DDoS 2024-2025

2025/01

ノキアソリューションズアンドネットワークス合同会社

© 2024 Nokia

自己紹介

- 名前: 石井俊行 (Ishii Toshiyuki)
- 所属: ノキアソリューションズ&ネットワークス合同会社
  IP製品部門 シニアソリューションアーキテクト
- Janog参加歴: Janog21(2008年)@熊本～
- Janog登壇歴: Janog53 DDoS最前線
- Email toshiyuki.ishii@nokia.com

© 2024 Nokia

目次

1. DDoS 観測方法
2. DDoS 2024
3. DDoS 対策 2025 Next Step

 © 2024 Nokia

1. DDoS観測方法

なぜ Nokia が DDoS?

End To Endでモバイル/固定/ISP/データセンタ/エンタープライズあらゆるネットワークソリューションを提供しています

DDoSトラフィックに対してはフローコレクターをベースとしたインターネット観測技術を開発し、また10年以上にわたり世界各国のコラボレーション企業と協力しながらインターネットトラフィックの実情を分析しています

© 2024 Nokia

1. DDoS観測方法

どうやってDDoS観測をしている？
１:自発的に探す(Nokia開発)

Deepfield Genome

世界中のすべての IPv4 とアクティブな IPv6 をクロール

Deepfield Secure Genome

Deepfield Cloud Genome®

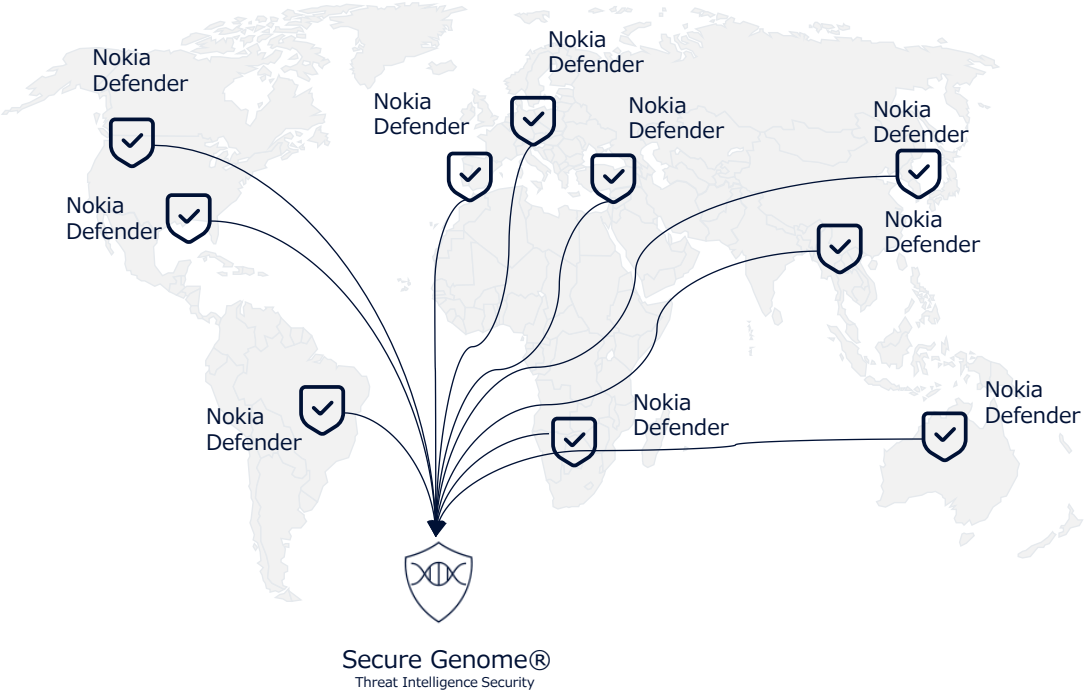
OTT サービス、アプリケーション、CDN、ISP、サーバー、ホスティング、既知のボットネット
CVE 、誤設定、脆弱なサーバー、アプリケーション、デバイス
IoT デバイスの種類、侵害されたサーバー、アクティブなボット メンバー
などを検出

© 2024 Nokia

1. DDoS観測方法

どうやってDDoS観測をしている？
2 :世界中の協力企業から情報を集める

- 任意メンバーシップ (オプトイン)
- プライバシーと匿名性を念頭に置いて構築
  - EU GDPRなど
- 攻撃のメタデータ/特性を追跡
  - 攻撃元 IP、上位ベクトルなど
  - 匿名性を保証するため、攻撃を受けている IP は除外
- Nokia Deepfield Secure Genome を強化し、世界中の DDoS トラフィックを発信するボットネットを特定



© 2024 Nokia

1. DDoS観測方法

どうやってDDoS観測をしている？

～2023年のDDoS状況は以下をチェック～

Janog53 - DDoS最前線 DDoSトラフィックの変化と課題
https://www.janog.gr.jp/meeting/janog53/wp-content/uploads/2023/11/Janog-DDoS-Ishii-1.pdf

© 2024 Nokia

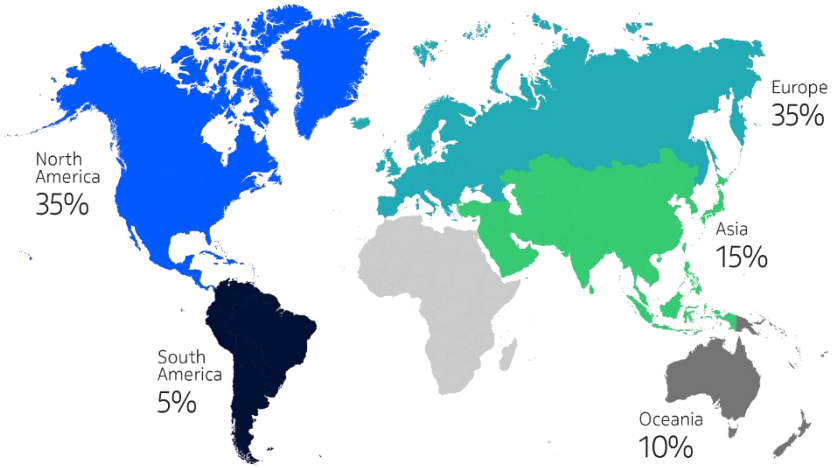
2.DDoS 2024年

調査結果と傾向

1.世界的トラフィックの増加

DDoSトラフィックは、他の種類のネットワークトラフィックよりも高い割合で増加し続けており、2023年6月から2024年6月の間に**166%増加**。
多くのネットワークでは、これらのイベントの頻度は、1日に一回または二回から、1日に**100回以上**に増加。

また重要な地域(経済的、技術的)への継続的な集中が確認され、サイバーセキュリティ防御に対する継続的なリスクを浮き彫りに



通信分野におけるサイバー攻撃の地域分布
Source:Nokia

© 2024 Nokia

2.DDoS 2024年

調査結果と傾向

2.DDoSトラフィックの変化と割合

DNS増幅の継続的な使用：DNS増幅攻撃がもっとも多くしめている

Botnet/Quicが多数を占め始めている

その他のベクターは、前年比で20–70%減少(NTP、CLDAP、Memcache増幅など)。

Source:Nokia

	DNS	Botnet	quic	Fragment	SYN Flood	Total
Global	~ 45.5%	~ 17.8%	~ 9.7%	~ 9.2%	~ 8.2%	**~ 90.4%**
North America	~ 32.5%	~ 28.9%	~ 14.5%	~ 9.4%	~ 4.9%	**~ 90.2%**
South America	~ 53.7%	~ 12.6%	~ 10.8%	~4.63%	~ 14.9%	**~ 96.3%**

さらにスプーフィングトラフィック + UDP フラッド + リセット フラッド + ICMP フラッド + TCP リフレクション攻撃トラフィックを含めると95%となる

アプリケーションレイヤの攻撃は5%以下

© 2024 Nokia

2.DDoS 2024年

調査結果と傾向

3.ボットネット

DDoS攻撃の状況では依然として主要なドライバー。更に巧妙化してDDoS攻撃を試みている

2024年 ボットネット攻撃成功例

Time	TTL	Proto	TCPFlag	Peer	Src IP	SPort	Dst IP	DPort	Detect
04:55:30		6	A	[redacted]	[redacted]	51550	XX.XX.139.76	443	
09:22:40	124	6	A	[redacted]	[redacted]	58129	XX.XX.139.114	443	146 proxy_web
08:51:10	60	6	A	[redacted]	[redacted]	44090	XX.XX.139.76	443	146 proxy_web
07:55:00	123	6	A	[redacted]	[redacted]	51933	XX.XX.139.81	443	146 proxy_web
10:28:40	252	6	A	[redacted]	[redacted]	56058	XX.XX.139.80	443	146 proxy_web
09:32:30	60	6	A	[redacted]	[redacted]	46854	XX.XX.139.80	443	146 proxy_web
06:40:50	124	6	A	[redacted]	[redacted]	50810	XX.XX.139.80	443	146 proxy_web
06:38:50	124	6	A	[redacted]	[redacted]	50746	XX.XX.139.80	443	146 proxy_web
10:31:30	62	6	A	[redacted]	[redacted]	50536	XX.XX.139.80	443	146 proxy_web

- スプーフィングされていない攻撃
- すべてのトラフィックが有効な加入者デバイスから
- 従来のしきい値ベースのDDoS検知、ミティゲーションでは正常トラフィックかどうか判断ができない(特にQUIC)

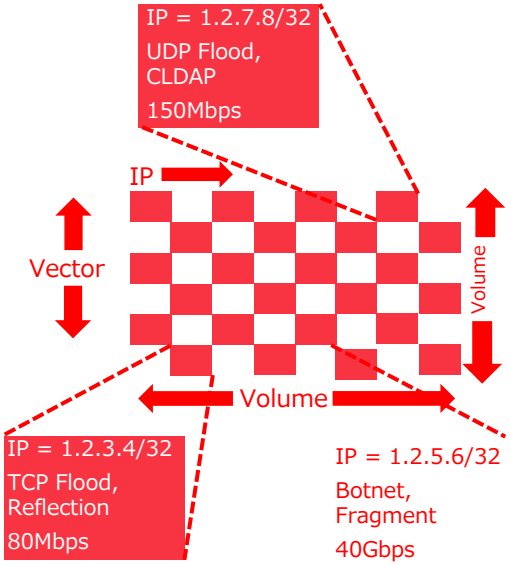
© 2024 Nokia

2.DDoS 2024年

調査結果と傾向

4.カーペットボム(絨毯爆撃攻撃)

これらのDDoS攻撃の範囲は拡大中。**13%**は256以上の宛先IPを対象とし、**2.8%**は**1,024以上のIPを対象**。
観測された最大の攻撃は16,000以上のIPアドレスを標的に。



Attack 例1 各アドレスへの帯域高	1,550 DDOS SRC IP	374 DDOS DST IP	53.7 PEAK GBPS
Attack 例2 多数の送信元IP Peakは少ない	135,713 DDOS SRC IP	1,954 DDOS DST IP	1.3 PEAK GBPS
Attack 例3 全部のっけもり	17,140 DDOS SRC IP	2,048 DDOS DST IP	1.6 PEAK TBPS

 © 2024 Nokia

2.DDoS 2024年

調査結果と傾向

5.攻撃の高度化 – 住宅用プロキシ

2024年には、**AIと自動化**によってDDoS攻撃が高度化し、大規模なDDoS攻撃で**住宅用プロキシ**が著しく乱用されていることが確認

例:NoName016(57) と呼ばれる親ロシア派のハクティビスト グループは、DDoSia ツールキット ソフトウェアを使用して、毎日ボランティアに攻撃対象のリストを提供

例:2024 年にはアプリケーション DDoS で大規模に採用され、ボットネットの最大 1,000 倍の大きさで急速な IP 変更され、商用アプリケーションと犯罪アプリケーションの両方で使用される

MALWARE & THREATS

VPN Apps on Google Play Turn Android Devices Into Proxies

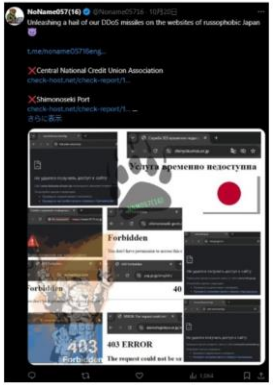
Human Security identifies 28 VPN applications for Android and an SDK that turn devices into proxies.

By Ionut Arghire
March 27, 2024

2024年10月に入ってから、特定のグループが国内組織へのサイバー攻撃に成功したと主張する、X（旧Twitter）やTelegramへの書き込みが相次いで見つかった。

書き込みは2つの攻撃者グループによるもので、それぞれ「NoName057（16）」（以下、NoName）と「CyberVolk」と名乗る。書き込み内容は大きく異なり、NoNameはDDoS（Distributed DoS）攻撃によって国内組織のWebサイトをダウンさせたというもの。CyberVolkは国内組織から窃取した情報をリークすると脅迫し、身代金を要求するものだった。

NoNameが犯行声明で挙げた国内組織の一部はDDoS攻撃による被害を公表し、テレビや新聞などで報道された。一方、CyberVolkが挙げた国内組織で被害を公表した事例を確認できていない。被害はなかったのだろうか。



攻撃者グループNoName057（16）によるXへの書き込み
（出所：X）

https://xtech.nikkei.com/atcl/nxt/column/18/00138/102501633/

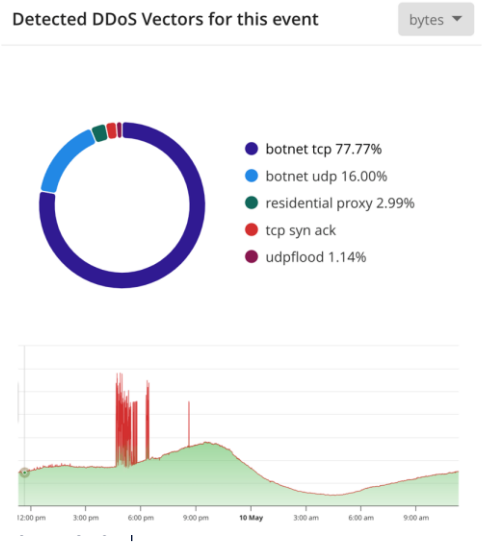
© 2024 Nokia

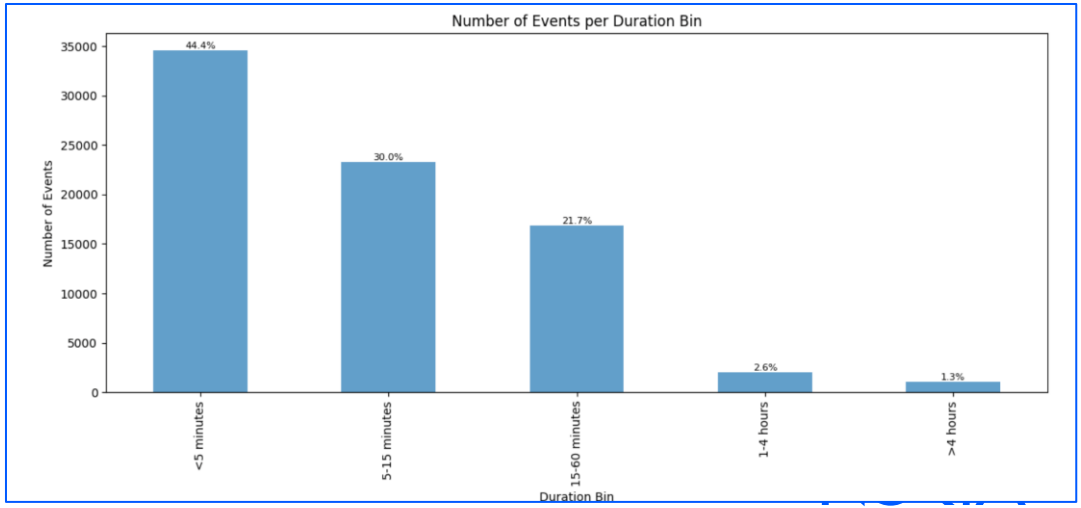
2.DDoS 2024年

調査結果と傾向

6. 攻撃時間の短縮 - マイクロバースト化

DDoS攻撃の**44%**は5分以内に終了
急速に進化し、自動化され、高度に分散された攻撃が大幅に増加。ソース、宛先、ポート、プロトコル、ペイロードを含む DDoS 対策の変更に対する応答が 10 秒未満。
従来の DDoS スクラバーにとって困難 – より強力で動的な緩和が必要





3.DDoS 2025年～

DDoS対策 Next Step

- **継続的なモニタリング/トラッキングとリアルタイムアップデート**をし、ボットネットおよび住宅用プロキシから発生する新しい攻撃ポイントを広範囲にわたって確認、特定が必要

- インターネットピアリング/中継リンクのみを引き続き保護するのではなく、すべてのネットワークエッジにわたって、受信と送信の**すべての方向からの保護**を可能にすることも必要

- **しきい値ベースではなく精度と速度が向上した新世代＋未知の攻撃を検出する機能**に基づいて、DDoS軽減ソリューションを評価が必要

© 2024 Nokia

NOKIA