2023年
7·8月
JULY/AUGUST

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説

キヤノンマーケティングジャパン株式会社

はじめに

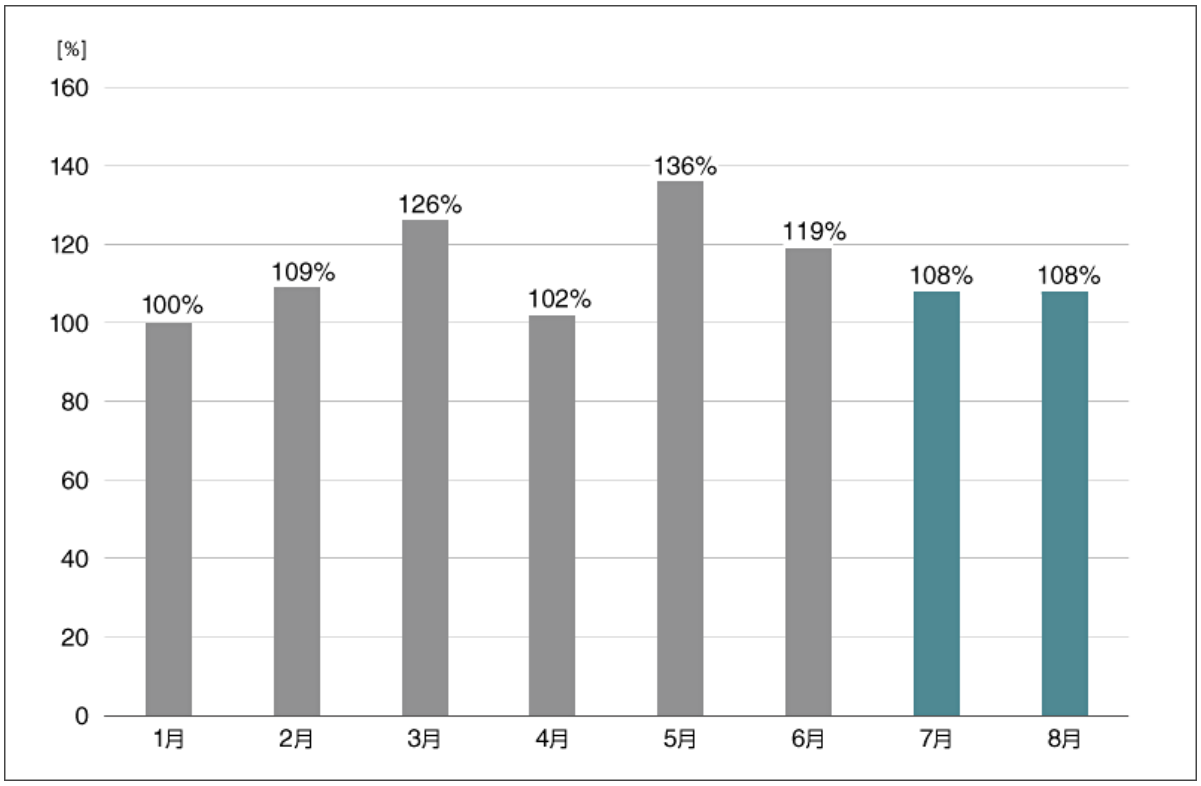
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

2023 年 7 月･8 月マルウェア検出状況

2023 年 7 月（7 月 1 日～7 月 31 日）と 8 月（8 月 1 日～8 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。



国内マルウェア検出数*1の推移
(2023 年 3 月の全検出数を 100%として比較)

*1 検出数には PUA（Potentially Unwanted/Unsafe Application；必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

2023 年 7 月と 8 月の国内マルウェア検出数は、2023 年 6 月と比較して減少しました。検出されたマルウェアの内訳は以下のとおりです。

国内マルウェア検出数[*2] 上位（2023 年 7 月･8 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	34.7%	アドウェア
2	HTML/Phishing.Agent	11.2%	メールに添付された不正な HTML ファイル
3	DOC/Fraud	8.8%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	JS/Adware.TerraClicks	8.2%	アドウェア
5	JS/Adware.Sculinst	3.6%	アドウェア
6	HTML/Fraud	2.3%	詐欺サイトのリンクが埋め込まれた HTML ファイル
7	JS/Agent	2.2%	不正な JavaScript の汎用検出名
8	MSIL/TrojanDownloader.Agent	1.5%	ダウンローダー
9	Win32/Exploit.CVE-2017-11882	1.3%	脆弱性を悪用するマルウェア
10	HTML/Phishing	1.3%	詐欺を目的とした不正な HTML ファイル

国内マルウェア検出数*2 上位（2023 年 7 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	36.2%	アドウェア
2	DOC/Fraud	11.9%	詐欺サイトのリンクが埋め込まれた DOC ファイル
3	HTML/Phishing.Agent	9.5%	メールに添付された不正な HTML ファイル
4	JS/Adware.TerraClicks	7.9%	アドウェア
5	HTML/Fraud	3.2%	詐欺サイトのリンクが埋め込まれた HTML ファイル
6	JS/Adware.Sculinst	2.1%	アドウェア
7	Win32/Exploit.CVE-2017-11882	1.4%	脆弱性を悪用するマルウェア
8	JS/Agent	1.3%	不正な JavaScript の汎用検出名
9	MSIL/TrojanDownloader.Agent	1.0%	ダウンローダー
10	HTML/Phishing	1.0%	詐欺を目的とした不正な HTML ファイル

国内マルウェア検出数*2 上位（2023 年 8 月）

順位	マルウェア	割合	種別
1	JS/Adware.Agent	33.2%	アドウェア
2	HTML/Phishing.Agent	12.8%	メールに添付された不正な HTML ファイル
3	JS/Adware.TerraClicks	8.5%	アドウェア
4	DOC/Fraud	5.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Adware.Sculinst	5.0%	アドウェア
6	JS/Agent	3.2%	不正な JavaScript の汎用検出名
7	MSIL/TrojanDownloader.Agent	2.0%	ダウンローダー
8	HTML/Phishing	1.7%	詐欺を目的とした不正な HTML ファイル
9	HTML/Fraud	1.5%	詐欺サイトのリンクが埋め込まれた

			HTML ファイル
10	Win32/Exploit.CVE-2017-11882	1.3%	脆弱性を悪用するマルウェア

*2 本表には PUA を含めていません。

7 月と 8 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

Web サーバーに対する侵害

2023 年 8 月 1 日に、IPA より「【注意喚起】インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～」[*3]という記事が公開されました。「企業や組織のネットワークとインターネットとの境界に設置されるセキュリティ製品の脆弱性が狙われ、ネットワーク貫通型攻撃として APT 攻撃に利用されている」という趣旨の記事です。攻撃者によるネットワーク内部への侵入を許してしまった場合、バックドアの設置や Web サーバーの改ざんといった被害に遭ってしまいます。
また、サイバーセキュリティラボでは、独自にセキュリティインシデントの情報を収集しています。それによると、2023 年 7 月･8 月にも国内の Web サーバーに対する改ざん被害が複数発生しており、ユーザーのパスワードやクレジットカード情報が窃取されるインシデントも確認されています。

*3 【注意喚起】インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～ | IPA 独立行政法人情報処理推進機構

こうした Web サーバーへの侵害は、Web サイトの画像やテキストの改ざんなど目に見える被害が発生するまで、なかなか気づくことができません。
こうした背景を踏まえ、今月のマルウェアレポートでは、Win32/Chopper を例に Web サーバーに対して設置されるバックドアの実例と対策について紹介します。

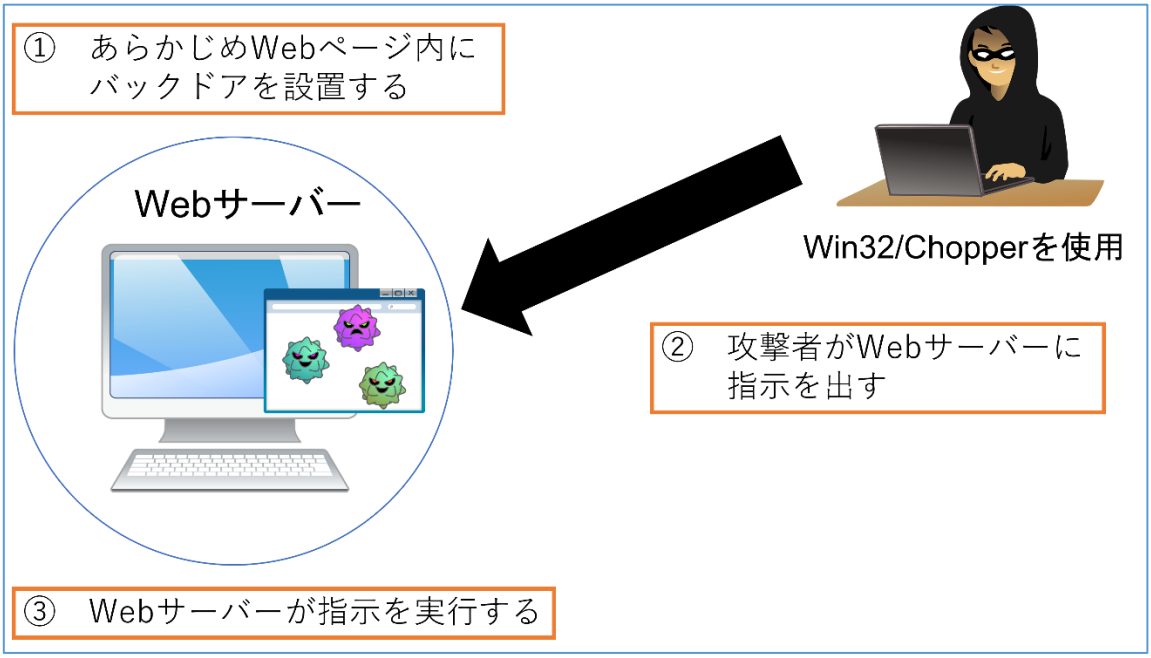
Win32/Chopper の概要

Win32/Chopper は攻撃対象の Web サーバーにあらかじめ設置されたバックドアに対し、さまざまな指令を与えるために使用されるマルウェアです。Win32/Chopper を使用することで、攻撃者は Web サーバーに対する

ファイルのアップロードやダウンロード、システムコマンドの実行を容易に行うことができます。これはつまり、バックドアの設置を許してしまった場合、攻撃者の任意のタイミングで Web ページの改ざんや機密情報の閲覧が可能となってしまうことを意味します。

Win32/Chopper で悪用されるバックドアは、ASP/Webshell.DD など複数の検出名で検出されます。与えられた文字列をプログラムのコードとして評価し実行する eval 関数を用いて、Web サーバー側で任意のコードを実行させる非常にシンプルな仕組みとなっており、Web ページ内に設置されたわずか 1 行のコードがバックドアとして機能します。

攻撃者がバックドアを通じて Web サーバーに指示を出す様子を以下に示します。



攻撃者が Web サーバーに指示を出す様子

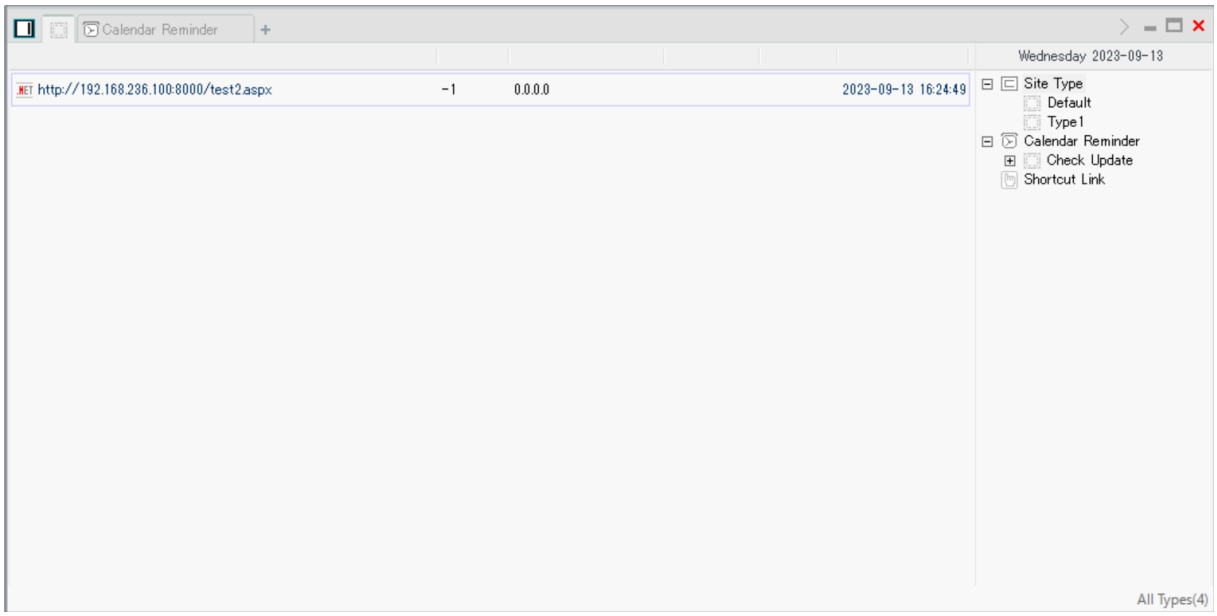
Win32/Chopper は 2012 年ごろから悪用が報告されており、2021 年には大規模な攻撃キャンペーンで使用されたことが確認されています。[*4]

*4 China Chopper Web シェルを使用した Microsoft Exchange Server に対する攻撃の分析 | Palo Alt Networks

Win32/Chopper の動作

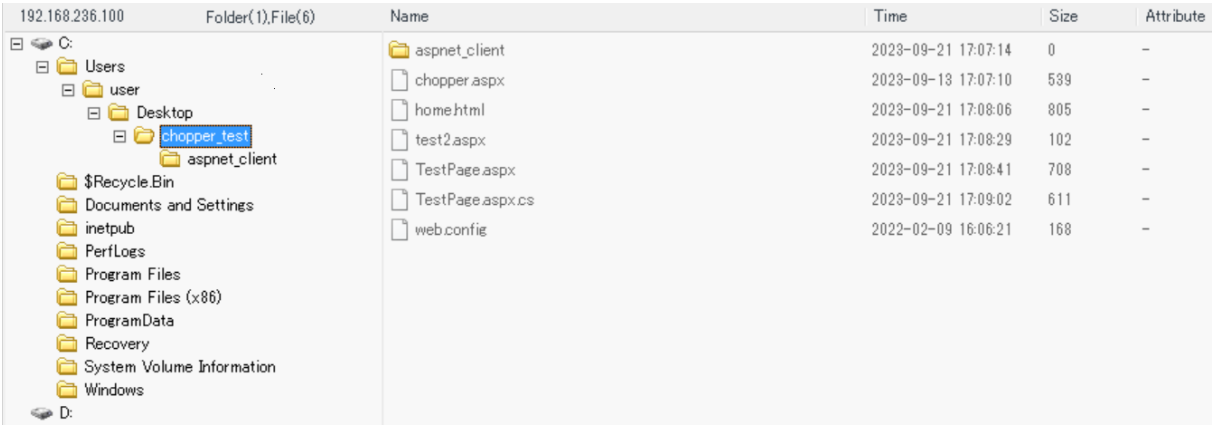
バックドアが設置された Web サーバーに対し、Win32/Chopper がどのように指示を出すのかを解説します。攻撃対象としてテスト用の IIS（Internet Information Services）サーバーを用意し、そのサーバー内にバックドアとして機能する aspx ファイルを設置しました。ネットワーク内の別のパソコンで Win32/Chopper を実行し、テスト用の IIS サーバーに対し指示を送ります。

Win32/Chopper を実行すると以下のような画面が表示されます。この画面から、設定された攻撃対象の Web サーバーを一覧で確認することができます。



Win32/Chopper 実行時の画面

Win32/Chopper の機能をいくつか確認します。
まず、ファイル操作を行う機能です。攻撃対象の Web サーバーを選択し、右クリックで表示されるメニューから「Files Management」を実行すると、以下のような画面が表示されます。

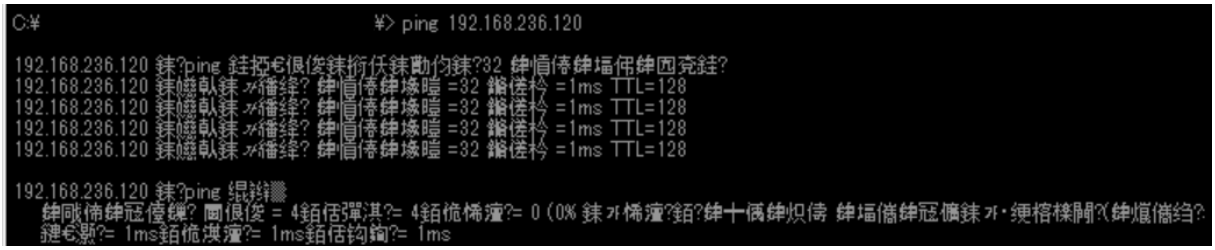


Web サーバーのファイル構造が表示された画面

表示されているのは、Web サーバー内のフォルダーとファイルです。左側にフォルダー構造が表示され、右側に選択したフォルダー内のファイルが表示されています。Web サーバーの権限設定が正しく行われていない場合、以下に示す動作を攻撃者に許してしまう可能性があります。

- インターネットに公開していないファイルの閲覧
- ファイルの改ざん、アップロード、削除

次に、システムコマンドの実行を試します。Win32/Chopper では、攻撃対象の Web サーバーを選択してターミナルを呼び出すことができます。



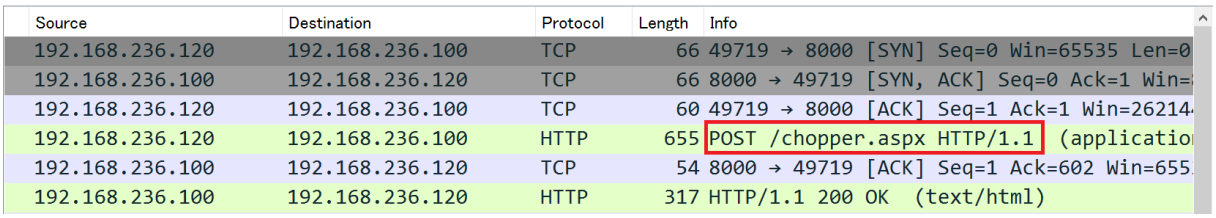
攻撃対象の Web サーバーから ping コマンドを実行する様子

呼び出した Web サーバーのターミナルから ping コマンドを実行する様子を上の画像に示しました。Web サーバーが日本語環境で動作しているためか文字化けしていますが、ping コマンドは正しく実行されていることがわかります。

攻撃者による任意の外部サーバーへの接続など、システムコマンドが実行されることによって発生する可能性のある被害は多岐にわたります。

Win32/Chopper の特徴

Win32/Chopper は Web サーバーに対して操作を行う際に、POST 通信を使用します。



Source	Destination	Protocol	Length	Info
192.168.236.120	192.168.236.100	TCP	66	49719 → 8000 [SYN] Seq=0 Win=65535 Len=0
192.168.236.100	192.168.236.120	TCP	66	8000 → 49719 [SYN, ACK] Seq=0 Ack=1 Win=
192.168.236.120	192.168.236.100	TCP	60	49719 → 8000 [ACK] Seq=1 Ack=1 Win=26214
192.168.236.120	192.168.236.100	HTTP	655	POST /chopper.aspx HTTP/1.1 (applicatio
192.168.236.100	192.168.236.120	TCP	54	8000 → 49719 [ACK] Seq=1 Ack=602 Win=655
192.168.236.100	192.168.236.120	HTTP	317	HTTP/1.1 200 OK (text/html)

バックドアが設置されたページに POST 通信が行われている様子

上の画像は、Win32/Chopper を実行しているパソコン（192.168.236.120）から Web サーバー（192.168.236.100）に対して操作を行う様子を WireShark で確認したものです。赤枠で示したように、バックドアが設置されたページに対して POST 通信が行われています。

```
Secret=Response.Write("->|");var
err:Exception;try{eval(System.Text.Encoding.GetEncoding(936).G
etString(System.Convert.FromBase64String("dmFyIGM9bmV3IFN5c3Rl
bS5EaWFnbm9zdGljcy5Qcm9jZXNzU3RhcnRJbmZvKFN5c3RlbS5UZXh0LkVuY2
9kaW5nLkdldEVuY29kaW5nKDkzNikuR2V0U3RyaW5nKFN5c3RlbS5Db252ZXJ0
LkZyb21CYXNlNjRTdHJpbmcoUmVxdWVzdC5JdGVtWyJ6MSJdKSkpO3ZhciBlPW
5ldyBTeXN0ZW0uRGlhZ25vc3RpY3MuUHJvY2VzcygpO3ZhciBvdXQ6U3lzdGVt
LklPLlN0cmVhbVJlYWRlcixFSTpTeXN0ZW0uSU8uU3RyZWFtUmVhZGVyO2MuVX
NlU2hlbGxFeGVjdXRlPWZhbHNlO2MuUmVkaXJlY3RTdGFuZGFyZE91dHB1dD10
cnVlO2MuUmVkaXJlY3RTdGFuZGFyZEVycm9yPXRydWU7ZS5TdGFydEluZm89Yz
tjLkFyZ3VtZW50cz0iL2MgIitTeXN0ZW0uVGV4dC5FbmNvZGluZy5HZXRFbmNv
ZGluZyg5MzYpLkdldFN0cmluZyhTeXN0ZW0uQ29udmVydC5Gcm9tQmFzZTY0U3
RyaW5nKFJlcXVlc3QuSXRlbVsiejIiXSkpO2UuU3RhcnQoKTtvdXQ9ZS5TdGFu
ZGFyZE91dHB1dDtFST1lLlN0YW5kYXJkRXJyb3I7ZS5DbG9zZSgpO1Jlc3Bvbn
NlLldyaXRlKG91dC5SZWFkVG9FbmQoKStFSS5SZWFkVG9FbmQoKSk7")),"uns
afe");}catch(err){Response.Write("ERROR:// "%2Berr.message);}
```

Win32/Chopper が送る POST 通信

Win32/Chopper が送る POST 通信の中身の一部を上に示しました。この通信では、Web サーバーで netstat コマンドを実行させ、TCP コネクションの状態を表示させています。Web サーバーに対する命令は Base64 形式でエンコードされており、内容を読むためにはデコードする必要があります。
POST 通信は Win32/Chopper が操作を行うたびに発生するため、上記のように Base64 形式でエンコードされた不審な POST 通信が Web サーバーに対して複数回行われていた場合、バックドアの存在を疑う必要があります。

バックドアによる被害を受けないために

Win32/Chopper などバックドアを利用するマルウェアによる被害を受けないために何より大切なことは、バックドアを設置させないことです。攻撃者はサーバーに侵入する際に、機器やソフトウェアの脆弱性を悪用したり、無害を装ったファイルを実行させたりします。ネットワークや各種ソフトウェア、機器のログをチェックし、異常を検知できる体制を整えてください。
また、既知のバックドアの多くは、セキュリティソフトによって検知されます。Web サーバーのセキュリティソフトは常に最新を保つようにしてください。仮にバックドアの設置を許してしまったとしても、被害が発生する前にバックドアを削除できる可能性があります。

これらの対策を実施しても、バックドアが設置されてしまうことがあります。そうした場合の被害を最小にするために、以下のような対策も必要です。

- Web サーバー内のファイルに対するアクセス権限を正しく設定する
- Web サーバー内のファイルが改ざんされていないか定期的にチェックする
- 使用している機器、ソフトウェアの脆弱性情報を収集する

Web サーバー内のファイルに対するアクセスを制限することで、ファイルの改ざんを防ぎ、被害の範囲を抑えることができます。
また、バックドアの存在に早期に気づくために、定期的なファイルのチェックや使用している機器、ソフトウェアの脆弱性情報の収集を行ってください。例えば、今回紹介した Win32/Chopper は POST 通信が多数発生するという特徴があります。そうした個々の動作の特徴を把握することで、見逃してしまいがちな痕跡に気づくことができます。

まとめ

今月のマルウェアレポートでは、Web サーバーに設置されるバックドアの実例と対策について紹介しました。Web サーバーに対して設置されたバックドアの存在には、なかなか気づくことができません。セキュリティソフトなどで侵入を防いだ上で、万が一侵入されてしまった場合の対策も用意しておくことが大切です。本記事の対策の項も参考に、今一度 Web サーバーのセキュリティについて見直してみてください。

■常日頃からリスク軽減するための対策について
各記事でご案内しているようなリスク軽減の対策をご案内いたします。下記の対策を実施してください。

1．セキュリティ製品の適切な利用

1-1. ESET 製品の検出エンジン（ウイルス定義データベース）をアップデートする

ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しています。最新の脅威に対応できるよう、検出エンジン（ウイルス定義データベース）を最新の状態にアップデートしてください。

1-2. 複数の層で守る

1 つの対策に頼りすぎることなく、エンドポイントやゲートウェイなど複数の層で守ることが重要です。

2．脆弱性への対応

2-1. セキュリティパッチを適用する

マルウェアの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。「Windows Update」などの OS のアップデートを行ってください。また、マルウェアの多くが狙う「脆弱性」は、Office 製品、Adobe Reader などのアプリケーションにも含まれています。各種アプリケーションのアップデートを行ってください。

2-2. 脆弱性診断を活用する

より強固なセキュリティを実現するためにも、脆弱性診断製品やサービスを活用していきましょう。

3．セキュリティ教育と体制構築

3-1. 脅威が存在することを知る

「セキュリティ上の最大のリスクは“人”だ」とも言われています。知らないことに対して備えることができる人は多くありませんが、知っていることには多くの人が「危険だ」と気づくことができます。

3-2. インシデント発生時の対応を明確化する

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

4．情報収集と情報共有

4-1. 情報収集

最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社を始め、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。

4-2. 情報共有

同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられます。同じ攻撃者グループの場合、同じマルウェアや戦略が使われる可能性が高いと考えられます。分野ごとの ISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。

※ESET は、ESET, spol. s r.o.の登録商標です。Microsoft、Windows および Win32 は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

引用・出典元

■【注意喚起】インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～ | IPA 独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html
■China Chopper Web シェルを使用した Microsoft Exchange Server に対する攻撃の分析 | Palo Alt Networks
https://unit42.paloaltonetworks.jp/china-chopper-webshell/

Canon

キヤノンマーケティングジャパン株式会社