JPAAWG | JAPAN ANTI-ABUSE WORKING GROUP

メールの不正利用手法と脆弱性の解説

JPAAWG若手メールエンジニア向けメールセキュリティトレーニング

Messaging Research Institute (MRI) / JPAAWG / IAjapan / UEC

SAKURABA Shuji, Ph.D.

About Me

- 櫻庭 秀次（SAKURABA Shuji），博士（工学）
- 活動概要
  - (一社)メッセージング研究所 理事長
  - (一財)インターネット協会 迷惑メール対策委員会 委員長，客員研究員
  - 迷惑メール対策推進協議会 座長代理，技術 WG 主査
  - M^{3}AAWG (Messaging, Malware, and Mobile Anti-Abuse Working Group) 創設時からのメンバ
  - JPAAWG (Japan Anti-Abuse Working Group) 会長
  - 国立大学法人電気通信大学 協力研究員

IA japan　JP AAWG　M^{3}AAWG MESSAGING MALWARE MOBILE

Agenda

- EchoSpoofing
- BreakSPF
- HADES Attack
- You’ve Got Report

時間の範囲内でお話しさせていただきます…

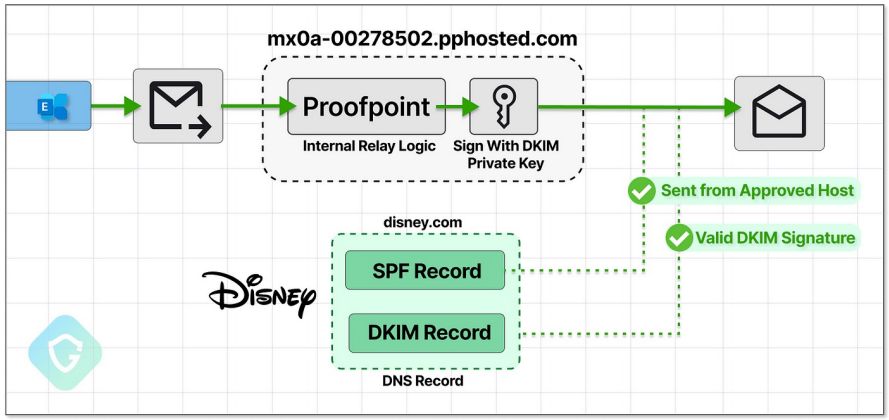
EchoSpoofing

- 出典
  - *“EchoSpoofing” - A Massive Phishing Campaign Exploiting Proofpoint’s Email Protection to Dispatch Millions of Perfectly Spoofed Emails* (2024.07.24, Nati Tal, Head of Guardio Labs)
  - https://labs.guard.io/echospoofing-a-massive-phishing-campaign-exploiting-proofpoints-email-protection-to-dispatch-3dd6b5417db6
- 概要
  - SPF, DKIM に対応した詐称メールが送信可能な手法 (現在は対策済み)
  - 対象となったのは，メール送信に Microsoft 365 と Proofpoint の組み合わせで利用しているドメイン (ex. Disney, IBM, Nike, Best-Buy, Coca-Cola, etc)
  - いわゆるメールの共有型 gateway サービスを提供し，送信時の最終段 (DKIM 署名機能など) を担う場合に同様の課題が発生する可能性がある

EchoSpoofing

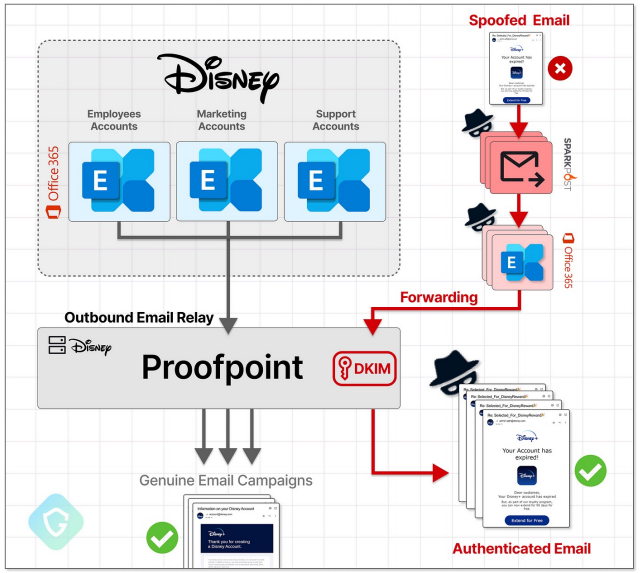
- 状況
  - 有名企業やブランドを完全に偽装したフィッシングメールを何百万通も送信可能
  - SPF レコードに設定されている認証済みサーバから送信 (SPF pass)
  - 当該ブランドのみが所有する正規の鍵で DKIM 署名 (DKIM pass)
  - 受信側 (ex. Gmail) でも正しく認証されていた
- 詐称メールの配送経路

  仮想サーバ (SMTP server) →
  Office 365 Online Exchange →
  Proofpoint (DKIM署名, SPF 対象)
  → ターゲット



EchoSpoofing

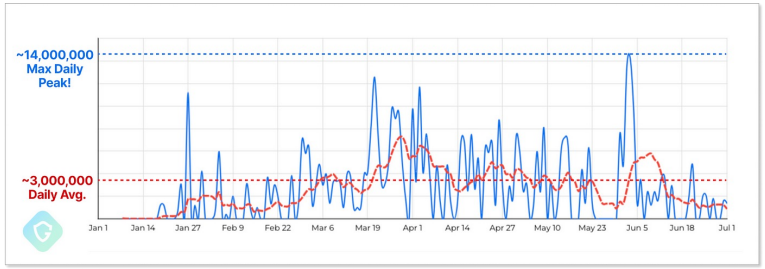
- 詐称手法
  - 通常のアカウントからは RFC5322.From は変更できない
  - ただしリレーサーバ (Exchange?) は SMTP でそのまま受け付ける (らしい)
  - Proofpoint の送信サーバは Email Mail Flow 機能で指定されたサーバからのみ受け付ける (MS, Google は 1click で OK)
  - Proofpoint は顧客毎に outbound の接続先が決まっているが，inbound の受信先 MX レコードをみれば識別できるようになっている (らしい)
  - M365 を契約し，outbound の connector 機能を使って，詐称対象の Proofpoint の接続先 (MXから判断) を指定
    → なりすましメール送信




```
; ANSWER SECTION:
disney.com. 2987 IN MX 10 mxb-00278502.gslb.pphosted.com.
disney.com. 2987 IN MX 10 mxa-00278502.gslb.pphosted.com.
```

EchoSpoofing

- 詐称状況
  - 2024.01 あたりから活動が行われ，準備 (サーバ，ドメイン，O365アカウント) はその 2ヶ月前から実施
  - 観測では詐称メール送信は平均 300万通/日, 最大 1,400万通/日



- 対応と対策
  - 2024.05 これを発見した Guardio 社は Proofpoint 社 (2024.03 あたりに状況は把握していたと主張) に連絡をし，共同対応を開始
  - Microsoft 社がリレーサーバを含む全ての送信メールに付加する，顧客を示すヘッダ情報 (X-OriginatorOrg) を利用し，許可された顧客以外のメールを Proofpoint が受け付けないよう修正

EchoSpoofing

- コメント
  - ゲートウェイ型サービスにおける outbound の顧客毎の処理は難しい
  - 通常宛先 (RFC532{1,2}.To) に対応する処理をするのが MTA (inbound)
  - Outbound における顧客は送信者 (RFC532{1,2}.From) であるが，メールにおいては本来信用できない情報
  - 別途信頼できる情報に基づいた判断および処理が必要となる (SMTP-AUTHの認証 ID, 送信元 IP アドレス，など) のが outbound 方向

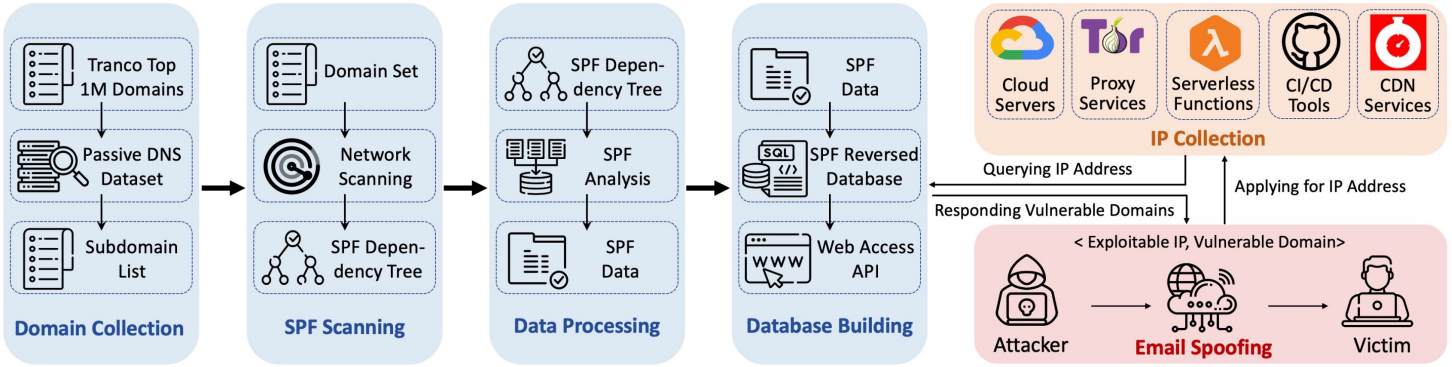
BreakSPF

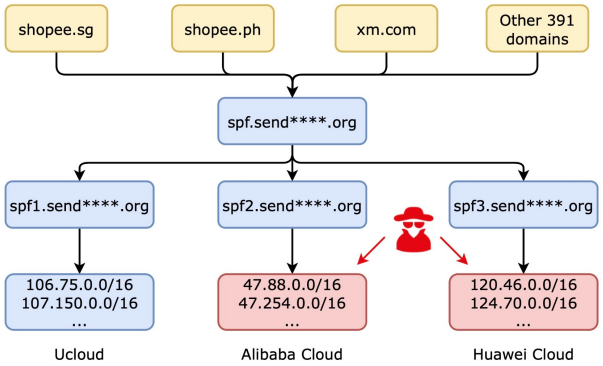
- 出典
  - *BreakSPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet* (NDSS* 2024, 所属: Tsinghua University, Zhongguancun Lab., Quan Cheng Lab., Coremail Tech.)
- 概要
  - SPF 検証を pass してなりすましメールを送信する手法 = BreakSPF
  - 共有 IP pool を利用する cloud service, proxies, CDNs を利用
  - 人気ドメインランキング (Tranco) の上位100万ドメインのうち 23,916 ドメインがこの手法に対して脆弱であった (との報告)

* Network and Distributed System Security Symposium (ISOC)

BreakSPF

- 手順
  1. ドメイン名の収集 (人気ドメイン，passive DNS からの情報)
  2. SPF レコードの収集と依存関係 (include, redirect) の分析
  3. SPF dependency tree を解析し逆から辿れるようにする
  4. IP アドレスから SPF ドメイン名を辿れるようにデータベースを構築





BreakSPF

- SPF ドメインの調査
  - Tranco top million domains が対象
  - SPF レコードの 8.4% が文法エラー
  - 51.7% が 2^{16} 以上のネットワーク幅

TABLE I. SPF ADOPTION RATE AMONG TRANCO TOP 1 MILLION DOMAINS.

Status	Top1M Domains # (%)	Email Domains[1] # (%)
Total domains	1000000 (100.0 %)	738310 (100.0 %)
w/ SPF	609,236 (60.92 %)	586,316 (79.41 %)
w/ valid SPF	559,296 (55.93 %)	536,976 (72.73 %)
Soft Fail	311,277 (31.13 %)	305,326 (41.35 %)
Hard Fail	205,181 (20.52 %)	189,984 (25.73 %)
Neutral	25,997 (2.60 %)	25,266 (3.42 %)
Pass	742 (0.07 %)	670 (0.09 %)
w/ Include	417,144 (41.71 %)	410,899 (55.65 %)
w/ Redirect	13,737 (1.37 %)	13,520 (1.83 %)

[1] Email domains refer to domains configured with email services, including domains configured with MX records and domains that provide email services on port 25 at their A records.

TABLE II. ANALYSIS OF SPF MISCONFIGURATION.

Misconfiguration Type	# Domain	%
Too Many DNS Lookups	32,254	63.15%
Double SPF Records	15,700	30.74%
Format Errors	2,838	5.56%
Spelling Errors	986	1.93%
Coexisting `all` and `redirect`	612	1.20%
Total	51,076	100.00%

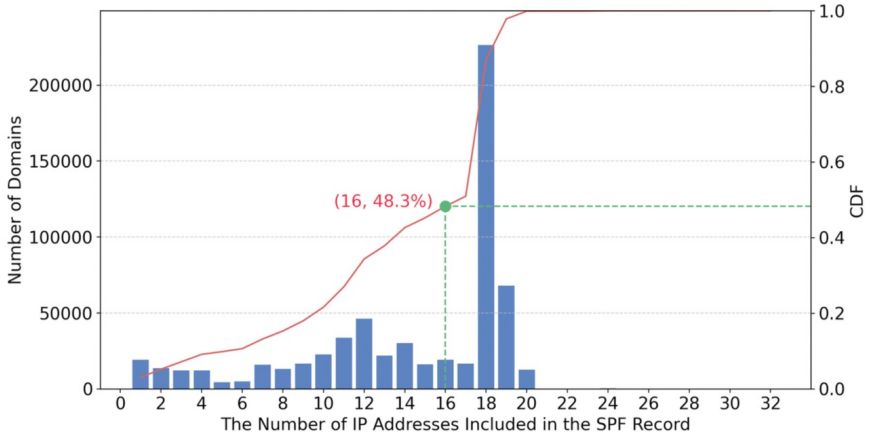


Fig. 7. IP Coverage Analysis of SPF Records. The x-axis represents the number of IP addresses included in the SPF records, calculated with the log_2^{number} function. For example, 51.7% of domains have SPF records that contain more than 65,536 (2^{16}) IP addresses.

送信ドメイン認証関連レコードの間違い

- DMARC
  - JP ドメイン名の DMARC レコードで policy 設定が間違っているドメイン名の割合: 0.06%
    - 区切りは “;” だがカンマ “,” や空白 “ ” で区切る
    - “p” は小文字だが “P=“ (大文字) となっている
    - 値が違う(1): None, Quarantine, Reject
    - 値が違う(2): nome, non, XXXX
    - 値が違う(3): qarantine, quarantin, quaratine, quatantine
- SPF
  - JP ドメイン名の SPF レコードで pemerror となるドメイン名の割合: 1.70%

JPAAWG 7th General Meeting より

SPFレコードの設定間違い

- SPFレコードが複数 (31.2%)
  - 複数の SPF レコードが設定されていた場合 permerror となる (RFC7208#4.5)
- include 対象のドメイン名にSPFレコードが存在しない (20.1%)
  - 再帰的なレコード評価で none となれば permerror (RFC7208#5.2)
- DNS の lookup 回数超過 (18.5%)
  - DNS に過度の負荷がかからないように制限されている (RFC7204#4.6.4)
- mechanism の間違い (9.2%)
  - 多くは typo が原因
  - 区切り (空白) が無いことで前後が密着

JPAAWG 7th General Meeting より

BreakSPF

- 分析結果
  - 23,916 のドメイン名に影響を与える可能性がある
  - そのうちTranco Top 1,000ドメイン中 23ドメインが含まれている
  - Tranco Top 10,000 ドメインでは 1,653 ドメインが含まれている
  - 影響を与えているドメイン: 表 VI
  - SPFの集約化 (というよりサービスの) により一つのIPが数千のドメイン名に影響を与える可能性があることがわかった
  - 場合によっては 1 IP で1万以上のドメイン名に影響を与えるものがあることが判明

TABLE VI. TOP 10 WELL-KNOWN DOMAINS INFLUENCED BY BYPASSSPF ATTACK.

Domain	Rank	IP	Source
microsoft.com	5	20.*.*.30	CI/CD Platforms
qq.com	11	114.*.*.86	Cloud Servers
csdn.net	76	114.*.*.86	Cloud Servers
huanqiu.com	110	114.*.*.86	Cloud Servers
godaddy.com	142	72.*.*.69	Tor
rednet.cn	306	114.*.*.86	Cloud Servers
mama.cn	311	114.*.*.86	Cloud Servers
zhihu.com	420	114.*.*.86	Cloud Servers
ieee.org	523	201.*.*.173	RESIP
ucla.edu	610	131.*.*.85	VPN

BreakSPF

TABLE IV. OVERVIEW OF THE BREAK SPF EXPERIMENT.

Services		IP Obtained	Unique IPs	Successful Hit	IP diversity				Port	
					/8	/16	/24	ASN	25	465
Cloud Servers	Alibaba	1,028	909	887	19	55	721	2	◑	●
	Amazon	9,680	9,679	8,788	21	449	7,304	2	◑	●
	Azure	33,580	30,498	6,255	22	376	10,998	1	◑	●
	Digitalocean	987	976	967	34	55	822	1	●	●
	Google	1,036	216	216	7	88	215	1	◑	●
	Linode	1,017	989	977	28	45	426	1	●	●
	Tencent	1,009	996	944	25	65	730	2	◑	●
	Vultr	307	282	277	31	46	232	1	◑	●
Proxy Services	VPN	389	339	309	102	282	306	101	◑	●
	Open Proxy	68,653	3,061	13,704	189	1,811	2,713	1,985	●	●
	RESIP	30,000	23,876	22,468	193	8,063	16,533	2,851	●	●
	Tor	1,213	1,208	1,068	108	378	592	238	◑	◑
Serverless Function	Alibaba	3,269	39	33	4	13	33	2	●	●
	Amazon	100	3	1	2	3	3	1	●	●
	Azure	1,879	13	0	1	3	4	1	●	●
	Baidu	60	3	3	2	2	3	1	●	●
	Google	46	4	4	2	2	4	1	●	●
	Huawei	234	6	6	5	5	6	3	●	●
	Tencent	7,398	62	32	8	9	38	2	●	●
CI/CD Platforms	Circleci	4,446	377	329	13	147	372	1	●	●
	Github	5,000	3,648	1,388	14	148	2,578	1	●	●
	Vercel	3,209	3,198	2,196	4	50	2,405	1	●	●
CDN Service	Gcore	13,514	200	87	18	35	74	1	●	●
	Verizon	11,157	1,097	989	4	4	13	1	●	●
	Alibaba	14,615	549	546	11	12	23	5	●	●
	Fastly	16,917	5,127	4,838	9	9	113	1	●	●
	Tencent	14,385	70	61	23	33	48	10	●	●

●: This means that the current IP source opens port 25 for outbound communication.
◑: For cloud hosting, this means that the provider uses the default blocking policy, but users can open port 25 by submitting an application form. For proxy services, this means that part of the proxy nodes have opened port 25.
●: This means that the current IP source blocks port 25 for outbound communication.

JPAAWG

BreakSPF

- コメント
  - BreakSPF というほど SPF は破られてはいない (あくまで運用方法の問題)
  - とはいえ，include の使い方には気をつけるべき (lookup 回数や消えた SPF レコードの問題など，あと IP アドレスの管理についても)
  - 様々な形態でのクラウドサービスが増えてきている現在，もう一度　IP アドレスの使われ方は確認しておくべき (特にサービス提供側)

HADES Attack

- 出典
  - *HADES Attack: Understanding and Evaluating Manipulation Risks of Email Blocklists* (NDSS* 2025, 所属: Tsinghua Univ., Zhongguancun Lab., Fudan Univ., Coremail Tech., Zhejiang Gongshang Univ., Zhejiang Key Lab. of Big Data and Future E-commerce Tech.)
- 概要
  - HADES はギリシャ神話にある冥界の神，攻撃者が DNSBL の honeypot (capture server) にメールを送信することで block list に登録させる攻撃から
  - DNSBL の登録手法を調査，対象は 29の DNBL プロバイダ，実際に 14 の DNSBL に登録することに成功
  - 5 つの DNSBL プロバイダがこうした問題を認めた

* Network and Distributed System Security Symposium (ISOC)

HADES Attack

- 攻撃手法
  - DNSBL は capture server に大きく依存しているので，そこにメールを送れば DNSBL に登録される仕組みになっている
  - Caputre servers (メールアドレス) が分かれば，どこかのメールサーバのアカウントを使ったり (内部攻撃) や，何らかの登録サービスを悪用してメール送信させるなどの手段が行える
  - 一定期間後に自動削除されるものが多いが，繰り返し行うことで伸ばすことも可能

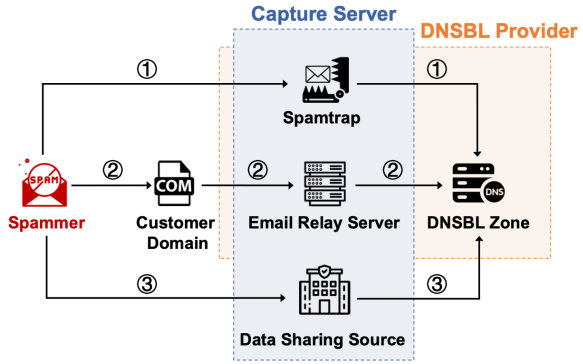


Figure 2. Three types of capture servers.

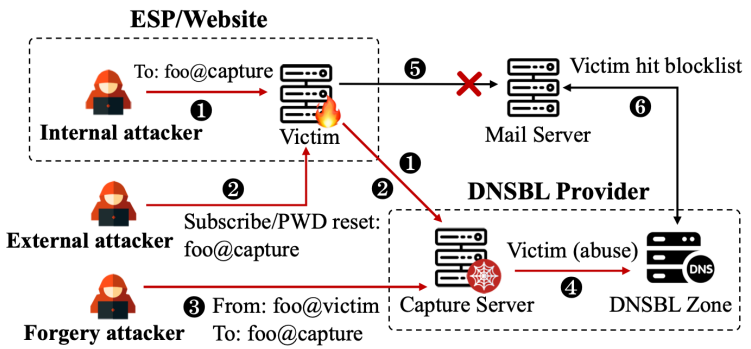


Figure 3. Workflow of the HADES attack.

HADES Attack

- 調査方法
  - Spamtrap は通常のメールサーバと異なる特徴 (詐称でも何でも受信する) があるのでそれを利用して判定
  - Coremail (よく DNSBL に登録される) の送信ログから宛先を抽出
  - 宛先毎に 5時間，1通/分で送信，DNSBL に登録されているか確認
  - 一般的な手法についても提案
    - まずは宛先ドメインを収集 (Web, 人気Topドメインなど)
    - その MX 宛に詐称メールなどでも受け取るかを試す
    - 送った後に DNSBL に登録されているかを確認
- 結論
  - 30万ドメインが DNSBL を使っている
  - 3通のメールでSpamhausに1週間登録可能だった
  - こうした攻撃 (HADES) は実際に行われている
  - 調査には倫理に気を遣って行ったとのこと

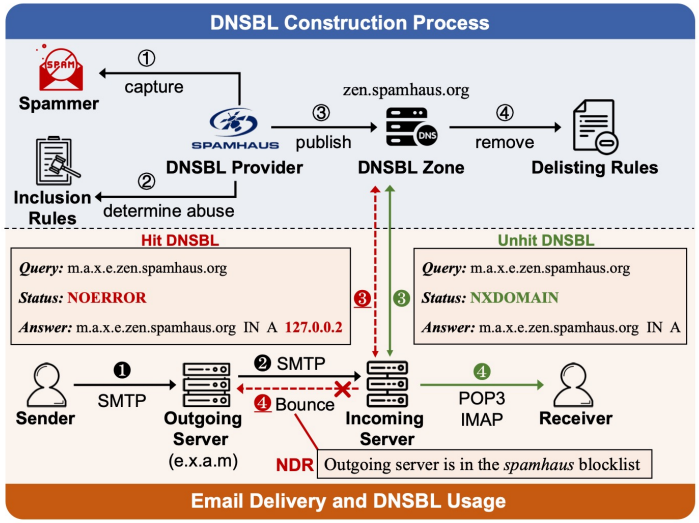


Figure 1. The construction process and usage of the DNSBL.

HADES Attack

- コメント
  - 特に国内では DNSBL の扱いには議論があるところ (しかしながら費用対効果が大きい対策であることも事実)
  - 同様の試みは絶対にやめましょう
  - ドメインレピュテーションの研究もしています，興味ある方は別途連絡を

You've Got Report

- 出典
  - *You've Got Report: Measurement and Security Implications of DMARC Reporting* (32nd USENIX Security Symposium, 所属: Virginia Tech, Max-Planck-Institut für Informatik)
- 概要
  - DMARC レポートの管理設定が不十分だと攻撃者に悪用される可能性がある
  - .com, .net, .org, .se の 2nd レベルのドメイン名に対して調査を実施
  - 7つのメールホスティングサービスと2つのDMRCレポーティングのオープンソースソフトウェアを調査
  - DMARCレポートに関してセキュリティ上管理不十分な設定があることがわかった

You've Got Report

- DMARC レポートに関するセキュリティ上の懸念部分
  - RFCの曖昧な部分
    - Exp.1: レポート送信先の数
    - Exp.2: 重複したレポート送信先アドレス
    - Exp.3: サブドメインをまとめてレポートするかどうか
  - 設定が不十分(EDV)
    - Exp.4: レポートの外部ドメイン送信の事前確認 (External Destination Verification)
  - RFC Expolit
    - Exp.5: EDVのためのレコードのredirect設定(複数設定)
- その他
  - TLS-RPTにも同様の課題がある(Exp.6)

You've Got Report

- 大手メールサービスプロバイダの調査

EHP	Report Size (B)	# of addr.	EDV		Email Address Aggr.			RI		RUF Support
			Check (Exp. 4)	Overriding (Exp. 5)	Addr. (Exp. 2)	Domain (Exp. 1)	Subdomain (Exp. 3)	Respect (Exp. 7)	Predictable	
Google	3,962	50	✗	-	✗	✗	✗	✗	✓	✗
Yahoo	4,626	50	✗	-	✗	✗	✗	✗	✓	✗
QQ	3,628	50	✗	-	✗	✗	✗	✗	✓	✗
Gmail	3,962	1	✗	-	-	-	-	✗	✓	✗
163	4,034	50	✓	✗	✓	✗	✗	✗	✓	✗
Amazon	4,324	50	✓	✗	✓	✗	✗	✗	✗	✗
FastMail	4,839	10	✓	✓	✓	✗	✗	✗	✓	✗
OpenDMARC	2,238	8-12[6]	✗	-	✗	✗	✗	✗	✓	✓
Rspamd	2,320	50	✓	✗	✓	✗	✗	✗	✓	✗

Table 3: Table showing the 7 popular email hosting providers (EHPs) and two software that support DMARC reporting. `Exp.` in parentheses indicates which column maps to which experiment in §4.2. Each experiment is evaluated based on security criteria: marks are colored red if the experiment is vulnerable to exploitation by attackers, green if it is not, and black if it is neutral. Note that if email providers do not implement EDV, we do not test whether they override EDV or not (hence the –). In case of `Gmail`, it only sends one report to the first recipient listed in the `rua` tag; so, aggregation check is not tested (hence the –).

You've Got Report

- 攻撃手法
  - Report Reflection (RR) Attack
    - EDVの確認が行われないと無関係の宛先にDMARCレポートが送信されてしまう
    - レポート先を多数設定可能である場合，DMARCレポートが増幅される
    - EDVでレポート先が上書き可能で複数宛先が設定可能であるとより増幅される
  - これらの攻撃により
    - レポート受信先のspoolが溢れる可能性がある(Inbox flooding)
    - レポート受信側のSMTP接続が溢れる可能性がある(SMTP connection flooding)
- 改善提案
  - DMARC レポート送信数に制限を加えるべき, rua の制限だけでは不十分
  - EDV (外部ドメインへのレポート送信時の検証) を必須にしないと，リフレクタ攻撃に使われる
  - TLS-RPT の外部ドメイン検証は考慮されていないが (TLSが失敗した場合なので), 検討すべき

Thank you