資料41－3

Microsoft

国際的なサイバーセキュリティ・ボットネット対策
－ DCU活動からの報告

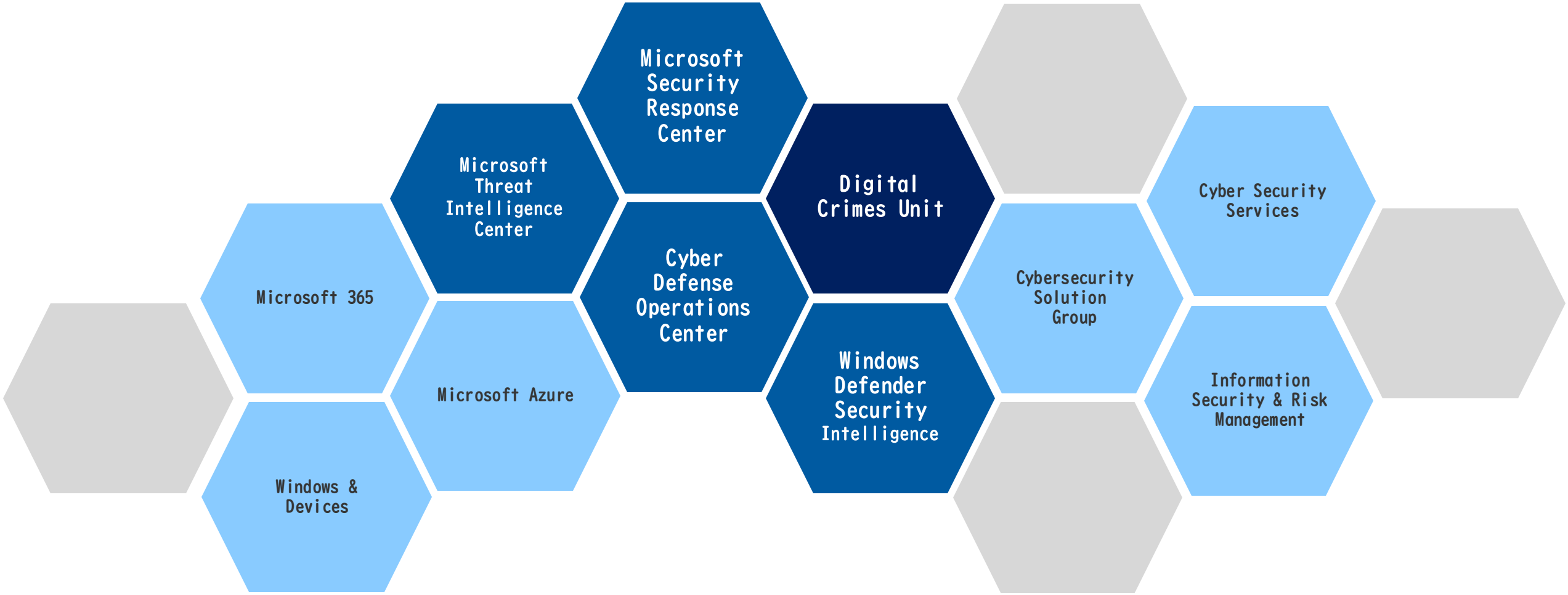
日本マイクロソフト株式会社
松尾早苗

デジタルクライムユニット | ミッションステートメント

サイバー犯罪との戦いを主導し、**お客様の安全を守り、マイクロソフトに対する世界の信頼を得る**

- テクノロジー
- フォレンジック
- 民事訴訟
- 捜査機関への情報提供
- 官民・民間同士の協力
- セキュリティとプライバシー

様々なチーム、技術的要素が連携



Digital Crimes Unit | 戦略と注力分野

打撃と抑止 民事上の措置を通じて犯罪インフラをたたき、警察機関への情報提供によって、刑事的な措置を支援

お客様の保護 情報共有により被害回復を支援し、製品やサービスに常に新たな技術的対抗策を更新していく

サイバー犯罪の戦いにおける連携やリーダーシップ 政策提言、官民連携、教育キャンペーンによりサイバー犯罪がより実施困難なものにしていく

マルウェア

MALWARE INFRASTRUCTURE AND NATION-STATE DISRUPTIONS

ランサムウェア

RANSOMWARE ATTACKS

Azure Fraud

FRAUDULENT ACCESS TO AZURE USED IN FURTHERANCE OF CYBERCRIME

ビジネス詐欺メール

CREDENTIAL THEFT AND CYBER-ENABLED FRAUD

テクニカルサポート詐欺

TECHNICAL SUPPORT SCAMS

ソフトウェアの安全な供給

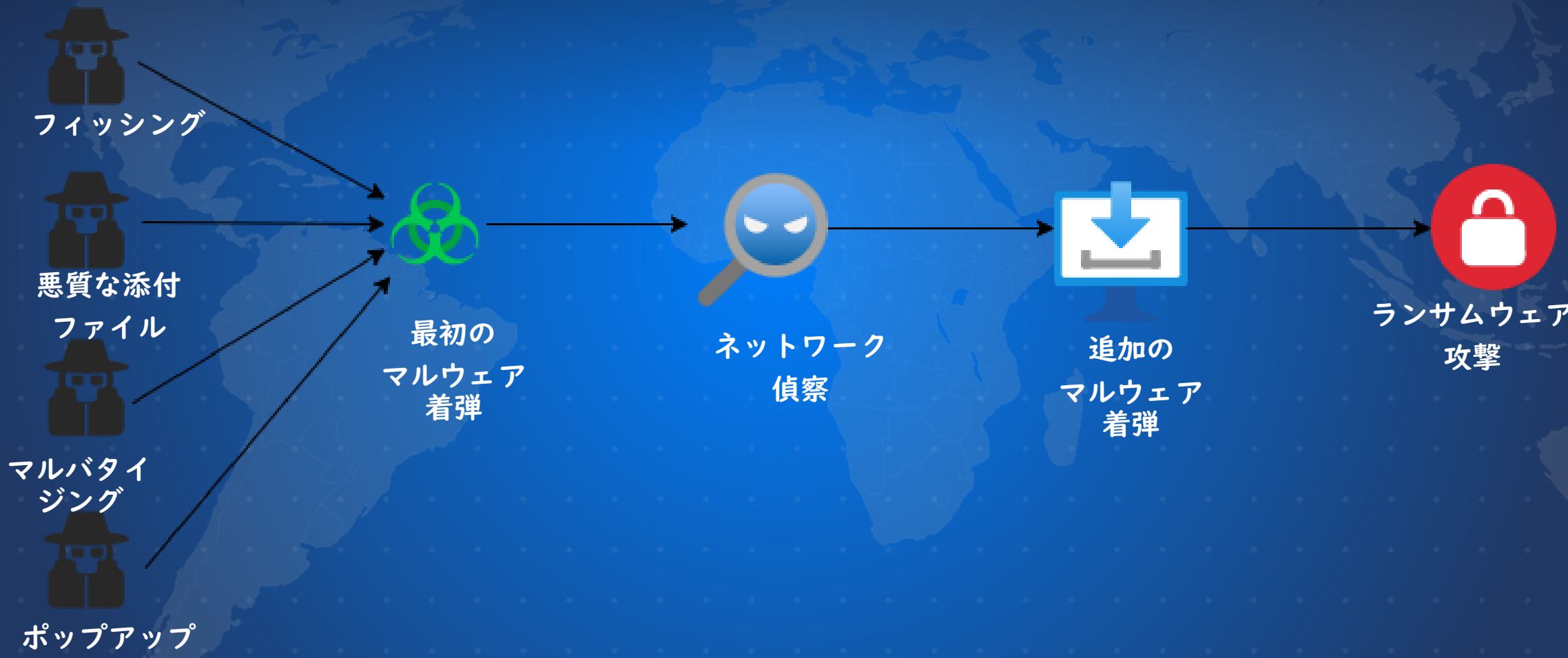
SUPPLY CHAIN FRAUD AND THEFT

DCU 犯罪インフラを分断することに注力

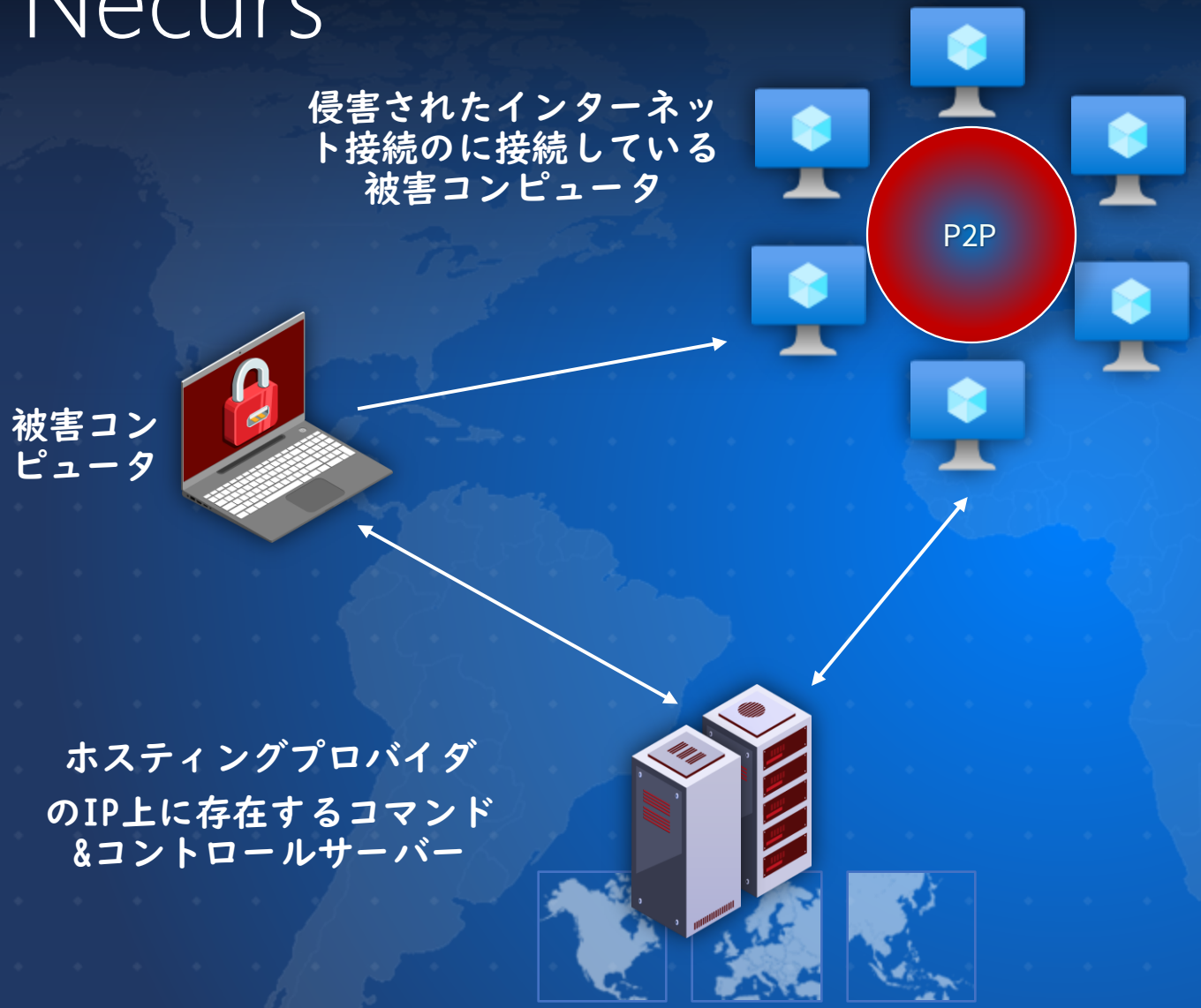
敵：サイバー犯罪者	遂行能力	インフラ	被害者
サイバー犯罪を行っているアクター/組織	サイバー攻撃に使われるツールや技術	サイバー攻撃を実施し、被害コンピュータとの通信手段・媒介となる物理的・論理的インフラ	攻撃者のターゲット
警察の注力分野	製品サービスのセキュリティ機能を強化	DCUの貢献機会	被害者救済機関との連携

IPアドレス	ドメイン	決済アカウント	IOT 機器	URLS	CLOUD ストレージ	HOP-THROUGH POINTS
電話番号	EMAIL アドレス	仮想マシン（VM）		SERVERS	ソーシャルメディア	その他

今日のマルウェア生態系



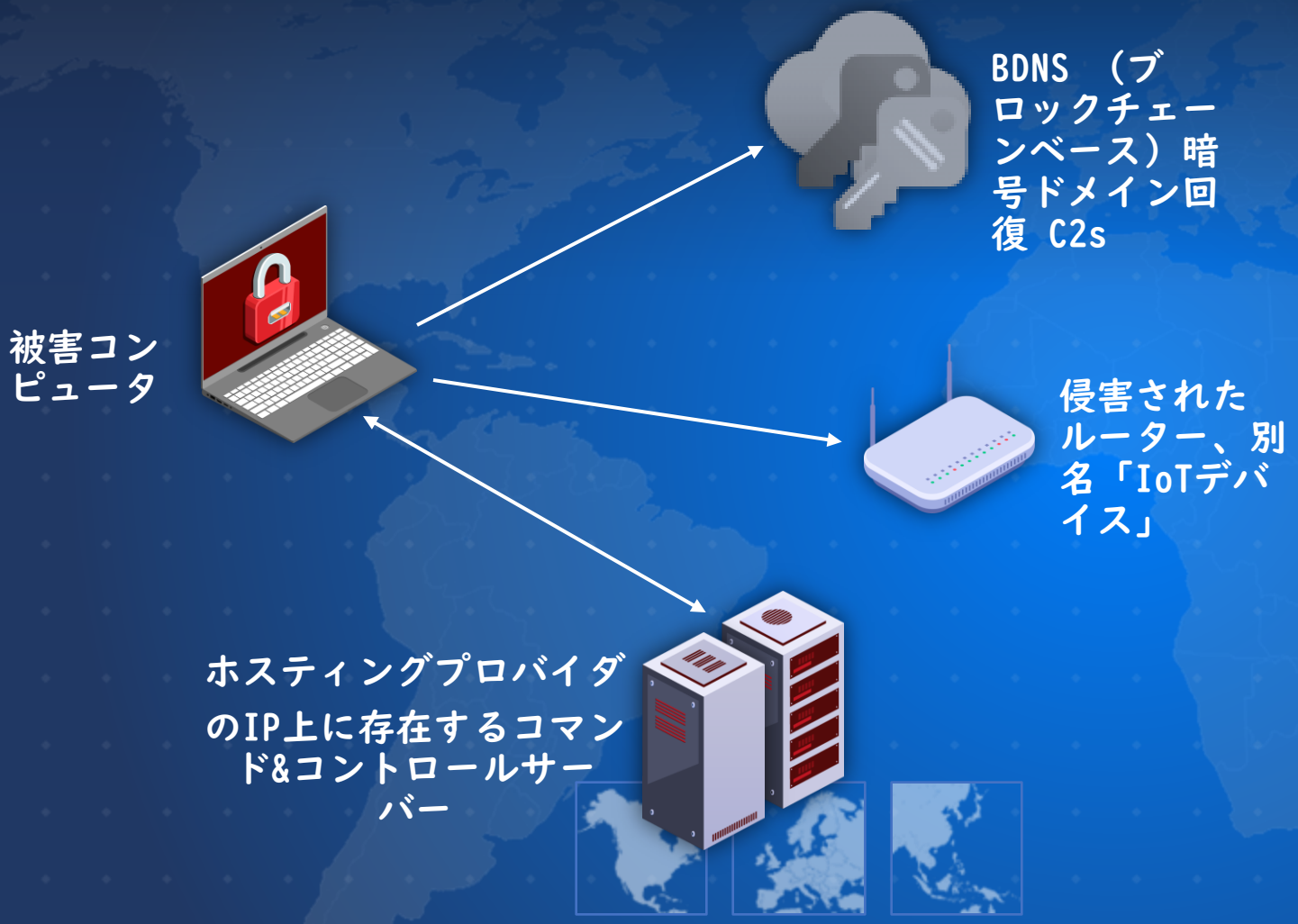
Necurs



Capabilities

- 他のマルウェア、ランサムウェア、詐欺スキームを含む悪意のあるペイロードを配信するMaaS +スパムボット
- 洗練された冗長C2インフラストラクチャ
- コア C2、スパム C2、P2P C2、DGA C2（難読化された IP を使用）
- 8 つのアクティブなボットネット
- ハイブリッドP2Pネットワークバックアップ C2チャンネル
- DGAは43のTLDで構成され、ボットネットごとに4日ごとに2048のドメインを生成します（1か月あたり約131,000ドメイン）
- アンチ分析とアンチサンドボックスのテクニック
- マルウェア対策/ウイルス対策プログラムを無効にします。

Trickbot



Trickbot Tier Ⅰ犯罪インフラ

Capabilities

- 悪意のあるペイロードを配信し、詐欺行為を行うMaaSボットであり、金融トロイの木馬
- 洗練されたIPベースのC2インフラストラクチャ
- コア C2、IoT C2、暗号ドメイン回復 C2
- 侵害されたIoTホームルーターは、悪意のあるモジュールを提供するためにC2として悪用された
- アンチ分析とアンチサンドボックスのテクニック
- マルウェア対策/ウイルス対策プログラムを無効化
-

Emotet

被害コンピュータ

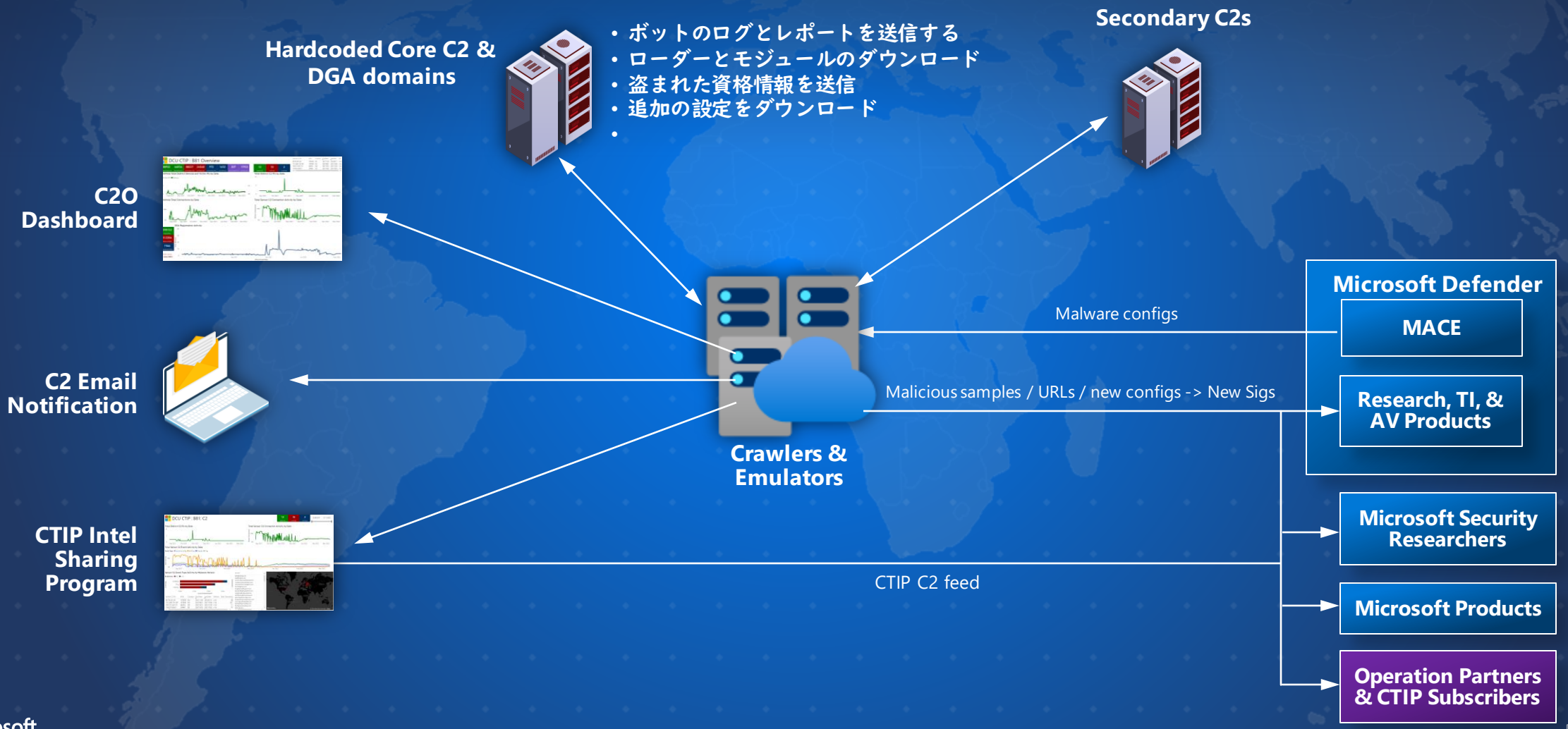
グローバルに分散したコマンド&コントロールサーバー

Emotet Tier 1 犯罪インフラ

Capabilities

- 悪意のあるペイロード、スパムを配信し、詐欺行為を行うMaaSボットであり金融トロイの木馬
- 洗練されたIPベースのC2インフラストラクチャ
- コア C2
- 資格情報の盗難
- アンチ分析とアンチサンドボックスのテクニック
- ワームに似た自己複製型の感染拡大
- 多数のTirel C2 IP
-

マルウェアセンサー


Hardcoded Core C2 & DGA domains
• ボットのログとレポートを送信する
• ローダーとモジュールのダウンロード
• 盗まれた資格情報を送信
• 追加の設定をダウンロード
•
Secondary C2s
C2O Dashboard
C2 Email Notification
CTIP Intel Sharing Program
Crawlers & Emulators
Malware configs
Malicious samples / URLs / new configs -> New Sigs
CTIP C2 feed
Microsoft Defender
MACE
Research, TI, & AV Products
Microsoft Security Researchers
Microsoft Products
Operation Partners & CTIP Subscribers

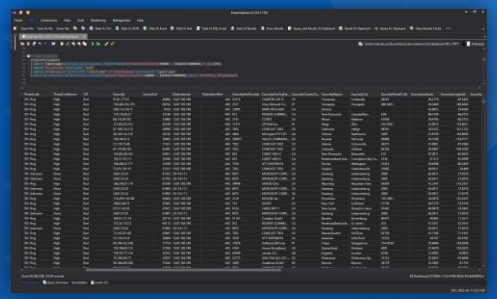
感染状況のモニタリング

感染コンピュータ

DCU Sinkhole

収集されるデータ:
被害ンピューターのIP
ボット/マルウェアキャンペーン ID
悪意のあるモジュール
接続アクティビティ

CTIP Intel Sharing Program



Azure Data Explorer
Realtime Sinkhole
Monitoring

CTIP Infected feed

- Microsoft Security Researchers
- Microsoft Products
- Operation Partners
- CTIP Subscribers

様々な連携

Defender Research, TI, & Products

MSTIC

DART

Domains

Digital Crimes Unit

MAD Team

RAD Team

CST-E

DCU Field

Microsoft internal

ICANN

ESET

RoLR

Avast

BITSIGHT

LUMEN BLACK LOTUS LABS™

paloalto NETWORKS

H-ISAC™ HEALTH - ISAC

FS-ISAC

NTT

VERISIGN

EUROPOL EC3 European Cybercrime Centre

Symantec

external

DCU Malware Disruption Operations

ZLOADER
APRIL 2022
FINANCIAL FRAUD/ MALWARE+RANSOMWARE DELIVERY BOTNET

Run by global internet-based organized crime gang operating "malware as a service" designed to steal and extort money.

NICKEL
DECEMBER 2021
NATION-STATE

China-based threat actor targeting governments, diplomatic entities and NGOs primarily in the Americas and Europe.

TRICKBOT
OCTOBER 2020
FINANCIAL FRAUD/ MALWARE+RANSOMWARE DELIVERY BOTNET

Globally dispersed financial trojan and malware distribution botnet with a compromised IoT-based command and control infrastructure; also used to deliver ransomware.

NECURS
MARCH 2020
MALWARE AND SPAM SPREADING BOTNET

Globally dispersed spam and malware distribution botnet with a sophisticated and redundant command and control infrastructure; used to deliver ransomware, financial malware, spam, and stock scams.

THALLIUM
DECEMBER 2019
NATION-STATE

North Korea-based threat actor targeting government employees, think tanks, university staff, organizations focused on world peace and human rights, and individuals that work on nuclear proliferation issues, primarily in the US, as well as Japan and South Korea.

PHOSPHORUS
MARCH 2019
NATION-STATE

Iran-based threat actor (aka APT 35, Charming Kitten, and Ajax Security Team) targeting prominent individuals in business and government to steal credentials, including activists and journalists – especially those involved in advocacy and reporting on issues related to the Middle East.

GAMARUE
NOVEMBER 2017
MALWARE SPREADING BOTNET

Sold as a Crime kit, first seen in 2012. Distributed at least 80 different malware families.

AVALANCHE
NOVEMBER 2017
CRIMINAL SYNDICATE

International criminal syndicate involved in phishing attacks, online bank fraud, and ransomware. Also refers to the network of systems used to carry out the activity.

BARIUM
NOVEMBER 2017
NATION-STATE

China-based threat actor heavily targeting gaming and internet content industries, including theft of sensitive information using a custom malware toolkit with extensive capabilities.

STRONTIUM
AUGUST 2016
NATION-STATE

Russia-based threat actor (aka APT28, Fancy Bear) targeting theft of sensitive information; uses zero-day exploits and spear phishing attacks to gain network/account access.

DORKBOT
DECEMBER 2015
IDENTITY THEFT, FINANCIAL FRAUD

Disables security, steals credentials, personal info., distributes other malware. Spreads via USB, messaging, and social networks.

RAMNIT
FEBRUARY 2015
IDENTITY THEFT, FINANCIAL FRAUD

Module-based malware which concentrates on stealing credential information from banking websites.

SIMDA
APRIL 2015
IDENTITY THEFT, FINANCIAL FRAUD

Uses remote access to steal personal and banking info, as well as install other malware.

CAPHAW
JULY 2014
IDENTITY THEFT, FINANCIAL FRAUD

Focused on online financial fraud and responsible for more than $250M in losses.

GAMEOVER ZEUS
JUNE 2014
IDENTITY THEFT, FINANCIAL FRAUD

Extremely sophisticated trojan which steals banking credentials; spread via spam or phishing messages.

BLADABINDI & JENXCUS AKA B106
JUNE 2014
IDENTITY THEFT, FINANCIAL FRAUD, PRIVACY INVASION

Discovered July 2012. Pervasive family of malware spread through infected removable drives and downloaded by other malware.

ZEROACCESS AKA SIREFEF
DECEMBER 2013
ADVERTISING CLICK-FRAUD

Hijacks search results, takes victim to dangerous sites. Cost online advertisers upwards of $2.7 million each month.

CITADEL
JUNE 2013
IDENTITY THEFT, FINANCIAL FRAUD

Committed online financial fraud responsible for more than $500M in losses.

BAMITAL
FEBRUARY 2013
ADVERTISING CLICK-FRAUD

Hijacked user's search results, took victims to dangerous sites.

NITOL
SEPTEMBER 2012
MALWARE SPREADING BOTNET, DISTRIBUTED DOS ATTACKS

Introduced in the supply chain relied on by Chinese consumers.

ZEUS AKA ZBOT
MARCH 2012
IDENTIFY THEFT, FINANCIAL FRAUD

Steals identity, financial information, controls PC, turns off firewall, installs other malware, ransomware.

KELIHOS
SEPTEMBER 2011
SPAM, BITCOIN MINING, DISTRIBUTED DOS ATTACKS

Trojan that distributes spam, steals logins, bitcoins, downloads and executes files.

RUSTOCK
MARCH 2011
SPAM

Rootkit-enabled back door Trojans which distributed spam e-mail.

CONFICKER
FEBRUARY 2010
BOTNET WORM

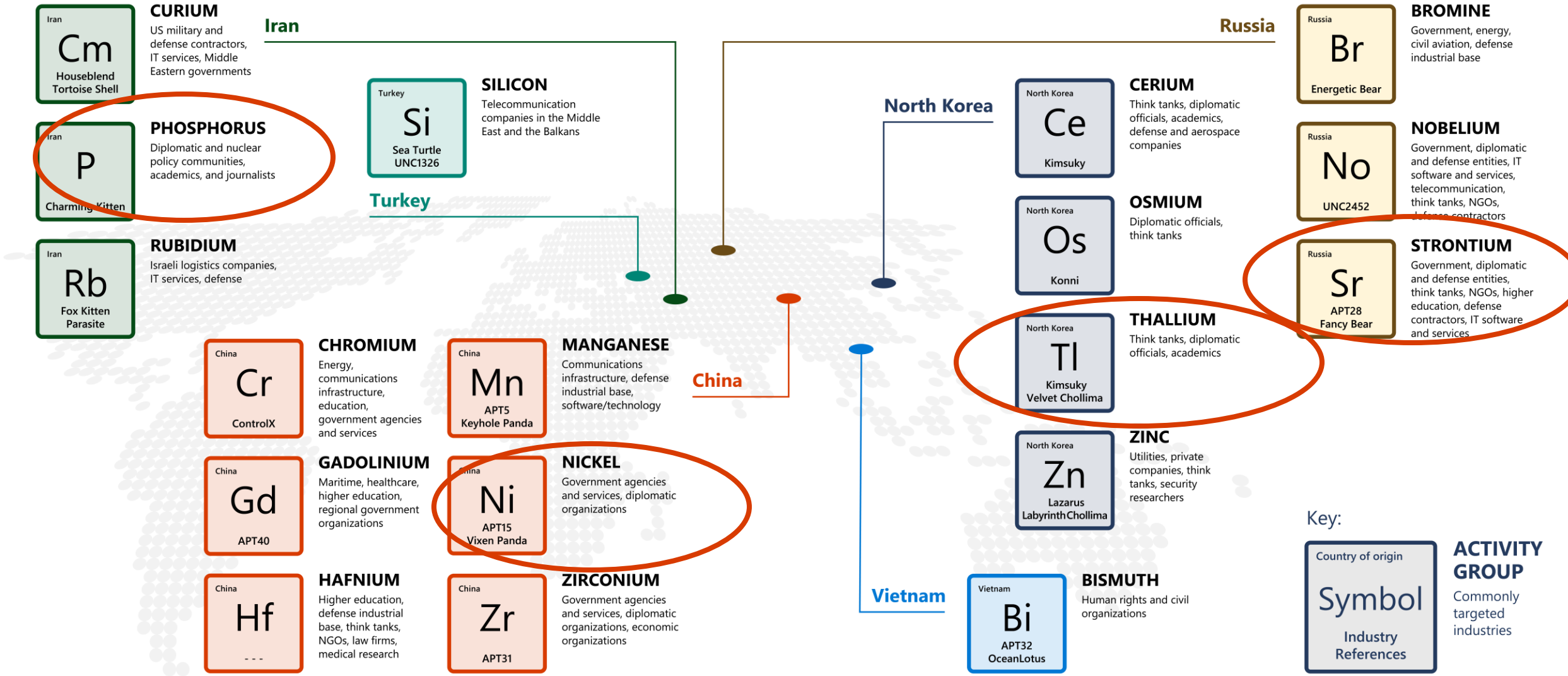
Worm spread via USB and internet. Would infect other devices in common network.

WALEDAC
FEBRUARY 2010
SPAM

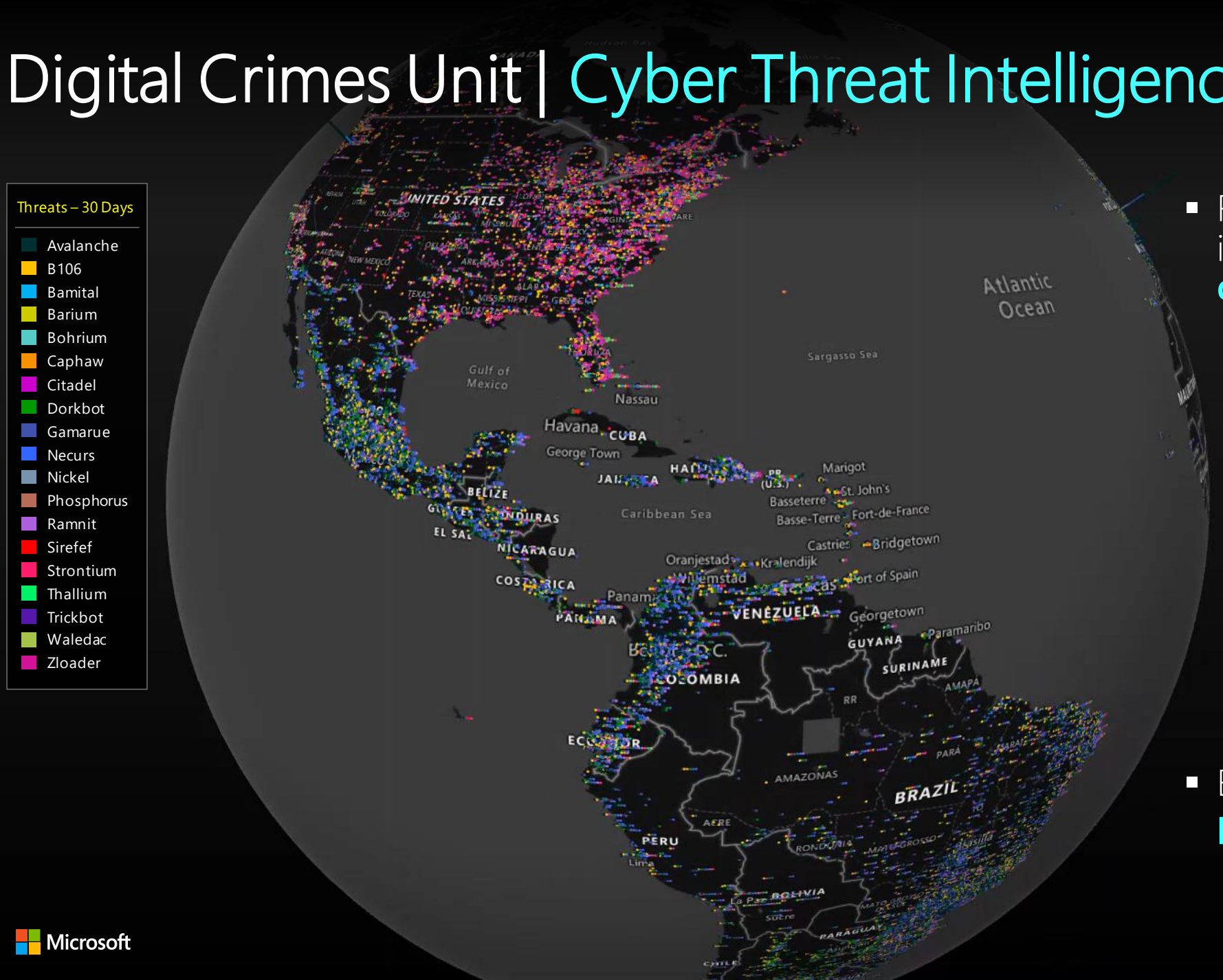
Trojan that collects email addresses, distributes spam, post data to webs, downloads executable files.

マイクロソフトが観測している主要な国家アクター

Sample of nation state actors and their activities



Digital Crimes Unit | Cyber Threat Intelligence Program (CTIP)



- Real time, actionable threat intelligence from DCU **malware disruption operations**
  - Includes **victim and criminal infrastructure** data
    - Shared with **trusted partners** including CERTs, ISPs and ISACs
  - Included as an offering in Microsoft's **Government Security Program** (GSP)
- Engineered into Microsoft **products and services**

最後に：ユーザーの皆様にお願いしたい事

1. 多要素認証を取り入れる(MFA)
2. eメールのハイジーン　（例：セーフリンクなど）
3. アプリとシステムに最新のパッチを適用する
4. 最小限の特権アクセスの付与
5. ネットワークのセグメンテーションにより攻撃のスピードを遅らせる

Slow attacks with network segmentation