Today's Presenter: Jim Banach

NA Practice Group Lead, Modern Workplace

Has been with New Signature since 2005

Over 30 Microsoft Certifications, including Microsoft Certified Systems Engineer, Microsoft Certified IT Professional, Microsoft Certified Technology Specialist, and Microsoft Certified Systems Engineer: Security.
Catching and Cleaning Phish

Hi,

Thanks for using ITSolutions. We are currently undergoing a major upgrade to our product line and have a new service that we think you'll be interested in. Our new Enterprise Package includes a number of updates, such as premium support, improved data analysis, and state of the art security features.

Currently, this service is being offered as a free trial. To update your account, simply click the link below.

www.itservices.com/enterprise

This is a limited time offer, so be sure to act quickly.

Thank you,
James Robinson
IT Solutions Sales Executive

IT SERVICES
Protect business critical data
Most security experts agree that email remains the #1 attack vector

- 400 Billion emails analyzed every month in Office 365
- ~57% of all email traffic is spam (Mar ‘17)²
- 6000% increase in ransomware-infected emails (2016-2017)¹

Large attack surface
Majority of email negatively impacts productivity
The threat level is increasing
Protect leveraging Machine Learning Models identifying phish lures

Learning from the good and bad

- Millions of samples
- Model generation

Applying what we learned

- Base protection
  - ML Model
  - Good - Inbox
  - Bad - Phish action
Protect with Office 365 ATP enhanced Anti-phish Capabilities

Domain Spoof
- DMARC, DKIM
- SPF
- Intra Org spoof
- Cross domain spoof

Compromised
- Compromised account

Impersonation
- Look alike domains
- Display name tricks

Content
- Attachments
- URLs
- Text

Standard protection
- Implicit Spoof Protection; DMARC; SPF
- Content based protection
- URL verification against known phishing lists
- Safety Tips for mails detected as phish
- Inline Reporting

Advanced protection
- Machine Learning Models
- Time of Click Protection (Safe links)
- Detonation of Content
- Users contact graph
### Office 365 Phish Protection Stack *(Enhanced)*

#### Mail Flow Protection
- **Sender Authentication Checks**
- **Implicit Intra Org Domain Spoof Detection**
- **ATP Implicit External Domain Spoof Detection**
- **ATP User Intelligence**
- **ATP User Impersonation Detection**
- **ATP Domain Impersonation Detection**
- **URL Reputation Scan**
- **AV Engine Scan**
- **Phish Content Analysis Heuristics/Rules**
- **Windows 10 based Rep Scan**

#### Post Delivery Protection
- **ATP Safe link Time of click Protection**
- **ATP Heuristic Clustering**
- **ATP ZAP**
- **ATP block of attachments with bad URLs**
- **ATP Attachment Detonation for phishing**

#### Detect & Respond
- **Client Tips for Suspicious Mails**
- **Tenant Block URL for Safe links**
- **Monitor for risky user/App activity**
- **Threat Explorer**
- **Rich Reports & Insights**
- **Explore malicious submissions in Threat Explorer**

---

*New: Safe link for Internal Mail*

*New: ATP block of attachments with bad URLs*

*New: Windows 10 based Rep Scan*

*Enhanced: Safe link for Office Clients*
Protect your data

• **Advanced Threat Protection Safe Attachments**: detonating malicious attachments
Protect: Admins can create enhanced **Anti-impersonation settings**

- User impersonation
- Domain impersonation
- Mailbox Intelligence
Protect with Mailbox Intelligence

- First Contact Graph
- Machine Learning
- Provides tip when email is received from for first time from address
**Protect**: Admins can apply internal safe links for intra-org emails

- Protects against compromised accounts
- Only security service that can do intra-org link analysis within compliance boundary of Office 365
- Easily enabled
Protect: Admins can apply sophisticated anti-spoof settings
The User Experience
Announcement: Azure Databricks unit reservations now available

To Jeff Dunmoll

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Microsoft Cloud Yammer Community

Tram Nguyen (The Spur Group Inc) posted a new announcement in CSP Yammer Partner Community

Azure Databricks unit reservations now available

Impacted audience
All CSP partners

Summary
Microsoft is excited to introduce Azure Databricks unit reservations for the Cloud Solution Provider.
This sender might be impersonating a domain that's associated with your organization. Learn why this could be a risk Feedback

Your user account is going to be disabled. Login now to prevent suspension.

Go to the sign-in page, https://portal.office.com

Sincerely,
The Microsoft Office 365 Team

This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager.

This message was sent from an unmonitored e-mail address. Please do not reply to this.
This website has been classified as malicious.

Opening this website might not be safe.

http://spamlink.contoso.com

We recommend that you don’t open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

X Close this page

Continue anyway (not recommended)

Powered by Office 365 Advanced Threat Protection
Investigating Phish in Office 365
### Message trace

Run a message trace to track the flow of email messages in your organization. This can help you troubleshoot mail flow issues by determining if messages were received, rejected, deferred, delivered, and more. Learn more about message trace

**Start a trace**

<table>
<thead>
<tr>
<th>Queries Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default queries (1)</td>
<td>Queries provided by Office 365</td>
</tr>
<tr>
<td>Custom queries (1)</td>
<td>Queries created and saved by admins in your organization</td>
</tr>
<tr>
<td>Autosaved queries (1)</td>
<td>Last 10 queries that were run but not saved manually</td>
</tr>
<tr>
<td>Downloadable reports (1)</td>
<td>Downloadable message trace reports (completed and pending)</td>
</tr>
</tbody>
</table>
Run a message trace to track the flow of email messages in your organization. This can help you troubleshoot mail flow issues by determining if messages were sent and received as expected.

- **Start a trace**
- **Refresh**

**Default queries (1)**
- Queries provided by Office 365

**Custom queries (1)**
- Queries created and saved by admins in your organization

**Autosaved queries (0)**
- Last 10 queries that were run but not saved manually

**Downloadable reports (0)**
- Downloadable message trace reports (completed and pending)

**Find messages that were sent:**

- By these people
- To these people

Within this time range (UTC 07:00) - DST

**Message ID**

**Direction**

Original client IP address

Choose report type

- Summary report

Search | Save | Cancel
Run a message trace to track the flow of email messages in your organization. This can help you troubleshoot mail flow issues by determining if messages were sent, received, or if they failed.

**New message trace**

- **Find messages that were sent:**
  - By these people: All senders
  - To these people: A@john.com
  - Within this time range (UTC 07:00 - 12:00 DST): 1 day

**Delivery status**
- All
- Delivered
- Pending
- Expanded
- Failed
- Quarantined
- Filtered as spam
- Getting status

**Original client IP address**

- **Choose report type:** Summary report

**More search options**

**Home > Message trace**
Run a message trace to track the flow of email messages in your organization. This can help you troubleshoot mail flow issues by determining if messages were sent, delivered, or failed to deliver.

**Find messages that were sent:**
- By these people:
  - All senders
- To these people:
  - An@W@BRITISH.COM

**Within this time range (UTC 07:00) - DST**
- Last 2 days (from 07/14 07:00 to 07/16 07:00 UTC)

**More search options**
- Delivery status:
  - Delivered
- Message ID
- Direction:
  - All
- Original client IP address

**Choose report type**
- Summary report
Automated Detection, Investigation & Remediation with Microsoft Threat Protection
## View Alerts

<table>
<thead>
<tr>
<th>Severity</th>
<th>Alert Name</th>
<th>Status</th>
<th>Category</th>
<th>Activity count</th>
<th>Last occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Weaponized URL in mail</td>
<td>Resolved</td>
<td>Threat Management</td>
<td>1</td>
<td>4 hours ago</td>
</tr>
<tr>
<td>Medium</td>
<td>Unusual volume of external file sharing</td>
<td>Active</td>
<td>Data Governance</td>
<td>1</td>
<td>3 hours ago</td>
</tr>
<tr>
<td>Medium</td>
<td>Mass download</td>
<td>Resolved</td>
<td>Data Loss Prevention</td>
<td>1</td>
<td>2 hours ago</td>
</tr>
<tr>
<td>High</td>
<td>Risky sign-in from unknown location</td>
<td>Resolved</td>
<td>Threat Management</td>
<td>1</td>
<td>2 hours ago</td>
</tr>
</tbody>
</table>
Weaponized URL in mail discovered by Office 365 ATP

Investigation #11371 is complete - Remediated

Emails investigated (53)
  Intra-org Phish (6)

Users investigated (5)
  Users impacted (1):
    Jeffs@ignitedaemon.com

Anomalies detected (2):
  Suspicious login (1)
  Mass downloads (1)

Machines (1)
  Compromised Device - Malware (1)

Actions
  Remediated
    URL Blocked (1)
    Emails Deleted (6)
    User Password Reset (1)
    MFA enabled (1)
## Weaponized URL in mail discovered by Office 365 ATP

Investigation #11371 is complete - Remediated

### Investigation graph

<table>
<thead>
<tr>
<th>Alert Name</th>
<th>Service</th>
<th>Severity</th>
<th>Status</th>
<th>Impacted User</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weaponized URL in mail</td>
<td>Exchange Online</td>
<td>High</td>
<td>Resolved</td>
<td><a href="mailto:jeff@Ignitedemo.onmicrosoft">jeff@Ignitedemo.onmicrosoft</a>...</td>
<td>Triggering alert</td>
</tr>
<tr>
<td>Risky sign-in from unknown location</td>
<td>Azure Active Directory</td>
<td>High</td>
<td>Resolved</td>
<td><a href="mailto:jeff@Ignitedemo.onmicrosoft">jeff@Ignitedemo.onmicrosoft</a>...</td>
<td>Correlated alert: User at risk</td>
</tr>
<tr>
<td>Mass download</td>
<td>SharePoint Online</td>
<td>Medium</td>
<td>Resolved</td>
<td><a href="mailto:jeff@Ignitedemo.onmicrosoft">jeff@Ignitedemo.onmicrosoft</a>...</td>
<td>Correlated alert: Data at risk</td>
</tr>
</tbody>
</table>
Weaponized URL in mail discovered by Office 365 ATP

Investigation #11371 is complete - Remediated

Investigation graph  Alerts  Email  Users  Machines  Entities  Log  Actions

Cluster  Verdict  Directionality  Submissions  Total  Malware  Phish  Delivered  Junked  Replaced  Blocked
URL, Sender, Subject  Phish  Intra-org  0  6  0  0  6  0  0  0
Sender domain, IP  Clean  Inbound  0  12  0  0  12  0  0  0

<table>
<thead>
<tr>
<th>Date</th>
<th>Subject</th>
<th>Recipient</th>
<th>Sender</th>
<th>Sender IP</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/19/18 10:14AM</td>
<td>Project details requested - September Update</td>
<td><a href="mailto:Ron@IgniteDemo.onmicrosoft.com">Ron@IgniteDemo.onmicrosoft.com</a></td>
<td><a href="mailto:Jeff@IgniteDemo.onmicrosoft.com">Jeff@IgniteDemo.onmicrosoft.com</a></td>
<td>13.70.184.243</td>
<td>Delivered</td>
</tr>
<tr>
<td>9/19/18 10:14AM</td>
<td>Project details requested - September Update</td>
<td><a href="mailto:Bob@IgniteDemo.onmicrosoft.com">Bob@IgniteDemo.onmicrosoft.com</a></td>
<td><a href="mailto:Jeff@IgniteDemo.onmicrosoft.com">Jeff@IgniteDemo.onmicrosoft.com</a></td>
<td>13.70.184.243</td>
<td>Delivered</td>
</tr>
<tr>
<td>9/19/18 10:14AM</td>
<td>Project details requested - September Update</td>
<td><a href="mailto:Dan@IgniteDemo.onmicrosoft.com">Dan@IgniteDemo.onmicrosoft.com</a></td>
<td><a href="mailto:Jeff@IgniteDemo.onmicrosoft.com">Jeff@IgniteDemo.onmicrosoft.com</a></td>
<td>13.70.184.243</td>
<td>Delivered</td>
</tr>
<tr>
<td>9/19/18 10:14AM</td>
<td>Project details requested - September Update</td>
<td><a href="mailto:Jim@IgniteDemo.onmicrosoft.com">Jim@IgniteDemo.onmicrosoft.com</a></td>
<td><a href="mailto:Jeff@IgniteDemo.onmicrosoft.com">Jeff@IgniteDemo.onmicrosoft.com</a></td>
<td>13.70.184.243</td>
<td>Delivered</td>
</tr>
<tr>
<td>9/19/18 10:14AM</td>
<td>Project details requested - September Update</td>
<td><a href="mailto:Jane@IgniteDemo.onmicrosoft.com">Jane@IgniteDemo.onmicrosoft.com</a></td>
<td><a href="mailto:Jeff@IgniteDemo.onmicrosoft.com">Jeff@IgniteDemo.onmicrosoft.com</a></td>
<td>13.70.184.243</td>
<td>Delivered</td>
</tr>
</tbody>
</table>
Weaponized URL in mail discovered by Office 365 ATP

Investigation #11371 is complete - Remediated

Users | Risk Level | Risk Indicators
--- | --- | ---
Jeff@lgn.com | High | Compromised user - sending phishing email
User activity anomalies detected - suspicious login
User activity anomalies detected - mass download

Service | Risky Activities
--- | ---
Exchange Online
Azure Active Directory
SharePoint Online
### Weaponized URL in mail discovered by Office 365 ATP

**Investigation #11371 is complete - Remediated**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Entity</th>
<th>Threats</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email indicators extraction</td>
<td>Extract indicators from header, body and content of the email for investigation</td>
<td>Email</td>
<td>Email - Phish: Intra-org</td>
<td>Completed</td>
</tr>
<tr>
<td>Email cluster identification</td>
<td>Email cluster analysis based on header, body, content and URLs</td>
<td>Email</td>
<td>Email - Phish: Intra-org</td>
<td>Completed</td>
</tr>
<tr>
<td>On-demand detonation</td>
<td>On-demand detonation triggered with Office 365 ATP for emails, attachments and URLs</td>
<td>Email</td>
<td>Malicious URL</td>
<td>Completed</td>
</tr>
<tr>
<td>Intra-org/Outbound anomaly investigation</td>
<td>Detect intra-org and outbound malware, phish or spam originating from users in your organization</td>
<td>Email</td>
<td>Email - Phish: Intra-org</td>
<td>Completed</td>
</tr>
<tr>
<td>URL clicks investigation</td>
<td>Investigate clicks from users protected by O365 ATP safe links in your organization</td>
<td>Email</td>
<td>URL click block override</td>
<td>Completed</td>
</tr>
<tr>
<td>User activity investigation</td>
<td>Analyze user activity anomalies across Azure Active Directory and other Office 365 services including SharePoint, OneDrive, Teams, Yammer and PowerShell, including any detections from Microsoft Cloud App Security</td>
<td>User</td>
<td>Suspicious Login Malware Downloads</td>
<td>Completed</td>
</tr>
<tr>
<td>Sender domain investigation</td>
<td>On-demand check of domain reputation from Microsoft's ISG and external threat intelligence sources</td>
<td>Email</td>
<td>None</td>
<td>Completed</td>
</tr>
<tr>
<td>Sender IP investigation</td>
<td>On-demand check of IP reputation from Microsoft's ISG and external threat intelligence sources</td>
<td>Email</td>
<td>None</td>
<td>Completed</td>
</tr>
<tr>
<td>Mail cluster volume analysis</td>
<td>Email cluster analysis based on outbound mail flow volume patterns</td>
<td>Email</td>
<td>None</td>
<td>Completed</td>
</tr>
<tr>
<td>Admin user investigation</td>
<td>Analyze admin permissions and roles assigned to Office 365 user for Security and Compliance Center and Exchange Admin Center</td>
<td>User</td>
<td>None</td>
<td>Completed</td>
</tr>
<tr>
<td>DLP violations investigation</td>
<td>Investigate any violations detected by Office 365 Data Loss Prevention (DLP)</td>
<td>Data</td>
<td>None</td>
<td>Completed</td>
</tr>
<tr>
<td>Mail delegation investigation</td>
<td>Investigate mail delegation access for user mailboxes related to this investigation</td>
<td>Email</td>
<td>None</td>
<td>Completed</td>
</tr>
<tr>
<td>Mail forwarding rules investigation</td>
<td>Investigate any mail forwarding rules for user mailboxes related to this investigation</td>
<td>Email</td>
<td>None</td>
<td>Completed</td>
</tr>
<tr>
<td>OWA settings investigation</td>
<td>Investigate Outlook Web Access (OWA) configurations for user mailboxes related to this investigation</td>
<td>Email</td>
<td>None</td>
<td>Completed</td>
</tr>
</tbody>
</table>
### Weaponized URL in mail discovered by Office 365 ATP

**Investigation #11371 is complete - Remediated**

<table>
<thead>
<tr>
<th>Id</th>
<th>Status</th>
<th>Machine Owner</th>
<th>Machines</th>
<th>Start Date</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>4F4472CE7F3F6A34F9A3...</td>
<td>Success</td>
<td><a href="mailto:JeffV@Ignitedemo.onmicrosoft.com">JeffV@Ignitedemo.onmicrosoft.com</a></td>
<td>IFFV_DSKTP-PC</td>
<td>9/19/18 4:55 PM</td>
<td>00:01:59</td>
</tr>
</tbody>
</table>
Office 365 Alert - Weaponized URL in mail discovered by Office 365 ATP

Investigation #1 is complete - Remediated

Alert severity: Informational

Category: Malware Download

Detection source: Office 365

Alert received:
Automated Investigation triggered by Office 365
Office 365 Alert - Weaponized URL in mail discovered

Entities analyzed (3613):
- Files
- Remediated
- Processes
- CR Services
- 365 Drivers
- IP Addresses
- 365 Persistence Methods

Threat found:
1 threat found

Result:
Remediated
6C92F7A6C4 c:\user\yfy\desktop\appdata\local\pac
- JEFFV_DSKTP-PC
### Investigation details

**Status**: Remediated

Malicious entities found were successfully remediated.

**Alert severity**: Informational

**Category**: Malware Download

**Detection source**: Office 365

---

<table>
<thead>
<tr>
<th>Investigation graph</th>
<th>Alert (1)</th>
<th>Machines (1)</th>
<th>Threats (1)</th>
<th>Entities (3,61k)</th>
<th>Log (38)</th>
<th>Actions (1)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Status</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collect SenseIR Trace Log</td>
<td>✔ Completed</td>
<td>Uploading the SenseIR trace log.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Uris by Hash</td>
<td>✔ Completed</td>
<td>Get file data for af1a861c2333c35c1bc0e74d83d45851bc60b7.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Endpoints by File Hash</td>
<td>✔ Completed</td>
<td>Get known paths on investigated endpoints with file hash “35c1bc0e74d83d45851bc60b7”.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Uris by Hash</td>
<td>✔ Completed</td>
<td>Get file data for b51642af563778b0a50c42c956fe088a337.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Endpoints by File Hash</td>
<td>✔ Completed</td>
<td>Get known paths on investigated endpoints with file hash “563778b0a50c42c956fe088a337”.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze Multiple Persistency Methods</td>
<td>✔ Completed</td>
<td>Threat intelligence analysis for 398 persistency methods.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze File Metadata</td>
<td>✔ Completed</td>
<td>Analyzing the metadata of 3 files to determine if malicious.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze File Content</td>
<td>✔ Completed</td>
<td>Analyzing file content with external services.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Quarantine</td>
<td>✔ Completed</td>
<td>Quarantine “<em>\lmicrosoft data backup 092018\herling\downloads\freewav.exe</em>” with quarantine for 2 files.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze File Content</td>
<td>✔ Completed</td>
<td>Analyzing file content with external services.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Quarantine</td>
<td>✔ Completed</td>
<td>Quarantine “<em>\lmicrosoft data backup 092018\herling\downloads\avira_free.exe</em>” with quarantine for 2 files.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze File Content</td>
<td>✔ Completed</td>
<td>Analyzing file content with external services.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident name</td>
<td>Severity</td>
<td>Category</td>
<td>Detection source</td>
<td>Alerted entity</td>
<td>Last activity</td>
<td>Classification</td>
<td>Status</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>----------</td>
<td>---------------------------</td>
<td>-------------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>--------</td>
</tr>
<tr>
<td>Incident #496</td>
<td>High</td>
<td>Credential Theft, Compromised Account</td>
<td>Email, Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:26:22</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Communication from remote process, Remote shell, Kernel...</td>
<td>High</td>
<td>Privilege Escalation</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:26:00</td>
<td>Not set</td>
<td>Active</td>
</tr>
<tr>
<td>Install Core unwanted software</td>
<td>High</td>
<td>Persistence</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:23:29</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Malicious URL, Active Sleeppro malware</td>
<td>High</td>
<td>Suspicious Activity</td>
<td>Email, Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 09:23:24</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Ransomware attack</td>
<td>High</td>
<td>Suspicious Activity, Persistence</td>
<td>Email</td>
<td>@jonawolcott</td>
<td>April 10, 2018 09:23:24</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Suspicious file, Suspicious script</td>
<td>Medium</td>
<td>Suspicious Activity</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 09:24:23</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Malicious URL, Active Sleeppro malware</td>
<td>Medium</td>
<td>Reconnaissance</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 08:15:24</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Suspicious script</td>
<td>Medium</td>
<td>Reconnaissance</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:25:26</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Incident #415</td>
<td>Medium</td>
<td>Suspicious Activity</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:25:22</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Malicious URL, Active Sleeppro malware</td>
<td>Medium</td>
<td>Suspicious Activity</td>
<td>Email</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:25:16</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Incident #422</td>
<td>Medium</td>
<td>Suspicious Activity</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:15:45</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Incident #413</td>
<td>Medium</td>
<td>Suspicious Activity</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:24:43</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Newly registered domain</td>
<td>Medium</td>
<td>Suspicious Activity</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:25:28</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Incident #456</td>
<td>Low</td>
<td>Suspicious Activity</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:25:24</td>
<td>Not set</td>
<td>Active</td>
</tr>
<tr>
<td>An active 'Azede' malware was detected</td>
<td>Low</td>
<td>Persistence</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:25:29</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>Newly registered domain</td>
<td>Low</td>
<td>Persistence</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:25:13</td>
<td>True</td>
<td>Active</td>
</tr>
<tr>
<td>'Reimage' unwanted software was detected</td>
<td>Low</td>
<td>Persistence</td>
<td>Device, User</td>
<td>@jonawolcott</td>
<td>April 10, 2018 10:55:43</td>
<td>True</td>
<td>Active</td>
</tr>
</tbody>
</table>
Dashboard > Incident

6 active alerts

- High (1)
- Medium (3)
- Low (2)
- Informational (0)

Related evidence

- Machines: 1
- Users: 1
- Mailboxes: 213
- Files: 9
- Processes: 4
- IPs: 1
- Applications: 0
- Services: 0
- Persistence methods: 1

Alerts  Machines  Emails  Users  Investigations  Incident graph  Action center

- Triggering alert
  - Email reported as phishing
  - Suspicious PowerShell
  - Golden ticket compromised
  - Spear-phishing attack

Investigation state

- Remediated
- Running

Investigated entities

- cont-jonawolcott@contoso
- jonathan.wolcott@contoso
- Jonathos Wolcott
- cont-jonawolcott

Start date

- Jul 03, 2018 09:26 AM
- Jul 03, 2018 09:26 AM
- Jul 03, 2018 09:26 AM
- Jul 03, 2018 09:26 AM

Duration

- 00h: 03m: 23s
How can I possibly stay on top of this?

Turing traditional Managed Security Services on their Side with New Signature
NetSecOps – Traditional MSSP

- Ingest Log Data
- Put into Product (Splunk)
- Do home grown smart analysis
- Apply business rules
- Send alerts to SOC
- Tell customer

So... what about the Internet?
NetSecOps – New Signature

Microsoft Security Operations

Thousands of people
AI / Machine Learning
6.5 Trillion Signals

Send email

Apply business rules

Send incidents to SOC

Mitigate Incident

Collaborate with Customer

Ingest Log Data

Put into Product (Splunk)

Do home grown smart analysis

Apply business rules

Send alerts to SOC

Tell customer
Azure Sentinel

- **Azure Sentinel** is Microsoft’s new cloud-native SIEM service that augments our security managed services. Sentinel integrates data from all available sources and applies machine learning and knowledge-based detections derived from the trillions of signals analyzed by Microsoft daily. Long term Log Analytics retention allow our analysts to detect latent threats and rapidly scope the impact of a breach, leading to faster remediation.
New Signature Security Managed Services for Office 365

- **Identity Advanced Security** is a managed service that protects employee Azure Active Directory credentials from compromise by investigating risk events, flagged user accounts, and performing detection and risk audits. Our experts also provide proactive services using Identity Secure Score to determine gaps in identity security and provide reporting and ongoing recommendations.

- **Office 365 Advanced Security** protects your business from attack by monitoring and maintaining Office 365 Advanced Threat Protection (ATP) suite of software. We provide 24x7 phishing incident investigation and proactive security services to maintain and enhance your Office 365 tenant security over time.