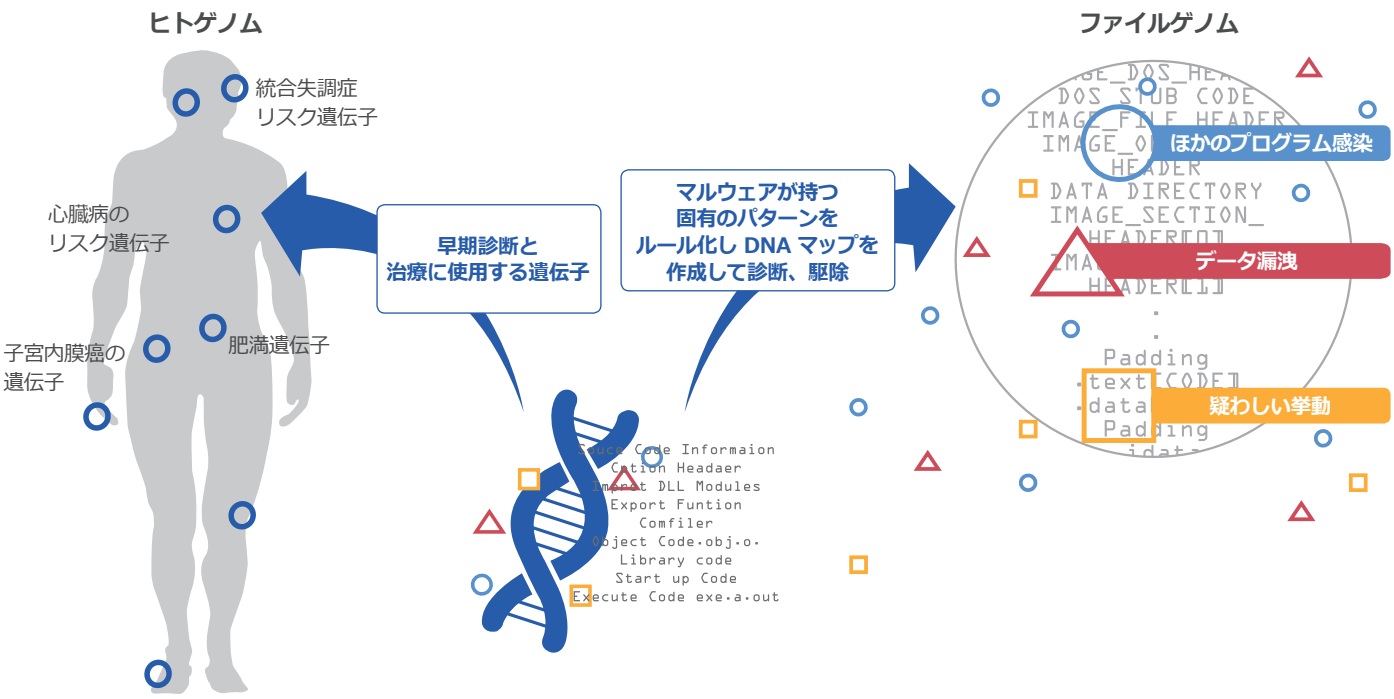
ASD により判定されたマルウェア

マルウェアの DNA を判定する

アンラボが、マルウェアおよび亜種の類似点を分析した結果、すべてのマルウェアにおいて正規ソフトウェアとは異なる固有のデジタル指紋がある事がわかりました。犯罪者に例えると、外見は変装できてもその人間固有の DNA を変えることができないのと同じように、マルウェアには変えることができない識別特性があります。本ソリューションではこれらの特性に注目し、マルウェアを識別するため DNA スキャン技術を採用しました。

DNA スキャンは、ASD データベースに保存された約 5 億個のサンプルと約 2 万個の DNA ルールに基づいて実行されます。抽出した特性に基づき、安全/マルウェアのパターンをルール化するためにDNA マップを作成しました。この方法は、シグネチャベースの検出方法の限界を克服し、ハードウェアリソースを十分活用して偽陽性を最小限に抑えることができます。

DNA スキャンはネットワークに接続できない環境でも活用できるように、サーバーとクライアントの両方のマシンに実装されます。



マルウェアの DNA マップ

より速く、正確なジャッジメント

1対1でファイルマッチングを行う従来の対処方法では、現存数 6 百万といわれているマルウェアをブロックするには 6 百万のシグネチャで対応する必要があります。DNA スキャン方式を採用すると、マルウェアのパターンを識別してルール化することにより 1 つのシグネチャで数千ものマルウェアをブロックできます。シグネチャをアップデートせずに DNA スキャンを単独で適用した場合でも、ARP スプーフィングツールの 90% 以上を検出します。また、パターンのルール化に基づきコードスタイルや使用頻度などを抽出することで、同じ製作者が製作した悪意あるコードをブロックすることも可能です。

DNA スキャン技術は、他の検出方法に比べて偽陽性リスクを低減させた非常に有効で安全な方法です。パターンのルール化は、検出結果の妥当性を確保するため ASD データベースに毎日アップデートされ、3 億以上に及ぶ信頼性の高いファイルとの比較検証を行った後、配布されます。

アンラボでは V3 セキュリティソリューションに DNA スキャンルールを組み込み、国際的なテスト認証機関である Virus Bulletin から偽陽性ゼロの結果を示す「VB 100 Award」を受賞しました。

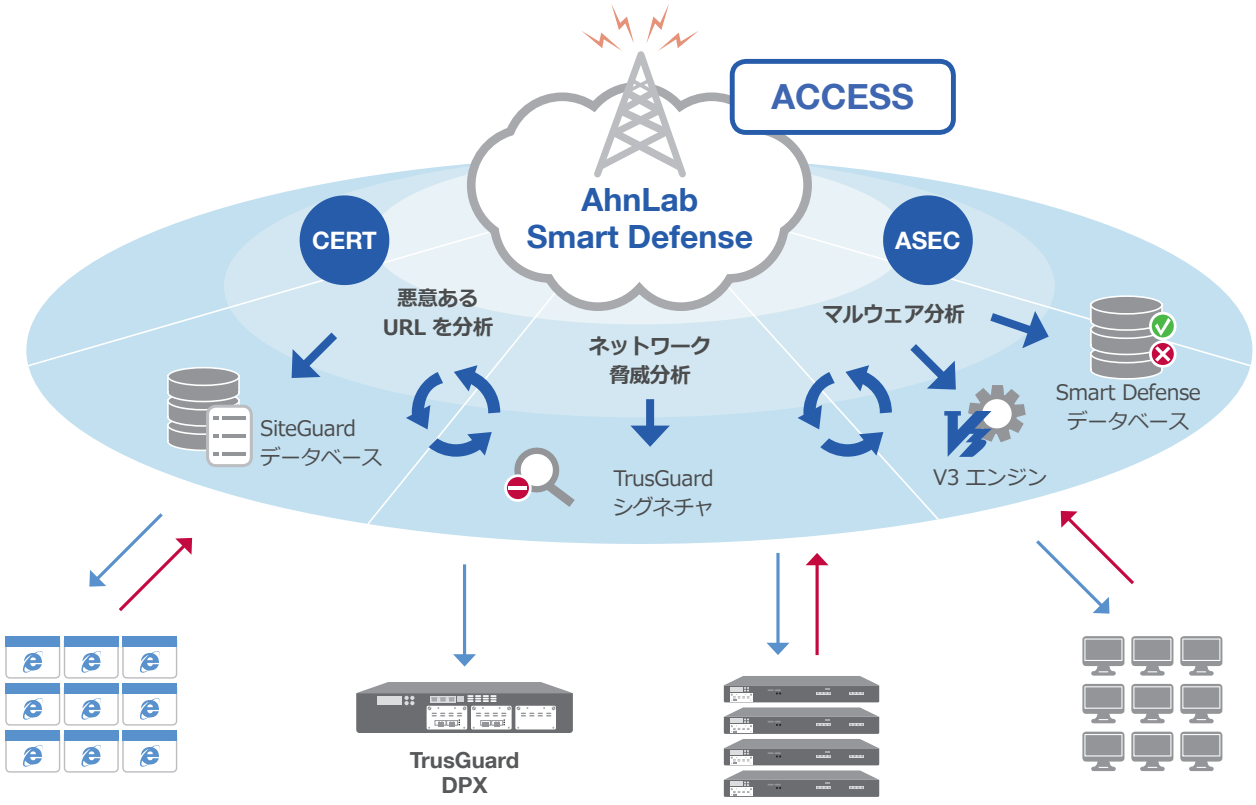
これは DNA スキャンの性能と ASD サーバーに基づくシステムを組み合わせることで実現した成果であり、従来のセキュリティソリューションが有する弱点を克服する結果に繋がっています。

コラボレーションによるシナジー効果

ASD と DNA スキャンは補完関係にあり、ASD はファイルデータを収集してコードが保有する DNA の特性を識別、膨大な数のサンプルを分析しパターンをルール化します。ASD センターに送信されるすべてのデータは分析後、シグネチャをアップデートしてからエンドポイントに配布されます。この循環サイクルからシナジー効果が生まれ、新種のマルウェアにスピーディかつ的確な対応が可能になり、シグネチャ中心であった既存のプログラムアップデートサイクルに存在した限界を克服しました。

ユーザーのコンピューター環境においてネットワーク接続が不安定だったり、インターネットにアクセスできないケースや、ユーザーが厳格なセキュリティポリシー下にいるためファイルの送信が禁止されている等の場合でも、DNA エンジンはコンピューターのローカル環境下でスキャンを実施し、マルウェアを識別することができます。ASDシステムの冗長性は、循環サイクルの変化による影響を最小化しながらリソースを浪費せずにユーザーに最大限の保護を提供します。

この統合型脅威管理プラットフォームは、クラウドベースのアンチマルウェアと専門家による分析能力を組み合わせたもので、ASD はアンラボのクラウドシステム全体で中心的な役割を果たしています。収集したデータを ASEC で精緻に分析し、Computer Emergency Response Team (以下「CERT」) で正確な分析と的確な対策を提示することでセキュリティにおける相乗効果を生み出しています。



AhnLab Cloud Computing E-Security Service (ACCESS)

まとめ

簡単にマルウェアを作成できるオーサリングツールの拡散に伴い、マルウェアやサイバー犯罪の急激な収益増加は経済および社会的に大きな被害を与えています。一部のアナリストは、2003 年 1 月までの攻撃による被害額は 1.55 億万ドル強を記録した一方、2009 年に韓国で発生した DDoS 攻撃の被害額は 5,000 万ドル超になると推測しています。

新規マルウェアの数は爆発的な増加を見せ、もはやこれらの脅威を個別に対処するために必要なシグネチャを作成してテストおよび配布することは不可能といえます。さらにこれらのサイバー攻撃に対して、ピンポイントで対応するセキュリティソリューションではあまり大きな効果は望めない状況です。

ASD は近年の高度化した脅威に対する多角的なソリューションを提供します。データはクラウドに収集され、クライアントコンピューター用にカスタマイズされたシグネチャデータベースを介して効率的なスキャンを実行することで、システムリソースの使用を低減できます。サーバーには、識別したマルウェアに対するシグネチャを迅速に作成するために HAS が搭載されたため、迅速な初動対応と被害の最小化が可能になりました。

そして、本ソリューションは DNA スキャン技術でさらにハイレベルなセキュリティを実現します。300 万以上のサンプルから抽出した特性に基づき、わずかなシグネチャセットを使用して数百万のマルウェアパターンをルール化します。このようなコラボレーション体制によって偽陽性を最小限に抑えると同時に検出率を向上し、効果的なアプローチで増加する脅威に対応します。

アンラボの ASEC と CERT を組み合わせた統合型脅威管理プラットフォームである「AhnLab Cloud Computing E-Security Service (以下「ACCESS」)」の中心に ASD があります。

このソリューションは目まぐるしく変化するお客様のビジネス継続性を確保し、よりセキュアなコンピューター環境を構築するために役立つことでしょう。

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発ベンダです。

1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。

アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

詳細は http://www.ahnlab.co.jp をご覧ください。

AhnLab, Inc.
www.ahnlab.com / global.sales@ahnlab.com / Tel: 1-888-537-4336
673, Sampyeong-dong, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-400, Korea