Threat Hunting with Qualys
Going Beyond Your EDR Solutions

Chris Carlson
VP Product Management, Qualys, Inc.
Adversary Threat Tactics are Changing

Early 2010s
Zero-day Vulnerabilities
(Nation State, Industrial Espionage, Black Market)

Today
Rapidly weaponizing newly-disclosed vulnerabilities
(Good, Fast, Cheap – Pick 3)
Known Critical Vulnerabilities are Increasing

14-16K vulnerabilities are disclosed 2017-2019

30-40% are ranked as “High” or “Critical” severity

Worm-able Vulnerabilities are increasing (WannaCry, BlueKeep)

“Mean Time to Weaponize” is rapidly decreasing year/year
## Time to Weaponize

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Vulnerability Disclosure</th>
<th>Exploit Date</th>
<th>Time</th>
<th>First Exploit Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WannaCry</strong></td>
<td>March 2017</td>
<td>May 2017*</td>
<td>2 months</td>
<td>Ransomware</td>
</tr>
<tr>
<td><strong>BlueKeep</strong></td>
<td>May 2019</td>
<td>Nov 2019</td>
<td>6 months</td>
<td>Cryptominer</td>
</tr>
<tr>
<td><strong>Citrix ADC</strong></td>
<td>Dec 2019</td>
<td>Jan 2020</td>
<td>1 month</td>
<td>Cryptominer</td>
</tr>
<tr>
<td><strong>CurveBall</strong></td>
<td>Jan 2020</td>
<td>Jan 2020 (PoC)</td>
<td>???</td>
<td>???</td>
</tr>
<tr>
<td><strong>Crypt32.dll</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Get Proactive – Reduce the Attack Surface

- Immediately discover assets and vulnerabilities
- Patch and verify remediation
- Change configuration to limit unauthorized access
- Control network access / cloud security groups
- Add Endpoint Detection and Response
Proactively Hunt, Detect, and Respond

Indication of Compromise
- Detect malware, IOCs, IOAs, and verify threat intel

Security Analytics (Summer 2020)
- Augment SIEMs by finding attacks using behavioral analytics and MITRE ATT&CK
Qualys IOC – Hunt Using Threat Intel

1. Threat intelligence lists attack information ...

2. Search for the file hash here...

3. Find the object there.
Detect Malware Missed by Anti-Virus

UK Government Contractor
- “Big 4” anti-virus installed
- Qualys Agent for Vulnerability Mgmt
- Added Qualys IOC on existing agents
- 256 hosts

Qualys IOC discovered...
- Dridex Banking Trojan (51)
- 4 domain controllers infected
- Backdoors (7) installed due to phishing campaigns
- Netcat (8) root kits installed
- 46 PUAs installed
DEMO

Indication of Compromise

Threat Intel Verification / Hunting
Malware Detection
EDR – Response Actions

5ceec909f3dfc890fdd1e76d6f3cc093465c9d980d68b9987fc3f5eb289b6bd2
a0c68e476f55d0b7cdd87b1b20a1e021672eec41f96e056d6289d8734491f9bb
Beyond Endpoint Detection and Response: How can I better protect my crown jewels?

Threat Hunting Assumptions:

- Every user machine can be compromised – it only takes one click
- Every Remote Code Execution (RCE) vulnerability can be exploited
- Local Privilege Escalation and Credential Harvesting to move laterally
- System misconfigurations are often overlooked and easy to exploit
- Network segmentation is rarely used or hard to manage (configuration drift)

All attacks are not equal: can Adversaries reach my Critical Servers?
Adversary Lateral Movements (Attack Paths)

1. Bad actor compromises a user machine (email, phishing, watering hole, etc.). Takes remote control of the machine.

2. Find systems in higher security tiers by looking for existing connections or network reconnaissance.

3. Laterally move to new system by:
   - Exploiting open vulnerabilities
   - Take advantage of misconfigurations
   - Use compromised credentials

4. Laterally move to new system by:
   - Exploiting open vulnerabilities
   - Take advantage of misconfigurations
   - Use compromised credentials

User Segments

Business Apps / IT Systems

Tier 0 Systems
“Crown Jewels”
Attack Path Discovery *(Summer 2020)*

**Network Reachability**
Determine connections between hosts using Cloud Agent (CA)
Passive + Active network collection
Store these connections in a Graph Database for fast query

**Asset Security Posture**
Remotely Exploitable Vulnerabilities
System Misconfigurations
Malware, IoCs, and Indicators of Activity
Attack Path Discovery
for
Proactive Threat Hunting
and Response Priority
<table>
<thead>
<tr>
<th>TIME</th>
<th>OBJECT</th>
<th>ASSET</th>
<th>SCORE</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 minutes ago 8:35:03 PM</td>
<td>WindowsAzureTelemetryService.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\WindowsAzureTelemetryService.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3 minutes ago 8:35:03 PM</td>
<td>QualysAgent.exe C:\Program Files\Qualys\QualysVMSQ\QualysAgent.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3 minutes ago 8:35:03 PM</td>
<td>WmiPrvSE.exe C:\Windows\System32\wbem\WmiPrvSE.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3 minutes ago 8:34:56 PM</td>
<td>125.227.222.242 (125.227-22-242.HINET-IP) .TCP CONNECTION - ESTABLISHED by svchost.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3 minutes ago 8:34:56 PM</td>
<td>13.82.189.202 : 63733 TCP CONNECTION - ESTABLISHED by svchost.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3 minutes ago 8:34:56 PM</td>
<td>fe80::281b:10bb:53e0:ff2%7 : 546 UDP CONNECTION - LISTENING by svchost.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3 minutes ago 8:34:59 PM</td>
<td>64.39.104.103 (qagpublic.qg2.apps.qualys.com).TCP CONNECTION - ESTABLISHED by QualysAgent.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3 minutes ago 8:34:49 PM</td>
<td>211.247.115.130 : 57533 TCP CONNECTION - ESTABLISHED by svchost.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3 minutes ago 8:34:44 PM</td>
<td>185.209.0.22 : 36585 TCP CONNECTION - ESTABLISHED by svchost.exe</td>
<td>WIN10PMIOC4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>TIME</td>
<td>OBJECT</td>
<td>ASSET</td>
<td>SCORE</td>
<td>DETAILS</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------</td>
<td>-------------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>21 hours ago</td>
<td>66.85.173.57 (tar.theoutlan.com) : 443</td>
<td>SHAREPT003</td>
<td>10</td>
<td>Trickbot</td>
</tr>
<tr>
<td>12:58:21 AM</td>
<td>TOP CONNECTION - ESTABLISHED by temp0291.exe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a day ago</td>
<td>temp0291.exe</td>
<td>SHAREPT003</td>
<td>8</td>
<td>Trojan</td>
</tr>
<tr>
<td>8:19:31 PM</td>
<td>c:\Users\qualys\AppData\Roaming</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a day ago</td>
<td>temp0291.exe</td>
<td>SHAREPT003</td>
<td>9</td>
<td>Trojan</td>
</tr>
<tr>
<td>3:12:28 PM</td>
<td>c:\Users\qualys\AppData\Roaming\temp0291.exe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a day ago</td>
<td>\BaseNamedObjects\4C3D653494D1128</td>
<td>SHAREPT003</td>
<td>9</td>
<td>Trojan</td>
</tr>
<tr>
<td>3:02:08 PM</td>
<td>temp0291.exe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 days ago</td>
<td>temp0291.exe</td>
<td>SHAREPT003</td>
<td>8</td>
<td>Trojan</td>
</tr>
<tr>
<td>11:18:23 AM</td>
<td>c:\Users\qualys\AppData\Roaming</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Quickly investigate the host to see the active attack
Take action on this host to stop the attacker in their tracks.
The following response will be executed for the selected processes and files on the defined hosts:

### Process (1)

<table>
<thead>
<tr>
<th>RISK SCORE</th>
<th>PROCESS NAME</th>
<th>MALWARE</th>
<th>PID</th>
<th>HOST</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>temp0291.exe</td>
<td>TrickBot</td>
<td>4417</td>
<td>SHAREPT003</td>
</tr>
</tbody>
</table>

- Kill Process
- Quarantine File

### File Type (3)

<table>
<thead>
<tr>
<th>RISK SCORE</th>
<th>FILE NAME</th>
<th>MALWARE</th>
<th>HOST</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WormDll64 (C:\Users\support\AppData\Roaming)</td>
<td>TrickBot</td>
<td>SHAREPT003</td>
</tr>
<tr>
<td>1</td>
<td>NetworkDll64 (C:\Users\support\AppData\Roaming)</td>
<td>TrickBot</td>
<td>SHAREPT003</td>
</tr>
<tr>
<td>1</td>
<td>ShareDll64 (C:\Users\support\AppData\Roaming)</td>
<td>TrickBot</td>
<td>SHAREPT003</td>
</tr>
</tbody>
</table>

- Quarantine File
Attack Path Discovery

to
Prioritize Patching
and
Improve Security Defenses
Attack path leads to this critical server
Patch this one asset to break the attack path to critical server
Vulnerability Remediation Prioritization

CVSSv2 / CVSSv3 base scores

**Qualys** QID Severity score

**Qualys** Tagging for Asset Business Criticality

**Qualys** Threat Protection Real-Time Indicators
(based on threat intel and live attacks)

**Qualys** VMDR Threat Prioritization
(Machine Learning model + Contextual Awareness)

**Qualys** Attack Path Discovery
Thank You

Chris Carlson
ccarlson@qualys.com