PRESS RELEASE

2017 年 11 月 17 日

報道関係者各位

デジタルアーツ株式会社

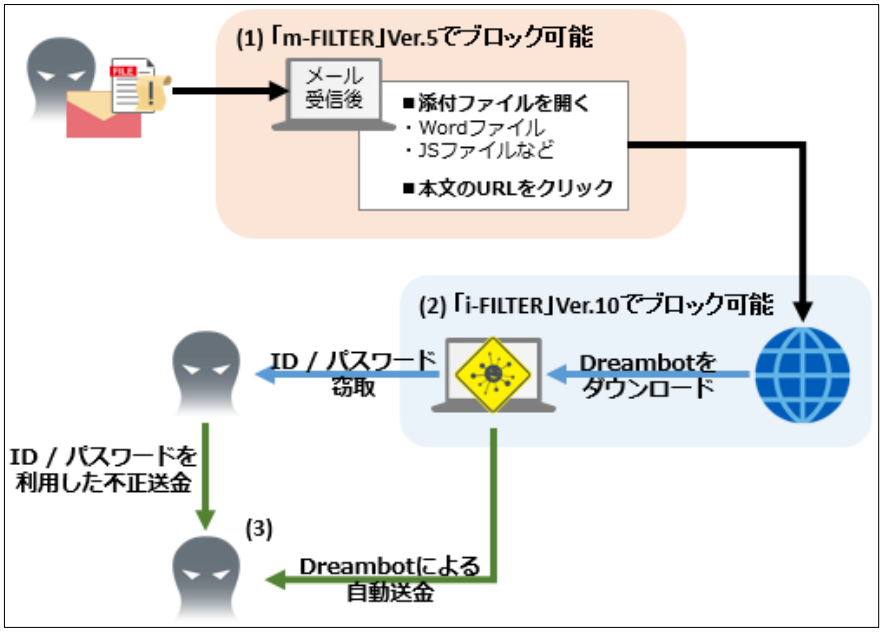
デジタルアーツの標的型攻撃対策ソリューションで バンキングマルウェアのブロックを確認

～最新版「i-FILTER」「m-FILTER」の連携ソリューションが 「Ursnif」「Dreambot」など入手した複数検体をブロック～

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下デジタルアーツ、証券コード 2326）は、2017 年 9 月に提供開始した企業・官公庁向け Web セキュリティソフト「i-FILTER」Ver.10 とメールセキュリティソフト「m-FILTER」Ver.5 の連携による標的型攻撃対策ソリューションにおいて、不正送金を目的としたインターネットバンキングを攻撃するマルウェア「Ursnif」「Dreambot」などのブロックが確認できたことを発表いたします。

2017 年初頭から銀行やクレジットカードの ID やパスワードの情報を盗むトロイの木馬の亜種のマルウェア「Ursnif」「Dreambot」が、日本でも確認され、2017 年 9 月以降再び活発化しており、2017 年 10 月の時点で多くの被害が報告されております。特に日本国内における被害額が 5 億円※1 を超えるという警察庁の報告があり、被害が多くなっているためマルウェアの感染拡大について日本サイバー犯罪対策センター(JC3)でも注意喚起情報※2 が公開されています。

デジタルアーツが提供する「i-FILTER」Ver.10 と「m-FILTER」Ver.5 を連携して使用いただくことで、「Ursnif」「Dreambot」などの入手した検体と同一のマルウェア※3 で検証した結果、ブロックが可能なことが実証されました。



(1) Dreambot をダウンロードするマクロを含んだ Office 文書、URL 等をメールで送信
⇒「m-FILTER」Ver.5 でブロック可能

(2) 添付ファイルを開く、本文の URL をクリックするなどで「Dreambot」をダウンロードし感染する
⇒「i-FILTER」Ver.10 でブロック可能

(3) 感染後は C&C サーバーと「Tor」を利用した指令により遠隔操作され「ID / パスワード」の窃取や自動送金が実施される

感染手法と「i-FILTER」Ver.10 / 「m-FILTER」Ver.5 でブロックできる範囲（例：「Dreambot」の場合）

【検証方法】：デジタルアーツで入手できたバンキングマルウェア「Ursnif」「Dreambot」自体をダウンロードする一時検体を含むメールを「m-FILTER」Ver.5 経由で受信し、さらに一時検体を起動し「Ursnif」「Dreambot」自体のダウンロードを「i-FILTER」Ver.10 経由で実施。

2017 年 9 月 19 日にリリースした Web セキュリティソフト「i-FILTER」Ver.10 とメールセキュリティソフト「m-FILTER」Ver.5 の連携による標的型攻撃対策ソリューションでは、まず「m-FILTER」が「Dreambot」感染手口の初段である「感染手法(1)」の時点でメール自体または添付ファイルのみが隔離されることが確認できました。

また、「i-FILTER」Ver.10 ではメールに添付されていたマクロやスクリプトによる「Dreambot」自体のダウンロード通信である「感染手法(2)」の時点でブロックされることも確認できました。

デジタルアーツでは、今後も引き続き各種マルウェアの検体を入手し、「i-FILTER」Ver.10 と「m-FILTER」Ver.5 との連携を通じて、複雑化する外部からの攻撃に対応した機能強化を実施してまいります。

■検証環境

・「i-FILTER」Ver.10.00R01(2017 年 9 月 19 日配信時のデータベース)
・「m-FILTER」Ver.5.00R01

■検証検体(メール)数とブロック率

33 通のメールにおいて 100%ブロック

■検証検体の SHA-256 値

9b25ec429a8451ad27fb7cf7258c24eb269a260d0b8cce7e3abc32f8c72de5c4	b0b052f2baa8666eb3c9acbbcb099a5ef721cd5f0b6893cd9ee8cb45196c50c0
608ea0663b4bc164982750d3ac32604b0848176fe12a3335998038a5f2926402	0b151717ee56bd00ca5df14dcf1a553e135b9ccb775c90e3af85fe103cd196ce
ecb7563f9679c79922257e285f54246685c6ed1b5e88e6ff88bdec00c900f0eb	4d8fb496bc5fe1e8f50d407be701ed3d674817c22bcfdbf0f894c434406ce7b7
a82024fbe5d6be2049d9d36c050202cac59078808f531d161419fee46cdab017	d39f7f6fee07130919ebb5fa1986d2faf827b03cb12dc4c28e9d8c7498c29f9c
0634216b34baf0fdc2930026329323122 93fc4854701b143c6f4735e8cd98b45	204ecc72a94c1d1ef60a08ccb132a5123d2e8dcfc16ef1cacebb20887049ec2d
6722d8e3ed437c700f7a76f29c089d500405993866043586e43572c43c66dfd4	dc6c17d5fdd67acfd28c08dfa6fef6c41938162e0c86a9bdd9a6f3296242e8d7
ed56f2032ac9f18663a453276e29ec1c9522e3d4fe9fa172286e0ab37828ba56	9d38f3405f9fae4f29db1b4d084631c21639efb9738f454a6e3acf9d26c6bc82
784dca5b402c493126ddf4488bc482ee579292f219fe7d8e20ec95b6379dea1b	ccfb8b3ad671111ebe79a217b0cf5b5da9f4018f4c59d8d6d81a7e6cd5a5f176
4596491155a1b31c3bf498e44589aaf8a84179723fc12f388977c36b70afd82c	5a1f0bf7e5f97afab02a3a573a6ddc75b2a7cf79b5ba084f47f516cd661d8a51
59727ea201d94d471bdbb353b1281cca3c5bebf5305b140a3c017e52a37be702	cb50848b4b11aec14b3fda4720d19a1b932d88bf247a1a11474bff5bb66f87b1
64ae13592c5d8b289be81ebb50e054cef49b0bdf50ea92dd44ed611dd274150f	dc3383e9faeb68e68425333d41aeb28b2883b30bde92068bdb55cdd05f9e0ecd
60834d0c9d0602ef18cd65289b0b0fab05bbdb512acd3af0b273b6414883f60e	9565ba41a3f056f6a9a5de8a489a696a98d79bc410b6b3b41227eb84941c92cb
9bdc25ce5e92a5b97969b03073d7e15370bac3a57651cb903a8924ee2e631dcd	50a5f5883000deb6f3fc0486c52b8398eabf9fa456a8867d7759a16f1c527d23
92cd557d10a247ab5b8417c91f12633c2628680464b5008415b97d3f8f906430	e865b9e06dcf244e2570474f25cd41f7a3ca286ec7a672f959042463fe7e70d3
65f7bb9bd290bce00b4ac777281b060be7001bd8f25ebc9200e5074dbaaab669	b31ea83885a69d1c014c4dd0d850a6446fcb4ab989ff3756a93ac92ec170563e
3ccd93419b0e167044da69a9db5dabd4feefd32adf049040a2eaa045d9190dee	3f415553b7b22919c75f733c3403aa6f4396d8d62d1178e9b3a4ba54ac53300e
a2602b9c94a2bdbcac75b95d4430d4cda3a79986c016ac2ef2211afb00420f24	

※1 出典: 警察庁 平成 29 年上半期におけるサイバー空間をめぐる脅威の情勢等について
(https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf)
※2 出典: インターネットバンキングマルウェア「Dreambot」による被害に注意(https://www.jc3.or.jp/topics/dreambot.html)
※3 バンキングマルウェア含むマルウェアには多くの亜種が存在します。今回のブロックまたは隔離はその全てに対しブロックまたは隔離できることを保証するものではありません。

PRESS RELEASE

■ 「i-FILTER」ついて　http://www.daj.jp/bs/ifmf/i-filter/

「i-FILTER」は、標的型攻撃を始めとした外部からの攻撃対策と、組織内部からの情報漏洩対策の両方を 1 つの製品で実現する、プロキシ型の Web セキュリティソフトです。国内における Web フィルタリングソフトのベンダー別売上金額シェア（2015 年度）において No.1 を獲得しました（2016 年 6 月 株式会社アイ・ティ・アール発行「ITR Market View：サイバー・セキュリティ対策市場 2016」）。業界最大級の Web フィルタリングデータベースで、未登録の URL を悪性 URL として Web 経由の標的型攻撃をブロックする安全な web の世界を実現します。また、同データベースを利用して業務中の閲覧が不適切な Web サイトのアクセスブロックや、Web メールの利用や掲示板の書き込みなどといった、Web 経由の情報漏洩も防ぐとともに、その内容を記録・確認・保存することが可能なため、内部統制対策としても有効なソリューションです。

■ 「m-FILTER」ついて　http://www.daj.jp/bs/ifmf/m-filter/

「m-FILTER」は、電子メールによる情報漏洩・監査要求・年々増加するスパムメール・標的型攻撃メールといった課題を 1 つの製品で対応できる、企業・官公庁・自治体様向けのゲートウェイ型電子メールセキュリティソフトです。

「m-FILTER」では、外部からの標的型メール攻撃対策機能や、内部からの情報漏洩対策機能を標準で実現する「m-FILTER MailFilter」、リアルタイムに添付ファイルを含めたメールを保存し、高速検索で運用負荷を軽減する「m-FILTER Archive」、業界最高水準の検知率である Cloudmark 社スパムエンジンによりスパムメールを徹底排除する「m-FILTER Anti-Spam」の 3 つの機能を提供します。これらの 3 つの機能から解決したい課題に合わせ機能を選択し、お客様のニーズに合わせた組み合わせで導入いただくことも、3 つの機能全てを導入いただくことも可能です。

■ デジタルアーツについて　http://www.daj.jp

デジタルアーツは、フィルタリング技術を核に、情報セキュリティ事業を展開する企業です。製品の企画・開発・販売・サポートまでを一貫して行い、国産初の Web フィルタリングソフトを市場に出したメーカーならではの付加価値を提供しています。また、フィルタリング製品の根幹を支える国内最大級の Web フィルタリングデータベースと、世界 27 の国と地域で特許を取得した技術力が高く評価されています。国内でトップシェアを誇る Web フィルタリングソフトとして、家庭及び個人向け「i-フィルター」・企業向け「i-FILTER」「i-FILTER ブラウザー＆クラウド」を提供する他、企業向けとしてゲートウェイ型電子メールセキュリティソフト「m-FILTER」、クライアント型電子メール誤送信防止ソフト「m-FILTER MailAdviser」、セキュア・プロキシ・アプライアンス製品「D-SPA」、ファイル暗号化・追跡ソリューション「FinalCode」を提供しています。