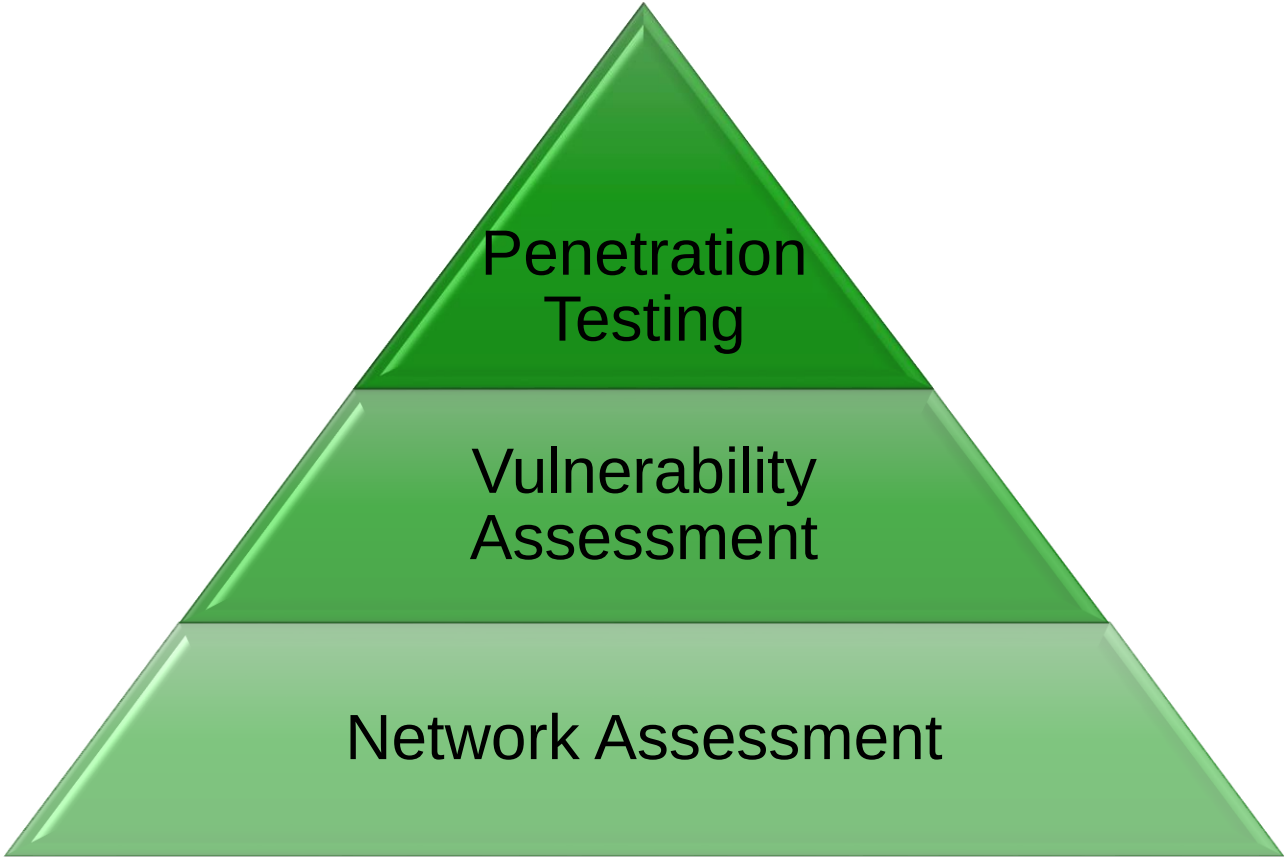
Weapons in Your Security Assessment Arsenal

Jared Hufferd, Security Evangelist, Vectra Networks

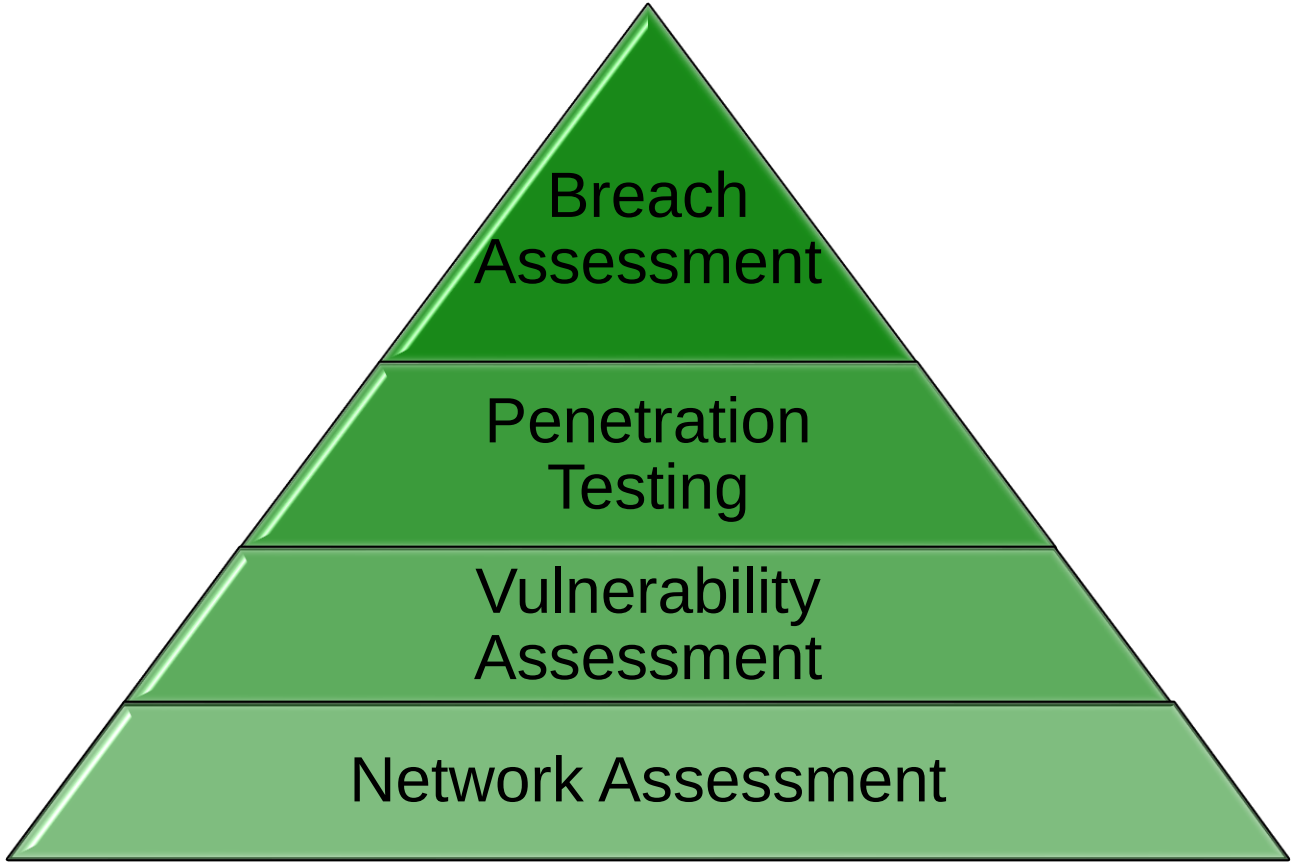
Professional Techniques – T13

ADDING TO THE STACK

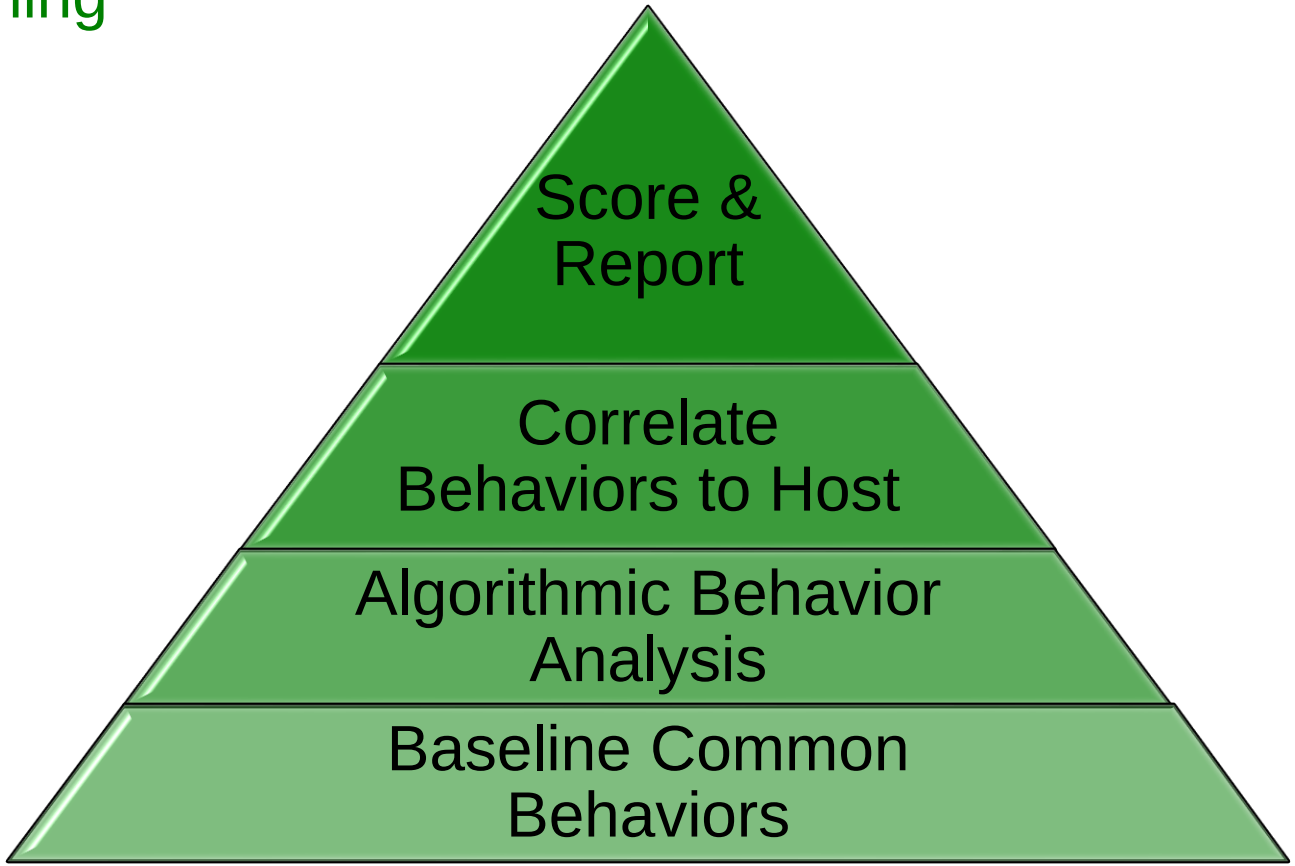
Security Assessment Stack – What Could Happen



Add Real-time Breach Assessment – What IS Happening



Real-time Breach Assessment Components – What IS Happening



WHY THIS NEW ADDITION TO THE ASSESSMENT STACK?

They all had the latest prevention

2000

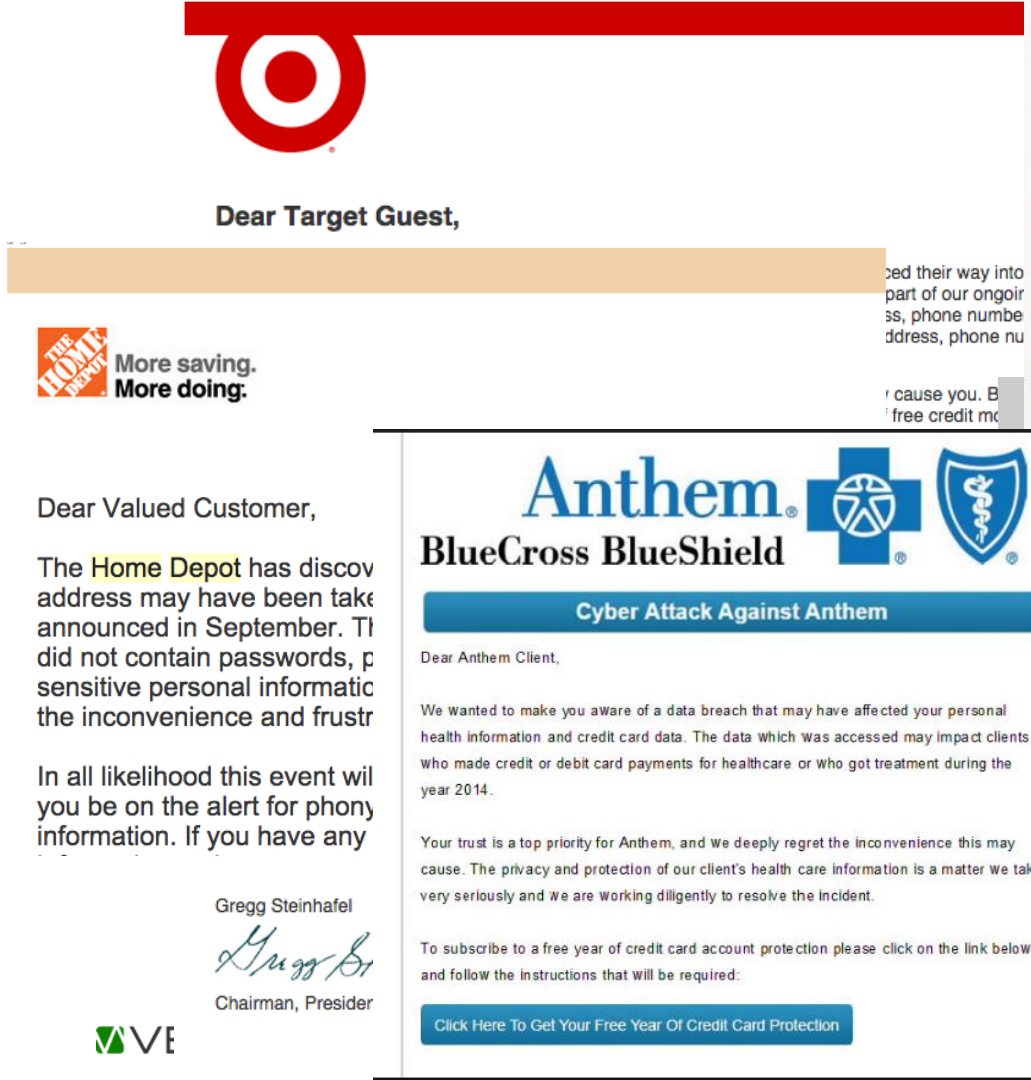
- Breaches are relatively simple (SQL Injection)
- Security: focus on preventing exploits

2007

- TJX Breach – systemic, massive financial impact
- Security: more prevention, cleanup and forensics

2013

- Breaches become a regular occurrence
- Security: evolving to a proactive daily effort to find active breaches



Dear Target Guest,

ced their way into
part of our ongoir
ss, phone numbe
ddress, phone nu

cause you. B
free credit mo

More saving.
More doing.

Dear Valued Customer,

The Home Depot has discov
address may have been take
announced in September. Th
did not contain passwords, p
sensitive personal informatic
the inconvenience and frustr

In all likelihood this event wil
you be on the alert for phony
information. If you have any

Gregg Steinhafel

Chairman, Presider

Anthem
BlueCross BlueShield

Cyber Attack Against Anthem

Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our client's health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

Click Here To Get Your Free Year Of Credit Card Protection

Neiman Marcus | Group

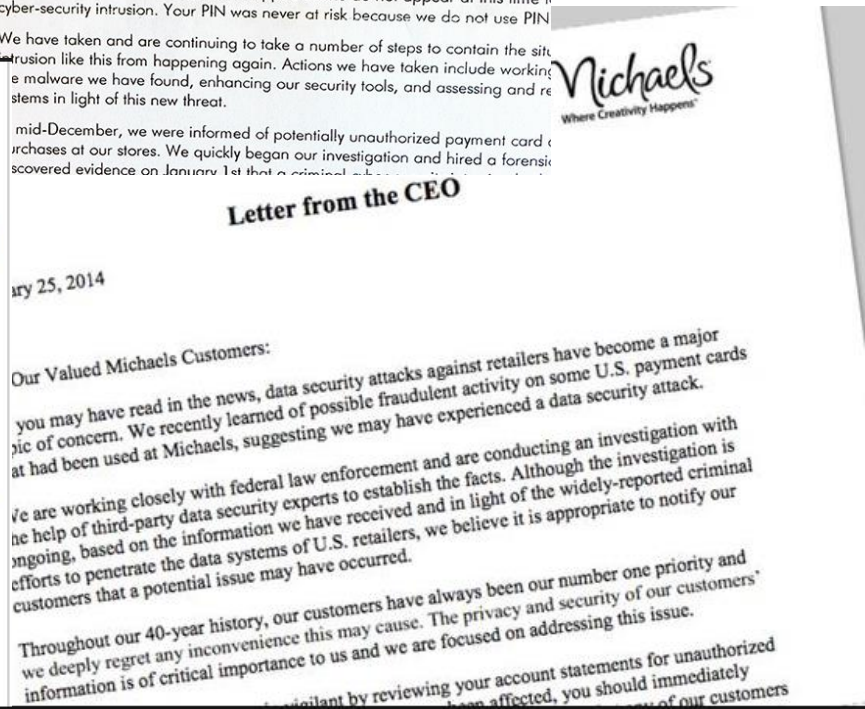
Karen Katz
President and Chief Executive Officer

Dear [redacted]

We deeply regret and are very sorry that some of our customers' payment card
purchases at our stores. We have taken steps to notify those affected customer
We aim to protect your personal and financial information. We want you alwa
Marcus and your trust in us is our absolute priority. As best we know today, soc
not compromised. Customers that shopped online do not appear at this time t
cyber-security intrusion. Your PIN was never at risk because we do not use PIN

We have taken and are continuing to take a number of steps to contain the situ
intrusion like this from happening again. Actions we have taken include working
e malware we have found, enhancing our security tools, and assessing and re
stems in light of this new threat.

mid-December, we were informed of potentially unauthorized payment card
rchases at our stores. We quickly began our investigation and hired a forensi
scovered evidence on January 1st that a criminal



Michaels
Where Creativity Happens

Letter from the CEO

ary 25, 2014

Our Valued Michaels Customers:

you may have read in the news, data security attacks against retailers have become a major
pic of concern. We recently learned of possible fraudulent activity on some U.S. payment cards
at had been used at Michaels, suggesting we may have experienced a data security attack.

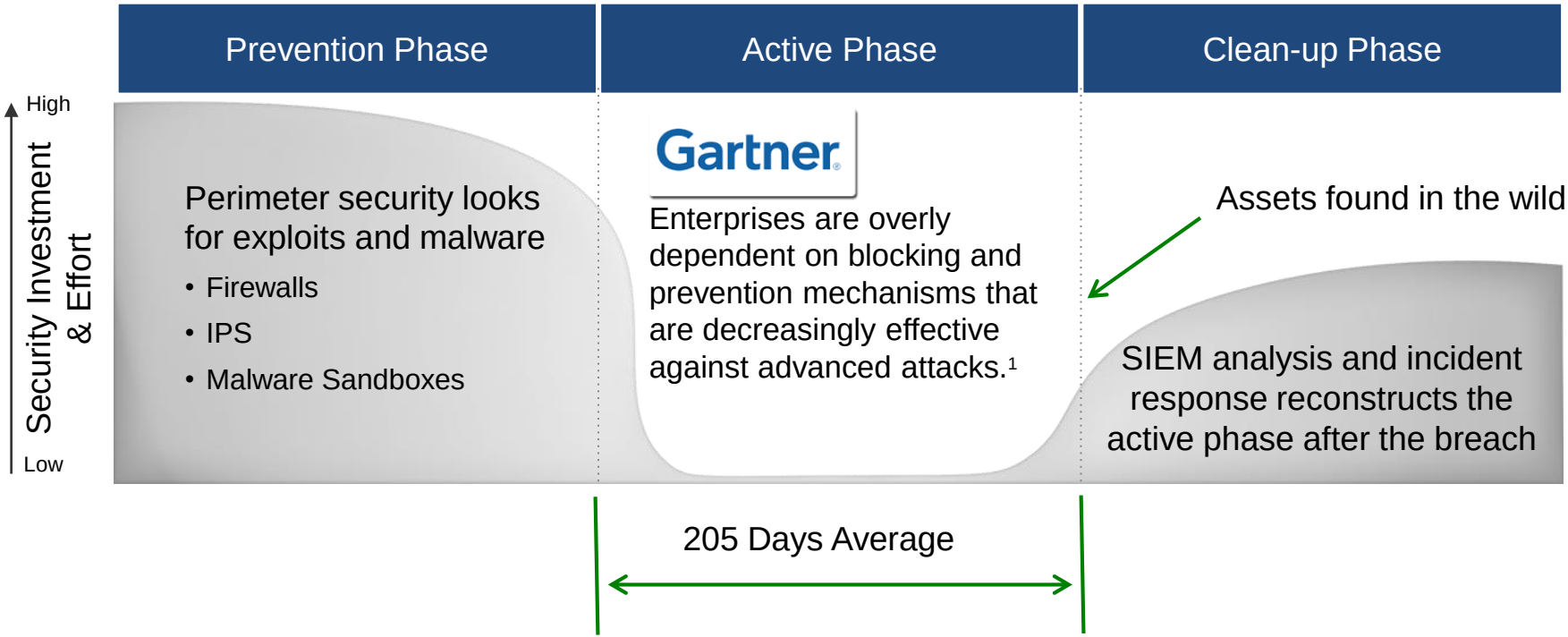
We are working closely with federal law enforcement and are conducting an investigation with
he help of third-party data security experts to establish the facts. Although the investigation is
ongoing, based on the information we have received and in light of the widely-reported criminal
efforts to penetrate the data systems of U.S. retailers, we believe it is appropriate to notify our
customers that a potential issue may have occurred.

Throughout our 40-year history, our customers have always been our number one priority and
we deeply regret any inconvenience this may cause. The privacy and security of our customers'
information is of critical importance to us and we are focused on addressing this issue.

vigilant by reviewing your account statements for unauthorized
affected, you should immediately
of our customers

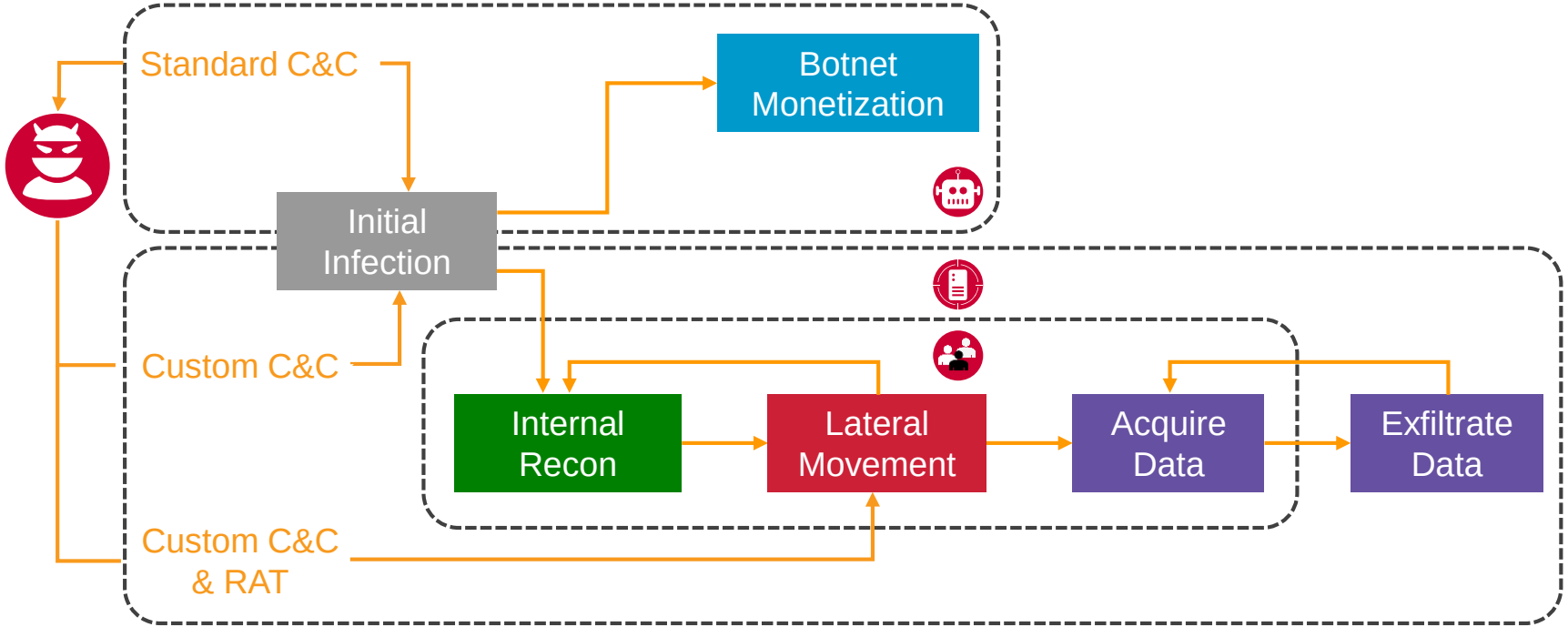
Security investment has traditionally been in two areas

The active phase is the gaping hole in enterprise security

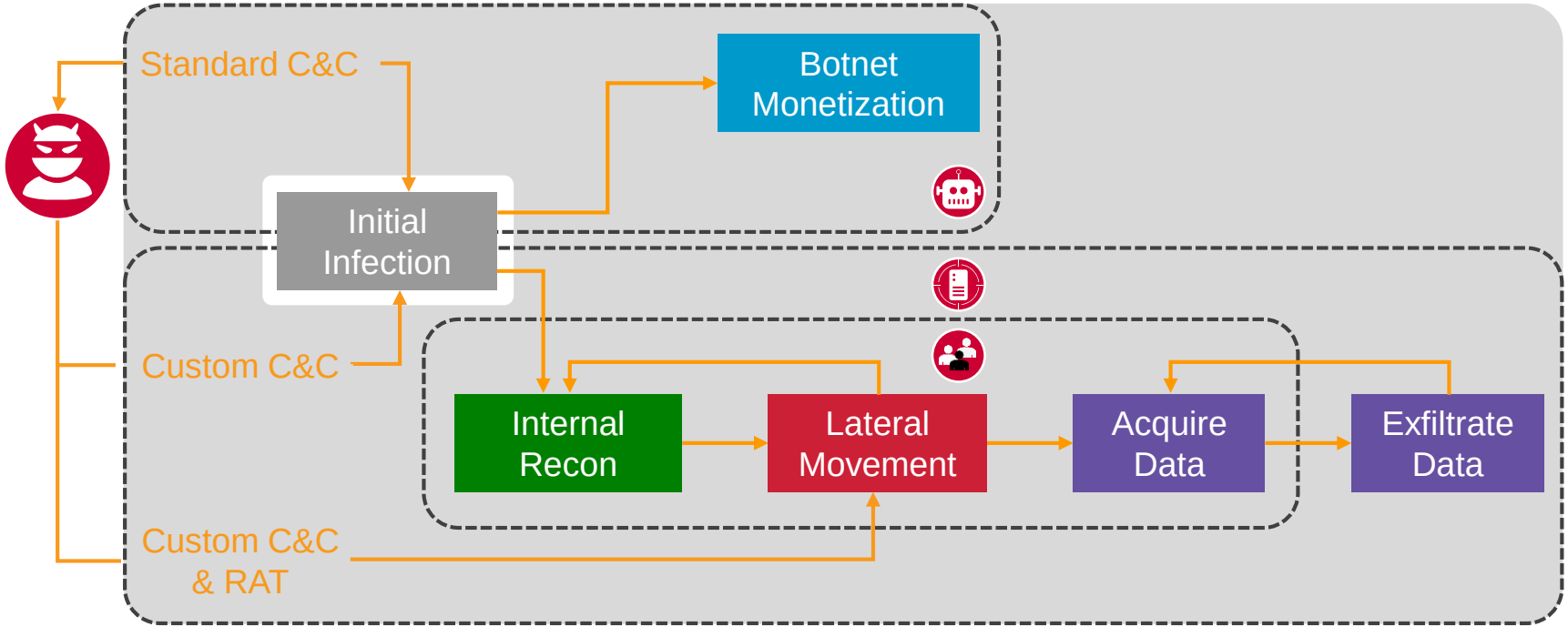


[1]Designing an Adaptive Security Architecture for Protection from Advanced Attacks, 12 February 2014, ID G00259490

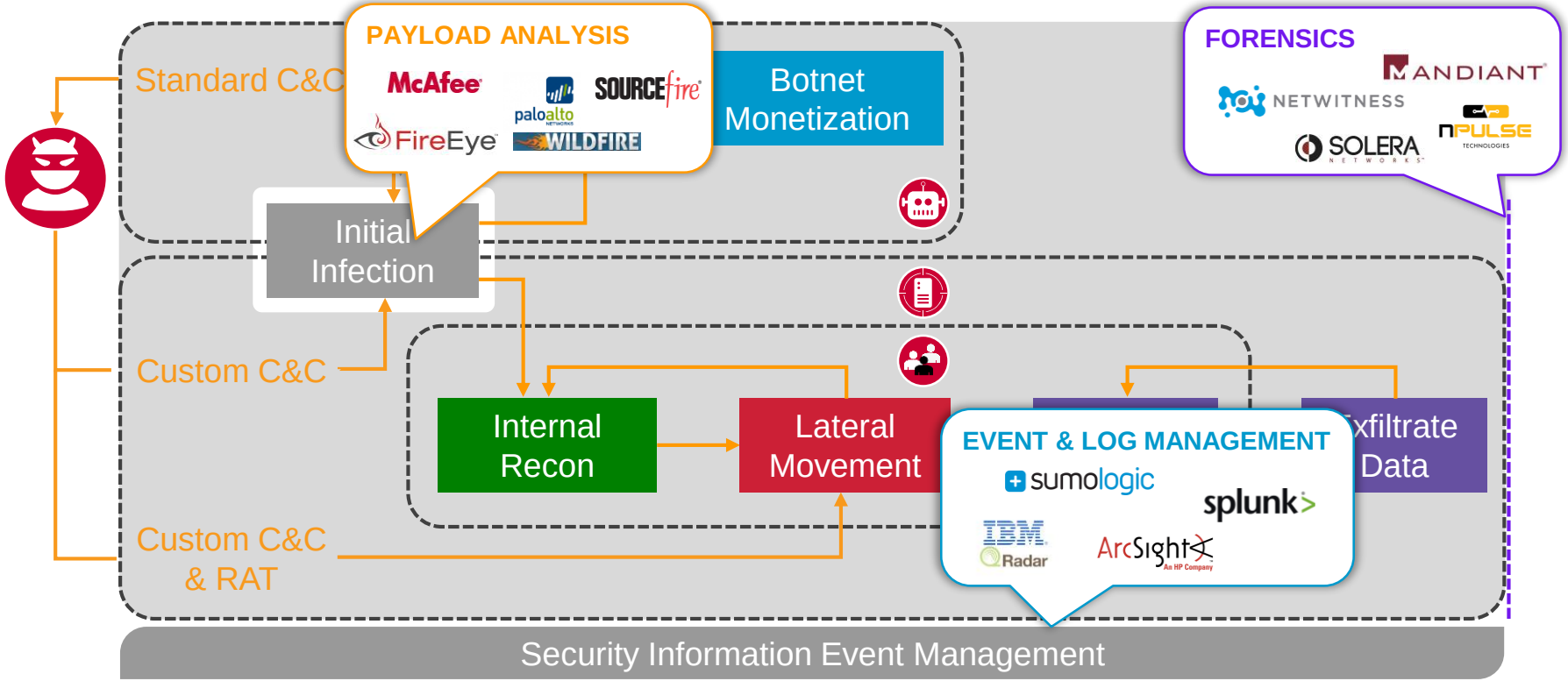
A closer look at the phases of modern cyber attacks



Detects all phases of a cyber attack in progress

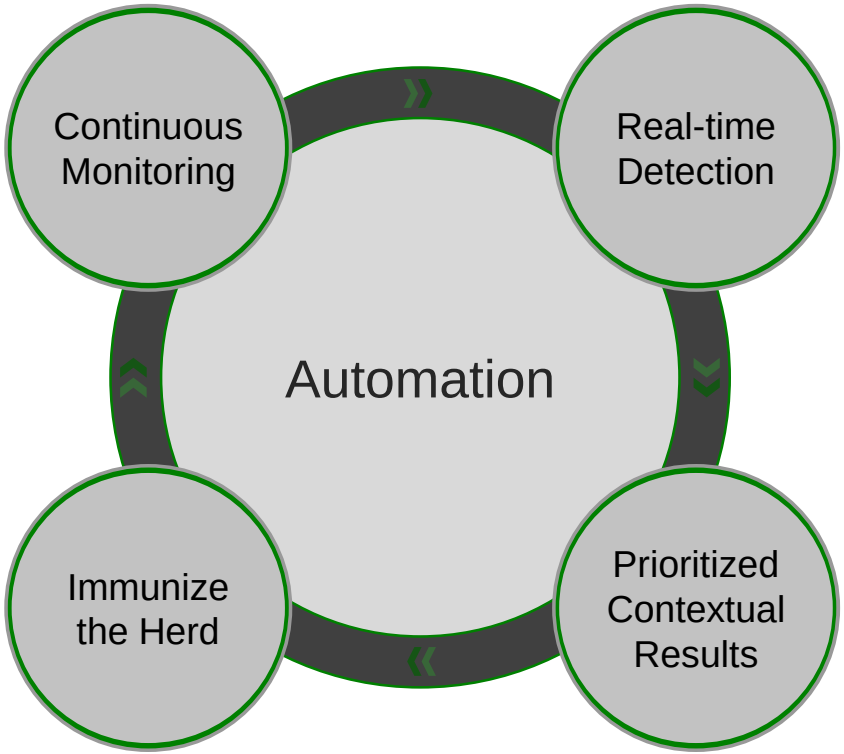


Alignment to existing security solutions



Automatically detect breaches in real time

- All packets
- N-S, E-W traffic
- Any OS, app, device

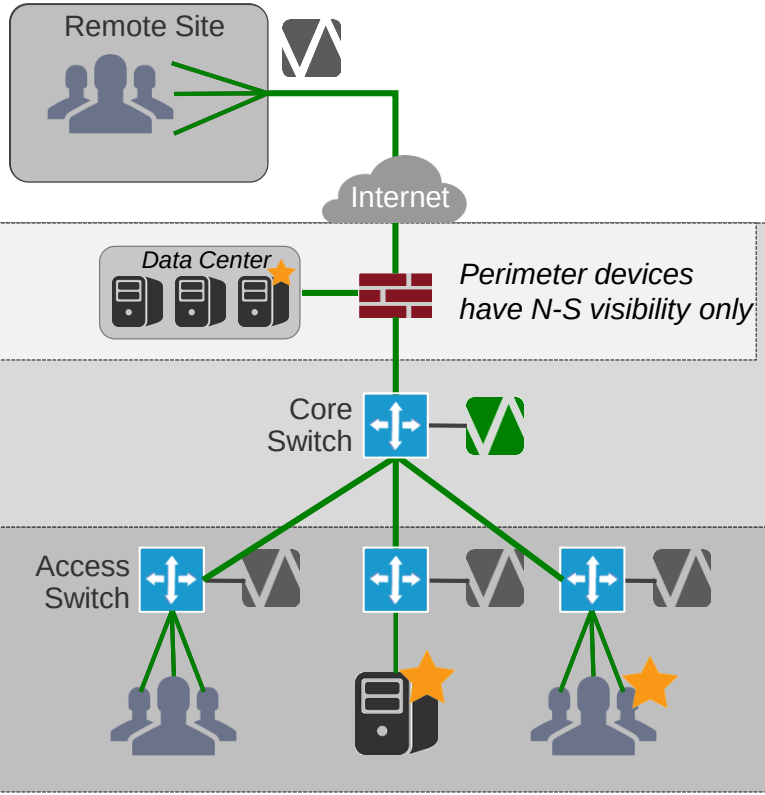


- Behavioral
- Machine learning
- Correlated over time

- Meta data to cloud
- Centralized learning
- No required rules

- Prioritized by risk
- Correlated by host
- Insight into attack

Full cyber security visibility - Watch all critical traffic



Brain

- Deployed at core switch
- Sees N-S Traffic
- Sees E-W Traffic that crosses a switch
  - *Malware spreading, privilege escalation, data theft*

Sensor

- Deployed at access switch/router
- Sees N-S Traffic
- Sees E-W Traffic within the switch
  - *Malware spreading, privilege escalation, data theft*

BEHAVIOR DETECTION TYPES

The Good, The Bad, The Ugly & The Ugliest Behaviors

- The Good
  - ***Legitimate*** applications run by ***authorized*** user/host behavior that acts like an infected host
    - C&C – WebEx, GoToMyPC
    - Scans/Scanners – Nessus, Qualys, VOIP PBX
    - Exfiltration – Box.com, AWS

Whitelist

- The Bad
  - ***Legitimate*** Applications with ***misconfigurations***
    - Brute force – Print server changed settings
    - Scans/Scanners – Asynchronous traffic

Noise – Help Desk

- The Ugly
  - ***Legitimate*** Applications run by ***unauthorized*** user/host behavior that acts like an infected host
    - C&C – WebEx, GoToMyPC, Canvas, CoreImpact,
    - Scans/Scanners – Nessus, NMAP
    - Exfiltration – Box.com, AWS

What Could Happen

- The Ugliest
  - Botnets
    - Pirate cloud – uses resources
    - Spam – hurts reputation
    - Password capture – See Fazio/Target
  - Targeted Attacks
    - Stealing IP/CC/PII
    - Damage - Corruption
    - See SONY

What is Happening

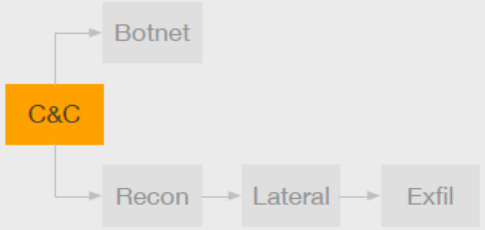
VECTRA

External Remote Access

THREAT RANGE

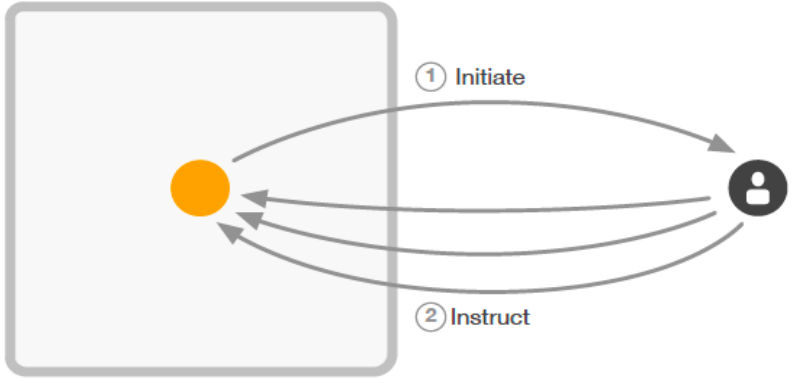
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

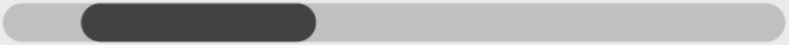
- An internal host is connecting to an external server and the pattern looks reversed from normal client to server traffic; the client appears to be receiving instructions from the server and a human on the outside appears to be controlling the exchange
- The threat score is driven by the quantity of data exchanged and longevity of the connection
- The certainty score is driven by the ratio of data sent by the internal host compared to data received from the server and the longevity of the connection



VECTRA

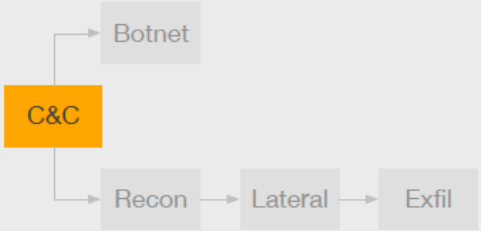
Fake Browser Activity

THREAT RANGE



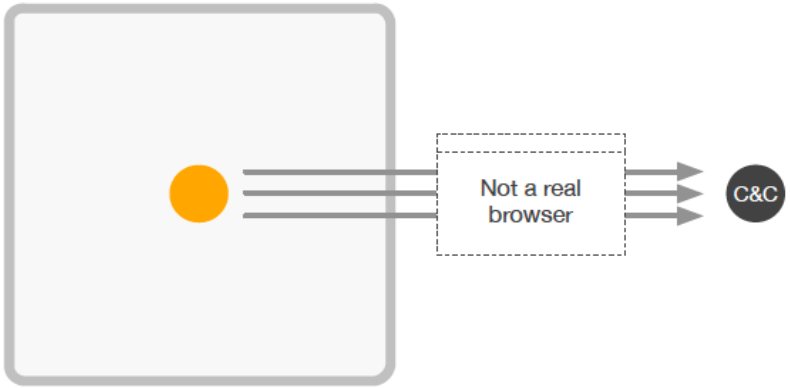
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

- Software on an internal host is impersonating a browser by transmitting a malformed User-Agent string which looks similar to one sent by browsers
- The communication occurs with a regular pattern indicating it is driven by machine rather than human action
- The threat score is driven by the type of activity (e.g. download of binaries) detected in the HTTP request
- The certainty score is driven by the count of HTTP requests with malformed User-Agents

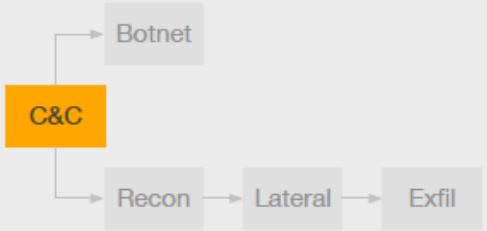


Hidden DNS Tunnel

THREAT RANGE

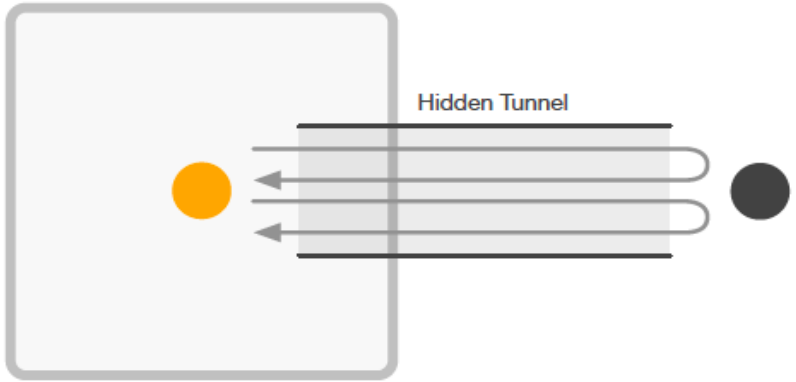
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

- An internal host is communicating with an outside IP using DNS where another protocol is running over the top of the DNS sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal DNS traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions



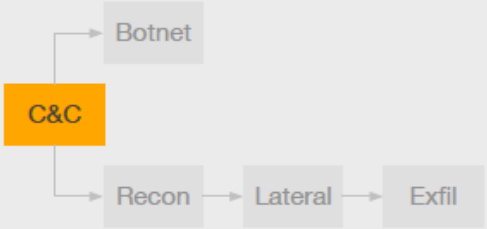
VECTRA

Hidden HTTP Tunnel

THREAT RANGE

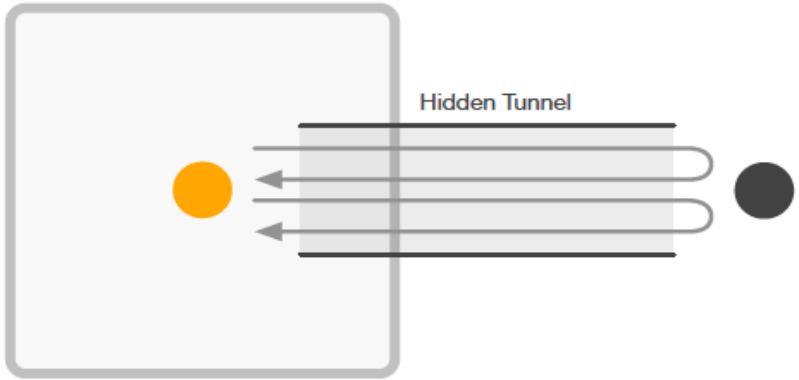
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

- An internal host is communicating with an outside IP using HTTP where another protocol is running over the top of the HTTP sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal Web traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions



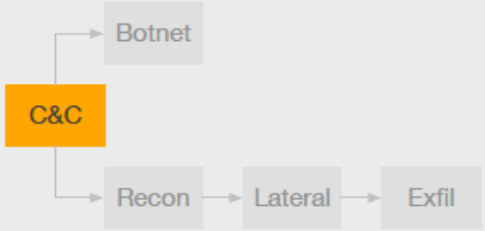
VECTRA

Hidden HTTPS Tunnel

THREAT RANGE

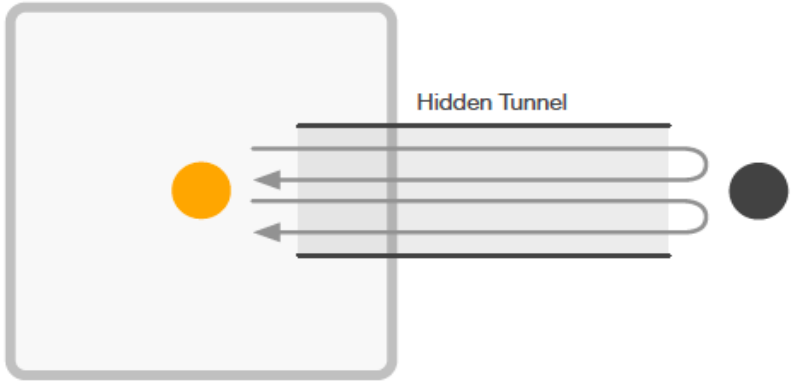
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

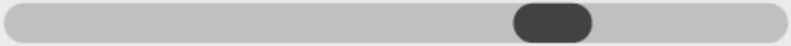
- An internal host is communicating with an outside IP using HTTPS where another protocol is running over the top of the HTTPS sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal encrypted Web traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions



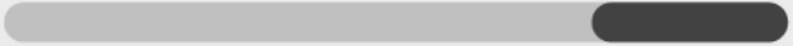
VECTRA

Malware Update

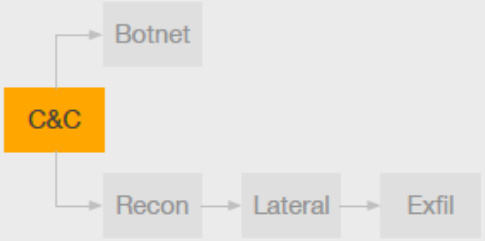
THREAT RANGE



CERTAINTY RANGE

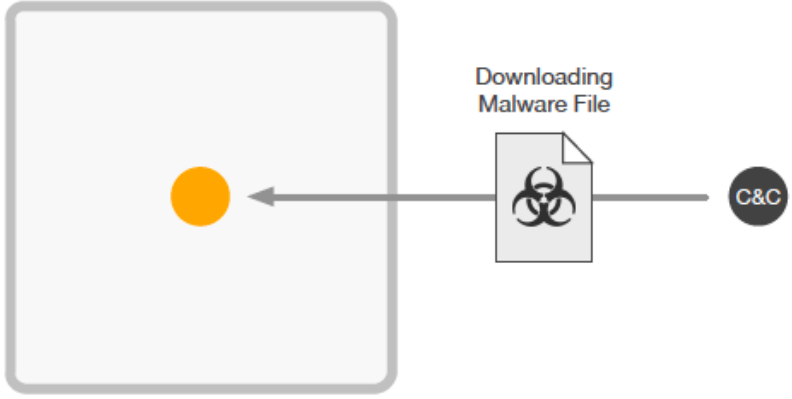


COMMAND & CONTROL



Triggers

- An internal host is downloading and installing software from the Internet
- The downloads are over HTTP, appear to be machine-driven, and follow a suspicious pattern of checking for availability of files before downloading them
- The threat score is driven by the number of executable files being downloaded
- The certainty score is driven by the pattern of machine-generated HTTP requests



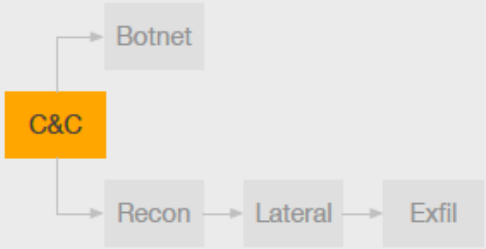
VECTRA

Peer-To-Peer

THREAT RANGE

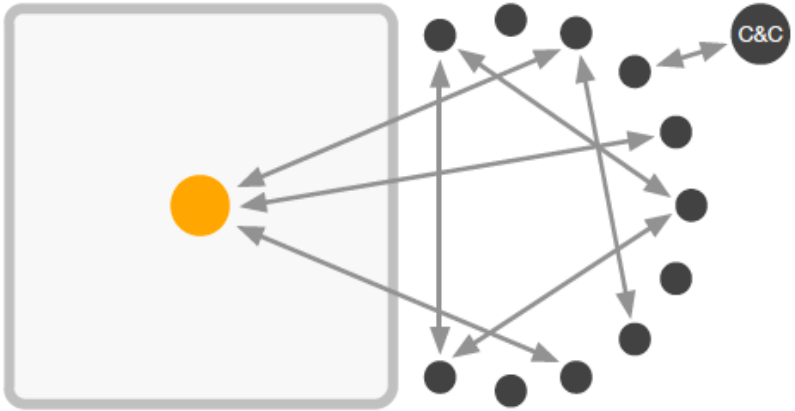
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

- An internal host is communicating with a set of external IP addresses with a pattern and low data rate common to peer-to-peer command and control
- The threat score is driven by the length of time over which communication with peers occurs
- The certainty score is driven by the number of reachable and unreachable peers



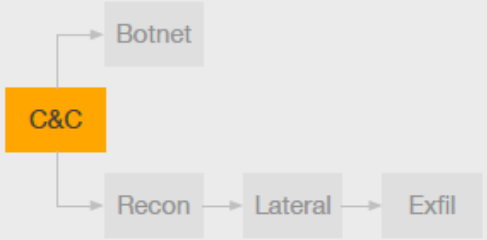
VECTRA

Pulling Instructions

THREAT RANGE

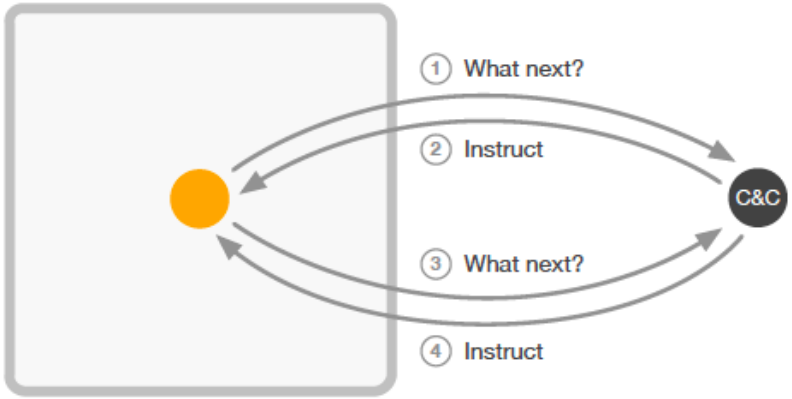
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

- An internal host is persistently communicating with an external entity identified by IP address and/or domain name, where the number and timing of requests and amounts of data exchanged follow a very rigid pattern; this is indicative of requesting instruction on what to do next
- The threat score is driven by the amount of data sent and bytes received
- The certainty score is driven by the frequency of requests



Add

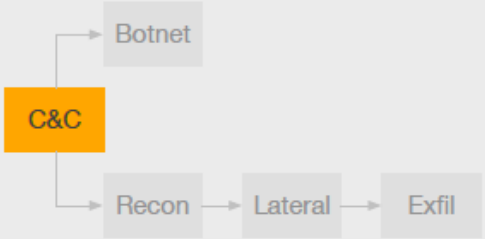
VECTRA

Stealth HTTP Post

THREAT RANGE

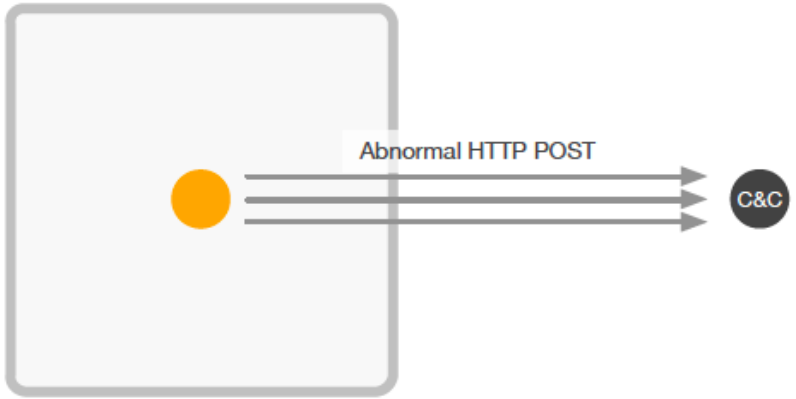
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

- An internal host is sending data to an external system in multiple HTTP Post requests without being referred and without software identification
- These posts appear to be machine generated since they occur with a regular timing pattern
- The threat score is driven by the number of overall sessions and length of their duration
- The certainty score is driven by the number and persistence of HTTP Post requests



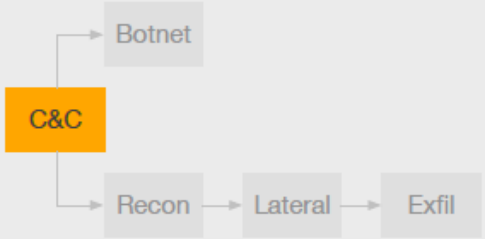
VECTRA

Suspect Domain Activity

THREAT RANGE

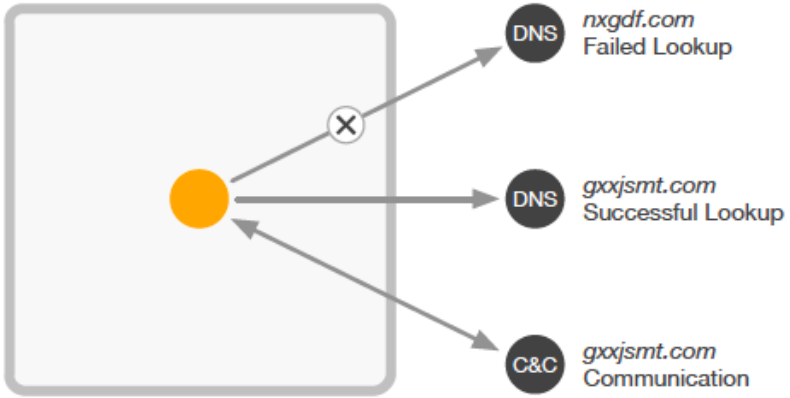
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

- An internal host is looking up suspicious external domains
- Suspicious activity may involve looking up machine-generated domain names or non-existent domain names in rapid succession
- The threat score is driven by successful lookups and the amount of data sent and received
- The certainty score is driven by the breadth of domain lookups and the characteristics of successful lookups



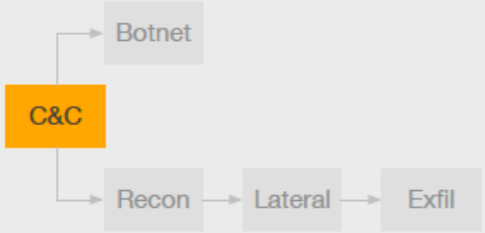
VECTRA

TOR Activity

THREAT RANGE

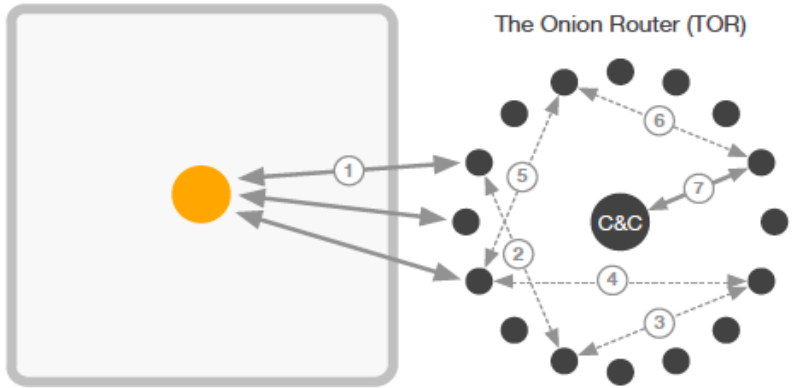
CERTAINTY RANGE

COMMAND & CONTROL



Triggers

- An internal host establishes connections with outside servers where protocol usage and data exchange approximates communicating via The Onion Router (TOR)
- One of the sessions becomes the active TOR session; after some use, the host automatically builds a new virtual circuit and switches to a new TOR session
- The threat score is low for browsing, medium for command and control and high for significant outbound data
- The certainty score is driven by the similarity of the packet-level patterns to that of TOR communication



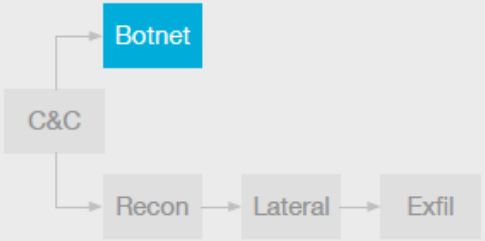
VECTRA

Abnormal Ad Activity

THREAT RANGE

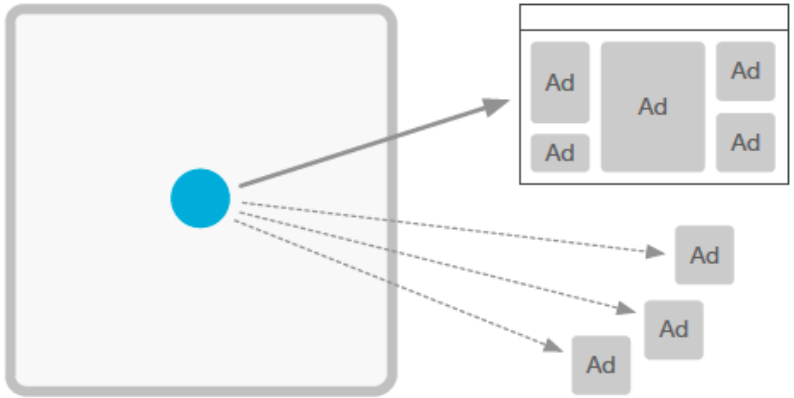
CERTAINTY RANGE

BOTNET ACTIVITY



Triggers

- An internal host is browsing the Web and encountering large amounts of online ads marked by unusually high numbers of HTTP redirects; online ads include display banners, pop-ups or contextual ads
- The host is virtually clicking on non-existent ad impressions with nothing visible on the host's screen; this is known as ad click fraud
- The certainty score is driven by the frequency and quantity of Web-traffic redirection



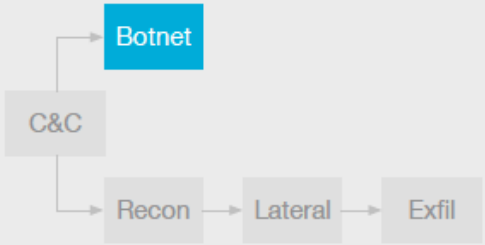
VECTRA

Abnormal Web Activity

THREAT RANGE

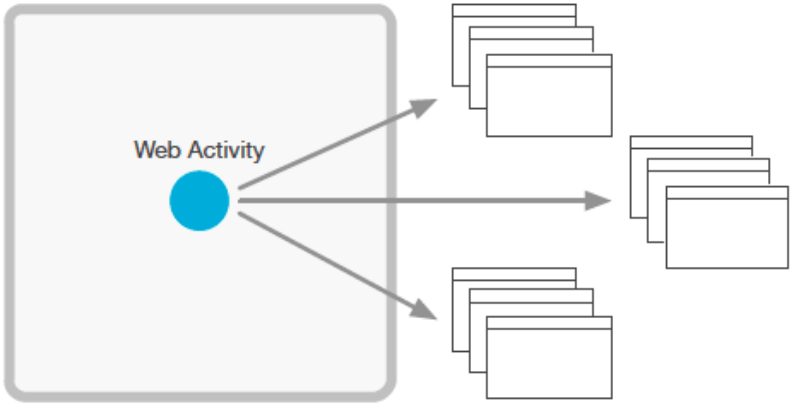
CERTAINTY RANGE

BOTNET ACTIVITY



Triggers

- An internal host is visiting external Web servers and downloading HTML content at a rate which is too high for human consumption
- This is likely happening without the knowledge of the host's user
- The certainty score is driven by the frequency and quantity of opened Web pages



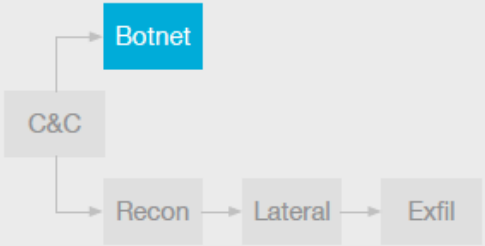
VECTRA

Bitcoin Mining

THREAT RANGE

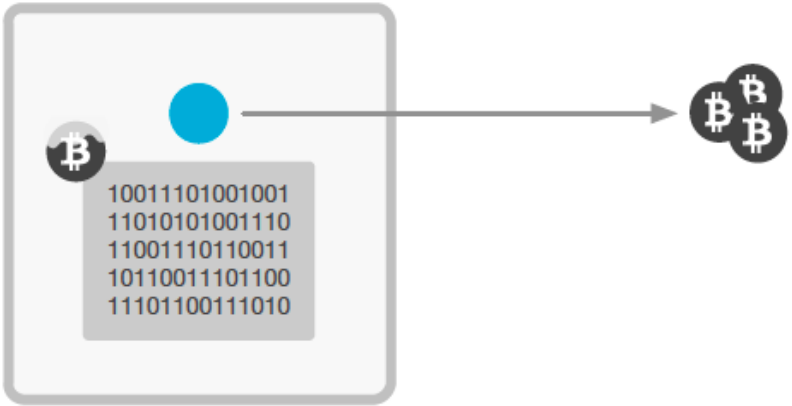
CERTAINTY RANGE

BOTNET ACTIVITY



Triggers

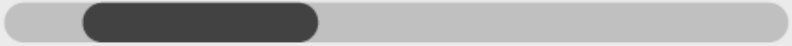
- An internal host is mining units of cyber currency of which Bitcoin is the most common variant
- Cyber currency mining is a common way for botnet operators to make money
- Cyber currency mining may involve communication via HTTP or via the Stratum mining protocol
- The threat score is driven by the rate at which mining activity is performed



VECTRA

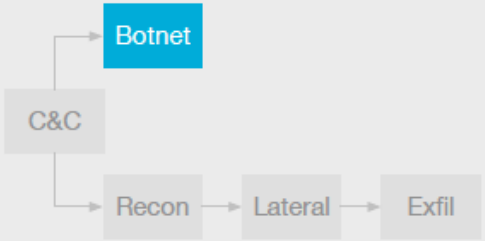
Brute-Force Attack

THREAT RANGE



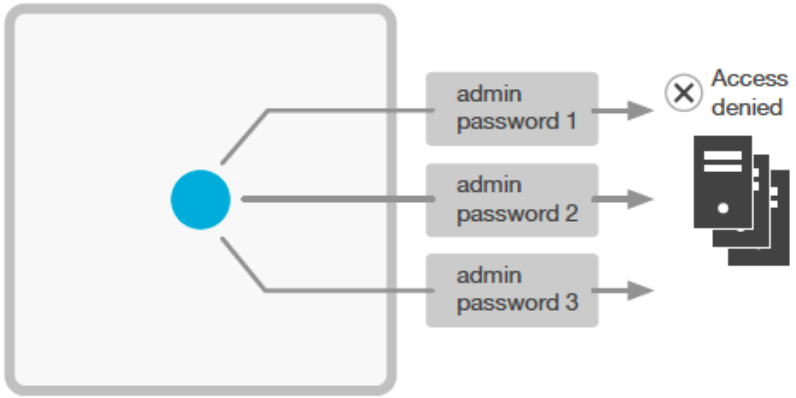
CERTAINTY RANGE

BOTNET ACTIVITY



Triggers

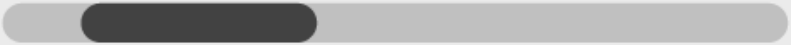
- An internal host is making an unusually high number of login attempts, a behavior which is consistent with a brute-force password-guessing attack on one or more external servers
- Such attacks can be performed via a number of different protocols
- The threat score is driven by the rate of attempts and timing at which the attack is performed
- The certainty score is driven by total number of sessions in the attack



VECTRA

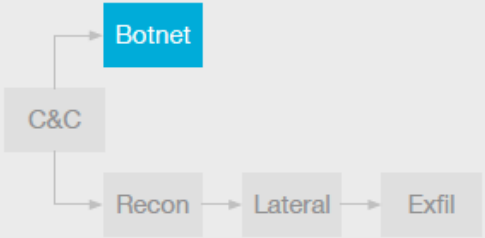
Outbound DoS

THREAT RANGE



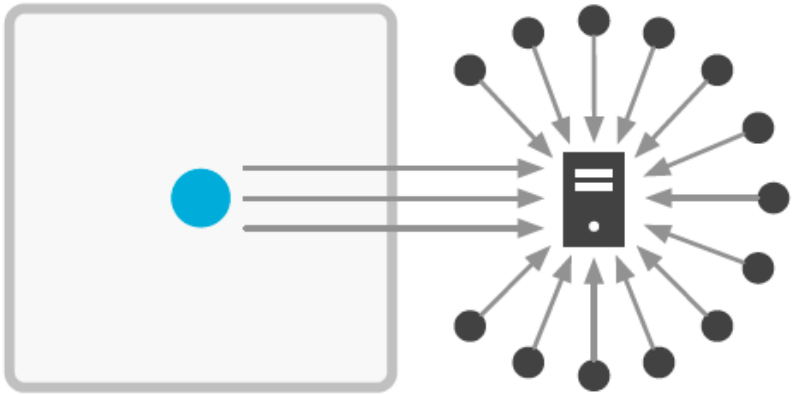
CERTAINTY RANGE

BOTNET ACTIVITY



Triggers

- An internal host appears to be taking part in a Denial-of-Service (DoS) campaign on an external IP address
- The form of DoS detection has two types: “SYN Flood” and “Slowloris”
- The threat score is driven by the volume of data sent in the detected DoS sessions
- The certainty score is driven by the volume of DoS sessions and the length of period the attack is sustained



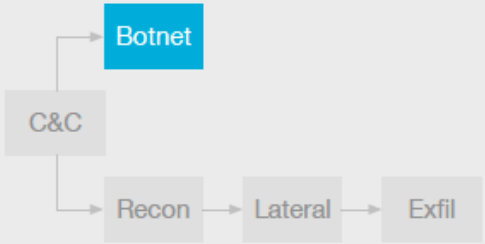
VECTRA

Outbound Scan

THREAT RANGE

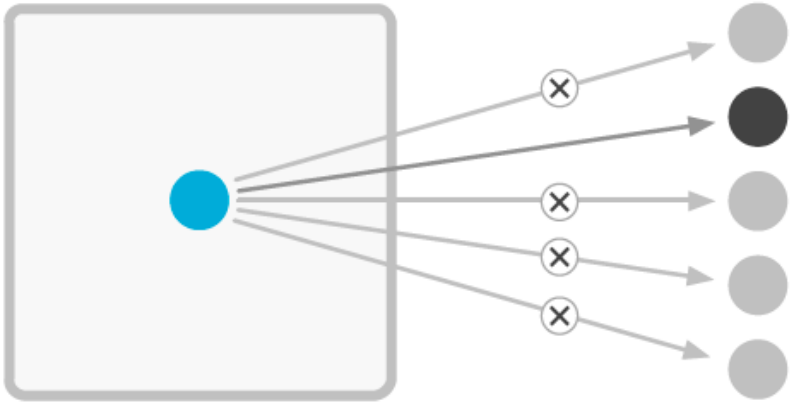
CERTAINTY RANGE

BOTNET ACTIVITY



Triggers

- An internal host is generating many more unsuccessful attempts to connect to external services than successful ones
- The threat score is driven by the breadth of IP addresses scanned and the pace at which the scan occurs
- The certainty score is driven by the failure rate of outbound connection attempts



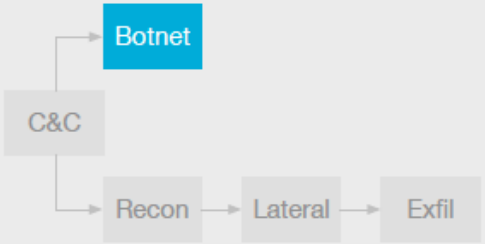
VECTRA

Outbound Spam

THREAT RANGE

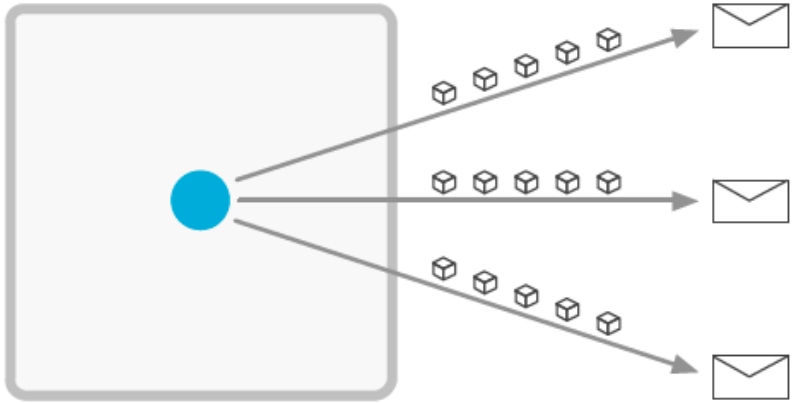
CERTAINTY RANGE

BOTNET ACTIVITY



Triggers

- An internal host uses an unusual number of mail servers to send many email messages via SMTP or HTTP, which looks like email spam activity
- The threat score is driven by the volume of data sent in the detected mail sessions
- The certainty score is driven by the volume of sessions and the number of mail servers used to send the email messages



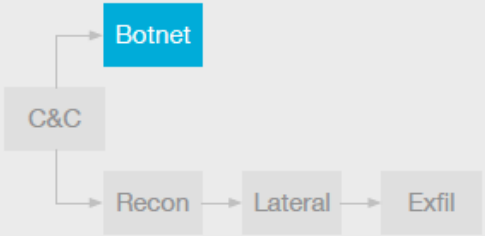
VECTRA

Relay Communication

THREAT RANGE

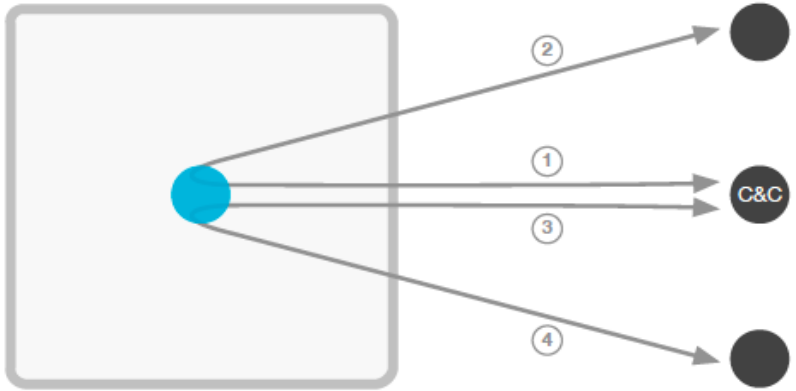
CERTAINTY RANGE

BOTNET ACTIVITY



Triggers

- An internal host initiates an outbound connection to its command and control (C&C) server to receive instructions; the host then connects to one or more external systems with the C&C server providing instructions on how to target them
- The host forwards the payload to the targets, the response from which it sends back to C&C server
- The threat score is driven by the volume of data exchanged
- The certainty score is driven by the number and relative timing of inbound and outbound connections



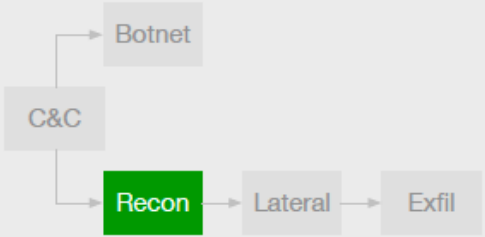
VECTRA

Internal Port Scan

THREAT RANGE

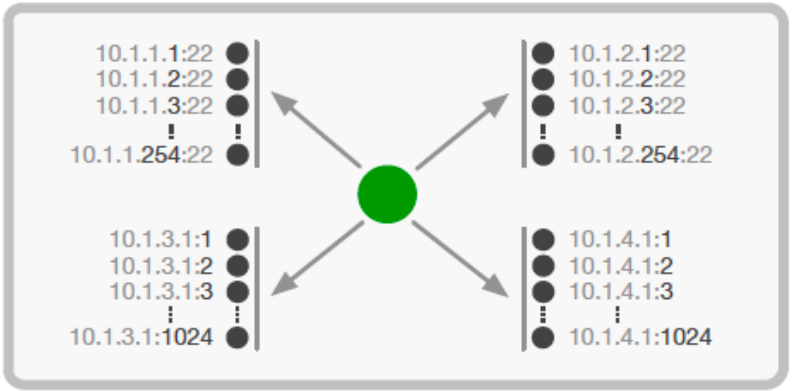
CERTAINTY RANGE

RECONNAISSANCE



Triggers

- An internal host has either attempted contact with a large number of internal IP addresses on a small number of ports – a network scan – or with many ports on a small number of internal IP addresses – a host scan
- The threat score is low for scattered scans, medium for scanning a single port across many IP addresses and high for thorough scans across many ports on a single IP address
- The certainty score is driven by the quantity and frequency of scanning attempts

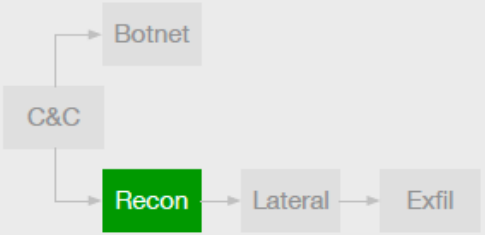


Internal Darknet Scan

THREAT RANGE

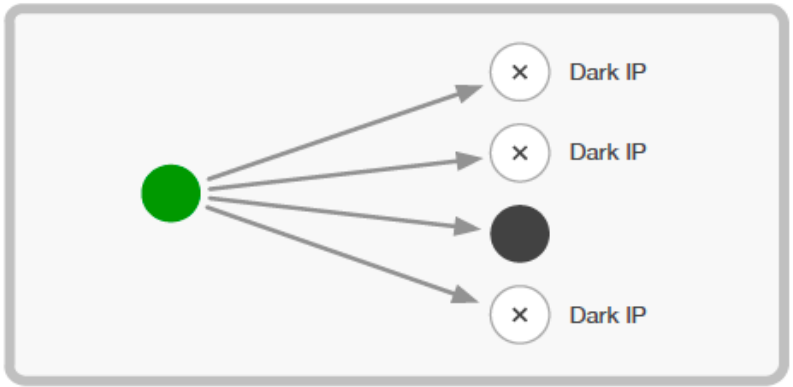
CERTAINTY RANGE

RECONNAISSANCE



Triggers

- An internal host has contacted a number of internal IPs that have not been active in the recent past
- Darknet detections cover longer periods than port scans and ignore contact to systems which do not respond to this host, but which are otherwise active
- The threat score places large weight on the spread of IPs, medium for spread of ports and low for the total number of dark IPs contacted
- The certainty score places equal weight on the spread of IPs, spread of ports and number of dark IPs contacted



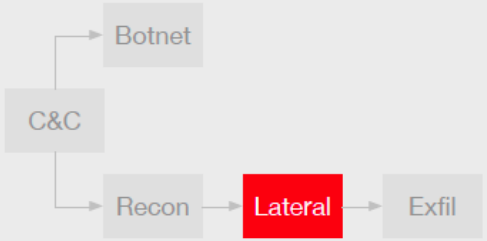
VECTRA

Automated Replication

THREAT RANGE

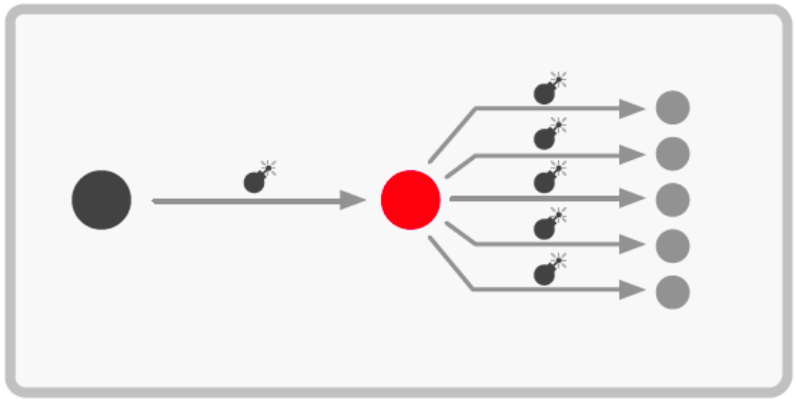
CERTAINTY RANGE

LATERAL MOVEMENT



Triggers

- An internal host is sending very similar payloads to several internal targets
- This may be the result of an infected host sending one or more exploits to other hosts in an attempt to infect them
- The certainty score is driven by the number of targeted hosts and the detection of an upstream propagator
- The threat score is driven by the number of targeted hosts and number of different exploits, particularly exploits on different ports

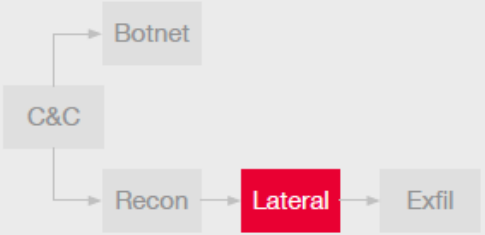


Brute-Force Attack

THREAT RANGE

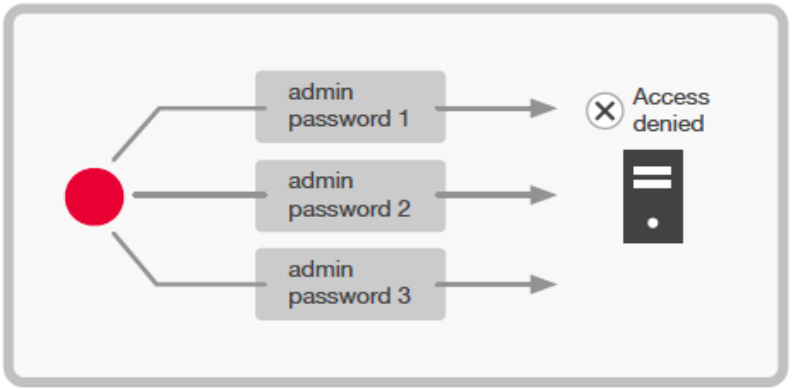
CERTAINTY RANGE

LATERAL MOVEMENT



Triggers

- An internal host is making many login attempts on an internal system, behavior which is consistent with a brute-force password attack
- Such attacks can be performed via different protocols (e.g. RDP, VNC, SSH, FTP, HTTP/S, SSL/TLS) and may also be a Heartbleed attack (e.g. memory scraping)
- The threat score is driven by the number of attempts and timing with which the attack is performed
- The certainty score is driven by the total number of sessions in the attack

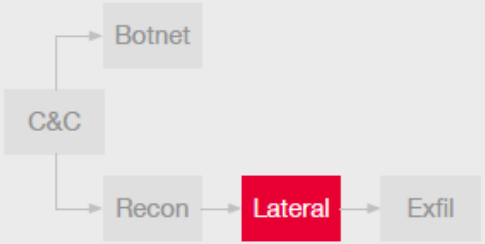


Kerberos Client Activity

THREAT RANGE

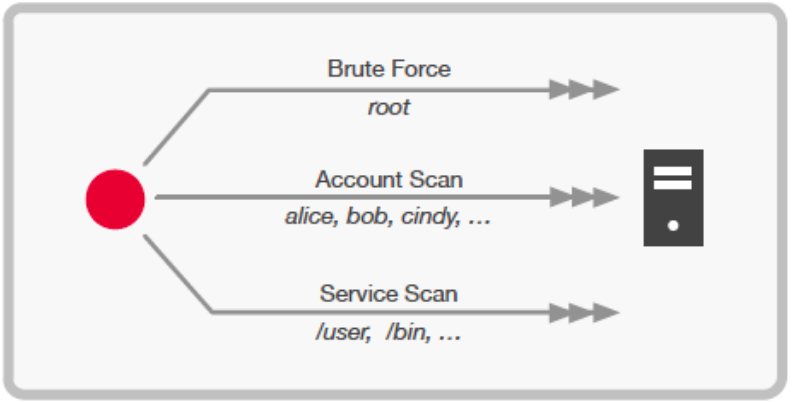
CERTAINTY RANGE

LATERAL MOVEMENT



Triggers

- A Kerberos client attempts a suspicious amount of authentication or service requests using either a small number of services and accounts (brute force), or a larger number of services and accounts (scan)
- The threat score is driven by the likely root cause of the authentication, either account/service scan or brute-force attack
- The certainty score is driven by deviations from previously observed usage patterns for each host



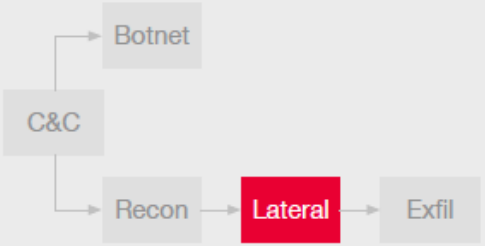
VECTRA

Kerberos Server Activity

THREAT RANGE

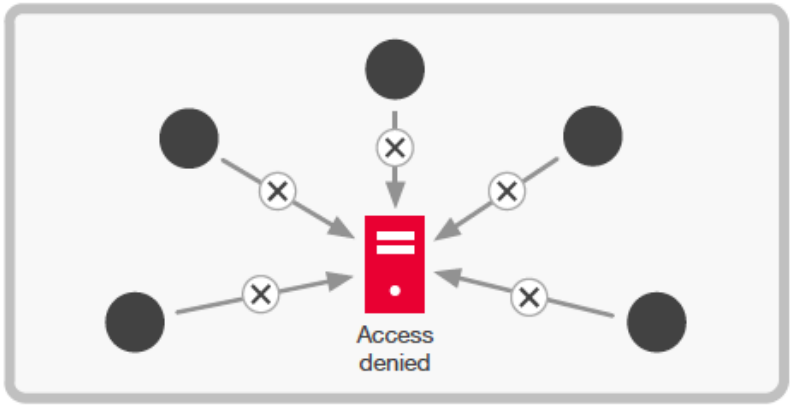
CERTAINTY RANGE

LATERAL MOVEMENT



Triggers

- A Kerberos server denies a suspicious amount of authentication requests from multiple clients using multiple services
- The threat score is driven by the type of anomaly detected, either account/service scan or brute-force attack
- The certainty score is driven by the deviations from previously observed usage patterns for the server



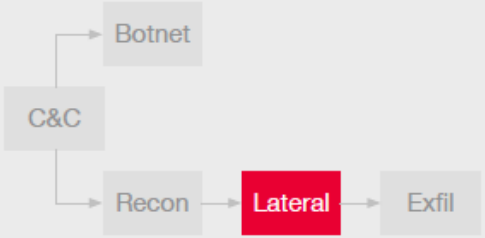
VECTRA

SQL Injection Activity

THREAT RANGE

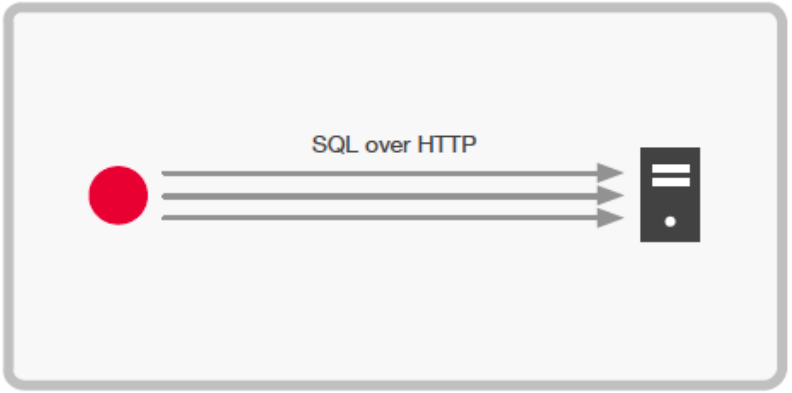
CERTAINTY RANGE

LATERAL MOVEMENT



Triggers

- An internal host sends requests to a Web server and embeds SQL fragments into HTTP Post data or the URL to gain access to the backend database; the requests appear machine-generated due to the large volume and rate of arrival
- The threat score is driven by the volume of HTTP requests containing SQL fragments and the size of the returned data
- The certainty score is driven by the number of requests sent and their classification as SQL fragments



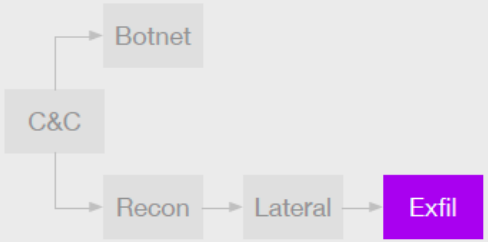
VECTRA

Data Smuggler

THREAT RANGE

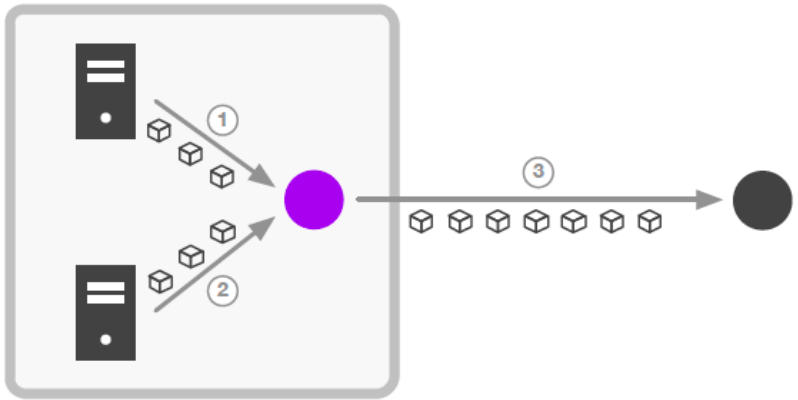
CERTAINTY RANGE

EXFILTRATION



Triggers

- An internal host is acquiring a large amount of data from one or more internal servers and is subsequently sending a significant amount of data to an external system
- The threat score is driven by the amount of data transmitted
- The certainty score is driven by the relationship between the time and size of the data acquired and the time and size of the data sent



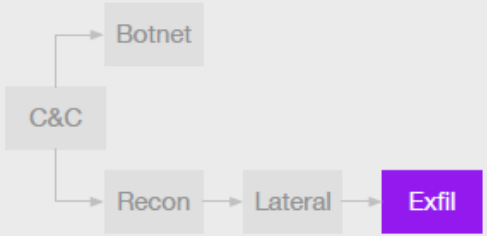
VECTRA

Hidden DNS Tunnel

THREAT RANGE

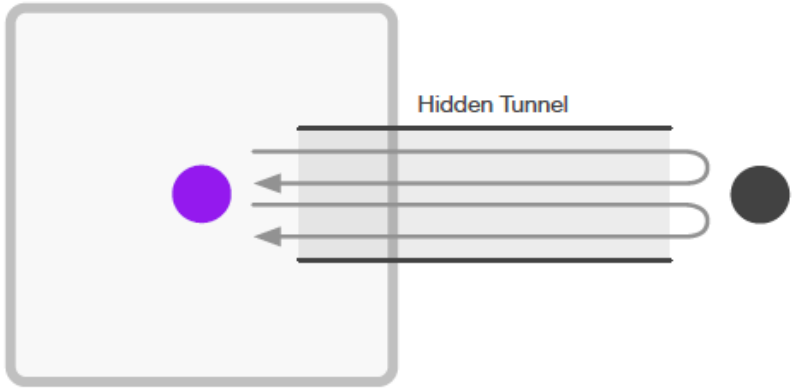
CERTAINTY RANGE

EXFILTRATION



Triggers

- An internal host is communicating with an outside IP using DNS where another protocol is running over the top of the DNS sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal DNS traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions



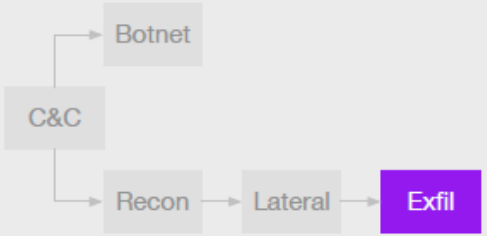
VECTRA

Hidden HTTP Tunnel

THREAT RANGE

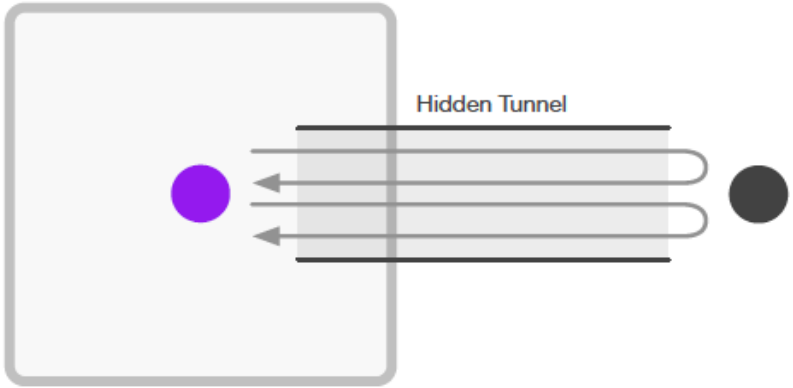
CERTAINTY RANGE

EXFILTRATION



Triggers

- An internal host is communicating with an outside IP using HTTP where another protocol is running over the top of the HTTP sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal Web traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions

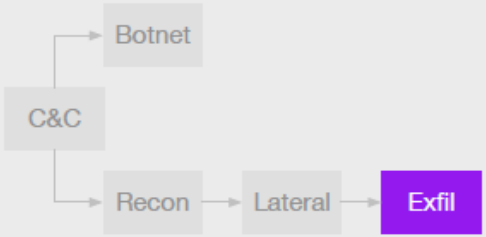


Hidden HTTPS Tunnel

THREAT RANGE

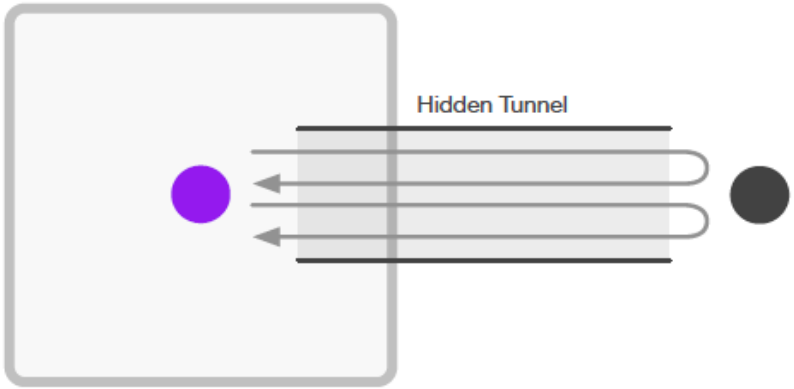
CERTAINTY RANGE

EXFILTRATION



Triggers

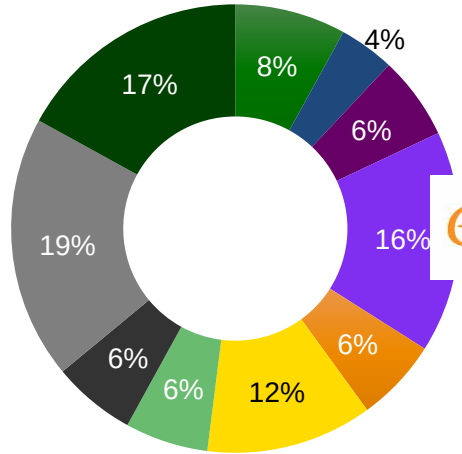
- An internal host is communicating with an outside IP using HTTPS where another protocol is running over the top of the HTTPS sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal encrypted Web traffic
- The threat score is driven by the quantity of data sent via the tunnel
- The certainty score is driven by the number and persistence of the sessions



VECTRA


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

Sample Vectra customers and vertical industries



The team

Leadership

Hitesh Sheth
President & CEO
Aruba, Juniper, Cisco

Oliver Tavakoli
CTO
Juniper, Funk

Jason Kehl
VP Engineering
Juniper, Cisco, Ironport

Alain Mayer
VP Product Mgmt
Cyphort, Redseal

Mike Banic
VP Marketing
HP, Juniper, Peribit

Rick Geehan
VP Americas Sales
Riverbed

Gerard Bauer
VP EMEA Sales
Riverbed

Mission

Automatically detect ongoing cyber attacks in real time

Customers

Education
Health

Energy
S&L Govt

Entertainment
Media

Finance
Technology

Legal
Other

Industry Recognition

Gartner 2015 Cool Vendor

RSAC Innovation Sandbox FINALIST

Computer Technology Review MVP Awards Most Valuable Products 2015

Cutting Edge Network Security Solution 2015 CDM

Cool Tool Award 2015 Winner network digest

Investors

khosla ventures

ACCEL PARTNERS

IA VENTURES

AME CLOUD VENTURES

intel capital

JUNOS INNOVATION FUND

LIVE DETECTION REVIEW