THE DOLLARS AND "SENSE" BEHIND THREAT INTELLIGENCE SHARING

2-11-2014
WHAT I DO

The ThreatConnect Intelligence Research Team (TCIRT) – Enrichments that expose the unseen

- Investigates new threats across industries
- Correlates incidents
- Provides ongoing and on-demand support

Customer: We were hit with this.

Your Organization

Peer to Peer

Common Community

Subscriber Community

Industry Community

ThreatConnect IRT

TCIRT: Here are more details...
WHO I SUPPORT

• Launched July 2013
• 1,700+ accounts
• Dozens of Fortune 100/500 Companies
• Many Industries Represented
• 66% Referral Rate
THE WHO’S WHO

• First Step: Recognize the players
“BOB3160”

• Second Step: Recognize the problem

Unless You Played one of these... ...this may carry little meaning

January 22nd, 2014 at 15:34 | #1

bob3160

Hello Joromir,
Thank you for the excellent analysis. Can you please also tell me in laymans terms how I can explain this to my audience which are mostly made up of Seniors like myself. How do I tell them what to look out for and, if they still don't understand, can I simply tell them not to worry, avast! has your back and is protecting you against this very sophisticated malware.

WHERE MY GEEKS AT?

• Third Step: Mind the Gap

Producer

“Wolverine”

Direct & Indirect Delivery Models

Consumer

“Technical Risk”

“Business Risk”
MEASURING IS MATURING

• What you do, costs someone / something (Time/Money)
• What does the org get between the 1\textsuperscript{st} & 15\textsuperscript{th}? 
• What does it cost to produce or consume? 
• What should I work on? X OR Y (WHERE X = (N) and Y = N) 
• Is what I am producing of value & How do I know? 
• How do I improve my process? (Make Faster & Cheaper)
Q3 2013 METRICS
ASSUMPTIONS & FACTS

Assumptions:
• Give data to get
• Have analysts will collaborate
• My perspective is not always correct

Facts:
• Time – Not enough
• Talent – Not enough
• Treasure – Not enough

Definition:
• What we mean when we say “Share”
Q3 2013 TCIRT SHARING METRICS

- In Q3 of 2013 TCIRT shared:
  - 143 Incidents, Threats or Emails
- When shared +1700 global users were enabled
- Consistent observables for July & August
- 47% Increase in September
- Data exported, consumed and processed within organizational systems

![2013 Q3 ThreatConnect Shares](chart)

© Cyber Squared Inc. 2014
DOING MORE WITH LESS

• Automation and Collaboration accounted for 33% reduction in time in September
  • During a time of a 47% increase in workload
• Optimization of Organizational Analysis Processes
• Good news for the resourced constrained

Q3 Average in Hours for TCIRT to Develop, Enrich & Share Data

<table>
<thead>
<tr>
<th>Month</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2013</td>
<td>3.24</td>
</tr>
<tr>
<td>August 2013</td>
<td>3.29</td>
</tr>
<tr>
<td>September 2013</td>
<td>2.18</td>
</tr>
</tbody>
</table>
FUZZY MATH (SHARES)

• 1 x ThreatIntel Analyst a year / amount produced in a month @ a specific rate of production.

$100,000 yr/12mo - $8333 mo / 39 Jul Shares = $213 share/mo. @3.24/hr - $65/hr
$100,000 yr/12mo - $8333 mo / 42 Aug Shares = $198 share/mo. @3.29/hr – $60/hr
$100,000 yr/12mo - $8333 mo / 62 Sep Shares = $134 share/mo. @2.18/hr – $61/hr
GIVING AWAY KNOWLEDGE = GROWTH

• Where did it all go?
• Two Communities that we own
  • Subscriber Community
  • Common Community
• Over half of TCIRT research was given away
• These Communities consist of individuals & organizations
• Global / All Industries
• Established lasting relationships & partnerships for future collaborative efforts
FREE AS IN BEER

- 1 x ThreatIntel Analyst shares incident data @3.24hrs to create w/ a Community of 1700 researchers. Where only 1% review/research the data for one hour. Only .5% review/research/respond.
  - 1% - 17 x Review/Research for one hour
  - .5% - 8.5 x Review/Research/Respond for one hour with additional findings
- The ThreatIntel Analyst / Org leverages another 8.5 hours of additional manpower (@162% increase) of analytics.
  - Analyst obtains additional info/data
  - Org obtains at least $552 value of outsourced analysis (8.5 x $65)
  - Community leverages the entire exchange
SHARING IS POWERFUL!

- Peer to Peer Sharing between two organizations
- Each Organization has their own private data
- Common System Wide Collaboration
- Each Industry Represented by their own Trusted Community

Organization (A) Data
Finance Industry Community
Private Community

Organization (B) Data
Moderated Common Community
Private Community
Oil & Gas Industry Community

Organization (C) Data
Peer to Peer Sharing
COMMUNITY STANDUP

• Since August
• Deployable Private Communities
  • Minutes to configure
  • By Industry
  • By Threat
  • By Geo
• Multiple Roles
• Vetting & Invitations
• Attrib / non-Attributable

Count of Private Communities & Membership

Private Industry

Private General

Regional Threat Based

Private Industries

Community 1 Community 2 Community 3 Community 4 Community 5

© Cyber Squared Inc. 2014
COMMUNITY INTERACTION

• Leadership is contagious
• Not all communities are created equal
• Variables:
  • Time
  • Leadership
  • Frequency
  • Size of membership
  • Culture
GIVIN’ VALUE PROPS

• Increase your eyes and ears by $N$
• Newcomers to the mission: “Where do I get started”? 
• Increase your probability for free beer at conferences 
• Understand what are Industry best practices? 
• Who else is dealing w/ cyber pandas? Successes / Failures that I should know about? 
• Distributed talent / distributed AS&W / increasing production times.
SOURCES OF INFO
Q3 2013 SOURCES OF TCIRT DATA

- Websense Blog
- TCIRT Roll-Up
- Taiwan CERT Bulletin
- Rapid7 Blog
- Microsoft Blog
- Kaspersky Blog
- FireEye Blog
- F-Secure Blog
- Dell Secureworks Blog
- Contagio Blog
- Citizenlab Blog
- AlienVault Blog
- AhnLab Blog
- Adversary Blog
- Webroot Blog
- Symantec Blog
- Malwr
- Jsunpack
- Securelist Blog
- Cyb3rsleuth Blog
- Virus Total
- Joe Security Document Analyzer
- FireEye Blog
- ThreatExpert
- Scumware
- URLQuery
- TCIRT Partner Tipper
- TCIRT Malware Analysis / Yara Detections

© Cyber Squared Inc. 2014
ITEMS TO CONSIDER

• Quality vs Quantity debate
  • more is not always better

• Accuracy vs Timeliness debate
  • being 100% wrong now vs. 50% correct later

• All Source vs Single Source
  • the wandering perspective

• Customers & Feedback loop
  • What sources yield positive feedback?

• Cost
  • time & money
SUMMARY

• Understand others, everyone looks at things differently
• Perfect the ability to communicate effectively to both the technical & non-technical audiences
• Understand the business costs associated w/ doing or not doing aspects of your job
• Make assumptions, Measure things, Make decisions
• We are relational creatures that crave success = find success through relationship
• If you are thinking in these terms & measuring you are likely postured for growth & maturity in this space.
HAPPY HUNTING!

Rich Barger
rbarger@threatconnect.com