Carbon Black.

端點威脅態勢感知

Endpoint Threat Situational Awareness

Bernie Png – Senior Security Engineer, APJ
<table>
<thead>
<tr>
<th>JAN</th>
<th>FEB</th>
<th>MAR</th>
<th>APR</th>
<th>MAY</th>
<th>JUN</th>
<th>JUL</th>
<th>AUG</th>
<th>SEP</th>
<th>OCT</th>
<th>NOV</th>
<th>DEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cellebrite</td>
<td>Vault 7&amp;8 (CIA leak)</td>
<td>Handbrake WannaCry</td>
<td>DocuSign OneLogin</td>
<td>Verizon</td>
<td>Virgin America</td>
<td>Equifax</td>
<td>SEC</td>
<td>Deloitte</td>
<td>Spectre</td>
<td>Meltdown</td>
<td></td>
</tr>
<tr>
<td>Cloudbleed</td>
<td>TSA</td>
<td>Shadow Brokers (NSA leak)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>198 Million Voter Records</td>
<td>NotPetya</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BadRabbit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Evolving Threat Landscape

MALWARE ATTACKS
- KNOWN
- UNKNOWN
- RANSOM
- OBFUSCATED

NON-MALWARE ATTACKS
- MEMORY
- MACROS
- REMOTE LOGIN
- POWERSHELL

48% OF BREACHES USE MALWARE
52% OF BREACHES ARE NON-MALWARE

2017 Carbon Black Threat Report
AN ORGANIZATION WITH 10,000 ENDPOINTS IS SEEING APPROXIMATELY 1,000 ATTACKS PER DAY.
Hackonomics: 'Cyber Black Market' more profitable than illegal drug trade

**Summary:** OPINION: A new report by RAND commissioned by Juniper Networks has some eyebrow-raising conclusions about the black market for hacks, cracks, data theft, botnets, and zero days.

By Violet Blue for Zero Day | March 26, 2014 -- 11:24 GMT (04:24 PDT)
Ransom Money Paid to Attackers

- **$24 MILLION**
  - 2015
- **$850 MILLION**
  - 2016
- **$5 BILLION**
  - 2017
Typical *time-to-compromise* continues to be measured in minutes, while *time-to-discovery* remains in weeks or months.

*Verizon Data Breach Report 2017*
214 DAYS

MEAN TIME TO IDENTIFY BREACH BY ROOT CAUSE

77 DAYS

MEAN TIME TO CONTAIN BREACH BY ROOT CAUSE
Attackers have gotten smarter and more sophisticated.

They have found ways to achieve their goals without deploying malware.

This is a big change in the way attacks are conducted – and therefore the way you need to defend against them.
1. The Adversary Automates
   - Attacker writes malicious code
   - Specialized malware compiler
     - Anti-signaturing
     - Anti-reverse eng
     - Anti-debugging
     - Anti-sandboxing
   - 100 million malware files
   - Raw malware repository
   - Screen out detected files
   - Zero-day arsenal
   - Multiple AV engines @ 99% effectiveness

2. The Adversary Outsources
   - HIGH INFECTION RATES
     - PETYA comes bundled with his little brother MISCHA. Since PETYA can’t do... (text cut off)
   - PROVABLY FAIR
     - As professional cybercriminals, we know that you can’t trust anyone. So we...
   - FREE CRYPTING SERVICE
     - We provide you FUD crypted binaries.
   - EASY ADMINISTRATION
     - Administrative Tasks like viewing the ...

3. The Adversary Adapts
   - KNOWN MALWARE
   - OBFUSCATED MALWARE
   - SCRIPTING ATTACKS
   - MEMORY ATTACKS
   - POWERSHELL
   - RANSOMWARE
   - REMOTE LOGIN
   - MACROS
   - UNKNOWN MALWARE
WHY THREAT HUNT?

01. PROACTIVELY STOP ATTACKS OTHERWISE MISSED

02. EVERY ATTACK MAKES THE NEXT ATTACK HARDER
SO, WHAT IS THREAT HUNTING...
THREAT HUNTING: THE LOW DOWN

WHAT IT IS?

• Proactive & iterative search for attacks
• Informed by knowledge of your environment
• Often hypothesis based
• Know the battlefield

WHAT IT IS NOT?

• Installing tools and waiting for alerts
• Simple indicators of compromise
• Incident Response & Forensics
• Acquiring or analyzing threat intel
KEY BUILDING BLOCKS TO DRIVE THREAT HUNTING

Search & Visualisation

Data

Enrichment

Automation

Objectives > Hypotheses > Expertise

DEVELOPING A STRATEGY

REDUCE ATTACK SURFACE

ESTABLISH VISIBILITY

THREAT HUNTING

ROOT CAUSE

INFORM CONTROLS
ATTACKS OFTEN “LIVE OFF THE LAND” (AND BLEND IN)
THE ATTACK CYCLE

ACCESS - ANALYSIS - STAGING - EXFILTRATION - PERSISTENCE

Recon & Weaponize

Targets
- Users
- Web Apps
- Vulnerabilities
- Networks

Additional Discovery

Gaining Access
Escalating Privileges
System Browsing
Tool Installation

Stealth

Carbon Black
KNOWING WHEN TO HUNT?

- When you come across new research
- When you read about an attack/breach
- When you encounter something odd
- When conducting proactive SecOps
EXECUTING AGAINST A PLAN

PREPARATION
- Determine Priorities
- Asset/Network Review
- What’s Normal

INVESTIGATION
- Define a Scope
- Gather & Analyze
- Expand Investigation

ADVERSARY REMOVAL
- Kill Process
- Quarantine system
- Repair

HUNTING REPORT
- Executive Report
- Scope & Timeline
- Root Cause
THE HUNT PROCESS

STARTING THE HUNT

REFINING THE HUNT

ROOT CAUSE ANALYSIS

RESPONSE

CONTINUOUS IMPROVEMENT

Search on suspicion (ex: Powershell)

Filter out legitimate activity

Deeper Investigation (in seconds)

Discover malicious activity

Scope the attack

Remediate the threat

Update defenses

Find suspicious activity

Discover malicious activity

Deeper Investigation (in seconds)

Filter out legitimate activity

Search on suspicion (ex: Powershell)
MAKING THE NEXT ATTACK HARDER

Many Attackers & Attack Types

Prevent

Detect & Respond

Successful Attack

X

X

X

Carbon Black
MAKING THE NEXT ATTACK HARDER

WE NEED TO FOCUS ON WHAT’S HAPPENING EARLIER IN THE ATTACK PROCESS
## Making the Next Attack Harder

### Many Attackers & Attack Types

<table>
<thead>
<tr>
<th>Visibility</th>
<th>Prevent</th>
<th>Detect &amp; Respond</th>
<th>Successful Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
</tr>
</tbody>
</table>

- **Visibility**
  - Prevent: X
  - Detect & Respond: X
  - Successful Attack: X

- **Many Attackers & Attack Types**
  - ![Image](image5.png)
  - ![Image](image6.png)
  - ![Image](image7.png)

### Notes

- Carbon Black, All Rights Reserved.
- CONFIDENTIAL
MAKING THE NEXT ATTACK HARDER

Many Attackers & Attack Types

VISIBILITY

ROOT CAUSE

Prevent
Detect & Respond
Successful Attack
### TYPICAL DATA SOURCES

#### Threat intelligence
- Third-party threat intel
- Open-source blacklist
- Internal threat intelligence

Attacker, known relay/C2 sites, infected sites, IOC, attack/campaign intent and attribution

#### Network
- Firewall, IDS, IPS
- DNS
- Email
- Web proxy
- NetFlow
- Network

Where they went, who talked to whom, attack transmitted, abnormal traffic, malware download

#### Endpoint
- Endpoint
- Malware detection
- Application Assets
- DHCP
- OS logs
- Patching

What process is running (malicious, abnormal, etc.)
Process owner, registry mods, attack/malware artifacts, patching level, attack susceptibility

#### Access/Identity
- Active Directory
- LDAP
- CMDB
- Operating system
- Database
- VPN, AAA, SSO

Access level, privileged users, likelihood of infection, where they might be in kill chain
SOME IDEAS TO GET STARTED

• Command shells establishing network connections (WMI, CMD, PowerShell)?
• Remote server/network administration tools on non-administrator systems?
• Office documents invoking new processes or spawning command shells?
• Flash or Java spawning command shells?
  ▪ Deviations in normal behavior of administrator accounts?
  ▪ Creation of new accounts locally or on domain?
  ▪ Windows processes (lsass, svchost, csrss) with strange parents?
CONTINUOUS RECORDING & CENTRALIZED STORAGE

CONTINUOUS RECORDING
- Find root cause
- Know impact of attack
- See attack patterns
- Understand full scope

CENTRALIZED STORAGE
- High performance
- Apply limitless threat intel
- 24/7 access to all activity
- Integrate with other data

WATCH AND RECORD EVERYTHING

SCANNING UNFILTERED REPUTATION PREVELANCE RELATIONSHIPS
Add User to infected machine

Actions & Activities of processes

- `net.exe`
- `net user Jim password9876 /add`
- `w7-low`
- `BIT9SEAD\user10`
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-06-12 15:16:56.569 GMT</td>
<td>childproc</td>
<td>PID 3316 ended \c:\windows\system32\cmd.exe Signed (ad7b9c14083b52bc532fa5948342b98)</td>
</tr>
<tr>
<td>2017-06-12 15:16:55.664 GMT</td>
<td>childproc</td>
<td>PID 2120 ended \c:\windows\system32\cmd.exe Signed (ad7b9c14083b52bc532fa5948342b98)</td>
</tr>
<tr>
<td>2017-06-12 15:16:55.103 GMT</td>
<td>childproc</td>
<td>PID 2120 started \c:\windows\system32\cmd.exe Signed (ad7b9c14083b52bc532fa5948342b98)</td>
</tr>
</tbody>
</table>

**Attacker covering their tracks**
- 2017-06-12 15:16:54.853 GMT: filemod, First wrote to \c:\users\user10\compress.bat
- 2017-06-12 15:16:54.838 GMT: filemod, Created \c:\users\user10\compress.bat
- 2017-06-12 15:16:54.838 GMT: filemod, Deleted \c:\users\user10\compress.bat

**Lateral Movement**
- 2017-06-12 15:16:54.697 GMT: filemod, Last wrote to \c:\windows\system32\7za.exe (42badc1d2f03a8b1e4875740d3d49336) (PE)
- 2017-06-12 15:16:54.682 GMT: filemod, First wrote to \c:\windows\system32\7za.exe
- 2017-06-12 15:16:54.042 GMT: filemod, Created \c:\windows\system32\7za.exe
- 2017-06-12 15:16:54.042 GMT: filemod, Deleted \c:\windows\system32\7za.exe
- 2017-06-12 15:11:09.980 GMT: netconn, Connection to 192.168.230.3 on tcp/4445 (bit9se.com)

<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-06-12 15:08:59.096 GMT</td>
<td>childproc</td>
<td>PID 3316 started \c:\windows\system32\cmd.exe Signed (ad7b9c14083b52bc532fa5948342b98)</td>
</tr>
<tr>
<td>2017-06-12 15:08:58.987 GMT</td>
<td>filemod</td>
<td>First wrote to \c:$recycle.bin\reg\12.bat</td>
</tr>
<tr>
<td>2017-06-12 15:08:58.972 GMT</td>
<td>filemod</td>
<td>Created \c:$recycle.bin\reg\12.bat</td>
</tr>
<tr>
<td>2017-06-12 15:08:58.972 GMT</td>
<td>filemod</td>
<td>Deleted \c:$recycle.bin\reg\12.bat</td>
</tr>
</tbody>
</table>
Different Endpoint

Mapping drive using the added user credentials from the first infected machine

Process in Focus

Elevated User

net.exe

Process

bit9server

Host

SYSTEM

User

Terminated 3 days ago a few seconds duration

net use t \192.168.230.5\Users\user10\Dump\user.Jim password9876

Command Line - Copy
THREAT HUNTING

KEY POINTS

- Proactively and iteratively searches for attacks
- Makes a difference – stop breaches, improves posture
- Doesn’t have to “break the bank” – requires the right data
- Puts you on the front row seat of the attack