Qualys Indication of Compromise

Bringing IOC to the Next Level

Chris Carlson
VP, Product Management, Qualys, Inc.
Vulnerabilities are Low Hanging Fruit

**Early 2010s**
Zero-day Vulnerabilities

**Today**
Rapidly weaponizing newly-disclosed vulnerabilities
Known Critical Vulnerabilities are Increasing

6-7K vulnerabilities are disclosed each year
30-40% are ranked as “High” or “Critical” severity
“Mean Time to Weaponize” is rapidly decreasing y/y
Vulnerability Management Lifecycle

- Asset Inventory
- Patch Management
- Remediation / Patch
- Prioritize Threats
- Report & Research
- Discover at Scale
- Vulnerability Management
- Threat Risk and Prioritization
Vulnerability Spread at Speed of DevOps

Red Hat 7.4 Marketplace Image
Auto-Deploy Qualys Cloud Agent
Vulnerability Results
Threat Protection: Exploitability Opportunity

- Total Vulnerabilities by RTIs: 72
- LATEST THREATS FROM LIVE FEED:
  - OpenSSH User name Enumeration Vulnerability : CVE-2018-15473 - HIGH - 8/29/2018
  - L1 Terminal Fault /Foreshadow Attack aka L1TF Attack - HIGH - 8/28/2018
  - PoC Exploit available for CVE-2018-15473 - MEDIUM - 8/28/2018
  - PoC Exploit available for CVE-2018-15473 - MEDIUM - 8/22/2018
  - PoC Exploit available for CVE-2018-15473 - MEDIUM - 8/20/2018
  - PoC Exploit available for CVE-2018-15473 - MEDIUM - 8/20/2018
  - PoC Exploit available for CVE-2018-15473 - MEDIUM - 8/15/2019
  - PoC Exploit available for CVE-2018-15473 - MEDIUM - 8/15/2019
  - SegmentSmack: CVE-2018-5390 - HIGH - 8/2/2018
Get Proactive – Reduce the Attack Surface

Immediately Identify Vulnerabilities in Production
Notify IT Asset Owner to Patch/Stop the Instance
Control Network Access / Cloud Security Groups

Add Detection and Response – Endpoint & Network
Proactively Hunt, Detect, and Respond

Indication of Compromise

Passive Network Sensor

Monitor the Network

System Indicators

Monitor the Network

Detect IOCs, IOAs, and verify Threat Intel

What new devices are on the network? Are there new/different traffic patterns?
Qualys IOC Use Cases –
Visibility Beyond AV

**Threat Intel Verification**
Threat Intel Feeds / Mandated to Verify
“Is this hash, registry, process, mutex on my network?”

**“Look Back” Investigation after a known breach**
Go back over months of stored events and find the first occurrence of a breach

**Hunting / Find Suspicious Activity**
Indicator of Activity hunting with pre-built and user-defined queries for Fileless attacks

**Detect Known/Unknown Malware Family Variants**
Using Qualys Malware Labs behavior models and Threat Feeds (OEM, customer)
Organizations Struggle to Answer Basic Questions

Are these hashes on/running in my network?
Are these mutexes / processes / registry keys?

Did any endpoints connect to these IPs / Domains?
Are there any connections to TOR exit nodes?

What system is the first impacted? “Patient Zero”
Did this spread to others systems? When?
Threat Intel Verification

1. Threat Intelligence lists attack information ...

2. Search for the file hash here...

3. Find the object there.

- NotPetya Ransomware spreading using ETERNALBLUE Vulnerability and Credential Stealing
- October 4, 2017
- On June 27, 2017, NCSC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list.
- Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods using the ETERNALBLUE vulnerability and credential stealing via a modified version of Mirai.

- VirusTotal reports 0/66 anti-virus vendors have signatures for the credential stealer as of the date of this report.
- Files:
  - Delivery — MD5: 71bd6ea493388e79b640c83e5653106d
  - Installation — MD5: 7e37a35e6c9c4e77e2452260f9d852d
  - Credential Stealer (new) — MD5: 92b67e760f9117f7a14a3c1e4e80f9

- Secondary Actions:
  - NotPetya leverages multiple propagation methods to spread within an infected network.
  - According to malware analysis, NotPetya attempts the lateral movement techniques below:
Malware Hides with Stolen Code-Signing Certificates

Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign

D-Link and Changing Information Technologies code-signing certificates stolen and abused by highly skilled cyberespionage group focused on East Asia, particularly Taiwan

New IOC CVE - File Reputation Threat Feed

Find Vulnerabilities

Verify that vulnerabilities have been remediated

Real-Time Indicators for which vulnerabilities have known / POC exploits

Prioritize vulnerability remediation on likelihood of attack

Threat Feed of malware hashes used in real-world vulnerability exploits

Prioritize vulnerability remediation based on successful attacks in your network
Indication of Compromise

Threat Intel Verification
Hunting
Alerting
Create Emergency Patch Job from CVE Exploitation

18fc1b9b29a2d281ec9310f9f226ad77e3cb9c558f696c37390bbac72baa8ba8
168.63.129.16
Qualys Cloud Agent

IT, Security, Compliance Apps

- Asset Inventory
- Vulnerability Management
- Policy Compliance
- Indication of Compromise Detection
- File Integrity Monitoring

Upcoming IT App  (Beta November 2018)

- Patch Management
Thank You

Chris Carlson
ccarlson@qualys.com