Global Information Assurance Certification Paper

Investigative Forensic Workflow-based Case Study for Vectra and Cyphort

GIAC (GCFE) Gold Certification

Author: Jennifer L. Mellone, jmellone@alum.wpi.edu

Advisor: Richard Carbone

Accepted: November 23, 2015

Abstract

This paper addresses real-world enterprise Vectra and Cyphort detections and walks through a detailed forensic workflow case study resulting in conclusive findings. Even though the workflow is based on the Vectra and Cyphort commercial detection platforms, this workflow is applicable to security events generated by other commercial or free products. Vectra performs behavioral analysis to detect malicious activities on the network. Cyphort performs malware detection. Upon notification of Vectra and Cyphort events, the security analyst must drill into the events with respect to the target host to find out if it was the victim of a malicious attack. This requires an investigative workflow using forensic tools and Internet research. Free forensic tools are primarily used for the analysis, but commercial products Bit9 and Carbon Black are also used to corroborate evidence. The workflow is the same whether the findings are confirmed to be true or false positives.

1. Introduction

Enterprise and organizational networks are vulnerable to malware in part because of users' endpoint laptops. Users routinely disconnect them from the corporate network with its due diligence perimeter security, connect to public and home networks, and reconnect to the corporate network. They may unwittingly click URLs or download software and files while on any network and become infected, possibly unbeknownst to the endpoint anti-virus and anti-malware software.

To help mitigate this problem, security engineers installed two diverse commercial detection product platforms from Silicon Valley "new guard" companies in their real-world production enterprise network infrastructure. The purpose of this equipment deployment is to produce visibility of potentially harmful network activities. It augments the existing signature-based intrusion prevention system (IPS) deployed as a component of their firewall. Both products, like an IPS, produce alerts that require human investigation. The operational security analyst, lacking any experience with the new equipment, must decide if the alerts are true or false positives. This requires a thorough investigative methodology.

The intent of this paper is to walk through an investigation as a case study, to see the methodology and thought process an analyst would use to determine if the alerts generated by the two new products are true or false positives. If there is a true positive (malicious detection), the analyst will determine if there is an actual security incident and execute the appropriate incident response procedure. In the case of a false positive (not a malicious detection), the analyst will apply filters to tune out future similar events and gradually learn what normal and abnormal behavior is. When future similar events take place, the analyst will have more experience and resolve alerts more expeditiously. Once this case study is understood, analysts can use it as a guide to perform investigations as part of their incident response playbook or use it in their syllabus to train new analysts.

The two new aforementioned products are Vectra (www.vectranetworks.com) and Cyphort (www.cyphort.com). Vectra performs behavioral analysis to detect malicious activities on the network that could be the result of malware execution. Cyphort performs malware detection.

Jennifer L. Mellone, jmellone@alum.wpi.edu

In this case study, both products produced alerts concerning a particular corporate laptop loaded with the Windows 7 Professional operating system. This laptop is the subject of this forensic investigation whose purpose is to determine if the Vectra and Cyphort detection alerts are true or false positives. Several tools are used to perform the investigation to resolve the alerts. The commercial Bit9 Security Platform (formerly Parity) endpoint protection and Bit9's Carbon Black endpoint detection and response products are used in the investigation. In addition, free forensic software tools installed on a forensic analysis workstation are utilized.

The methodology that the analyst uses to resolve Vectra and Cyphort detection alerts is presented at a high theoretical level in Section 2.4. Section 3 applies the methodology and walks through a real-world investigation in detail to demonstrate how the case is resolved.

2. Background

2.1. Experiments and Research

The experiment is in the form of an investigative case study. The purpose is to analyze some Vectra detection alerts of interest that are determined to be associated with a corporate laptop, and determine if they are true or false positives. The rationale for this determination is that a true positive is a security incident that requires action, such as reimaging the laptop.

Cyphort alerts pertaining to that same laptop that took place around the time of the Vectra detections are also investigated to see if they are related. The Vectra and Cyphort displays are analyzed at their face values, and packet captures pertaining to the events are downloaded from Vectra. Simple Internet research on the IP addresses and ports with respect to details and reputations is conducted, but that is not necessarily enough information to resolve the alerts and determine if Vectra showed malicious activities. Cyphort is examined in a similar manner. Knowing whether Cyphort events are related to those of Vectra can help tell a story. For example, the user downloads a malicious executable to a laptop and Cyphort detects the download. Next, upon execution of the downloaded file, the laptop sends out command and control (C2) traffic that is detected with Vectra.

Whether or not a correlation took place, it would be helpful to know if the laptop was infected. This would be an incident, and the response would be to potentially reimage the host

to prevent additional harm to it and other corporate assets. In order to move the investigation forward, traditional disk forensics using free software tools installed on an analysis workstation are performed against the forensic disk image of the laptop. The goal is to seek evidence concerning the Vectra detection. For example, if Skype or uTorrent activities are suspected from the analysis of Vectra, forensics can be used to prove that these activities occurred around the time of the Vectra detections. This would confirm a false positive. The combination of security threat intelligence analysis and endpoint threat protection techniques is accomplished with the Bit9 Security Platform and the Carbon Black endpoint threat detection and response products. They are employed as forensic systems to look for malicious software and behavior on the laptop to corroborate evidence gathered so far. They are also used to confirm Cyphort malware downloads in a safe virtual environment.

It is demonstrated that the methodology used in this case study answers the question – are the Vectra and Cyphort detections true or false positives?

2.2. Enterprise Network Infrastructure and Systems Used

The subject enterprise network with the products and systems used in this real-world investigative case study are shown in Figure 1. The diagram is condensed for simplicity because there are multiple network devices making up the corporate infrastructure, some of which are in high-availability mode. Vectra and Cyphort take center stage, as their detections concerning a user's corporate laptop (also in the spotlight) are under investigation. Supporting systems used in the investigation include the Bit9 server, Carbon Black server, and forensic analysis workstation loaded with analysis tools.

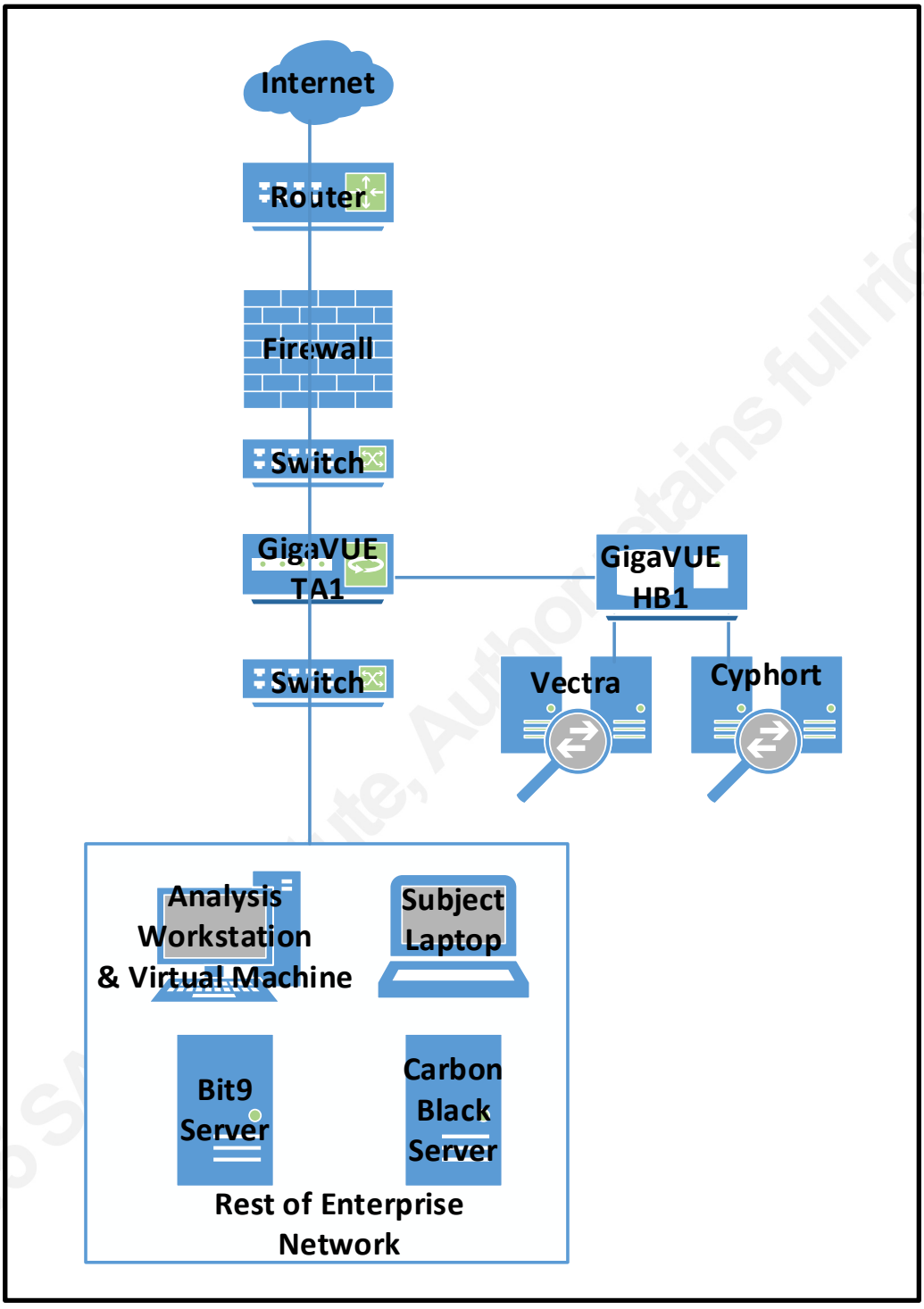


Figure 1: Subject Enterprise Network Diagram

2.2.1. Network

1. Backbone - Devices on the corporate network include switches, routers, firewalls (including one with a built-in IPS), and application delivery controllers. These legacy network components are depicted in Figure 1 that show the placement of products and tools on the network that are relevant to this investigation.
2. Security Platform Connectivity (Gigamon) - The deployment of the Vectra and Cyphort security detection platforms provide justification for the network team to procure a Gigamon Unified Visibility Fabric. Gigamon is used to deploy multiple security monitoring tools instead of using a traditional tap or switch span port. Vectra and Cyphort tools were the immediate need, but other products to be determined would come online in the future and could be connected to the Gigamon. The Gigamon GigaVUE-TA1 connects to the corporate infrastructure and aggregates the switches. GigaVUE-HB1 is the fabric foundation of connecting the Vectra and Cyphort security platforms. The benefits of Gigamon include avoid potential oversubscription, provide scalability, flexibility and avoid increased switch CPU utilization caused by port spanning, and packet de-duplication.

2.2.2. Systems

1. Vectra - Vectra is the heart of this case study because its detection alerts pertaining to a corporate laptop are under investigation. It performs behavioral analysis to detect malicious activities on the network, without using signatures. It receives threat intelligence from the Vectra cloud service to support its analytical function. This signatureless behavioral capability was missing from the corporate network, which was why it was procured. It can be deployed in a distributed architecture to cover multiple locations using X-series platforms and S-series sensors and can be deployed passively on a span or tap port to monitor traffic. Alternatively, sensors can be deployed inline, and will fail open to allow for continuous traffic flow. In this implementation, a Vectra X-series platform is passively deployed and connected using the Gigamon GigaVUE-HB1/TA1 Unified Visibility Fabric to scan the aggregated traffic from the switches and firewall. The management interface is connected to a switch on the corporate network, but is not illustrated in Figure 1 for simplicity. Vectra's detection volume on the subject

network is low, about two or three per day. The latest Vectra software version in use is 1.9.4.844, but an earlier version was used when the laptop detections took place. See Section 2.3.1 for further details on Vectra.

2. Cyphort - Cyphort is also the center of attention for this case study because its detection alerts pertaining to the same corporate laptop are also under investigation. The Cyphort Advanced Threat Defense Platform continuously monitors network traffic to detect advanced threats. Malware detection and sandboxing functionality was missing on the network, thus justifying its purchase. Cyphort platforms can be deployed in a distributed architecture to cover multiple locations using Core platforms, and in various locations, the Collector platforms. In this deployment, one Cyphort Core platform is deployed as a bare-metal appliance and connected passively through the Gigamon GigaVUE-HB1/TA1 Unified Visibility Fabric. The management interface is connected to a switch on the corporate network, but this is not illustrated in Figure 1 for the sake of simplicity. There is no implementation of the Cyphort blocking capability, as it was desired to instead use the security information and event management (SIEM) tool for correlation and scripts for blocking malicious IP addresses at the firewall currently under development at the time of the investigation. Cyphort detects one or two events per week on the subject network. The latest Cyphort software version used is 3.2.1.34, but an earlier version was used when the laptop detections took place. See Section 2.3.2 for further details on Cyphort.
3. Subject User Laptop - The subject of this forensic investigation is a user endpoint (laptop), which is the source of the Vectra and Cyphort detections in this case study. This host is running Windows 7 and is routinely connected non-corporate networks. Its IP address and hostname were identified by Vectra and confirmed by the user as IP address x.x.13.238 and xxxxx, respectively. Information is masked for sanitization purposes, along with usernames and handles identified during the investigation.
4. Forensic Analysis Workstation - The forensic analysis workstation is a 64-bit laptop running Windows 7 Professional SP 1 with 16GB RAM and Intel Core i5. The workstation was loaded with free forensic software tools on an as-needed basis as the investigation of the Vectra and Cyphort detections concerning the subject user laptop progressed. Tools are used for analyzing forensic artifacts gathered from the subject

laptop hard disk image, to help determine if the Vectra detections are true or false positives. See Section 2.3.3 for a description of the forensic software used. The analysis workstation hosts a Windows 7 Professional guest virtual machine (VM) instrumented with the Bit9 Security Platform and Carbon Black agents to detect malicious activities while visiting suspect websites and downloading suspicious software for examination using the Bit9 Security Platform and Carbon Black server consoles.

5. Bit9 Server - Bit9 is an application whitelisting and control software that alerts when malicious software is executing on a host with the Bit9 agent installed. Bit9 is deployed in the corporation to ban malicious software globally using human intervention. It was installed because the endpoint threat protection capability was not in-house, and it would augment traditional anti-virus and anti-malware tools already in house. Bit9 agents in this corporation are configured in low-enforcement mode for visibility purposes, without any application control enforcement. The Bit9 Security Platform server is a Windows Server 2008 VM running Bit9 software version 7.2.1.710 and earlier. This server is deployed to provide command and control of the Bit9 agents installed on Windows, OS X, and Linux corporate hosts, including the subject user's laptop and the guest VM on the analysis workstation. See Section 2.3.3 for further details on Bit9.
6. Carbon Black Server - Carbon Black provides the endpoint detection and response capability lacking in the corporation. It analyzes the behavior of suspect software on the hosts where Carbon Black agents are installed and alerts on malicious activity. For example, it determines which processes and network connections are launched upon software execution. The Carbon Black server is a CentOS Linux VM running Carbon Black software version 5.1.0.150625.0500 and earlier. This server is deployed to provide command and control of the Carbon Black agents installed on Windows, OS X, and Linux hosts, including the subject user's laptop and the guest VM on the analysis workstation. Carbon Black continuously "records" software activities even when the host is off the corporate network, and uploads them to the server when the host is back on the network. It provides the ability to acquire memory with no memory analysis capability. See Section 2.3.3 for further details on Carbon Black.

2.3. Detection Products and Forensic Tools

The alerts generated by the detection products Vectra and Cyphort are the heart of this investigation, introduced in Section 2.2 and expanded upon in sections 2.3.1 and Section 2.3.2, respectively. Throughout the investigation, multiple tools are employed to examine and analyze evidence used to draw conclusions regarding the Vectra and Cyphort detections concerning the subject corporate laptop. Some of these software tools are installed on the forensic analysis workstation detailed in Section 2.2. The tools themselves are covered in Section 2.3.3. Other tools including Bit9 Security Platform and Carbon Black were introduced in Section 2.2.2 and expanded on in Section 2.3.3. The only products used that are not cost-free are Vectra, Cyphort, Bit9 Security Platform, Carbon Black, supporting operating systems and hardware. All products are addressed in detail to provide additional context.

2.3.1. Vectra

The commercial Vectra platform analyzes inbound and outbound network traffic as well as lateral network traffic from inside the perimeter of the network. Vectra's competitors include Darktrace and LightCyber. Key Vectra product differentiators include algorithms that continuously assess network behavior and focus on detections that traverse the network laterally. Vectra's display of detection events are marked for easy triage. However, Vectra requires tuning. For example, if Vectra shows a detection and the analyst assesses that it is the result of a corporate anti-virus server reaching out to Sophos servers on the Internet using a port associated with Sophos, then Vectra can be configured or "tuned" to ignore future similar detections. Vectra complements, rather than competes with, the sandboxing functionality that Cyphort performs.

Vectra helps the analyst triage the detection events using a threat and certainty score as they relate to the internal host, which is the subject laptop investigated in this case study. This host was singled out for examination is because it had a high threat score of 87%. "The threat score is driven by the quantity of data exchanged and longevity of the connection." [1] In this case, the certainty score was not as significant as the threat score. "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." [2]

Vectra delivers a helpful guide entitled *Understanding Vectra Detections* that can be downloaded from the platform itself. This guide is an essential reference for the analyst to consult while investigating events. A condensed sample of guidance from this publication is detailed below, as it pertains to the actual detections involving the subject corporate laptop in this case study detailed in Section 3.1:

- Detection Category Command & Control and Type External Remote Access - This means that the inside host is "connecting to an external host with a human on the outside controlling the exchange" [3]. This is akin to an outside user accessing the subject inside host using a remote desktop protocol. External Remote Access could also be "malware with remote access capability that connects to a command and control server, receiving commands from a human" [4]. Finally, External Remote Access could be a "false positive, such as the internal user using chat software" [5].
- Detection Category Command & Control and Type Fake Browser Activity - This suggests that software on the inside host is "impersonating a browser by transmitting a malformed User-Agent string which looks similar to one sent by browser" [6]. This is probably machine driven because of the regular communication pattern. This could be the result of "malware, adware, or spyware communicating to its command and control servers" [7], or other software installed on the internal host that is sending a "malformed User-Agent in an automated pattern" [8].

2.3.2. Cyphort

The commercial Cyphort Advanced Threat Defense Platform performs local and cloud-based sandboxing virtual machine analysis of suspect files to determine whether they are malicious. Cyphort receives threat intelligence from the Cyphort Threat Network cloud service to support the analysis. It can be "tuned" to whitelist events, preventing repeated detections and can be configured to automatically or manually push the blocking of IP addresses, URLs, signatures to firewalls, secure web gateways, and IPSs.

Cyphort can be integrated with the Carbon Black endpoint detection and response product so the analyst can find out which host received malware and if it executed. If desired, the Bit9 Security Platform application control and whitelist product can be configured to

block the malware from executing on the target host and any additional hosts. The validation of malware execution on the host is important because it can help justify the decision to reimage the host. If the host executed the malware, then it should be reimaged. In the case of zero-day malware where there is no Bit9 black list entry, the "Bit9+Carbon Black solution can submit the file to the Cyphort Core and get a verdict before allowing execution of the file"[9] to protect the user.

Cyphort's competitors include FireEye and Trend Micro. Cyphort is different from its competitors because it is software-based, employs licensing based on bandwidth, and has a blocking capability. The software can be installed on customer-supplied servers in a virtual or non-virtual environment. It can augment deployments with competitor hardware appliances. For example, if competitor appliances are deployed at hub sites, and spoke sites are being added to the infrastructure, Cyphort can be deployed virtually to spoke sites in order to save hardware costs. A Core platform would still be required at the hub site, but the existing competitor infrastructure could remain in place if desired.

Cyphort incidents, or events, are marked with the "malware infection life cycle and Kill Chain" [10] stage as it pertains to the actual detections involving the subject corporate laptop detailed in Section 3.2 is download (DL). Other stages that can be outputted by Cyphort, but unused in this case study, include user upload (UL), execution (EX), exploit (XP), and infection (IN) for command and control. Incidents are also marked with severity levels, labeled as "Risk". Risk calculations are based on threat relevance, asset value, and severity. Relevance is based on two criteria: if anti-virus is configured on the endpoint, and if the operating system of the endpoint matches the target operating system of the malware. The Cyphort administrator must configure which anti-virus software is in use. If this is done, and the software is known to catch the threat, then the relevance score will be decreased. Asset value is based on whether the Cyphort administrator configured asset values for endpoints or network segments. For severity: "When a malicious event is detected, the Cyphort detection and analysis engines determine severity as part of their Threat Metric determinations. As indicated, an infected host can undergo a combination of events- an initial infection, a secondary binary drop, as well as a callback- coupled with asset value assessments and chain heuristics- that together contribute to determining the severity of the attack." [11]

Cyphort detects malicious software on the subject enterprise network - maybe one or two events per week and the investigations are straightforward. Cyphort can also be "tuned" to whitelist events.

2.3.3. Forensic Software and Systems

The forensic software tools and systems that used to perform the investigation are listed below with a description of how they were employed to analyze data:

1. Wireshark 1.10.8 – The well-known free network protocol analyzer which in this investigation is used to read packet captures downloaded from the Vectra platform to the analysis workstation via the tap port.
2. AccessData FTK Imager version 3.2.0.0 – Disk imaging software installed on a USB thumb drive, used to make a forensic copy of the subject laptop hard disk drive. The image is then placed on an external USB drive and analyzed using the analysis workstation for this investigation. An alternative is Guidance Software EnCase Forensic Imager. Both imagers are commercial but available as freeware. There are also many flavors of the free command line DD tool, which can be used to make exact bit-copies. DD should be used with caution to ensure that the source evidence disk is not overwritten by the contents of the destination disk.
3. Autopsy version 3.0.10 – Free digital forensics software installed on the analysis workstation to examine the subject laptop hard drive image, hunt for artifact files, and export them for further examination. Commercial products that can be used in lieu of Autopsy with additional capabilities including password recovery, rainbow tables, and memory analysis) are AccessData FTK and Guidance Software's EnCase.
4. Skyperious version 3.5 – Free tool used on the analysis workstation to open Skype database files which are in the SQLite database format, so evidence can be examined. A commercial alternative that includes Internet evidence (e.g., Dropbox, Bitcoin, and Facebook) is Internet Evidence Finder (IEF).
5. BEncode Editor Version 0.7.1.0 – Free software used on the analysis workstation to open uTorrent data files encoded using the BEncode scheme, so uTorrent evidence can be

examined. A commercial tool that can analyze uTorrent and other peer-to-peer (P2P) files along with other evidence including Skype, Google Drive, and Dropbox is PeerLab.

6. Bit9 Security Platform (formerly Parity) version 7.2.1.710 and earlier – Commercial tool employed as a forensic system in this case study, as described in Section 2.2.2. An alternative commercial product is McAfee Application Control, which has similar capabilities and supports integration with McAfee ePolicy Orchestrator (ePO). Another product is Palo Alto Networks Traps. The Bit9 advantage is its integration with Carbon Black. When integrated, threat feeds tied to Carbon Black can be further leveraged. Bit9 can also integrate with Check Point log server, with or without ThreatCloud or Threat Emulation appliance lookups. It also integrates with FireEye appliances. Finally, Bit9 integrates with Palo Alto Networks appliances, with or without the WildFire public cloud. The purpose of those integrations is to ban the execution of the detected software if desired using Bit9.
7. Carbon Black version 5.1.0.150625.0500 and earlier – Commercial tool employed as a forensic system in this case study, as described in Section 2.2.2. Bit9 acquired Carbon Black. It leverages intelligence from the Bit9 Threat Intelligence Cloud that includes the Bit9 Software Reputation Service (SRS), Bit9 and Carbon Black threat indicators, and third-party attack classification using Alliance Partner Feeds. A competing product is Mandiant Intelligence Response (MIR), offered by FireEye as its HX Series, and Tanium Trace and IOC Detect. Carbon Black integrates with Bit9 to "roll back the tape recording" and investigate Bit9 events. Carbon Black can be integrated with Cyphort to validate malware detections.

2.4. Investigation and Analysis Methodology Overview

Security monitoring platforms such as Vectra produce events that appear within the tool display, and in a SIEM if configured properly. A SIEM can be configured to correlate events from multiple sources, or the analyst can correlate manually. In this case, the analyst correlated manually and checked Cyphort for similar events. The same principle applies to Bit9 Security Platform and Carbon Black events, or any other events. The IPS events were accidentally overlooked in this case, and the SIEM was not receiving them at the time. Oftentimes, event data from one source is insufficient to make the true or false positive

judgment call, and more investigation is required. Multiple sources of data can help accelerate this process. Despite correct SIEM configuration, the analyst must still drill into the source platforms' events for more details.

Follow the steps below to resolve Vectra and Cyphort events. The steps are shown in chronological order, but they can be shuffled or removed as appropriate per the analyst's judgment for each specific case. The personnel who use them can modify the methodology and step details.

Step1: Analyze Vectra Events. Start with the events that have a high threat and certainty for triaging purposes. Gather as much information as possible by viewing the Vectra event at face value, and read Vectra's material available for download from the platform (*Understanding Vectra Detections*) to determine what the detection means and what to do to take action. Download the packet capture file from Vectra and examine it with Wireshark. Follow the TCP/UDP stream in Wireshark and determine if the traffic is encrypted; if it is, the analysis will be more difficult because less information will be visible. Determine which corporate assets are involved, and confirm the IP addresses and hostnames. Research external IP addresses online using an Internet search engine to find out what they are, and use reputation websites like https://www.virustotal.com to determine if the IP addresses and their domains are malicious.

It is a best practice to view Virus Total from a host that cannot be traced by malicious actors. Use the security tools to pivot over to Virus Total. For example, Bit9 can be used to do this later on in the workflow. Look at the ports in use, and research them online. Bear in mind that a hacker can use any port desired, and do not accept what is found at face value. Determine if there are any other Vectra events for the same corporate asset around the time of the original events and repeat the above. If the asset is a user's endpoint and it is practical to do so, ask the user what he was doing on the host during the target timeframe. For example, if Vectra detects a Data Smuggler (exfiltration) event, find out if the user was uploading files to a cloud service, such as Box, Dropbox, or Amazon Web Services. If so, find out if the IPs and ports reported are associated with the service. Does it make sense that one host should be sending traffic to another using a specific port, and is that destination host malicious? If the

answers are a definitive yes and no respectively, then it is a false positive. If unsure or curious, keep investigating.

Step 2: Analyze Cyphort Events. It is possible that Cyphort detected an infection of the same asset before the Vectra events examined above occurred. These are the events to focus on, for now. Gather as much information as possible by viewing the Cyphort events at face value. Research external IP addresses online using a search engine to find out what they are, and click the Virus Total link on the Cyphort appliance to see if the IP addresses, their domains, and downloaded executables detected by Cyphort are malicious. Download the packet capture from Cyphort and analyze it with Wireshark. If desired, download any available software sample from Cyphort using the analysis guest VM to avoid potentially infecting the analysis workstation. If practical, ask the user what actions he performed on the host at the time of the infection. Do any of the above match the information gathered from the Vectra detections? If not, the Cyphort events are probably unrelated, but the events are still worth looking into further in a separate case.

Step 3: Examine Carbon Black. Search the Carbon Black server display for any information gathered in the above steps associated with the subject asset, such as executable names or hashes, processes, and network connections to external IP addresses. File reputations are checked against Bit9's Threat Intelligence cloud service. Does Carbon Black confirm malicious behavior correlated to the Vectra or Cyphort detections? If so, the detections may be true positives.

Step 4: Examine Bit9. Search the Bit9 Security Platform server for events related to the subject host around the time of Vectra or Cyphort detections. File reputations are checked against Bit9's Software Reputation Service. If implemented, Check Point, FireEye, or Palo Alto Networks connectors may provide additional information to Bit9. Does Bit9 Security Platform confirm malicious behavior correlated to Vectra or Cyphort detections? If so, the detections may be true positives.

Step 5: Examine Suspect Websites and Software in a VM. This step may not be necessary if the investigation is resolved by performing the above steps. To take the investigation deeper, launch the analysis workstation VM that is instrumented with Bit9 and Carbon Black agents. If applicable, browse to the suspect website most likely identified by

Cyphort and monitor the Carbon Black server for abnormal network connections and processes originating from the VM. If applicable, download the malicious executable from the website and repeat. Launch the suspect software and repeat. At the same time, look at the Bit9 server to see if any events related to the VM have surfaced. If Bit9 and/or Carbon Black showed malicious activity on the VM resulting from visiting a website, downloading an executable, or running the software, then chances are a true positive is confirmed. Suspect software downloaded from the Cyphort platform can be analyzed using malware analysis tools that would have to be added to the VM. Bear in mind that analyzing malware in a sandbox environment takes the analysis to a deeper level that may not always be the best use of time. It may also be beyond the experience level of the analyst, but this would be a good skill to develop.

Step 6: Analyze Disk Forensic Artifacts. Skip this step if the investigation is resolved. In an ideal situation, the case is resolved by this time. If the previous research needs to be confirmed for business reasons, or if the analyst has the time to satisfy a curiosity and develop procedures for future investigations, then proceed.

The following are use-cases for analyzing forensic artifacts. For example - if an external IP address is associated with Skype, or a TCP port is associated with uTorrent, look for evidence of those program activities on the disk image, not just the mere presence of the programs. First determine what this evidence is and where it is located in an image by researching the Internet. Determine what free tools can be used to examine the evidence and install them on the forensic analysis workstation. Try out a few to find the one that works best. Image the subject asset hard disk drive using FTK Imager run from a USB thumb drive, and use an external USB hard drive to store the disk image. This step is intrusive for the user and takes time, so consider borrowing the user's laptop for a while and provide a loaner. It is more efficient to perform a disk acquisition over the network (requires commercial software) as long as the user remains connected. Disconnection may result in an incomplete disk image acquisition.

Using the forensic analysis workstation loaded with Autopsy, examine the disk image, and look for forensic artifacts as clues. Export the artifacts and use the appropriate tool to

view the evidence in human readable format, if needed. Here are some examples, for the Skype and uTorrent use-cases:

Skype. The Skype artifact *main.db* from */Users/xxxxx/AppData/Roaming/Skype/ xxxxxxxxxxxx* can be exported out of Autopsy. The database is examined with Skyperious to display the SQLite database that is exportable to a spreadsheet.

uTorrent: The uTorrent artifact *resume.dat* from *Users/xxxxx/AppData/Roaming/ uTorrent* can be exported out of Autopsy. This file is encoded with the BEncoding scheme and can be examined with BEncode Editor.

Most importantly, for Skype, uTorrent, or any other evidence, check the evidence timeline. Does the evidence activity take place around the time of the Vectra or Cyphort event? If so, the activity is confirmed.

Step 7: Dump and Analyze Memory. At this point, the case is probably solved. If the subject asset has remained powered on and connected to the corporate network since the Vectra and Cyphort detections, dump the memory with the Carbon Black Live Response feature, ideally at the first sign of infection or compromise to increase the probability of finding useful memory artifacts, and set it aside. Time is of the essence for memory acquisition because it is volatile. Examine it on the forensics workstation at an appropriate time using tools such as FireEye's Mandiant Redline or Volatility Framework (both free) to see if there is any supporting evidence for indications of compromise. This adds length to the process and requires additional expertise. This step should not be routine under normal everyday incidents, but if there is a business need, proceed with this step. This is a good exercise for the analyst to perform in order to develop and document procedures that can be used in other investigations.

Step 8. Execute Incident Response Plan. Decide if the asset is truly infected and needs re-imaging or other remediation, such as quarantining files if the malicious software is found by manually performing a traditional anti-virus scan. Use Bit9 to blacklist any unwanted malware that may have been downloaded, which will prevent it from being executed again on the subject asset and any other assets that have the agent installed. If Vectra and/or Cyphort events are false positives, then go back to the platform(s) and white list the events. Make

notes about the events and whether or not they are normal to help resolve future similar events.

2.5. Experimental Details and Findings

Vectra displayed External Remote Access detection events with high threat scores, which is why the case was opened. The events were traced to a corporate user's laptop. A search was performed to see if additional Vectra events were traced to the same laptop, and Fake Browser Activity detections were found about a month earlier. The packet captures were downloaded from Vectra for analysis using Wireshark, and the IP addresses and ports were researched on the Internet. It was assessed that the External Remote Access events were caused by uTorrent activity. Disk forensic artifacts examined using the analysis workstation confirmed that at the time of the detections, a uTorrent program was sharing (uploading) language training course files (e.g., .mp3 and .pdf) to users on the Internet. It was assessed that the earlier Fake Browser activity events were caused by Skype protocol activity. Disk forensic artifacts confirmed that at the time of the detections, the laptop was using a P2P protocol to communicate with Skype servers, and Skype software updates were downloaded. The uTorrent and Skype activities are unrelated and the Vectra detections are assessed to be false positives. These benign findings reveal the use of software that may not be approved by the organization.

Three Cyphort adware detections took place on the subject laptop. Executables associated with SUSP_CONDUIT.Rep and SUSP_LYCKRICKS.DC detections were downloaded to the laptop before the Vectra External Remote Access events, and the executable associated with the TROJAN_AGENT.DC was downloaded before the Vectra Fake Browser Activity events. The Cyphort detections were unrelated to the Vectra detections. At this point, Carbon Black and Bit9 were not deployed, so they could not be used to confirm the malicious downloads on the laptop.

The laptop was ultimately reimaged and later loaded with Bit9 and Carbon Black agents, and a Vectra Peer-to-Peer detection occurred shortly thereafter. Carbon Black confirmed the uTorrent process running at the time of the detection, and the network connection IP addresses identified by Carbon Black matched the addresses shown in the Vectra detection.

A Windows 7 Professional VM was deployed on the analysis workstation and was loaded with Bit9 and Carbon Black agents to create a safe environment for suspect software. Carbon Black was used to confirm that the executables associated with SUSP_CONDUIT.Rep and SUSP_LYCKRIKS.DC were malicious, and Bit9 confirmed that the SUSP_CONDUIT.Rep executable was malicious.

3. Investigation and Analysis Workflow Details

The results of the investigation and analysis methodology overview steps described in Section 2.4 and findings described in Section 2.5 are shown in detail for this particular case study, where the analyst's thought process can be followed. Evidence is presented, interpreted, analyzed, and assessments made. Not all steps were performed because they were impractical for the case (e.g., Step 7: Dump Memory). Unfortunately, Carbon Black and Bit9 had not been purchased at the start of this investigation and could not be used early on as described in Section 2.4 (Step 3: Examine Carbon Black and Step 4: Examine Bit9) to corroborate detection activities and potentially resolve the case sooner. However, once online, Carbon Black and Bit9 were used to revisit the investigation and quickly confirm some findings. The steps below are shown in the order performed by the analyst, but the labels "Step 1: Analyze Vectra Events", etc. parallel the nomenclature described in Section 2.4.

3.1. Step 1: Analyze Vectra Events

Vectra detects some events originating from the IP address x.x.13.238, which is traced to a corporate laptop belonging to user xxxxx. Figure 2 shows two types of Vectra events - "Category Command & Control" and "Type External Remote Access" and "Category Command & Control" and "Type Fake Browser Activity."

External Remote Access means that the subject inside host was being communicated with through an outside entity, via remote access, malware, or non-malicious activity such as a user using chat software.

Fake Browser Activity could be due to a machine driven malformed "User-Agent" string resulting from malware or non-malicious software.

Figure 2: Subject Laptop Vectra Detections

3.1.1. External Remote Access

Figure 3 shows the drill-down into the 31 July 2014 External Remote Access event. This particular External Remote Access event shows the highest threat score of 95%, out of all the detections for the subject laptop. It shows that the internal host x.x.13.238 sent 55.2 MB of data to the external host 223.205.105.130 on TCP port 62000. The external IP address was not found on the Virus Total website https://www.virustotal.com so its reputation is unknown. Multiple Internet searches reveal that this port could be used for a Torrent client, Apple's Xsan file storage system access, or Network Location Server (NLS). The subject host has the Windows 7 operating system, as opposed to an Apple operating system, and the NLS requires a Windows server operating system. The possibility of Bit Torrent activity remains, but this cannot be confirmed at this stage of the analysis. Malicious actors can design their code to use any port they desire to thwart defensive detections, and users can change their ports in their Torrent applications. This detection could possibly be a true positive or a false positive (not malicious) due to Bit Torrent activity.

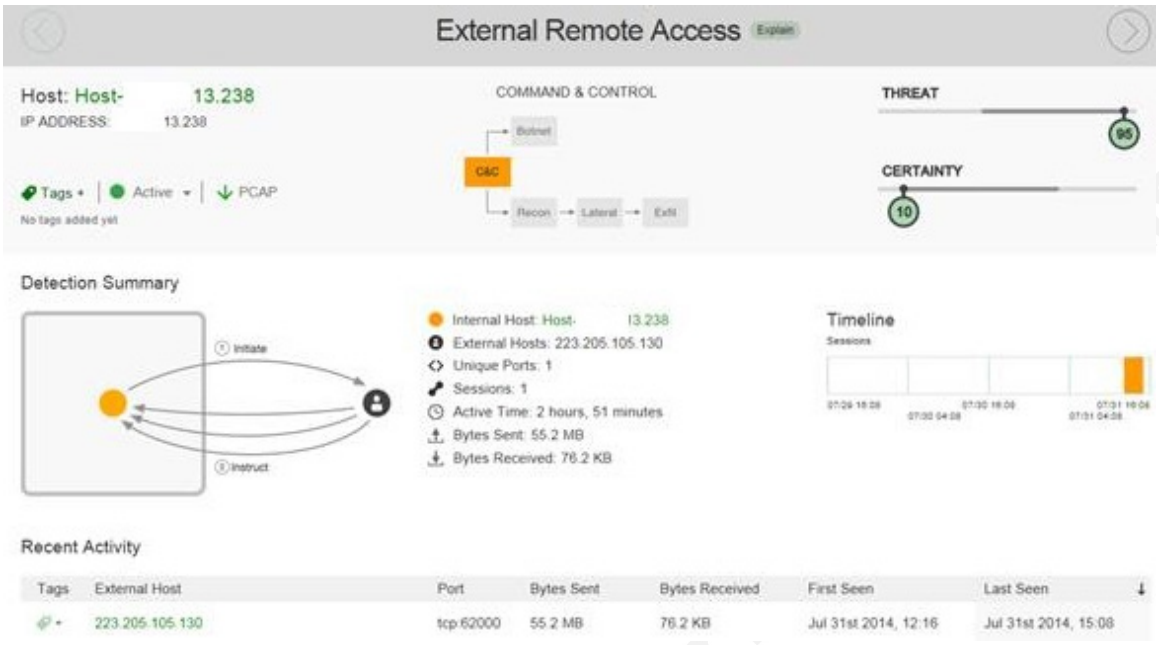


Figure 3: 31 July 2014 Vectra External Remote Access Event Drill-Down

A Wireshark examination of the Pcap file downloaded from the Vectra platform yields TCP traffic between x.x.13.238/port 51094 and 223.205.105.130/port 62000. The resulting "Follow TCP Stream" does not show any predictable text; it appears to be encrypted, as shown in Figure 4, which is truncated for brevity. Torrent connections can be encrypted, but whether this traffic is encrypted cannot be confirmed. Naturally, true malicious activity can also be encrypted.

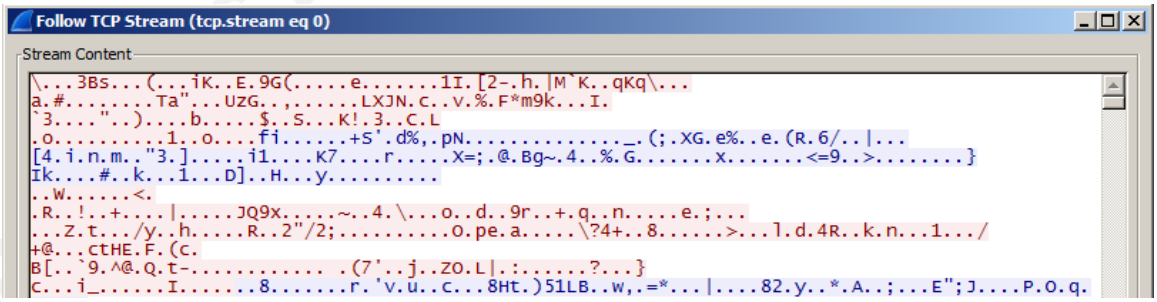


Figure 4: 31 July 2014 Vectra External Remote Access Event TCP Stream Excerpt

The 29 July 2014 External Remote Access event yields similar results with relatively large sent byte counts, as shown in the drill-down in Figure 5. A Wireshark examination of the Pcap file from Vectra yields TCP traffic between x.x.13.238/port 43078 and 108.45.47.2/port 51413. The external IP address was not found on the Virus Total website so

its reputation is unknown. The resulting Follow TCP Stream does not show any predictable text; it appears to be encrypted like the last Pcap sample. The online SANS port search https://isc.sans.edu/port.html?port=51413 reveals that TCP port 51413 can be used for a Torrent client or Apple's Xsan file storage system access. TCP port 6881 appears in the Figure 5 drill-down with external host 24.44.188.43, but does not surface in the Pcap. The external IP address was not found on the Virus Total website so its reputation is unknown. The online SANS Services List https://isc.sans.edu/services.html shows that TCP port 6881 is associated with Bit Torrent P2P protocol. Once again, the possibility of Bit Torrent false or true positives remains, but cannot be confirmed at this stage of the analysis. This is explored in detail in Section 3.4.1 upon examination of additional evidence.

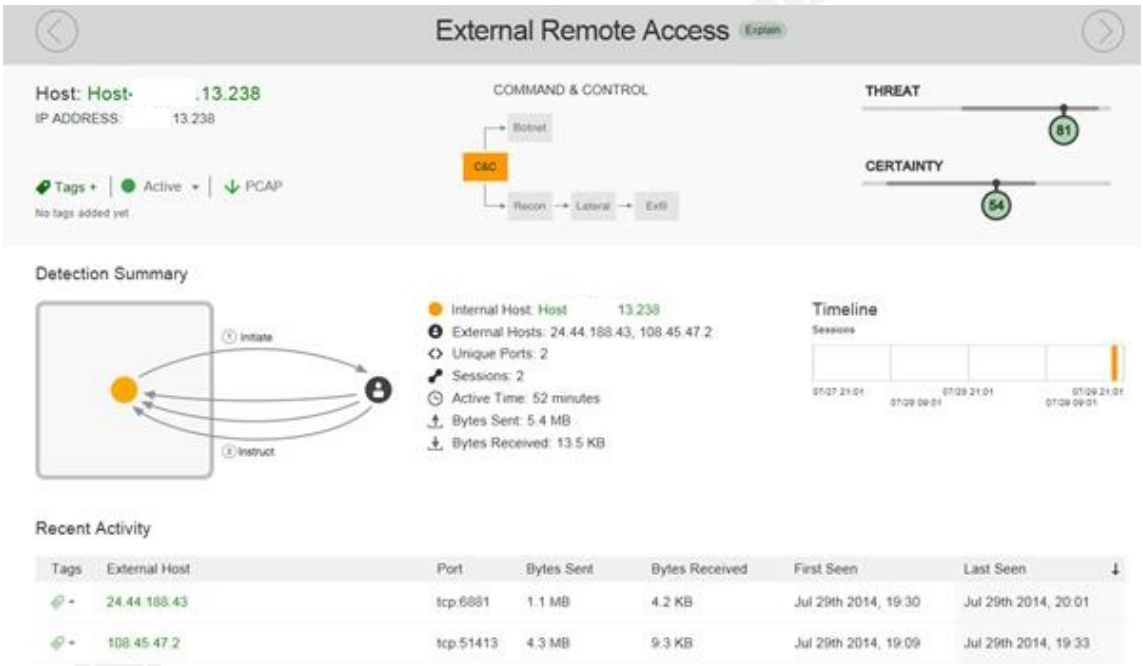


Figure 5: 29 July 2014 Vectra External Remote Access Event Drill-Down

3.1.2. Fake Browser Activity

Vectra detected Fake Browser Activity events about a month earlier - from 17-19 June 2014, with small consistent sent and received byte counts lending one to initially assess that the activity is a true positive - malicious C2 performed by a machine. Figure 6 shows a Fake Browser Activity drill-down for 19 June 2014.

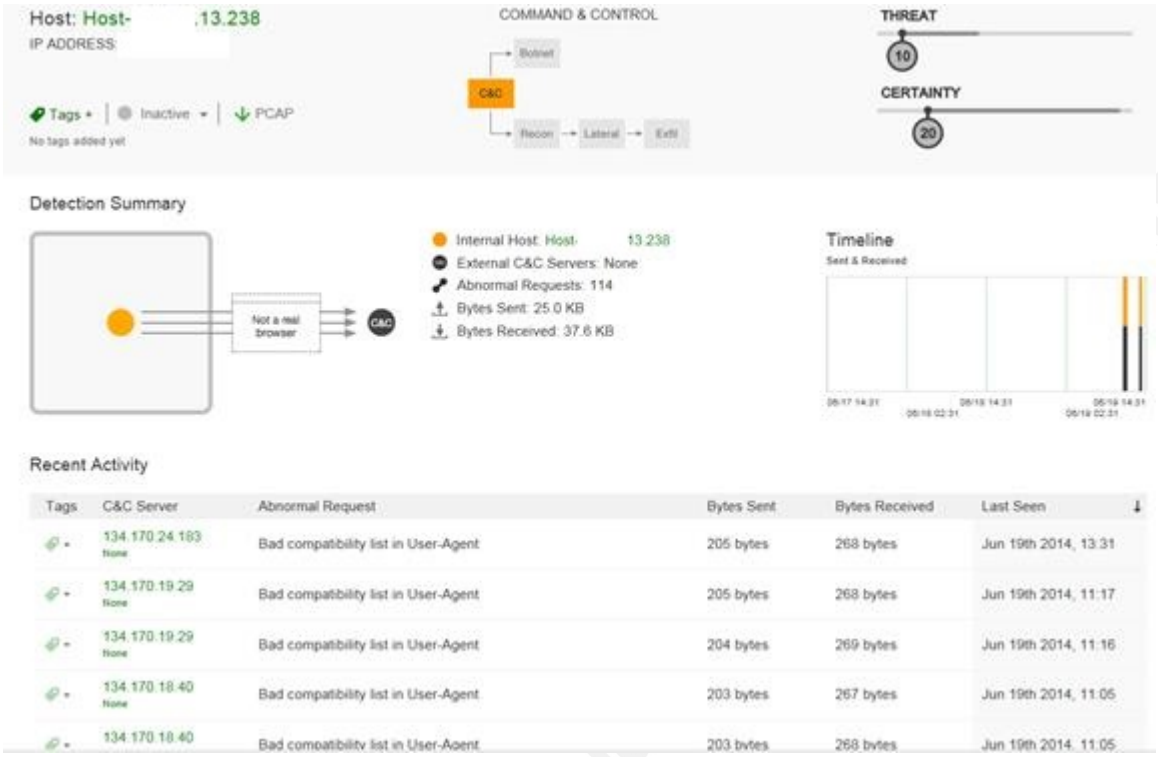


Figure 6: 19 June 2014 Vectra Fake Browser Activity Event Drill-Down

The Pcap files downloaded from Vectra and read with Wireshark show TCP port 80 traffic, and the Follow TCP Stream for the above event shows X-MSN-MESSENGER traffic to Microsoft owned IP addresses. The user-agent string is simply "Mozilla/4.0." According to http://www.useragentstring.com/, this string is compatible with Firefox and is historical when used with modern browsers. The user-agent strings do not appear to be malformed, leading to the assessment that the Vectra detections are false positives. An excerpt of the Pcap stream is shown in Figure 7.

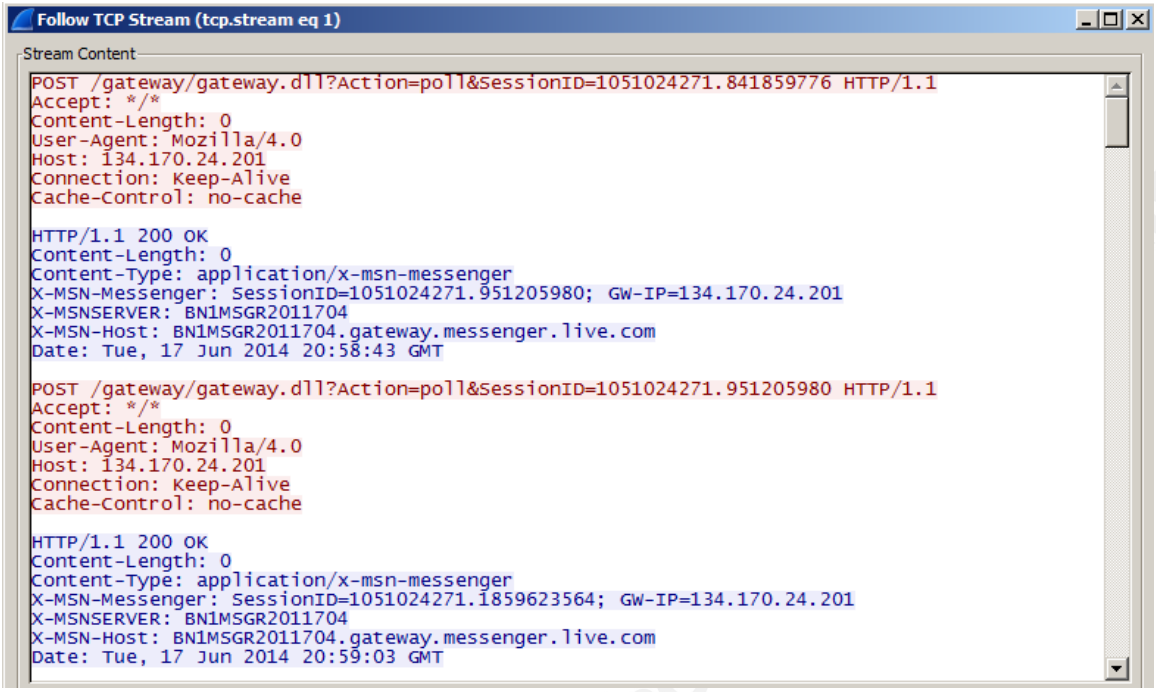


Figure 7: 19 June 2014 Vectra Fake Browser Activity Event TCP Stream Excerpt

Other sections of the Pcap in Figure 8 show the subject laptop user's Hotmail account (confirmed by an Internet search for the Hotmail email address), evidence that Skype or a Skype update is about to be downloaded, and the download itself, truncated for brevity.

...

Figure 8: Hotmail Account and Skype Download

Internet research reveals that Skype replaced Microsoft Messenger, and additional research confirms that Skype can utilize TCP port 80. This supports the information discerned from the Pcap. In addition, Skype's website indicates that actual messaging traffic is encrypted. Since the Pcap is clearly not encrypted, this leads to the assessment that the Pcap traffic is not actual messaging traffic, but possible Skype P2P protocol traffic executed between the subject laptop and the Skype servers. External Host IP address searches on the Virus Total website did not yield any associations with malicious activities, so the subject laptop was probably not part of a botnet with the Microsoft servers. This makes a stronger case that the Vectra detections are false positives resulting from Skype protocol activity versus malware at this stage of the analysis. It does not appear that the Skype activity is related to the uTorrent activity. It is not known at this point if actual Skype message traffic was being passed at the time of the Vectra detections. This is explored in detail in Section 3.4.2 upon examination of other evidence.

3.2. Step 2: Analyze Cyphort Events

Vectra behavioral detections for the subject laptop took place from 17-19 June 2014, 29 July 2014, and 31 July 2014. It is possible, but not confirmed, that Cyphort detected some malicious infections on the subject host, possibly causing the suspicious activities detected by Vectra. The SIEM had not yet been configured to correlate Vectra and Cyphort detections. Cyphort was examined manually. Cyphort detected some events originating from the subject laptop IP address x.x.13.238, as shown in Figure 9. The Risk column shows "High," which is the highest severity, and the Kill Chain column shows "DL." SUSP_CONDUIT.Rep was downloaded to the laptop from 23.203.225.66 on 16 July 2014 and TROJAN_AGENT.DC was downloaded to the laptop from 208.111.148.7 on 14 May 2014.

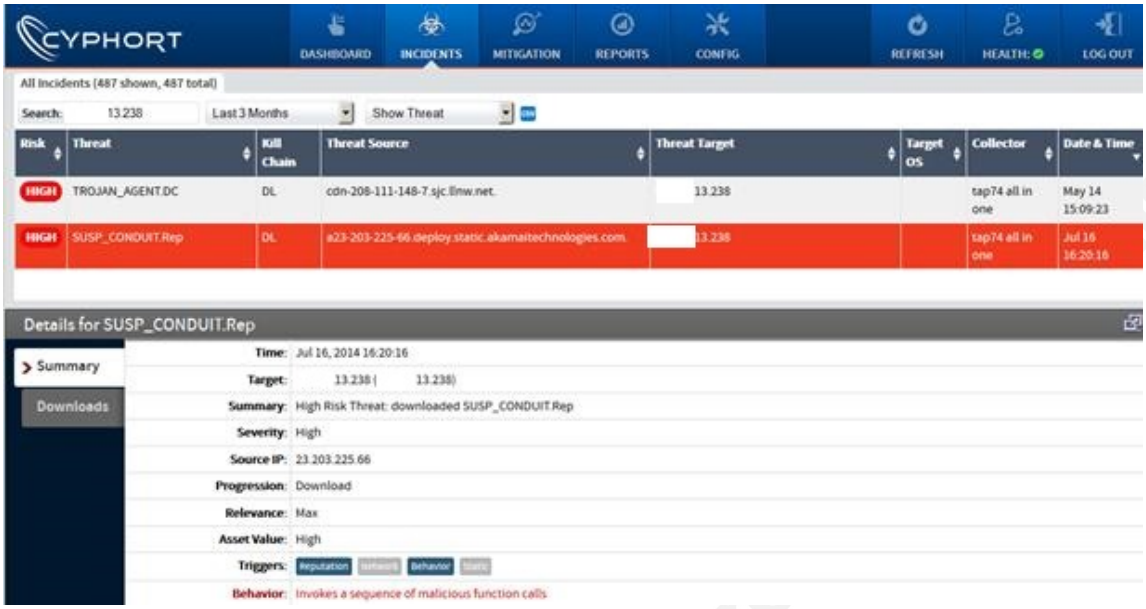


Figure 9: Subject Laptop Cyphort Events

3.2.1. SUSP_CONDUIT.Rep

Drilling down into the 16 July 2014 event yields two downloads to the subject laptop, as shown in Figure 10.

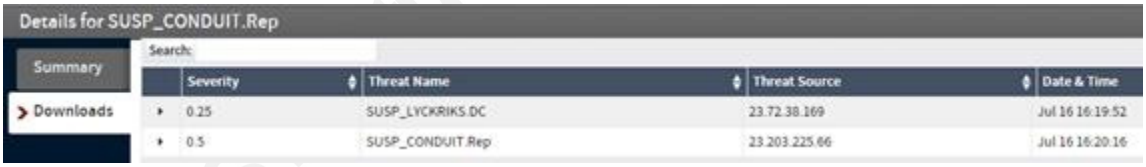


Figure 10: 16 July 2014 Cyphort Download Events

The SUSP_CONDUIT.Rep download from 23.203.225.66 is shown in Figure 11. Based on information from Virus Total (https://www.virustotal.com/en/file/e31ff6d53d70d013b57ef2a7da0d99e5e24f339ddcdd0b19bebe09bd1df3a425/analysis/), it is copyrighted by ClientConnect Ltd., version 2.4.2.3. Cyphort reveals that it was downloaded from http://sp-storage.spccinta.com/stub/spstub.exe.

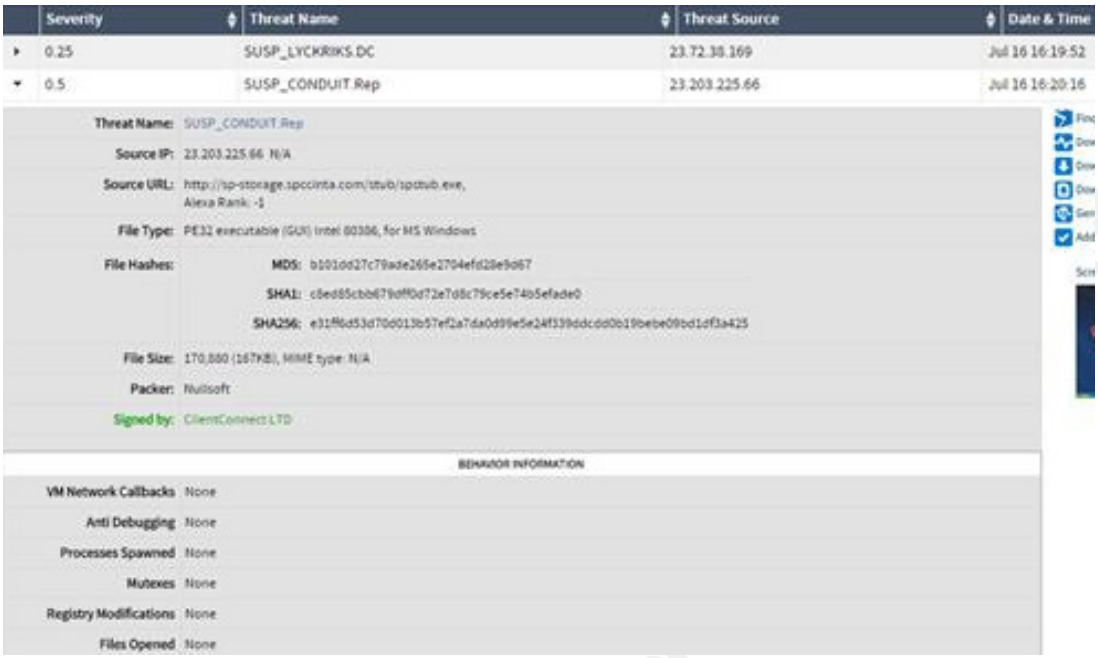


Figure 11: SUSP_CONDUIT.Rep Download from 23.203.225.66

3.2.2. SUSP_LYCKRICKS.DC

The SUSP_LYCKRICKS.DC download from 23.72.38.169 is shown in Figure 12.

Figure 12: SUSP_LYCKRICKS.DC Download from 23.72.38.169

Based on information from Virus Total (https://www.virustotal.com/en/file/589dcab63b44687ea01871eb51acbba44fcd881a25d289cc6bed2fba994f6574/analysis/), it is copyrighted adware, version 1.174.0.0. Cyphort reveals that it was downloaded from http://software-files-a.cnet.com/u/moff/passshow/1030-4004_PassShow.exe.

3.2.3. TROJAN_AGENT.DC

The TROJAN_AGENT.DC download from 208.111.148.7 is shown in Figure 13.

Figure 13: TROJAN_AGENT.DC Download from 208.111.148.7

Based on information from Virus Total (https://www.virustotal.com/en/file/51343f28402e91c286f988e55bca5e430d120c24cd1b18aecd76219c874b48ca/analysis/), it is copyrighted adware by OpenCandy Inc. Cyphort reveals that it was downloaded from http://cdn.opencandy.com/p/1086/installers/Installium_p1v0.exe.

3.3. Step 8: Execute Incident Response Plan (Partial)

The Cyphort detections alone are enough evidence to show that the subject laptop is infected and needs reimaging. Bit9 Security Platform and Carbon Black were not yet online, malicious software and blacklisting were not yet available.

3.4. Step 6: Analyze Disk Forensic Artifacts

At this point in the analysis, Vectra detections are assessed to be false positives due to benign Bit Torrent activities conducted by the user of the subject laptop, and Skype protocol activities. Cyphort detections are assessed to be true positives for adware. These analyses need to be corroborated using other forensic evidence gathered from the laptop's hard disk. The subject laptop hard drive, imaged prior to reimaging the laptop, was examined on the

analysis workstation. Appropriate artifacts were exported and analyzed with other tools on the analysis workstation. These artifacts were related to uTorrent and Skype.

3.4.1. uTorrent Activity

The laptop image was searched for the keyword "torrent" using Autopsy. It was discovered that the program *uTorrent.exe* was downloaded and part of the user's profile */Users/xxxxx/AppData/Roaming/uTorrent*. The profile was created 18 June 2014 at 16:53:14 PDT, prior to the first Vectra detection on 19 June 2014. This evidence is shown in Figure 14.

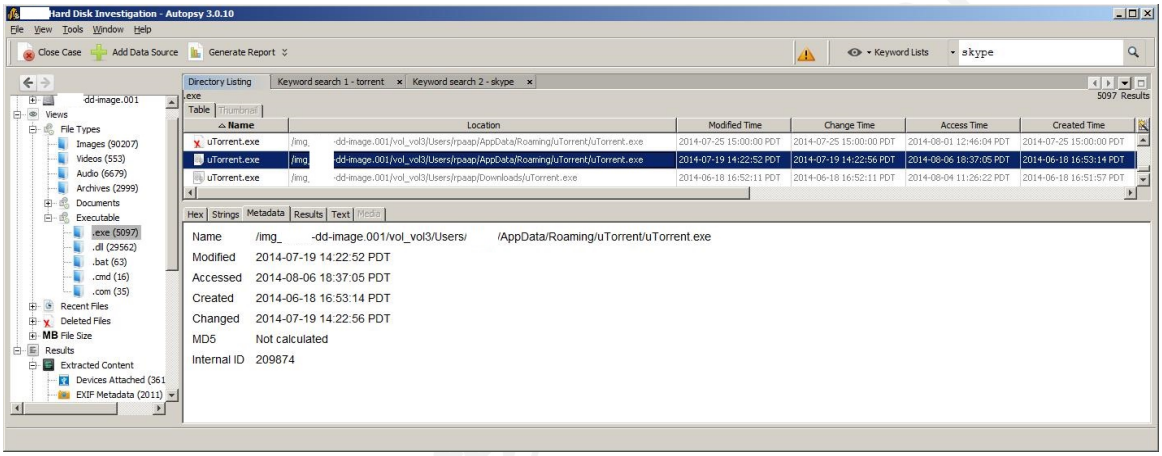


Figure 14: uTorrent Profile for Subject Laptop User

Internet research was conducted to see which Windows artifact could be examined for actual Bit Torrent activity, as opposed to the mere presence of uTorrent on the laptop. The artifact identified was *resume.dat*, exported from the subject hard disk image location */Users/xxxxx/AppData/Roaming/uTorrent* using Autopsy. The file is a BEncoded, based on [14]. It was examined on the analysis workstation using BEncode Editor. The uTorrent files on the laptop are listed in a screenshot of this evidence, shown in Figure 15.

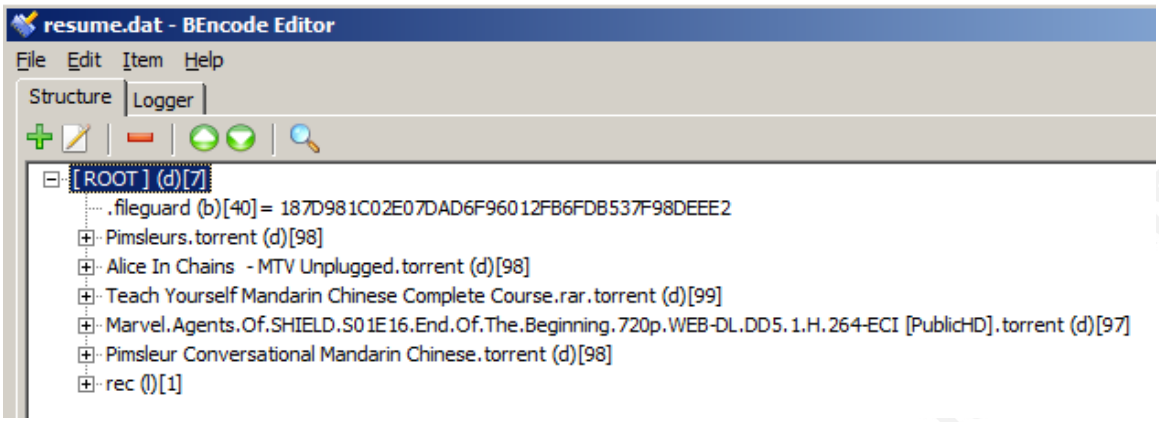


Figure 15: uTorrent Files on Subject Laptop

Each Torrent file was expanded within BEncode Editor and was carefully examined for clues to show uTorrent activity. Partial output from Pimsleurs.torrent (Part 1) is shown in Figure 16. The "added_on" entry shows when the file was added to the uTorrent profile on the laptop and the "completed_on" entry shows when it was finished. The "downloaded" entry shows how many bytes were downloaded to the laptop. All times are shown in Epoch time, which then had to be converted to local PDT.

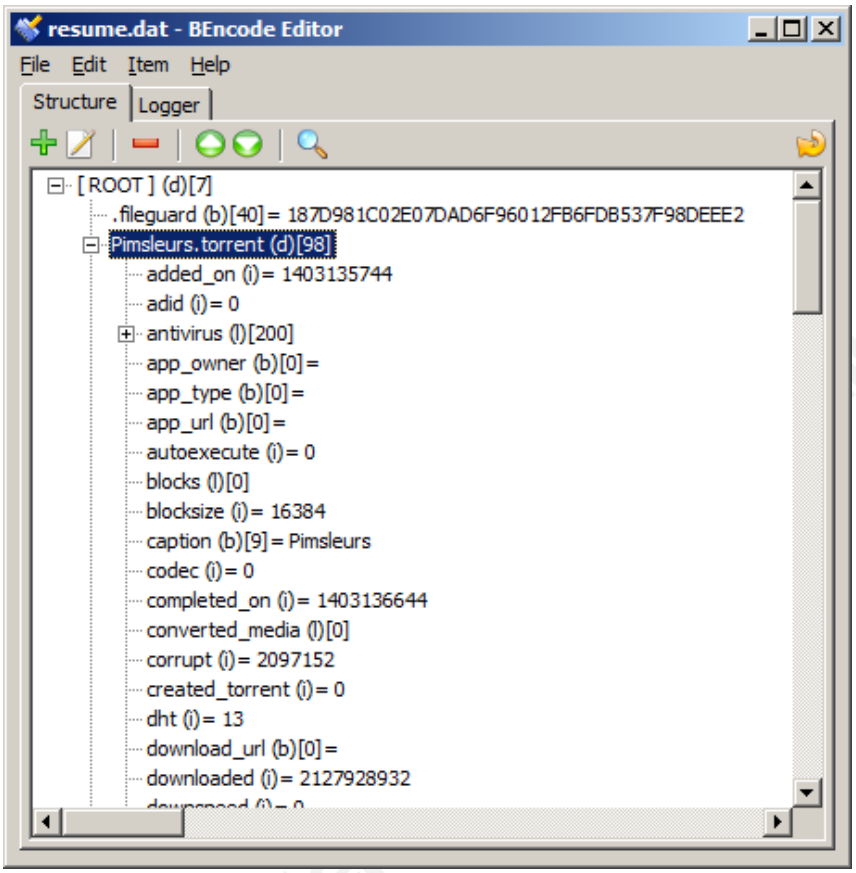


Figure 16: Pimsleurs.torrent BEncode Editor Partial Output – Part 1

Another partial output of the Pimsleurs.torrent (Part 2) is shown in Figure 17. The number of bytes uploaded is shown, but unfortunately, there is no time associated with the upload. The download directory is shown for the uTorrent file – for example, *C:\Users\xxxxx\Downloads\Pimsleurs*, where *Pimsleurs* is the uTorrent file and *xxxxx* is the username. The uTorrent trackers are shown, and after a quick hostnames lookup, it was identified that the IP addresses did not coincide with any of the IP addresses revealed in the Vectra detections. Trackers keep track of which hosts are uploading and downloading files (see http://www.quora.com/What-are-seeds-peers-trackers-pieces-in-uTorrent).

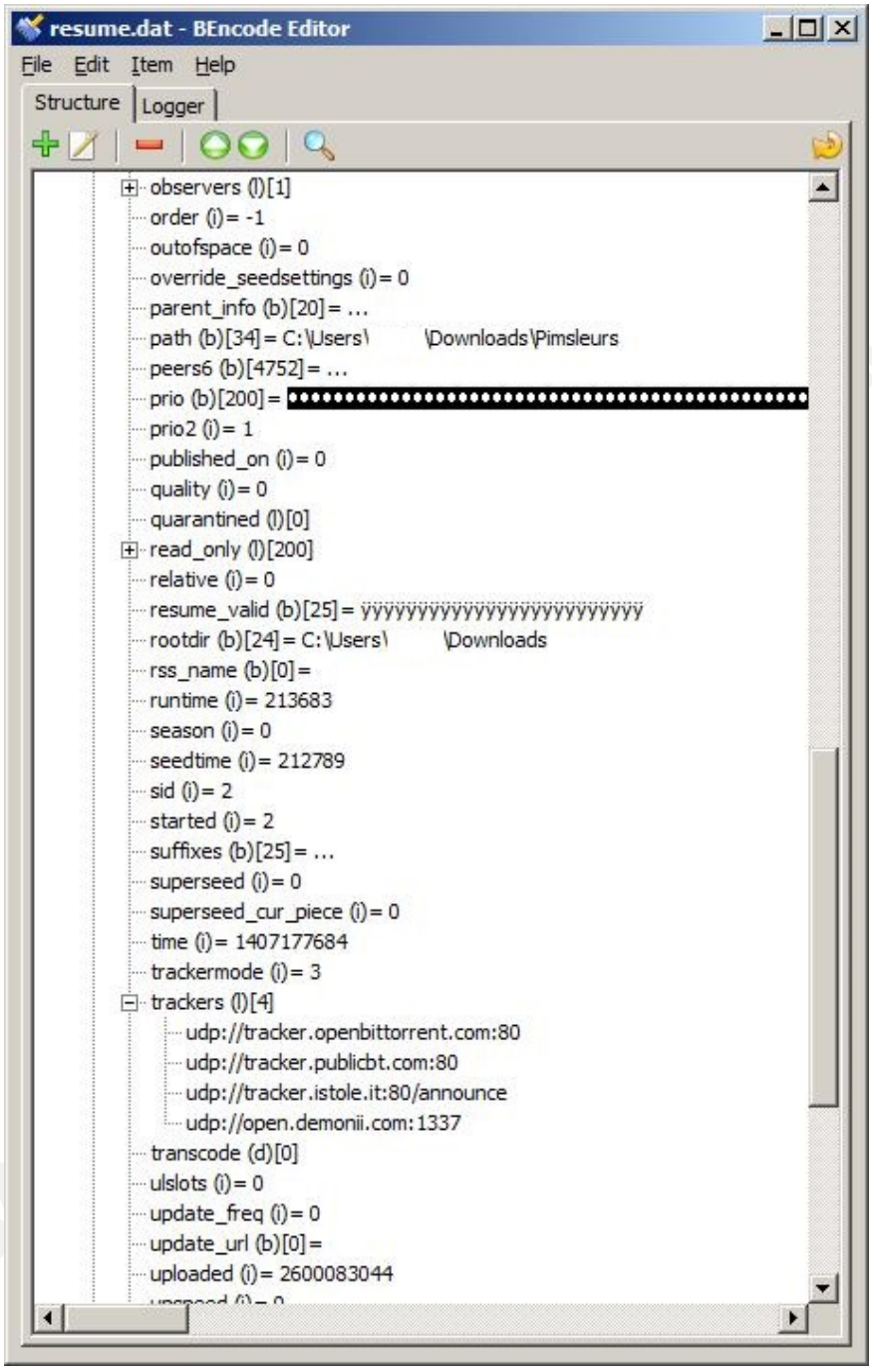


Figure 17: Pimsleurs.torrent BEncode Editor Partial Output – Part 2

After each Torrent was examined with BEncode Editor, each Torrent file was located in the disk image using Autopsy. The files were located in the *C:\Users\xxxxx\Downloads* directory, and the individual files within each Torrent were examined. A sample is shown in Figure 18. For the most part, each file's Access Time was examined to determine if the time

fell in the window of the 29 July or 31 July for Vectra External Remote Access detections that were being analyzed for uTorrent activity.

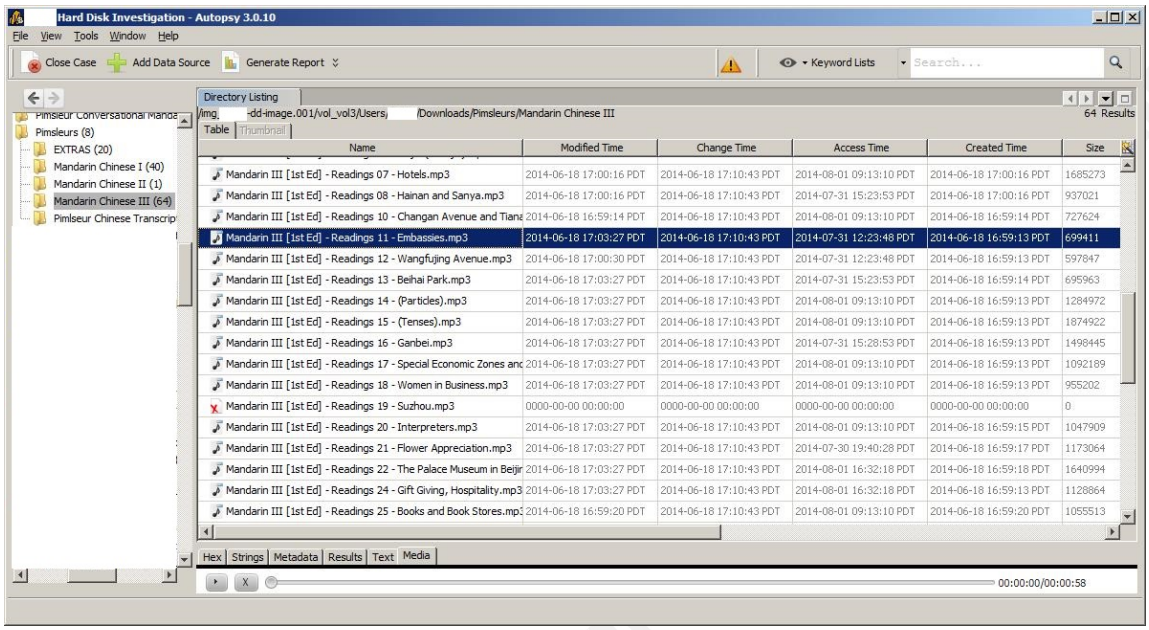


Figure 18: Sample Individual File Contained in a Torrent

Pimsleurs Torrent file folders and one .txt file downloaded into the download folder (created) between Jun 18 16:56:12 and Jun 18 17:08:12. The Torrent was complete Epoch 1403135744 (Jun 18 17:10:44 PDT) per *resume.dat*. These times were prior to the Vectra detection windows of Jul 29 and Jul 31. Multiple .pdf and .mp3 files had access times that were not within the 29 and 31 July Vectra detection windows for External Remote Access, but there were several that were indicative of uTorrent activity.

Table 1 shows a summary of the findings for uTorrent evidence. Two out of three Vectra External Remote Access detections coincide with evidence of uTorrent activity on the laptop, confirming that the detections are probably false positives, but it is unknown why the file size totals do not match. It is possible that some files were transferred to/from the subject laptop, and/or that other files not listed in the table were inbound/outbound. Some of the files not listed were barely outside the Vectra first and last seen detection windows.

Table 1: Vectra Detections with uTorrent Evidence

Vectra First and Last Seen (PDT)	External Host IP Address and Hostname	Vectra Detection	TCP Port	Bytes Out	Bytes In	uTorrent Evidence (PDT)
31Jul, 12:16-15:08	223.205.105.130 mx-ll-223.205.105-130.dynamic.3bb.co.th	External Remote Access	62000	55.2M	4.2K	*Pimsleur Conversational Mandarin Chinese Torrent PCMC Box Image 2.jpg* file access time Jul 31 12:59:40, 105,735 bytes Pimsleurs Torrent files: • *Mandarin III (1st Ed) Readings 11 – Embassies.mp3* access time Jul 31 12:23:48, 699,411 bytes • *Mandarin III (1st Ed) Readings 12 – Wang fujing Avenue.mp3* access time Jul 31 12:23:48, 597,847 bytes • *Mandarin III (1st Ed) Readings 28 – Exercising, Chinese - Style.mp3* access time Jul 31 12:28:48, 1,130,118 bytes • *pg_2006.pdf* access time Jul 31 16:43:53, 1,282,149 bytes All files above total to 3,815,260 bytes
29 Jul, 19:09-19:33	108.45.47.2 pool-108-45-47-2.washdc.fios.verizon.net	External Remote Access	51413	9.3K	268	Pimsleurs Torrent files: • *Owner's Manual.pdf* file access time Jul 29 19:20:44, 606,758 bytes • *mandarin1-18.pdf* file access time Jul 29 19:15:44, 184,065 bytes • *mandarin2-07.pdf* file access time Jul 29 19:10:44, 192,062 bytes All files above total to 982,885 bytes
29 Jul, 19:30-20:01	24.44.188.43 ool-182cbc2b.dyn.optonline.net	External Remote Access	6881	1.1M	9.3K	No evidence

3.4.2. Skype Activity

The laptop image was searched for the keyword "skype" using Autopsy. It was discovered that the program Skype was part of the user's profile */Users/xxxxx/AppData /Roaming/Skype*. The profile was created on 10 April 2014 at 16:53:38 PDT, prior to the first Vectra detection on 19 June 2014. This evidence is shown in Figure 19.

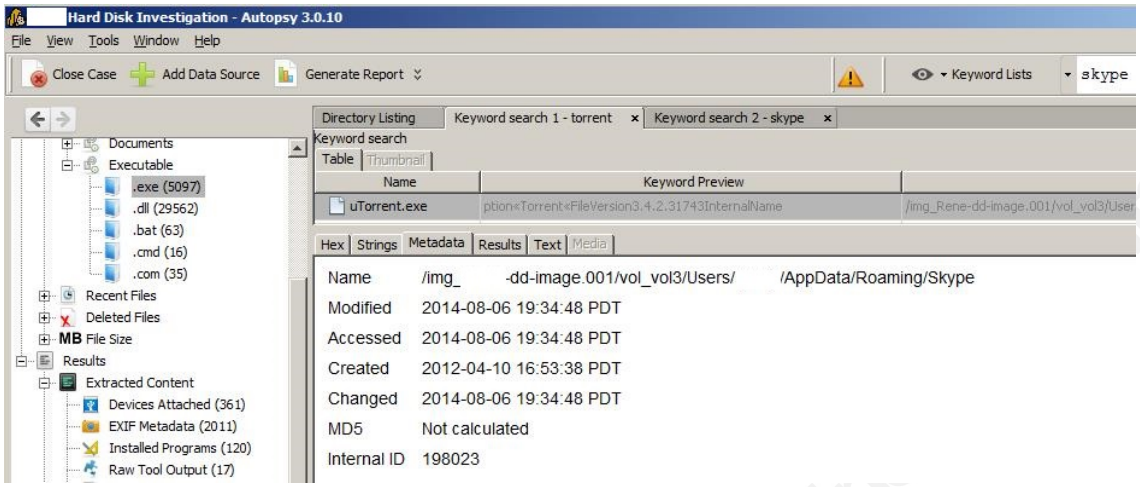


Figure 19: Skype Profile for Subject Laptop User

Internet research was conducted to determine which Windows artifact could be examined for actual Skype activity, as opposed to the mere presence of the Skype program on the laptop. The artifact identified was *main.db*, a database file that "contains information on a user's account, calls, messages, group chat, contacts, file transfers, voicemails, and SMS messages"[12] and is in "a regular SQLite database"[13]. *Main.db* was exported from the laptop hard disk image (path */Users/xxxxx/AppData/Roaming/Skype/xxxxxxxxxxxx*) using Autopsy, then examined on the analysis workstation with the free tool Skyperious, version 3.5. The file transfers and conversations were then exported to spreadsheets.

No file transfers' times coincided with any of the Vectra detections. However, there were messages that did coincide, as shown in Table 2.

Table 2: Vectra Detections with Skype Evidence

Vectra Last Seen (PDT)	External Host IP Address and Hostname	Vectra Detection	TCP Port	Bytes Out	Bytes In	Skype Message Evidence (Epoch & PDT)
17 Jun, 16:39	134.170.24.119 bn1msgr2011202.gateway.edge.messenger.live.com	Fake Browser Activity	80	205	268	1403045092 Tue Jun 17 2014 15:44:52 1403046451 Tue Jun 17 2014 16:07:31
17 Jun, 16:49	134.170.24.119 bn1msgr2011202.gateway.edge.messenger.live.com	Fake Browser Activity	80	204	268	1403048631 Tue Jun 17 2014 16:43:51 1403048644 Tue Jun 17 2014 16:44:04 1403048693 Tue Jun 17 2014 16:44:53 1403048709 Tue Jun 17 2014 16:45:09 1403048722 Tue Jun 17 2014 16:45:22 1403048732 Tue Jun 17 2014 16:45:32 1403048798 Tue Jun 17 2014 16:46:38

17 Jun, 16:50	134.170.24.119 bn1msgr2011202.gateway.edge.messenger.live.com	Fake Browser Activity	80	205	268	Same as above
18 Jun, 14:28	134.170.18.132 bn1msgr1011023.gateway.edge.messenger.live.com	Fake Browser Activity	80	205	268	1403126226 Wed Jun 18 2014 14:17:06 1403126235 Wed Jun 18 2014 14:17:15
18 Jun, 15:06	134.170.18.161 bn1msgr1011124.gateway.edge.messenger.live.com	Fake Browser Activity	80	205	269	1403129130 Wed Jun 18 2014 15:05:30 1403129146 Wed Jun 18 2014 15:05:46 1403129155 Wed Jun 18 2014 15:05:55 1403129211 Wed Jun 18 2014 15:06:51
19 Jun, 11:05	134.170.19.29 bn1msgr1011604.gateway.edge.messenger.live.com	Fake Browser Activity	80	203	268	1403200290 Thu Jun 19 2014 10:51:30 1403200294 Thu Jun 19 2014 10:51:34 1403200305 Thu Jun 19 2014 10:51:45
19 Jun, 11:05	134.170.19.29 bn1msgr1011604.gateway.edge.messenger.live.com	Fake Browser Activity	80	203	267	Same as above
19 Jun, 11:16	134.170.19.29 bn1msgr1011604.gateway.edge.messenger.live.com	Fake Browser Activity	80	204	169	Same as above
19 Jun, 11:17	134.170.19.29 bn1msgr1011604.gateway.edge.messenger.live.com	Fake Browser Activity	80	205	268	Same as above
19 Jun, 13:31	134.170.24.183 bn1msgr2011602.gateway.edge.messenger.live.com	Fake Browser Activity	80	205	268	Vectra detection before Skype evidence: 1403210771 Thu Jun 19 2014 13:46:11 1403210779 Thu Jun 19 2014 13:46:19 1403210786 Thu Jun 19 2014 13:46:26 1403210796 Thu Jun 19 2014 13:46:36
31Jul, 15:08	223.205.105.130 mx-ll-223.205.105-130.dynamic.3bb.co.th	External Remote Access	62000	55.2M	4.2K	Vectra detection too early: 1406832752 Thu Jul 31 2014 11:52:32
31 Jul, 19:33	108.45.47.2 pool-108-45-47-2.washdc.fios.verizon.net	External Remote Access	51413	9.3K	268	Vectra detection too early or too late: 1406847766 Thu Jul 31 2014 16:02:46 1406914148 Fri Aug 01 2014 10:29:08
31Jul, 20:01	24.44.188.43 ool-182cbc2b.dyn.optonline.net	External Remote Access	6881	1.1M	9.3K	Same as above

3.5. Step 3: Examine Carbon Black

Bit9 Security Platform and Carbon Black were not online at the time of the laptop Vectra and Cyphort detections, so this step could not be performed early on as described in Section 2.4. The laptop was eventually reimaged in Step 8: Execute Incident Response Plan, and was outfitted with Bit9 and Carbon Black agents after the Bit9 and Carbon Black servers were deployed. A completely new Vectra detection popped up for the newly reimaged laptop

later Sept. 2014, showing a Category Command and Control Peer-to-Peer detection, as shown in Figure 20.

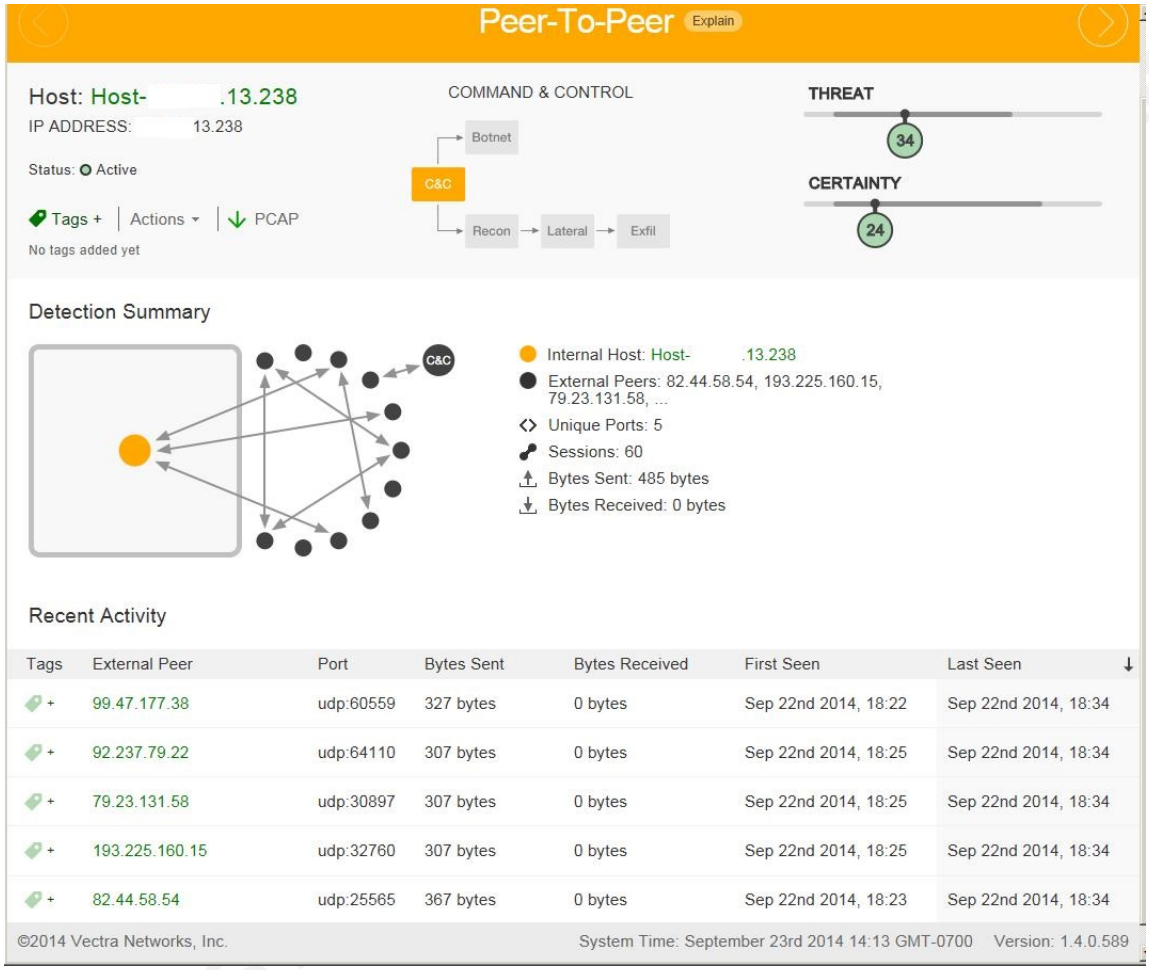


Figure 20: Vectra Peer-to-Peer Detection that Occurred after Subject Laptop Reimaging

The Carbon Black server was examined, and as shown in Figure 21, the uTorrent process was running 23 September 2014 01:27:28Z (18:27:28 PDT). The process, signed by uTorrent, was running during the Vectra detection first and last seen window. Virus Total was launched from Carbon Black, and the detection was deemed to be riskware. The events from the subject laptop were exported from Carbon Black, and the network connections spreadsheet (*netconns.csv*) was examined. This spreadsheet showed the IP addresses that the subject laptop was connected to, and these addresses matched the Vectra external peers. Vectra scored a false positive for malicious behavior, but correctly identified P2P activity. The user was running uTorrent that is approved software, but has a low risk reputation. If

Carbon Black had been present at the time of the original detections, then the investigation could have potentially been solved early on in the investigative methodology sequence through the identification of uTorrent and Skype processes active at the time of the detections.

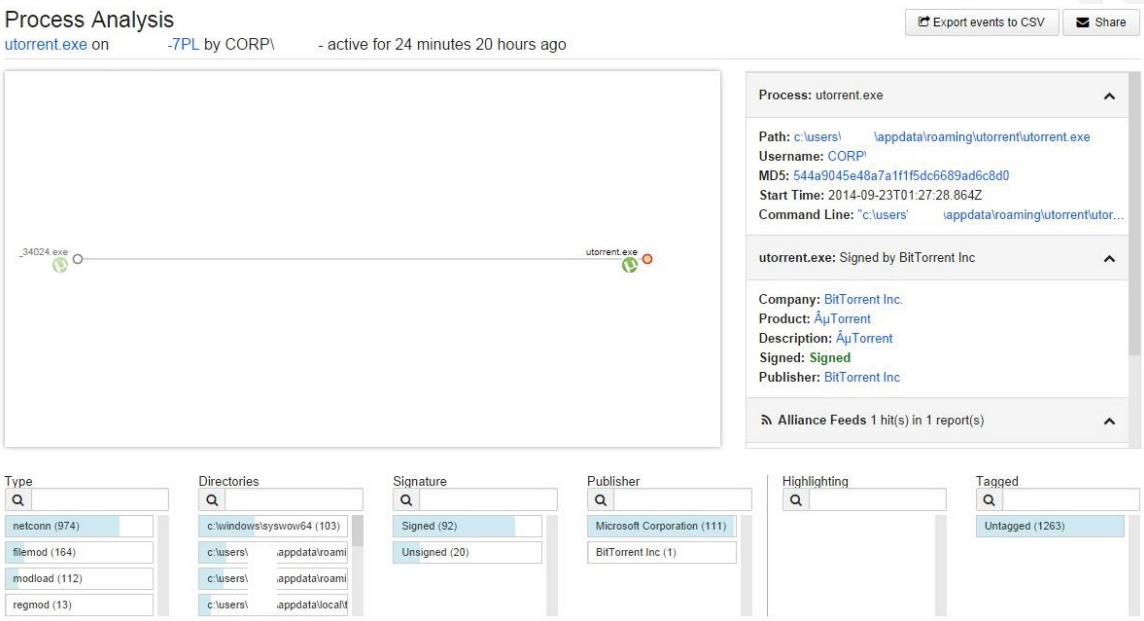


Figure 21: uTorrent Process Running as Shown in Carbon Black

3.6. Step 4: Examine Bit9

Bit9 Security Platform was not installed at the time of the subject laptop Vectra and Cyphort detections and was not examined as described in Section 2.4. If it had been present, it may have produced malicious software alerts at the time of the detections.

3.7. Step 5: Examine Suspect Websites and Software in a Virtual Machine

Suspect software was not downloaded from the Cyphort platform for malware analysis in a sandbox environment. Instead, Bit9 and Carbon Black were used to confirm the Cyphort detections. A Windows 7 VM on the analysis workstation was instrumented with Bit9 and Carbon Black agents. From the VM, the suspect URL detected by Cyphort in the SUSP_CONDUIT.rep detection was browsed to, and the suspect file *spstub.exe* was downloaded and executed. Bit9 detected that this file was malicious, as shown in figures 22

(event) and 23 (event drill-down). Ideally, this malicious file could be globally banned from executing on other hosts loaded with Bit9, as part of Step 8: Execute Incident Response Plan. In this case, the banning was performed in Step 5: Examine Suspect Websites and Software in a Virtual Machine.

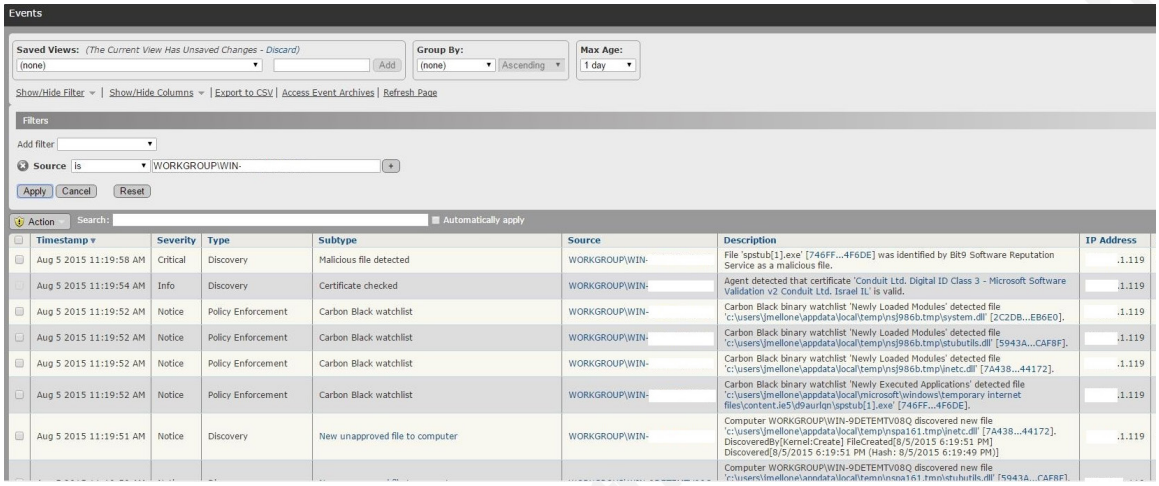
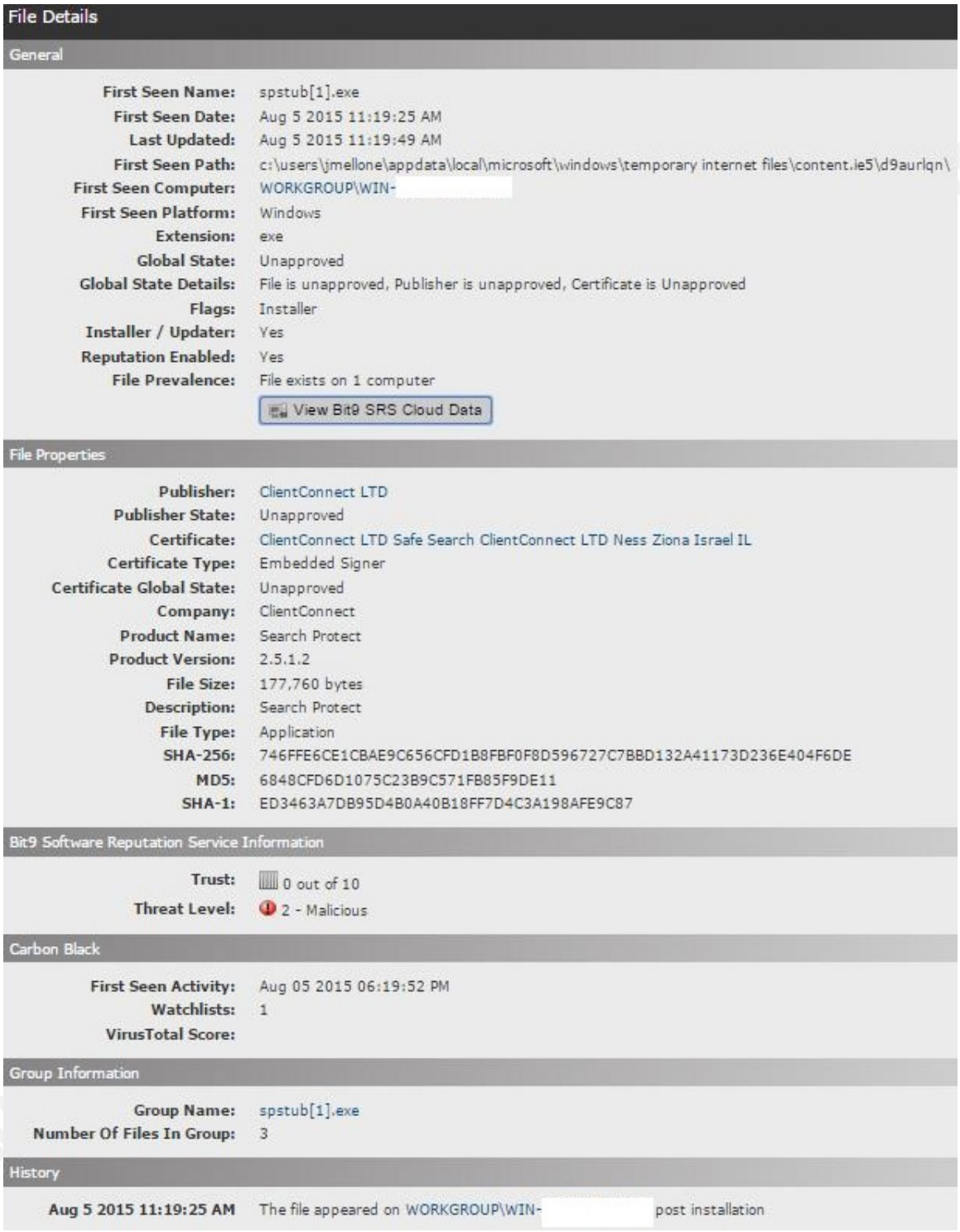


Figure 22: Malicious Executable File Detected Bit9 Event – spstub.exe



File Details

General

First Seen Name:	spstub[1].exe
First Seen Date:	Aug 5 2015 11:19:25 AM
Last Updated:	Aug 5 2015 11:19:49 AM
First Seen Path:	c:\users\jmellone\appdata\local\microsoft\windows\temporary internet files\content.ie5\d9aurlqn\
First Seen Computer:	WORKGROUP\WIN-
First Seen Platform:	Windows
Extension:	exe
Global State:	Unapproved
Global State Details:	File is unapproved, Publisher is unapproved, Certificate is Unapproved
Flags:	Installer
Installer / Updater:	Yes
Reputation Enabled:	Yes
File Prevalence:	File exists on 1 computer
	View Bit9 SRS Cloud Data

File Properties

Publisher:	ClientConnect LTD
Publisher State:	Unapproved
Certificate:	ClientConnect LTD Safe Search ClientConnect LTD Ness Ziona Israel IL
Certificate Type:	Embedded Signer
Certificate Global State:	Unapproved
Company:	ClientConnect
Product Name:	Search Protect
Product Version:	2.5.1.2
File Size:	177,760 bytes
Description:	Search Protect
File Type:	Application
SHA-256:	746FFE6CE1CBAE9C656CFD1B8FBF0F8D596727C7BBD132A41173D236E404F6DE
MD5:	6848CFD6D1075C23B9C571FB85F9DE11
SHA-1:	ED3463A7DB95D4B0A40B18FF7D4C3A198AFE9C87

Bit9 Software Reputation Service Information

Trust:	0 out of 10
Threat Level:	2 - Malicious

Carbon Black

First Seen Activity:	Aug 05 2015 06:19:52 PM
Watchlists:	1
VirusTotal Score:	

Group Information

Group Name:	spstub[1].exe
Number Of Files In Group:	3

History

Aug 5 2015 11:19:25 AM	The file appeared on WORKGROUP\WIN- post installation

Figure 23: Malicious Executable File Detected Bit9 Event – spstub.exe – Drill-Down

The *spstub.exe* process was analyzed using Carbon Black, which revealed that the network connection to the server from which the executable was downloaded is malicious. This is shown in Figure 24.

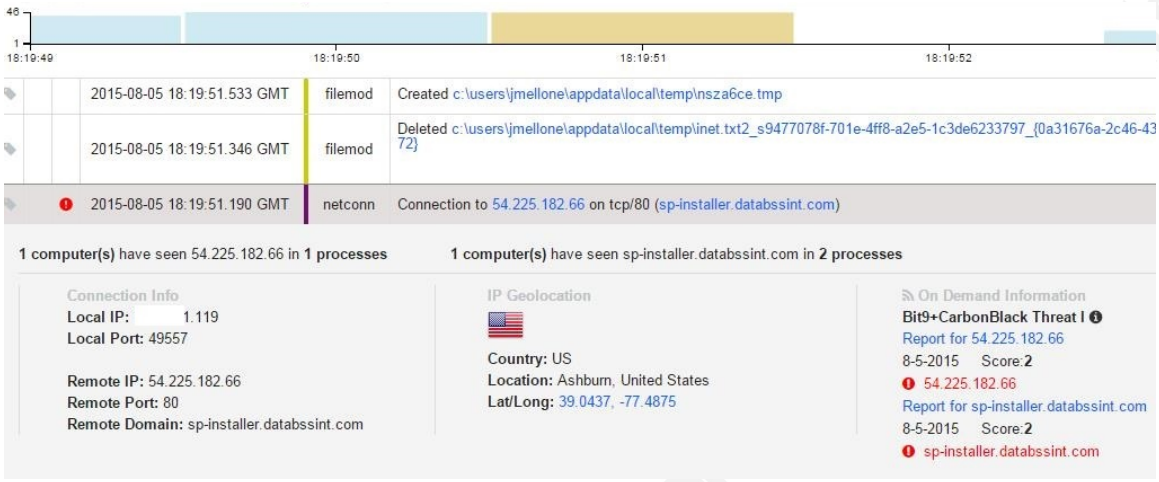


Figure 24: Malicious spstub.exe Process in Carbon Black

This process of using Bit9 and Carbon Black to confirm the other Cyphort detections was repeated in the same manner, so in the interest of brevity, the screenshots are not shown. According to Bit9, The SUSP_LYCKRIKS.DC Cyphort detection with its associated *1030-4004_PassShow.exe* executable was shown to be innocuous. However, Carbon Black classified it as malicious. The confirmation of the TROJAN_AGENT.DC Cyphort detection with its associated *Installium_p1v0.exe* executable was attempted, but the suspect website was not reachable.

3.8. Step 7: Dump and Analyze Memory

Carbon Black's Live Response feature allows the analyst to connect to the subject host. Memory can be dumped on the live host, moved to an analyst workstation loaded with memory analysis tools, and examined. This step was not performed. Carbon Black with the Live Response feature was not available at the time of this investigation, and the user had disconnected and shut down from the corporate network prior to the start of this investigation anyway, resulting in the loss of volatile memory content. In addition, the case had already been solved using the previous steps. However, this process should be executed on a live host so the analyst will know how to do it when needed.

Jennifer L. Mellone, jmellone@alum.wpi.edu

4. Conclusion

This real-world case was used to generate an investigation and analysis workflow, and most of the steps in this workflow were performed to resolve the case. A summary of the findings for the subject laptop are as follows:

Vectra External Remote Access detections showed the subject laptop sending data outbound to IP addresses on TCP ports used by Bit Torrent software. Packet captures downloaded from the Vectra platform were examined with Wireshark, showing encrypted traffic. It is known that Torrent traffic can be encrypted. The IP addresses were not malicious, according to the Virus Total website. Disk forensics showed that the uTorrent program was part of the user's profile - */Users/xxxxx/AppData/Roaming/uTorrent*, and was installed before the Vectra detections. The uTorrent artifact *resume.dat* from *Users/xxxxx/AppData/Roaming/uTorrent* was exported out of Autopsy. This file was encoded with the BEncoding scheme and was examined with BEncode Editor in human readable format. Several Torrent files were shown in the BEncode editor and were present in the user's download folder *C:\Users\xxxxx\Downloads*. Each Torrent was expanded in BEncode editor to see the underlying folders and files. The Access Time for each file was examined to determine if the time fell in the window of the Vectra External Remote Access detections being analyzed for uTorrent activity. Two out of three Vectra External Remote Access detections coincided with evidence of uTorrent activity on the laptop, confirming that the detections were probably false positives (not malicious) in this case.

Vectra Fake Browser Activity detections, which appeared a month prior to the aforementioned External Remote Access detections, showed the laptop sending data outbound to Microsoft-owned IP addresses on TCP port 80. Packet captures downloaded from the Vectra platform were examined with Wireshark, revealing the following: unencrypted traffic; x-msn-messenger HTTP content; user-agent strings that were assessed to not be malformed; the user's Hotmail email address; and the downloading of a Skype software update. The IP addresses were not malicious according to Virus Total. Skype replaced Microsoft Messenger, which explains the connection between Skype and Microsoft in the evidence. Disk forensics showed that the Skype program was part of the user's profile - */Users/xxxxx/AppData/Roaming/Skype*, and was installed before the Vectra detections. The

Skype artifact *main.db* from */Users/xxxxx/AppData/Roaming/Skype/xxxxxxxxxxxx* was exported out of Autopsy. The database was examined with Skyperious to display the SQLite database in human readable format, and data was exported into a spreadsheet. There were no Skype file transfers whose times coincided with any of the Vectra detections, but there were Skype messages that did coincide. According to Skype's website, port 80 can be used and the messaging is encrypted, but the packet capture shows unencrypted traffic. The packet capture traffic is probably Skype peer-to-peer protocol between the laptop and Skype servers. The Skype activity is not assessed to be related to the uTorrent activity. The aforementioned evidence shows that the Vectra detections were probably false positives in this case. Despite the false positives, which in this case were benign findings, the organization has gained visibility on user behavior. If uTorrent is unapproved software, then the user is in violation of policy and action can be taken to remove the software. Given more learning time in the environment, Vectra may produce true positives. Human intervention will be required to make the verdict - malicious or benign.

Cyphort produced three Cyphort adware detections pertaining to the subject laptop. Executables associated with detections SUSP_CONDUIT.Rep, SUSP_LYCKRICKS.DC, and TROJAN_AGENT.DC were downloaded to the laptop. SUSP_CONDUIT.Rep and SUSP_LYCKRICKS.DC were downloaded before the Vectra External Remote Access detections. TROJAN_AGENT.DC was downloaded before the Vectra Fake Browser Activity detections. The Cyphort detections were unrelated to the Vectra detections. Carbon Black and Bit9 were not deployed, so they could not be used to confirm the malicious downloads on the laptop.

The laptop was ultimately reimaged because of the Cyphort detections and it was later loaded with Bit9 and Carbon Black agents. A Vectra Peer-to-Peer detection occurred afterward; Carbon Black confirmed the uTorrent process running at the time of the detection, and the network connection IP addresses matched the addresses shown in the Vectra detection. This illustrates how Carbon Black can be used to speed up the incident response process when investigating Vectra detections.

The adware files were later downloaded to a Windows 7 VM instrumented with Bit9 and Carbon Black agents. The executable associated with SUSP_CONDUIT.Rep was

classified as malicious by Carbon Black and Bit9. The executable associated with SUSP_LYCKRIKS.DC was shown to not be malicious according to Bit9, but Carbon Black classified the executable as malicious. The website associated with TROJAN_AGENT.DC could not be reached for testing, but it is safe to say that all three Cyphort detections are true positives. This demonstrates how Cyphort detections can be crosschecked with Bit9 and Carbon Black. In a production environment, these adware files could be globally banned from executing on other hosts instrumented with Bit9.

Vectra and Cyphort complement one another in the area of detection. Bit9 can produce alerts that show the detection of malicious software; it does not have to be used solely as an application-whitelisting tool (except in low to medium enforcement mode), especially in a dynamic software development environment where laptops are undergoing software installation too frequently. Bit9, in medium or high enforcement modes, is better suited for more static hosts, such as point of sale devices and high-security hosts such as software source code repositories. Bit9 can be configured under the hood to automatically ban malicious software, but this is risky if a false positive alert triggers the ban. Carbon Black can be used in conjunction with all three products - Bit9, Vectra, and Cyphort.

5. References

[1] Vectra Networks. Section: *Scoring*. Application manual. (2015). Retrieved on July 8, 2015 from: Private URL

[2] Vectra Networks. Section: *Scoring*. Application manual. (2015). Retrieved on July 8, 2015 from: Private URL

[3] Vectra Networks. Section: *Understanding Vectra Detections*. Application manual. (2015). Retrieved on July 8, 2015 from: Private URL

[4] Vectra Networks. Section: *Understanding Vectra Detections*. Application manual. (2015). Retrieved on July 8, 2015 from: Private URL

[5] Vectra Networks. Section: *Understanding Vectra Detections*. Application manual. (2015). Retrieved on July 8, 2015 from: Private URL

[6] Vectra Networks. Section: *Understanding Vectra Detections*. Application manual. (2015). Retrieved on July 8, 2015 from: Private URL

[7] Vectra Networks. Section: *Understanding Vectra Detections*. Application manual. (2015). Retrieved on July 8, 2015 from: Private URL

[8] Vectra Networks. Section: *Understanding Vectra Detections*. Application manual. (2015). Retrieved on July 8, 2015 from: Private URL

[9] Cyphort. (2014). *Cyphort Advanced Threat Defense with Bit9 + Carbon Black*. Retrieved from http://www.cyphort.com/wp-content/uploads/2015/02/CYPHORT_SB1-Bit9.pdf

[10] Cyphort. (2014). *Cyphort Operators Guide 3.0.1 V2*. Received November 10, 2014 from Cyphort Technical Support

[11] Cyphort. (2014). *Cyphort Operators Guide 3.0.1 V2*. Received November 10, 2014 from Cyphort Technical Support

[12] McQuaid, Jamie. Magnet Forensics. (2014). *Skype Forensics: Analyzing Call and Chat Data from Computers and Mobile*. Retrieved October 12, 2015 from https://www.magnetforensics.com/wp-content/uploads/2014/04/Skype-Forensics-Analyzing-Call-and-Chat-Data-From-Computers-and-Mobile-Magnet-Forensics.pdf

[13] McQuaid, Jamie. Magnet Forensics. (2014). *Skype Forensics: Analyzing Call and Chat Data from Computers and Mobile*. Retrieved October 12, 2015 from https://www.magnetforensics.com/wp-content/uploads/2014/04/Skype-Forensics-Analyzing-Call-and-Chat-Data-From-Computers-and-Mobile-Magnet-Forensics.pdf

[14] uTorrent Community Forum. *BEncode Editor*. (2007). Retrieved October 2, 2015 from http://forum.utorrent.com/topic/26674-bencode-editor/

Jennifer L. Mellone, jmellone@alum.wpi.edu

6. Bibliography

Blum, Dan. *Cyphort Launches a New Advanced Threat Defense Platform*. Blog. February 19, 2014. Security Architects LLC. Retrieved on September 23, 2015 from http://security-architect.blogspot.com/2014/02/cyphort-launches-new-advanced-threat.html

Cyphort. *Network-based Next Generation APT Defense*. Product information. Cyphort. Retrieved on September 23, 2015 from http://www.cyphort.com/products

Torrentino, Mohit Mayank Jha. *What are seeds, peers, trackers, pieces in uTorrent?* Blog. Quora. Retrieved on September 23, 2015 from http://www.quora.com/What-are-seeds-peers-trackers-pieces-in-uTorrent

Vectra Networks. *A New Class of APT Defense*. Product information. Vectra Networks. Retrieved on September 23, 2015 from http://www.vectranetworks.com/product/

Wagner, Ray et al. *Cool Vendors in Security Intelligence*. Technical report. Gartner. April 24, 2015. Retrieved on September 23, 2015 from http://www.gartner.com/technology/reprints.do?id=1-2E1GX1S&ct=150427&st=sb

Westervelt, Robert. *Take Notice: 6 Security Startups Shaking Up The Industry*. Presentation. CRN. February 15, 2015. Retrieved on September 23, 2015 from http://www.crn.com/slide-shows/security/300075893/take-notice-6-security-startups-shaking-up-the-industry.htm