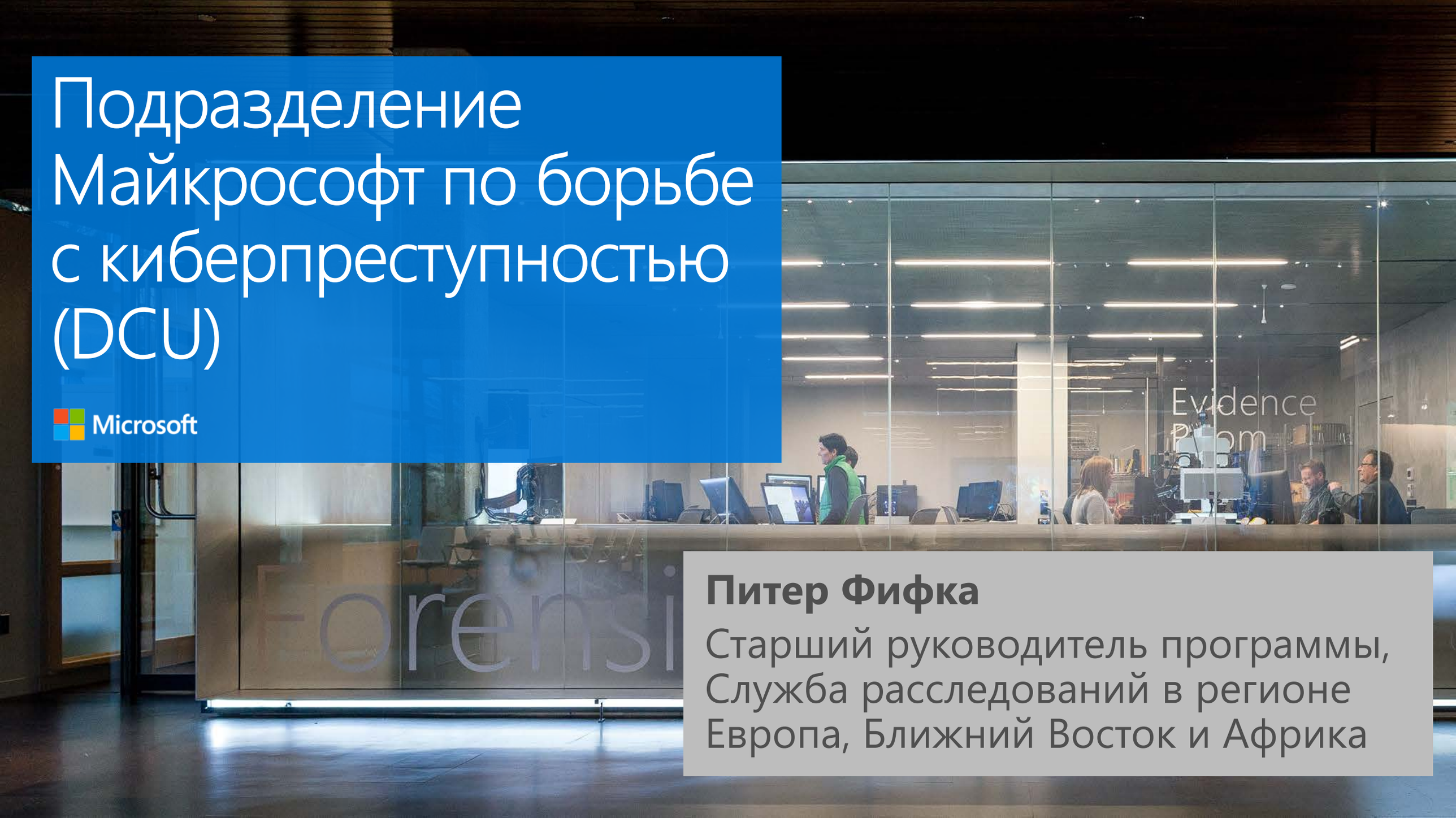
Подразделение Майкрософт по борьбе с киберпреступностью (DCU)

Microsoft



Питер Фифка

Старший руководитель программы,
Служба расследований в регионе
Европа, Ближний Восток и Африка

«Кибербезопасность – это проблема, которую необходимо решать на уровне главного исполнительного директора».

McKinsey & Co, Риски и ответственность в гипер-подключенном мире: Влияние на предприятие, январь 2014 года

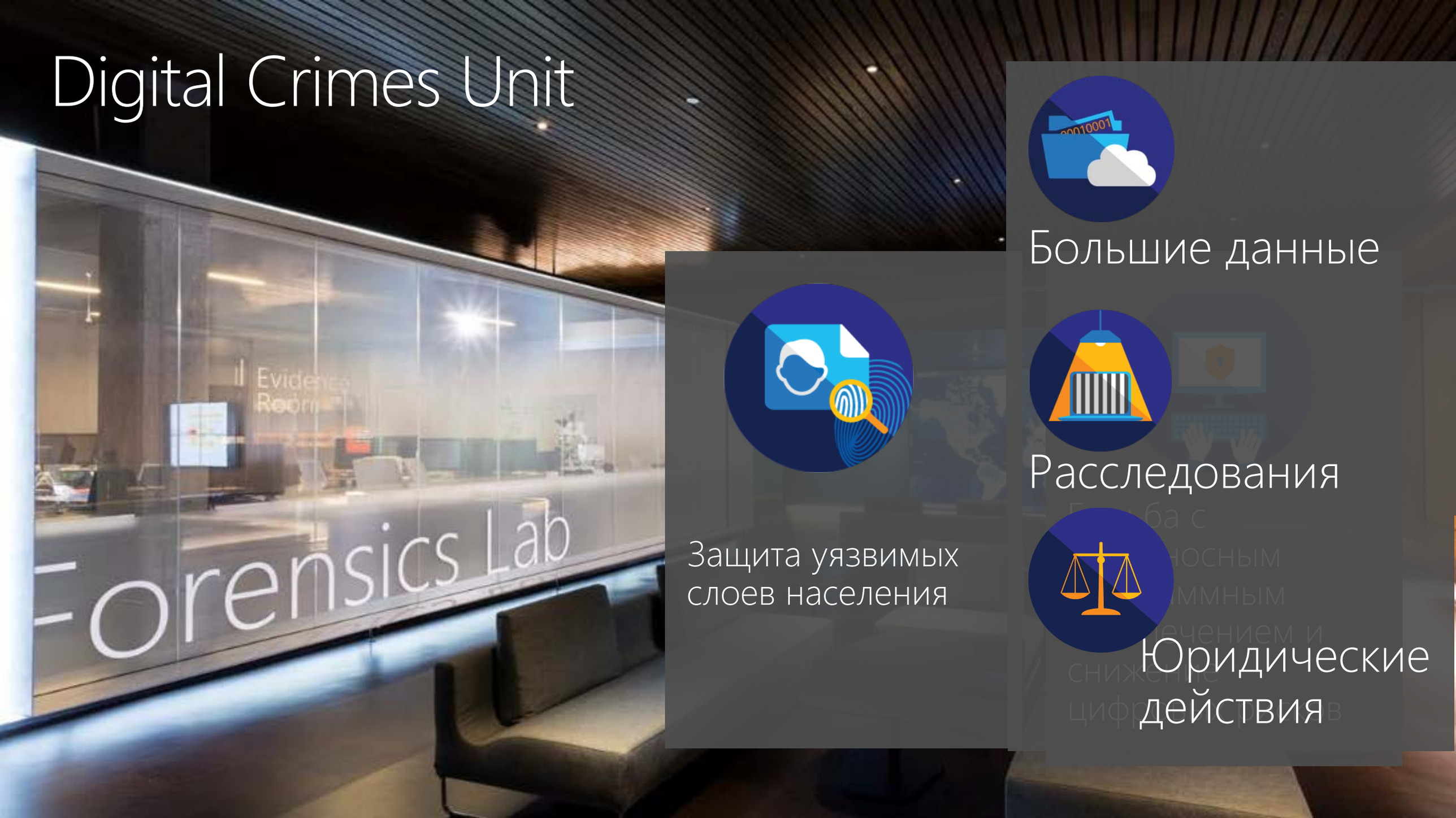
200+
дней нападавшие находятся в сети жертвы до обнаружения

140
Расчетное число стран развивающих кибер оружия

Кибер-атаки стоят $ 3 трлн в потерянной производительности и роста.

$3.5 million
Средняя стоимость утечки данных для компании (15% увеличение за год)

Digital Crimes Unit



Защита уязвимых слоев населения

Большие данные

Расследования

Юридические действия





Борьба с вредоносным программным обеспечением и снижение цифровых рисков





Microsoft leads disruption of largest infected global PC network

THE WALL STREET JOURNAL. | TECH

TOP STORIES IN TECH

You're Emailing Wrong

Twitter's Earnings: What to Watch

TECHNOLOGY

Inside the Effort to Kill a Web Fraud 'Botnet'

Working With Law Enforcement, Team Cuts Off Servers for Zombie Computers

By CHRISTOPHER S. STEWART and MERISSA MARR

Updated Dec. 5, 2013 8:55 p.m. ET

AP

THE BIG STORY

MALWARE ON NEW ...INA

LATEST NEWS

Fast-food protesters rallied at higher-pay rallies

Texas Supreme Court hears faith healing case

Legal or not, the pot business is still wacky

FAST COMPANY | DESIGN | EXIST | CREATE | LABS | FEATURES

REUTERS

REMOVE MALWARE - FREE

Quick Malware Removal in 2 minutes. Free Download (Highly Recommended)

Exclusive: Microsoft, FBI take aim at global cyber crime ring

(Reuters) - Microsoft Corp and the FBI, aided by authorities in more than 80 countries, have launched a major assault on one of the world's biggest cyber crime rings, believed to have stolen more than $500 million from bank accounts over the past six months.

Microsoft said its Digital Crimes Unit on Wednesday succeeded in taking down at least 1,000 of an estimated 1,400 malicious computer networks known as the Citadel Botnets.

Citadel infected as many as 5 million PCs around the world, according to Microsoft, was used to steal from dozens of financial institutions, including American Express, Bank of America, Citigroup, Credit Suisse, eBay's PayPal, HSBC, JPMorgan Chase, Royal Bank of Canada and Wells Fargo.

While the criminals remain at large and the authorities do not know the identities of any ringleaders, the internationally coordinated take-down dealt a significant blow to their cyber

Police shut down network 'used to steal bank details'

BBC NEWS

THE CODE

CRIMINA... UP AFTE...

MICROSOFT RECENTLY SEVERELY ... ZEROACCESS, BUT NOW IT'S SAYI... COMPLETELY.

NCA National Crime Agency

GETTY IMAGES

A network of computers that has spread malware to millions of machines has been shut down, police have said.

REUTERS

Exclusive: Microsoft ... disrupt cyber crime

KrebsonSecurity

In-depth security news and investigation

Forbes

European Cyber Police Try To Shut Down Ramnit Botnet That Infected 3 Million

British, Dutch, German and Italian police have claimed success in disrupting one of the world's biggest botnets; Ramnit. The Ramnit malware, which sought to steal victims' banking login data, was believed to have infected as many as 3.2 million Windows PCs. It is currently sitting on up to 350,000 compromised computers.

Anubis Networks, Microsoft and Symantec provided information to the law enforcement agencies, who worked together via the European Cybercrime Centre (EC3) working out of the Europol. The command and control servers for the malware have been shut down and infected users will now be cut off from Ramnit's creators, who used at least 300 web domains to control victims' machines from afar.

The Ramnit malware was spread via malicious emails and messages sent over social networks. It would steal passwords for online banking sites, spy on people's web activity, pilfer files and block anti-virus protection. Symantec noted that the group behind Ramnit has been operating for at least five years and "has evolved into a major criminal enterprise". Most victims were based in India, Indonesia and Vietnam.

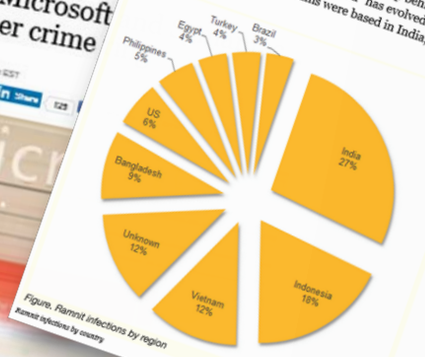


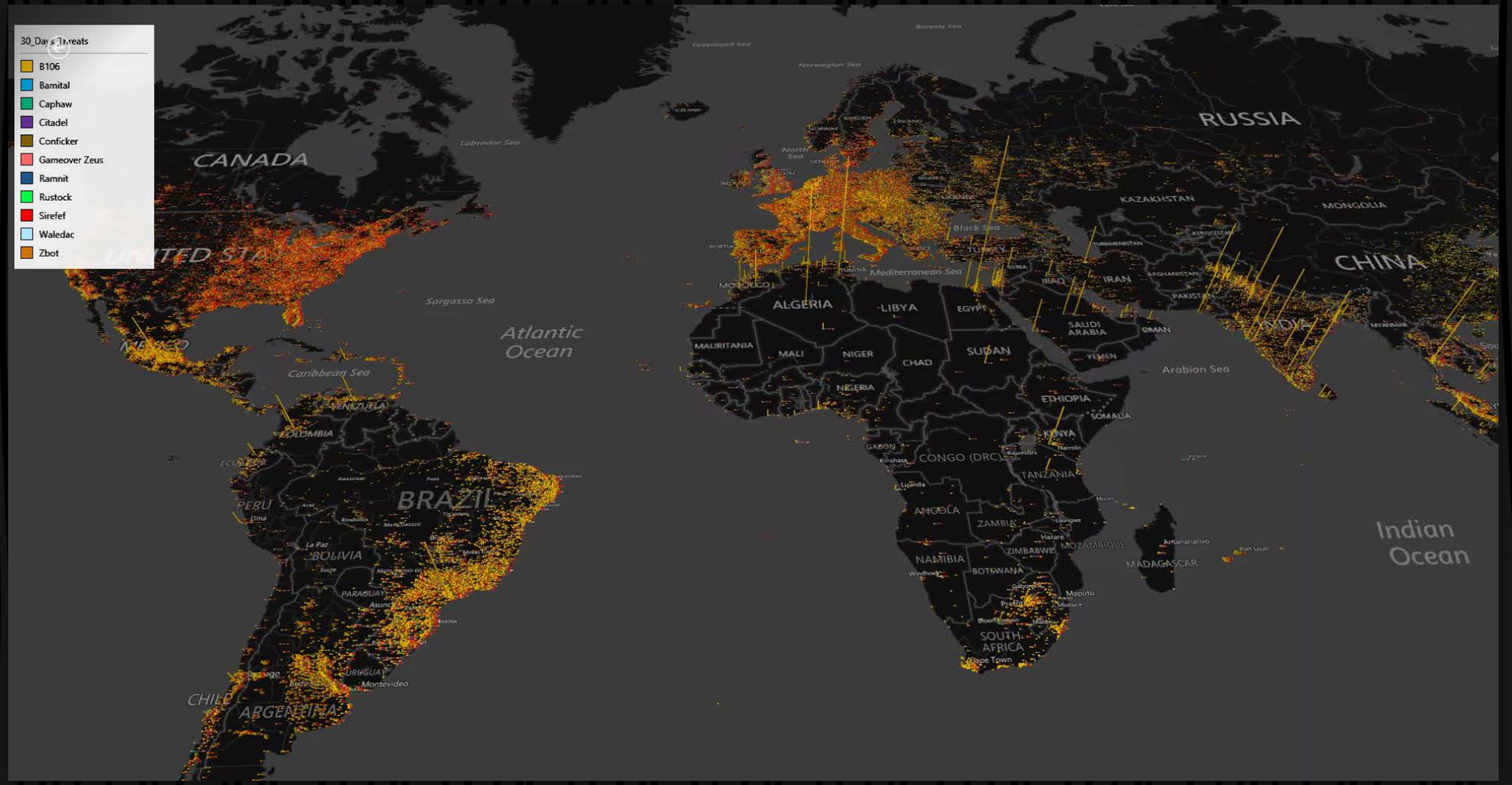
Figure. Ramnit infections by region

Программа по выявлению кибер-угроз

60 миллионов IP адресов

400 миллионов пингов в день

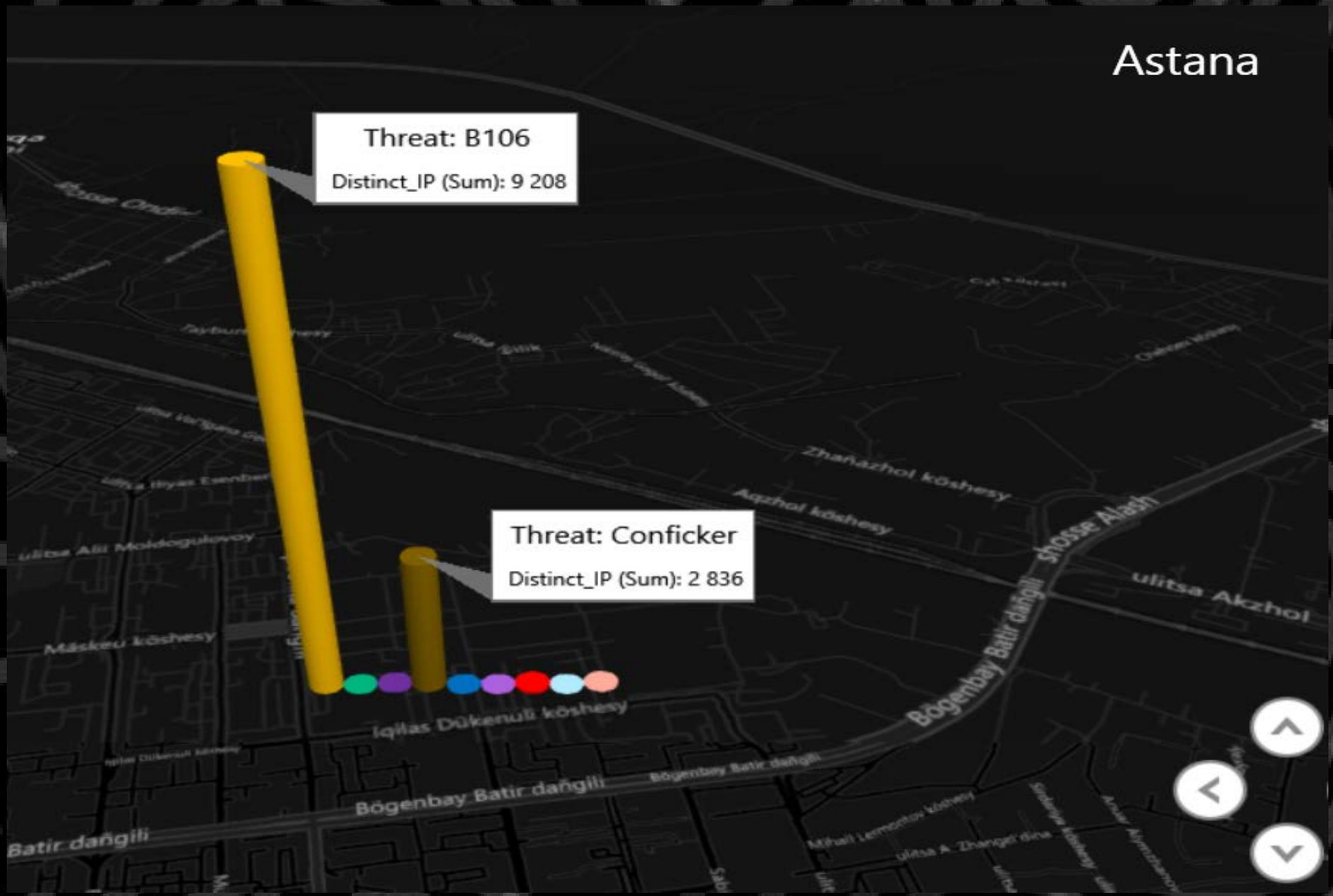
Объем постоянно меняется



Карта заражения Казахстана: 24.08. – 19.09. 2015

Алматы: 24.08 -19.09. 2015

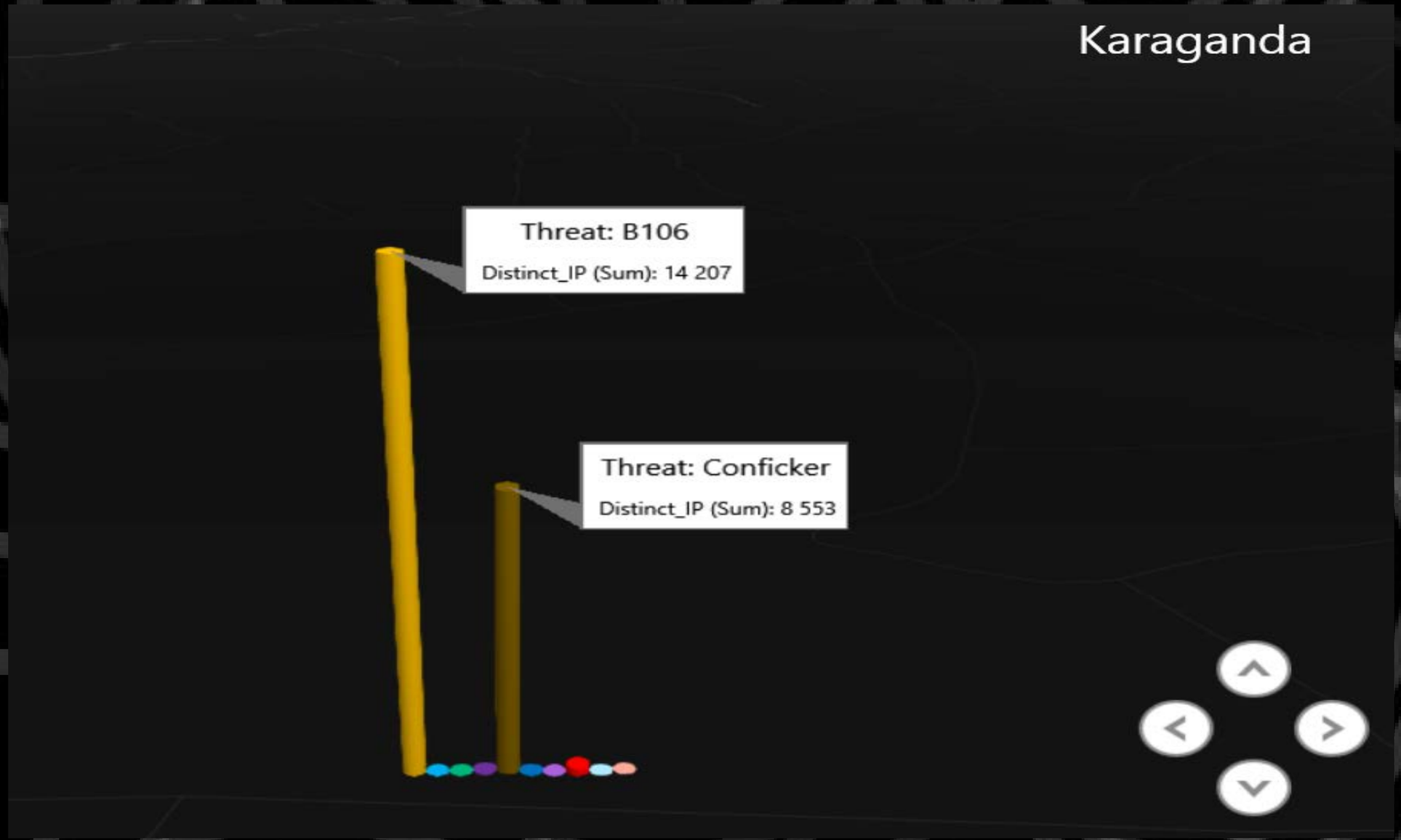
Астана: 24.08 -19.09. 2015



Threats 30 - Days

- B106
- Bamital
- Caphaw
- Citadel
- Conficker
- Gameover Zeus
- Ramnit
- Simda
- Sirefef
- Waledac
- Zbot

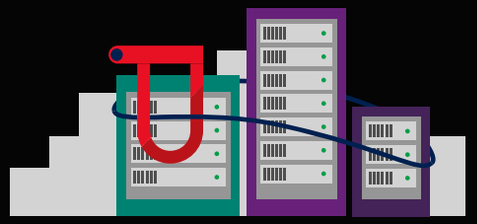
Караганда: 24.08 -19.09. 2015



Наиболее распространенные виды вредоносного программного обеспечения в Казахстане

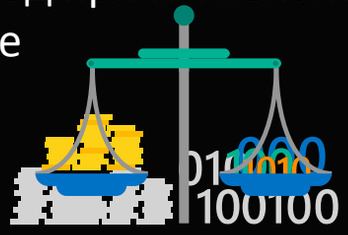
Conficker
26 874 IP адреса

Ботнет-червь, рассылающий спам и пытающийся украсть конфиденциальные данные и пароли



ZeroAccess/Sirefef
1 523 IP адреса

ZeroAccess использовал результаты поиска, направляя жертв на опасные сайты
Ущерб для онлайн-рекламодателей превышал 2,7 млн. долл. США в месяц
Кликфрод при контекстной рекламе



Bladabindi & Jenxcus
97 476 IP адрес

Вредоносное ПО, использующее Dynamic DNS для создания команд.
Включало кражу пароля и личных данных, веб-камеру и т.д.
Использовало более 200 различных типов вредоносного ПО.
Кража идентификационных данных/финансовое мошенничество/вторжение в частную жизнь

Ramnit
627 IP адрес

Модульное вредоносное программное обеспечение, которое крадет информацию об идентификации пользователя с интернет-сайтов банков.
Конфигурировано таким образом, что прячет само себя.
Кража идентификационной информации / отключение систем безопасности

Технологии сегодня

Облачные вычисления

Уже не будущее информационных технологий, а их настоящее

Трансформация ИТ: «лицом к пользователю»

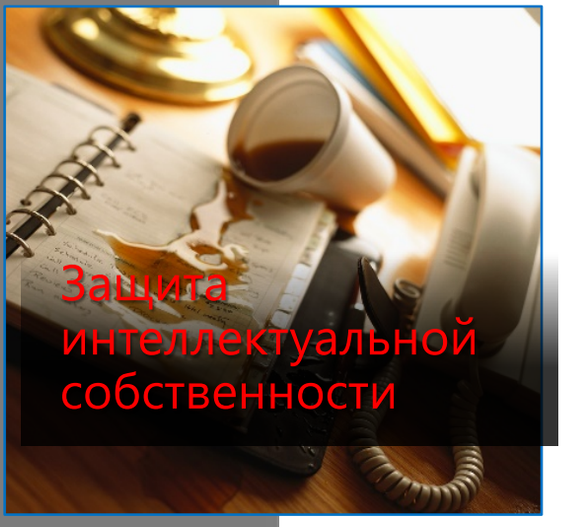
3.3 устройства на каждого пользователя в этом году

Новые модели приложений и социального взаимодействия

Социальные сети проникают в деятельность организаций

Взрывной рост данных

Объем данных удваивается каждые два года



Цифровые риски

Физические лица и/или компании подвергают свои сети и устройства цифровому риску каждый раз, когда они устанавливают и используют нелицензионное программное обеспечение

Риски могут включать без ограничения взлом систем ИТ безопасности, повышенные риски заражения вредоносным ПО, а также увеличение расходов

Microsoft придерживается принципов распространения информации, процессов и рекомендаций, позволяющих снизить предрасположенность клиентов к риску

«27% сотрудников устанавливали собственное ПО на рабочие компьютеры, что составляло почти 20% пиратского программного обеспечения на предприятиях»

«Компании потратят 127 млрд. долл. США на вопросы обеспечения безопасности как следствие установки нелицензионного ПО, содержащего вредоносное ПО»

«Компании потратят дополнительно 364 млрд. долл. США на защиту от уязвимости данных, являющейся следствием установки нелицензионного ПО, содержащего вредоносное ПО»

IDC
Analyze the Future

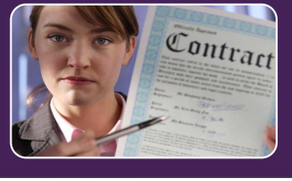
Управление программными активами (Software Asset Management) позволяет

Внедрить эффективные меры по управлению, контролю и защите активов ПО

Достоверно знать, какие технологии и активы есть в наличии, как они используются

Устранить ненужные расходы

Повысить отдачу от ПО и всего персонала организации

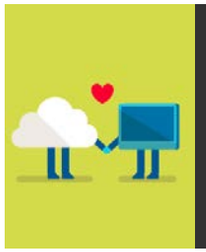


Существенно снизить риски, в том числе и юридические

SAM – международный отраслевой стандарт ISO/IEC 19770-1

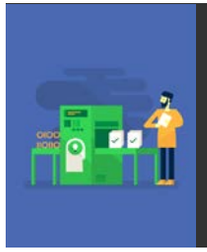
Microsoft

Виды SAM проектов

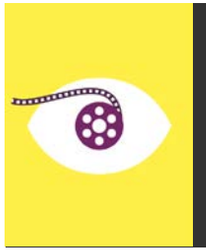


Подготовка к переходу на облачные сервисы

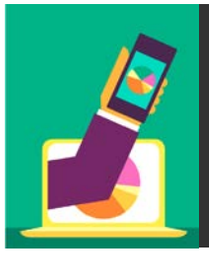
Виртуализация



SQL среда



Непродуктивная среда



Управление мобльными устройствами

Cybersecurity