Microsoft

Cyber in a World of Cloud

...and the new physics of defense

John Lambert, @JohnLaTwC
Microsoft Threat Intelligence Center

邵江宁，微软中国首席安全官

Microsoft
Threat
Intelligence
Center

Three Interacting Trends

The Race for Mastery of the Cyber Domain

- Militarization of cyber space
  - The "5th domain"
- Geopolitics increasingly colors national views
  - Data sovereignty
- Supply chain attacks
- Cyber trickle down

Three Interacting Trends

The new form factors: Dual core, WiFi, Bluetooth, runs Linux

OneDrive
- 12 billion files

Skype is the largest long distance provider
- 2 Billion mins/day

O365
- 32M paid seats, 600K paid tenants
- 35 PB of email data
- 15B messages per month

Outlook.com
- 400 Million active users

The Race for the Mastery of the Cyber Domain

- Miniaturization is shrinking computing form factors, all powered by cloud services
- SMB and Enterprises seeking IT services through SaaS
- Adversaries and threats following them to the cloud
- Customers adapting to cloud threats

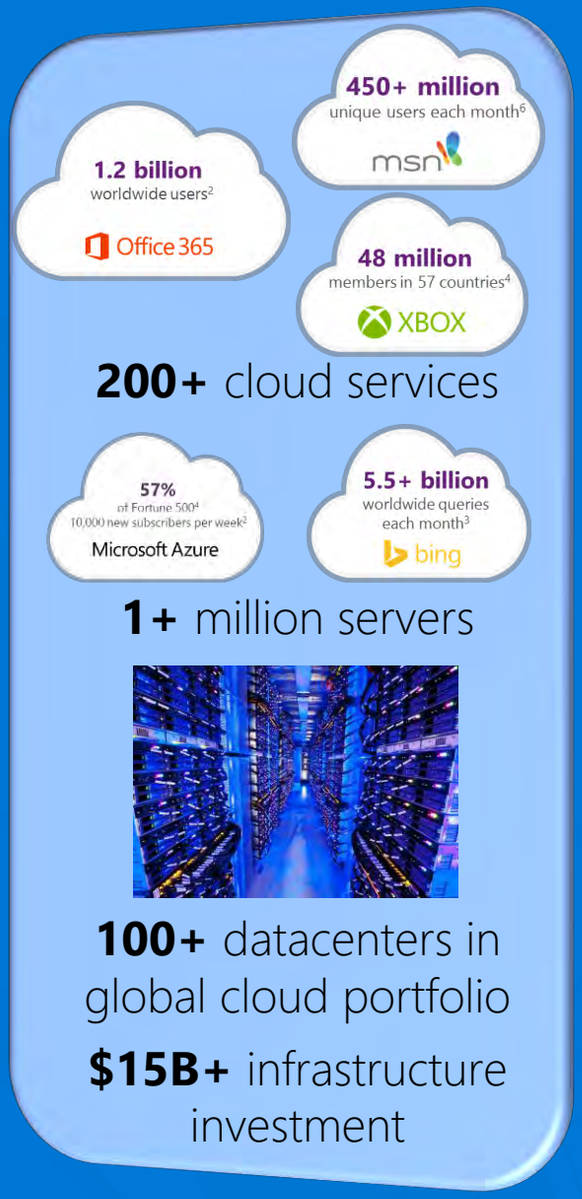
Adversaries following customers to the cloud

Three Interacting Trends

The Race for the Mastery of the Cyber Domain

Hyperscale clouds fueling defense innovation

- Demand for SaaS driving hyperscale cloud growth
- Brings economic dividend driving down prices in compute, storage, and networking
- Defenders harnessing new capabilities
- Some skillsets finding new life in cyber



Collecting cybersecurity data across Microsoft's global sensors

Exchange

More than **35 billion** messages scanned monthly

Daily tracking of **600,000** addresses sending spam

Windows

More than **250 million** users worldwide

Microsoft Security Essentials

Millions of consumers protected worldwide

Performs **billions** of malware removals per year worldwide

Microsoft System Center

Millions of computers running Microsoft enterprise anti-malware solutions

Outlook.com

More than **420 million** active users

Malicious Software Removal Tool

700 million computers reporting monthly

More than **40 billion** executions since 2005

Bing

18+ billion web-page scans per month

Microsoft Azure

1 billion customers across enterprise and consumer segments

200+ cloud services

Cyber & Cloud Providers

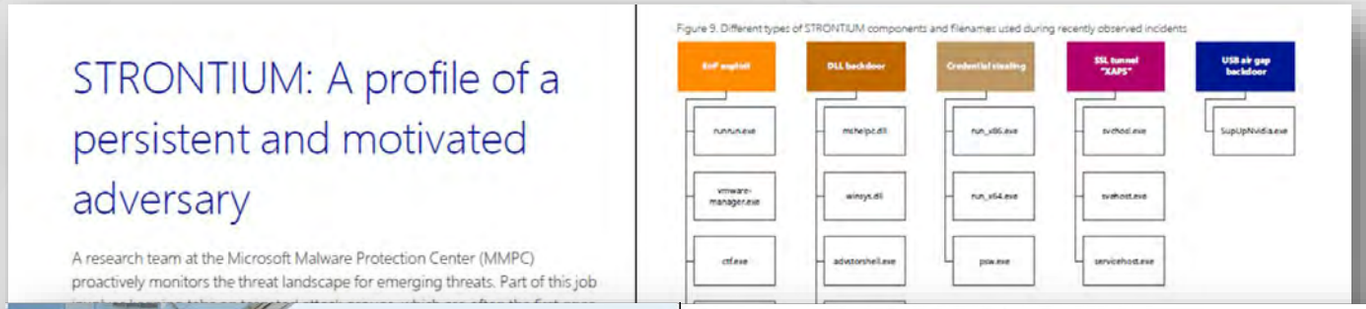
- Tenants bring their adversaries with them
  - Adversaries follow their targets from on-prem to the cloud
  - Customers may not be used to threats that they see in the cloud
- Innovate in defense by harnessing economic trends
  - Hyperscale cloud investments dropping costs in compute, storage, networking
  - Store richer data, from more layers, for longer and process it with richer algorithms
- We can use the cloud to protect itself
  - An attack on one tenant protects all tenants
  - Cloud services can protect each other

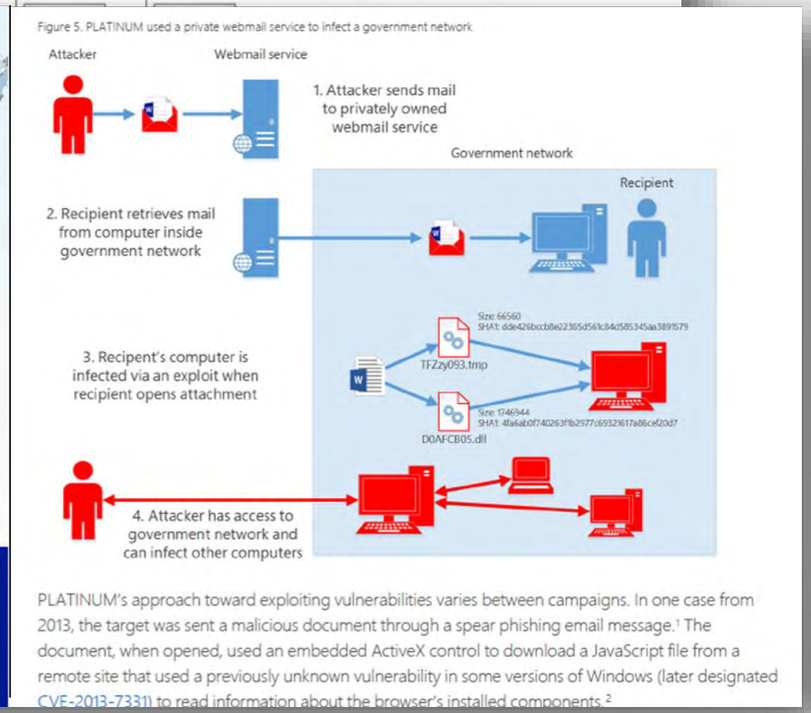
Tenants bring their adversaries with them

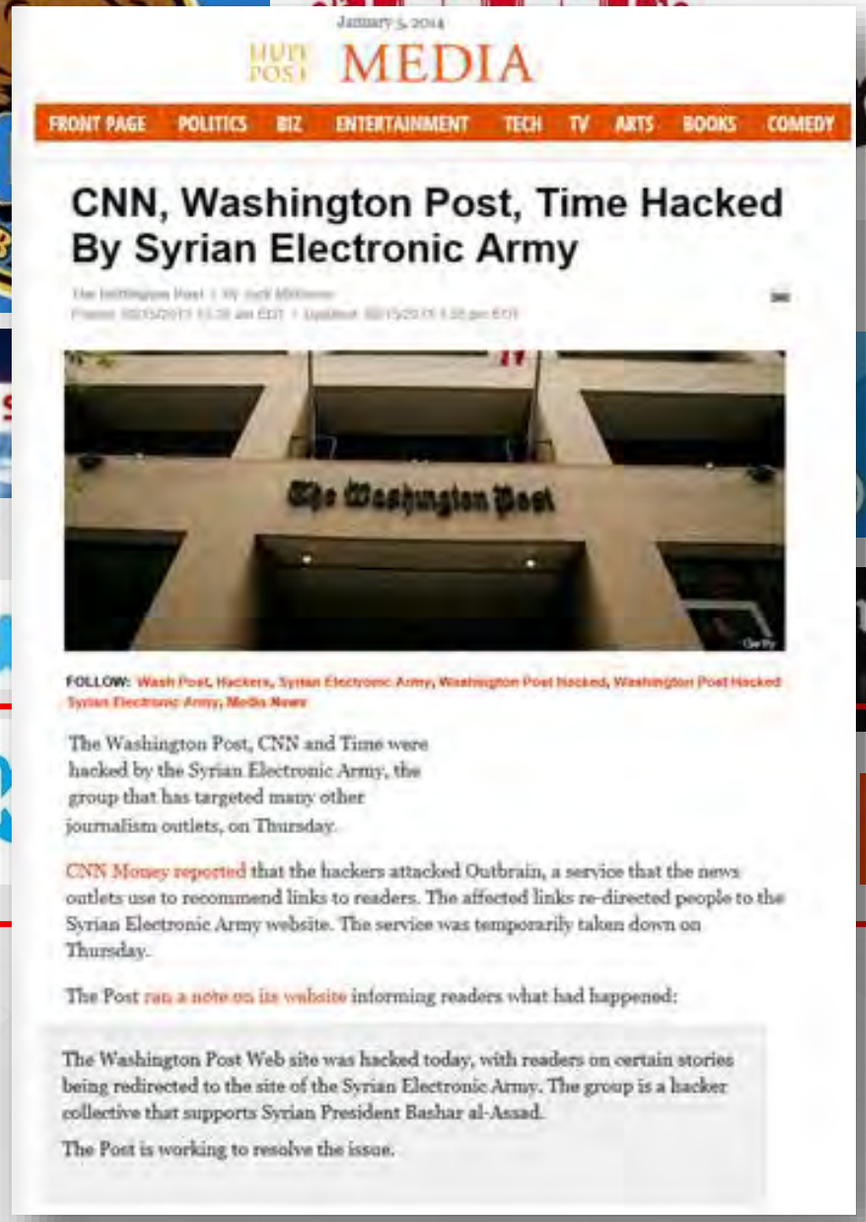
Tracking Adversaries

70 Targeted adversaries tracked in total

Actor Code Name	Industry Name
B BORON	APT3
He HELIUM	APT17
C CARBON	Wild Neutron
Sc SCANDIUM	APT8, APT18







January 5, 2014

HUFF POST MEDIA

FRONT PAGE | POLITICS | BIZ | ENTERTAINMENT | TECH | TV | ARTS | BOOKS | COMEDY

CNN, Washington Post, Time Hacked By Syrian Electronic Army

FOLLOW: Wash Post, Hackers, Syrian Electronic Army, Washington Post Hacked, Washington Post Hacked Syrian Electronic Army, Media News

The Washington Post, CNN and Time were hacked by the Syrian Electronic Army, the group that has targeted many other journalism outlets, on Thursday.

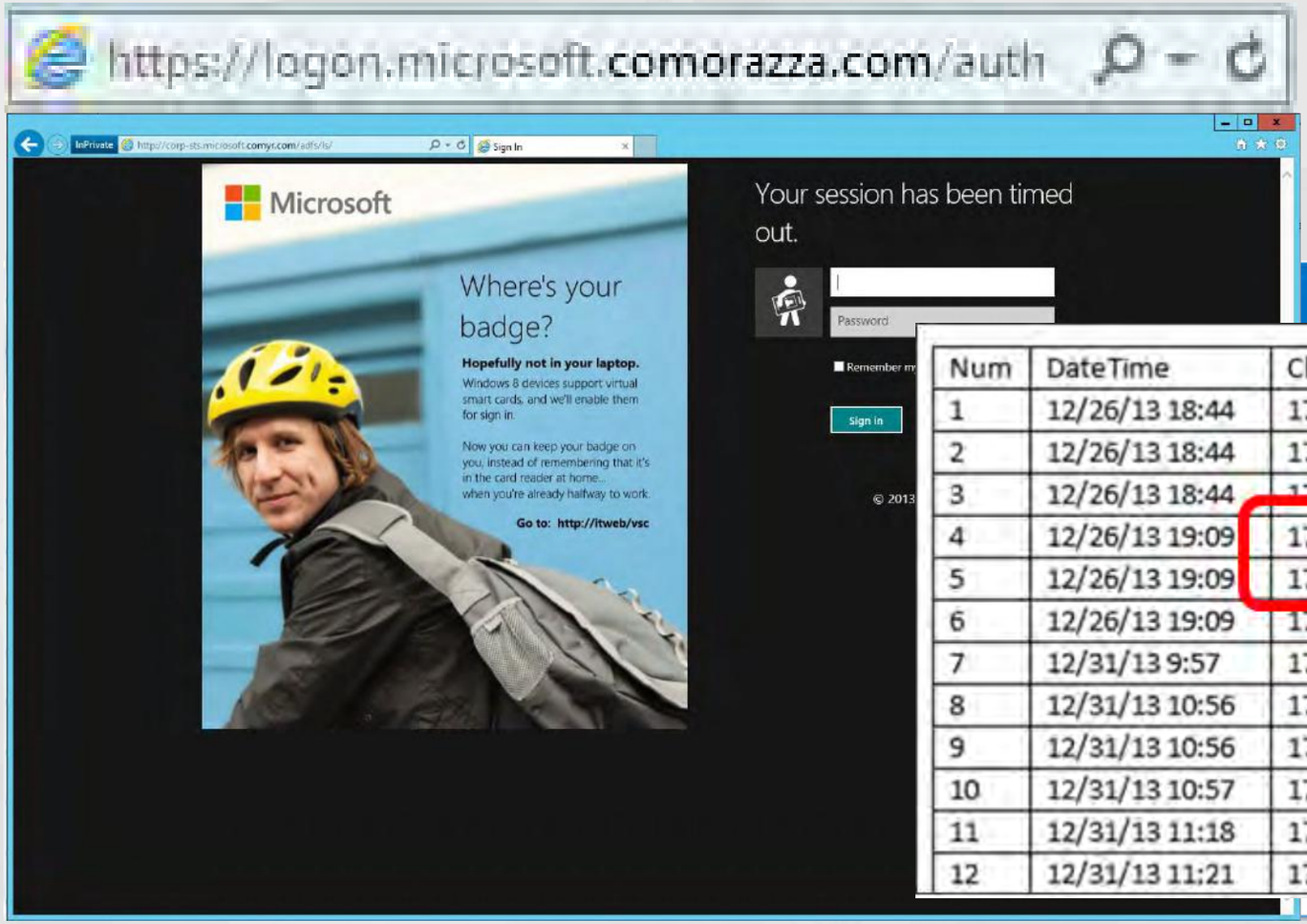
CNN Money reported that the hackers attacked Outbrain, a service that the news outlets use to recommend links to readers. The affected links re-directed people to the Syrian Electronic Army website. The service was temporarily taken down on Thursday.

The Post ran a note on its website informing readers what had happened:

> The Washington Post Web site was hacked today, with readers on certain stories being redirected to the site of the Syrian Electronic Army. The group is a hacker collective that supports Syrian President Bashar al-Assad.
>
> The Post is working to resolve the issue.

SEA Attack

Phish for Credentials

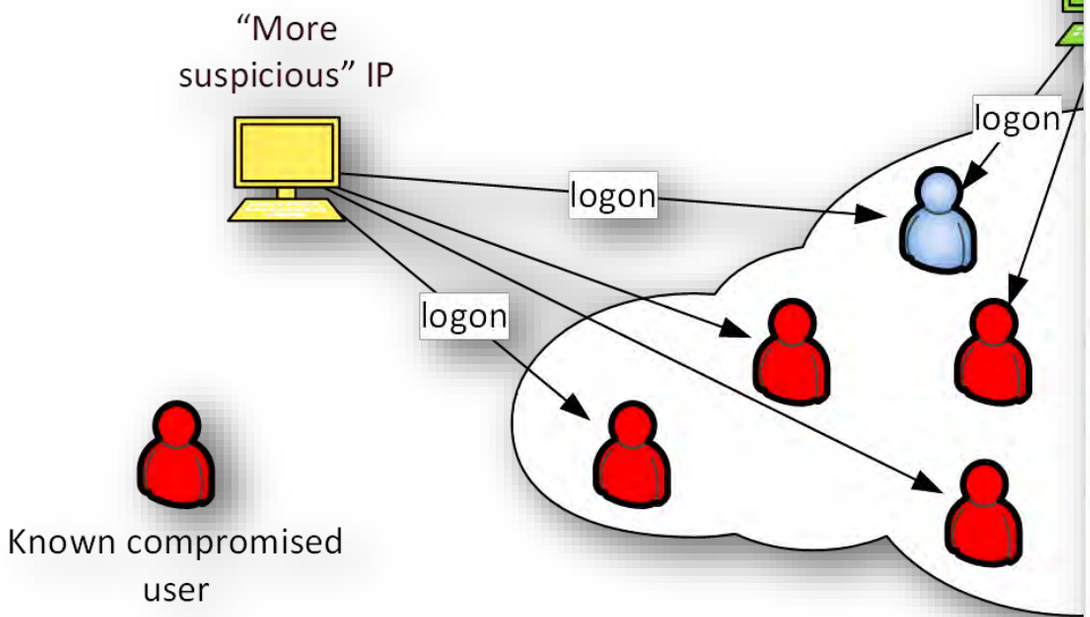


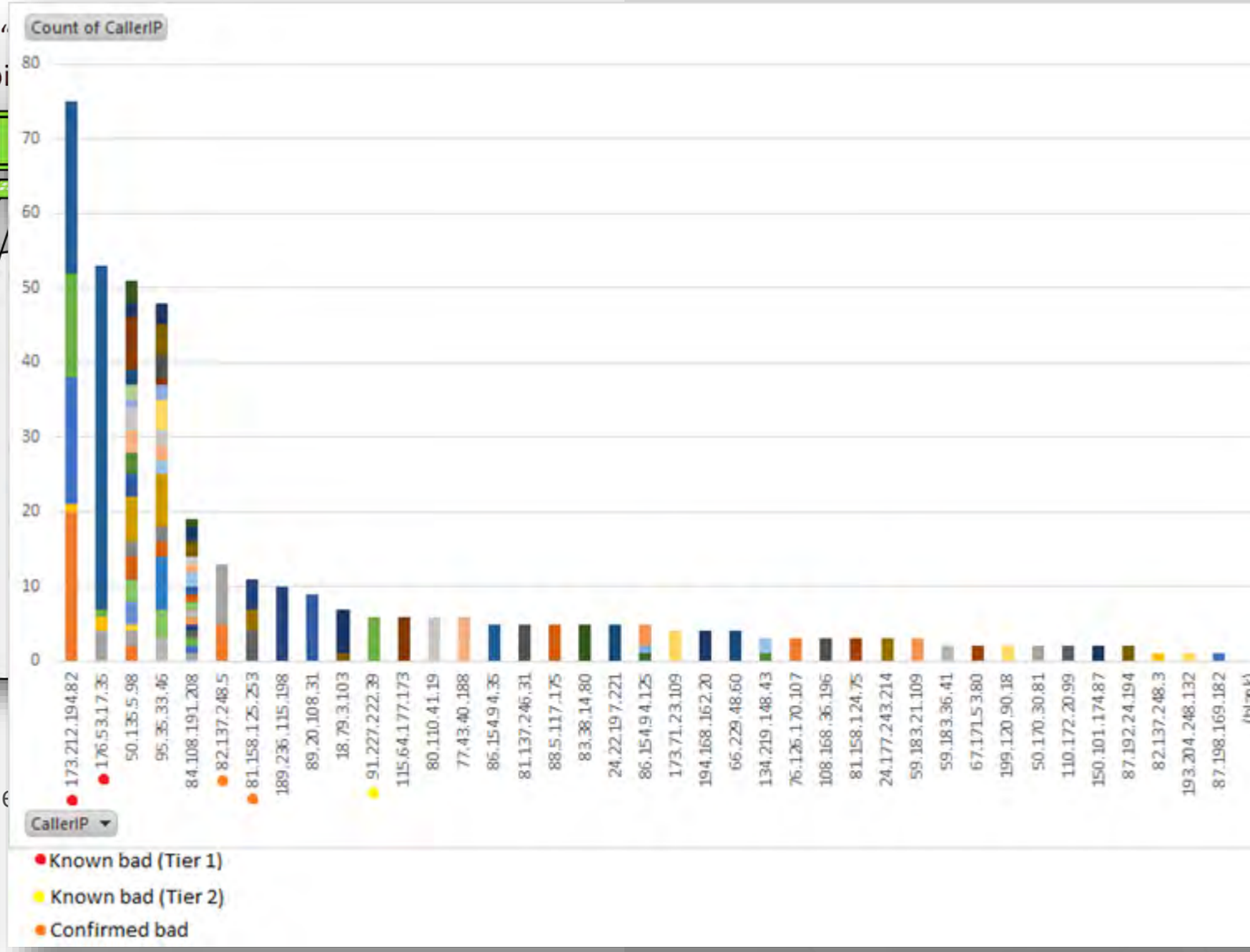
Reconnaissance

https://login.microsoftonline.com/getuserrealm.srf?login=xxx@yyy.com&xml=1

```
<RealmInfo Success="true">
        <State>3</State>
        <UserState>2</UserState>
        <Login>xxx@yyy.com</Login>
        <NameSpaceType>Federated</NameSpaceType>
```

Num	DateTime	ClientIP	HTTP_Method	Endpoint	QueryString_Snippet
1	12/26/13 18:44	173.212.194.82	GET	/GetUserRealm.srf	login=gordon@xbox360.com
2	12/26/13 18:44	173.212.194.82	GET	/GetUserRealm.srf	login=gordon@xbox360.com
3	12/26/13 18:44	173.212.194.82	GET	/GetUserRealm.srf	login=gordon@microsoft.com
4	12/26/13 19:09	173.212.194.82	GET	/GetUserRealm.srf	login=gg@xbox.com
5	12/26/13 19:09	173.212.194.82	GET	/GetUserRealm.srf	login=gg@xbox360.com
6	12/26/13 19:09	173.212.194.82	GET	/GetUserRealm.srf	login=gordon@xbox.com
7	12/31/13 9:57	176.53.17.35	GET	/GetUserRealm.srf	login=i-lasakr@microsoft.com
8	12/31/13 10:56	176.53.17.35	GET	/GetUserRealm.srf	login=dd@micrososft.com
9	12/31/13 10:56	176.53.17.35	GET	/GetUserRealm.srf	login=dd@microsoft.com
10	12/31/13 10:57	176.53.17.35	GET	/GetUserRealm.srf	login=gg@microsoft.com
11	12/31/13 11:18	176.53.17.35	GET	/GetUserRealm.srf	login=f@microsoft.com
12	12/31/13 11:21	176.53.17.35	GET	/GetUserRealm.srf	login=f@microsoft.com





Formula

$risk(IP) = \max(\sum_{U \in Owned} LogonExists(IP, U)$ - $\sum_{U \in$

where $LogonExists: (IP, U) \rightarrow \{0, 1\}$

Azure Active Directory Geo-Anomalous Login Detection

1st party == 3rd party