Nové stratégie prebiehajúceho boja proti počítačovej kriminalite pre zvýšenie dôvery a bezpečnosti v dnešnom svete cloudových služieb a mobility

Microsoft Digital Crimes Unit

Peter Fifka
Senior Program Manager
Investigations (EMEA)

Kybernetická bezpečnosť je dnes záležitosťou top manažmentu

71%
firiem pripúšťa, že sa stali obeťou úspešného kybernetického útoku

3 bilióny $
odhadovaná ekonomická hodnota aktivít produkovaných kybernetickou kriminalitou do roku 2020

556 miliónov
obetí počítačovej kriminality

400 miliárd $
škoda spôsobená kybernetickými útokmi za rok (2015)

160 miliónov
Kompromitovaných dátových záznamov z 8 top útokov v roku 2015

140+
mediánová hodnota dní od infiltrácie po detekciu

JEDINEČNÁ PERSPEKTÍVA SPOLOČNOSTI MICROSOFT

300 miliárd užívateľských autentifikácií každý mesiac

1 miliarda aktualizovaných zariadení Windows

200 miliárd analyzovaných emailov za účelom detekcie spamu a malwaru

CHRÁNIŤ

naprieč všetkými koncovými bodmi, od snímačov po dátové centrá

ODHALIŤ

pomocou cielených signálov, monitorovaním správania a strojovým učením

Bezpečnostná koncepcia Microsoftu

REAGOVAŤ

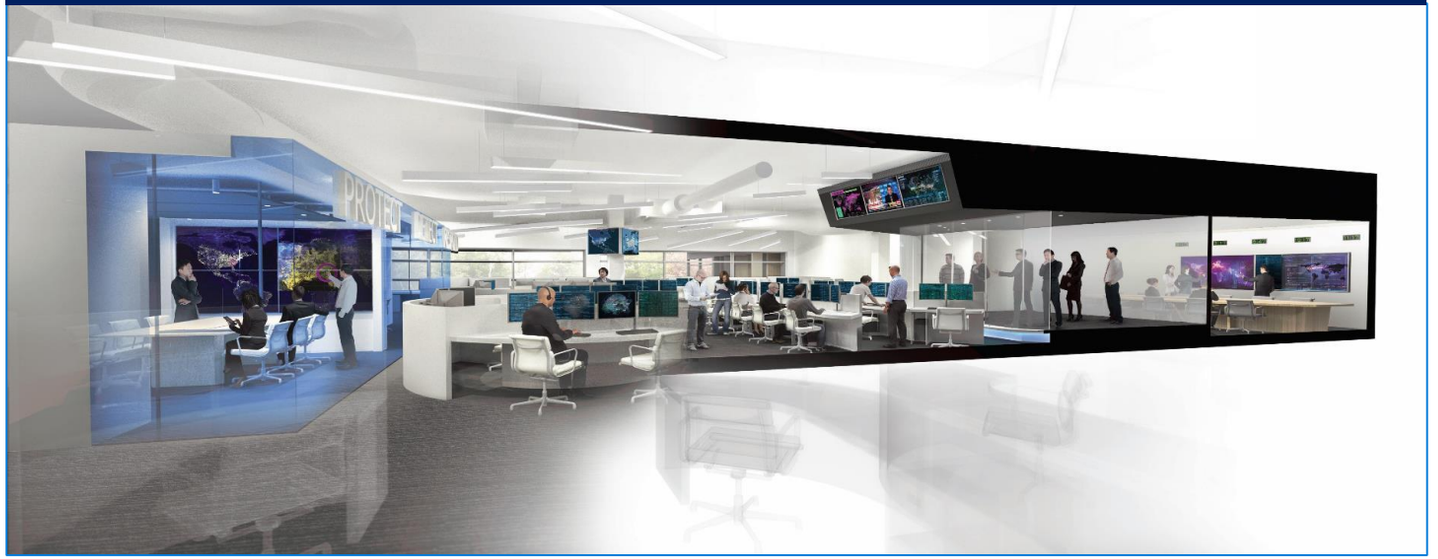
zmenšovaním rozdielov medzi odhalením a akciou proti hrozbe

Vrstvený prístup k bezpečnosti

Pomáha chrániť našich zákazníkov, našu spoločnosť a náš svet

Rastúce hrozby vyžadujú koordinovanú reakciu:

Cyber Defense Operations Center (CDOC)



- Cyber Security Services Engineering
- Digital Crimes Unit
- Information Security & Risk Management
- Microsoft Azure
- Microsoft Security Response Center
- Microsoft Threat Intelligence Center
- Office 365
- Windows & Devices Group

The Microsoft Digital Crimes Unit

Bezpečnejšia digitálna skúsenosť pre každého jednotlivca a organizáciu na svete

Kombináciou nových právnych stratégií, najmodernejších forenzných metód, cloudu a analytického spracovanie veľkých objemov dát

Partnerstvom medzi verejným a súkromným sektorom pre potlačovanie zneužívania technológií zločincami

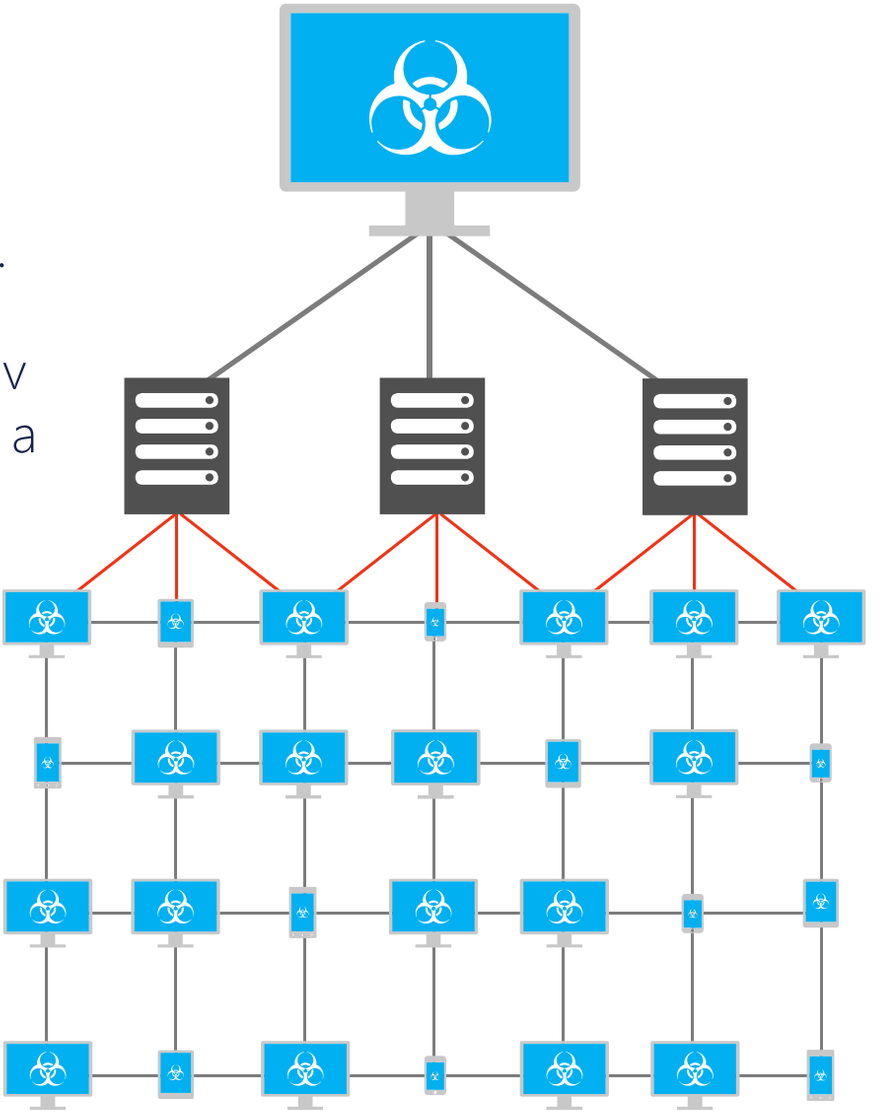
Znefunkčňovanie malwaru

Spolupráca s políciou a ďalšími organizáciami s cieľom narušiť a znefunkčniť infraštruktúru vytvorenú zločincami

DCU vyhľadáva ciele, analyzuje konkrétny malware, identifikuje ním vytvorenú infraštruktúru (botnety) a koordinuje globálne partnerstvá podnikajúce kroky k ich znefunkčneniu.

Informujeme CERT-y a poskytovateľov internetových služieb na celom svete a umožňujeme sanáciu napadnutých zariadení.

Získané informácie a poznatky sú vložené do produktov a služieb spoločnosti Microsoft



Partnerstvo medzi súkromným a verejným sektorom

Poháňa rozsah a dopad akcií

Pevné vzťahy s verejnými a súkromnými partnermi umožňujú DCU organizovať medzinárodne koordinované znefunkčnenia infraštruktúr vytvorených zločincami pomocou malwaru.

INTERPOL

FINANCIAL SERVICES ISAC

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

NCA National Crime Agency

bonn

universität wien

EUROPOL

neustar

Symantec

TREND MICRO

KASPERSKY SECURITY

Pfizer

VeriSign

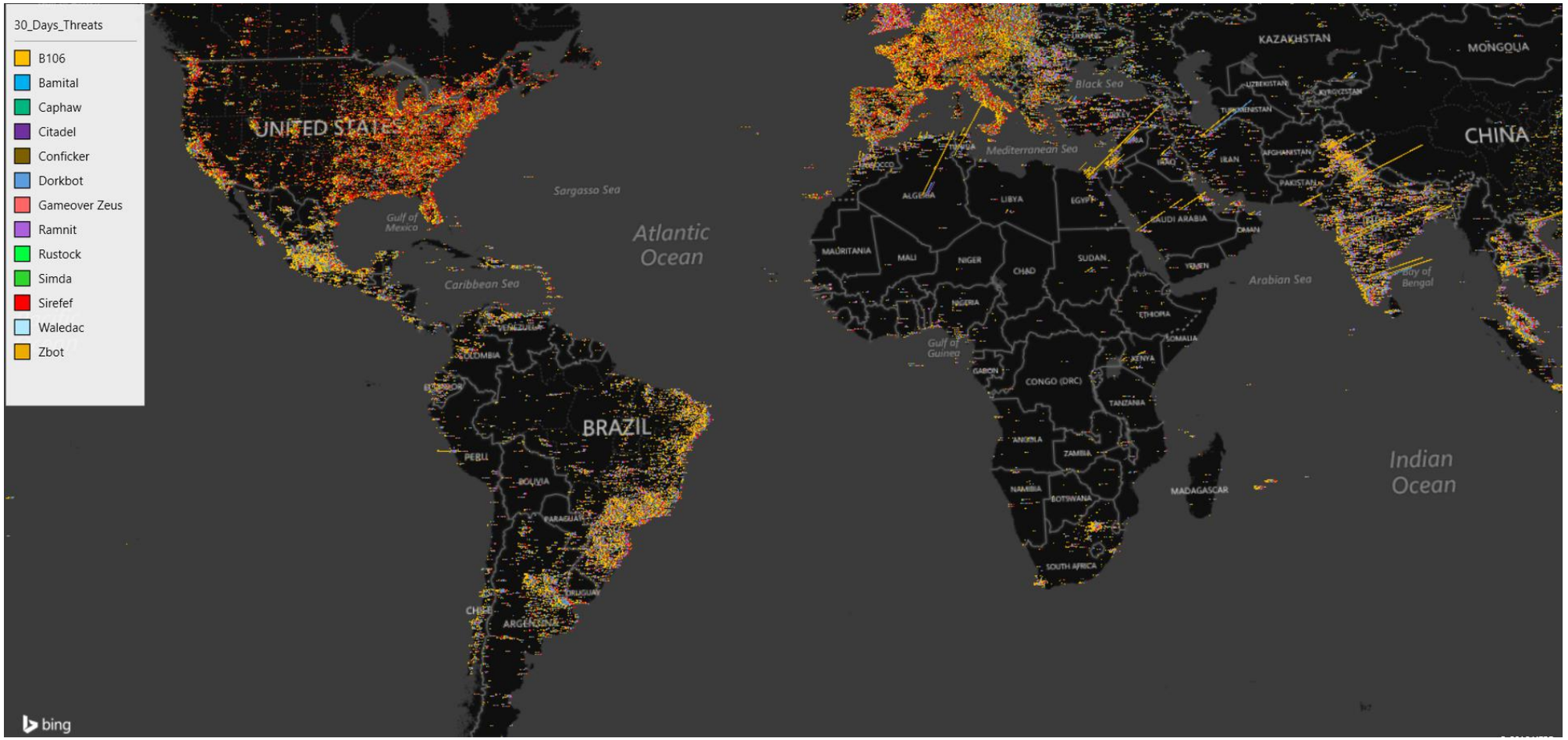
Cyber Threat Intelligence Program

cca 50 miliónov IP adries

300-400 miliónov spojení za deň

Permanentne sa meniaci objem komunikácie

Využiteľné informácie a poznatky z akcií DCU



The Microsoft **SECURITY PLATFORM**

Microsoft

Advanced Threat Analytics
Cloud App Security
Intune
Windows Server 2016
SQL Server 2016

Windows 10

Windows Trust Boot
Device Guard
Credential Guard
Microsoft Passport
Windows Hello
Windows Defender ATP
Windows Update for Business
Enterprise Data Protection

Microsoft Azure

Azure Active Directory
Azure Active Directory Premium
Azure Security Center
Azure Secure Store
Azure Key Vault

Office 365

Advanced Threat Protection
Anti-Spam / Anti-Malware
Message Encryption
Customer Lockbox
Data Loss Prevention

Government Security Program (GSP)

Spoločnosť Microsoft sa zaväzuje k budovaniu dôvery s vládami a zdieľaniu informácií majúcich vplyv na kybernetickú bezpečnosť

Government Security Program - ciele

- Pomáhať chrániť vlády a ich občanov
- Budovanie dôvery a transparentnosti
- Posilnenie partnerstva verejného a súkromného sektora

Priamy prístup k produktom Microsoftu a bezpečnostným zdrojom

- Prístup do tzv. Transparency Centers – umožnenie práce so zdrojovým kódom
- Vzdialený prístup k online zdrojovému kódu
- Technické údaje, vrátane Microsoft Azure and O365
- Zdieľanie informácií o hrozbách a zraniteľnostiach s využitím údajov z CTIPu

Chráňte si svoje IT prostredie

Osvedčené postupy

Investujte do svojej platformy	Investujte do svojho vybavenia	Investujte do svojich ľudí
Udržiavajte dobre zdokumentovaný súpis svojich IT zariadení	Získavajte / budujte nástroje potrebné k plnému sledovaniu siete, hostiteľov a protokolov	Budujte vzťahy a komunikáciu medzi tímom reakcie na incidenty a iných skupín
Zadefinujte svoju bezpečnostnú politiku s jasnými normami a pokyny	Aktívne udržiavajte kontrolné mechanizmy a opatrenia a pravidelne testujte ich presnosť a účinnosť	Prijmite princíp minimálnych správcovských privilégií; eliminujte časovo neobmedzené, pretrvávajúce admin práva
Používajte správnu IT hygienu - väčšine útokov možno predchádzať včasnou aktualizáciou záplat a antivírusu	Udržiavajte prísnu kontrolu nad politikou riadenia zmien	Využívajte ponaučenia získané analýzou z každej závažnej nehody
Používajte viacfaktorové overovania na posilnenie ochrany účtov a zariadení	Monitorujte abnormálne správanie sa účtu a poverených užívateľov	Vzdelávajte a naučte používateľov rozpoznať pravdepodobné hrozby a chápať ich úlohu pri ochrane firemných dát