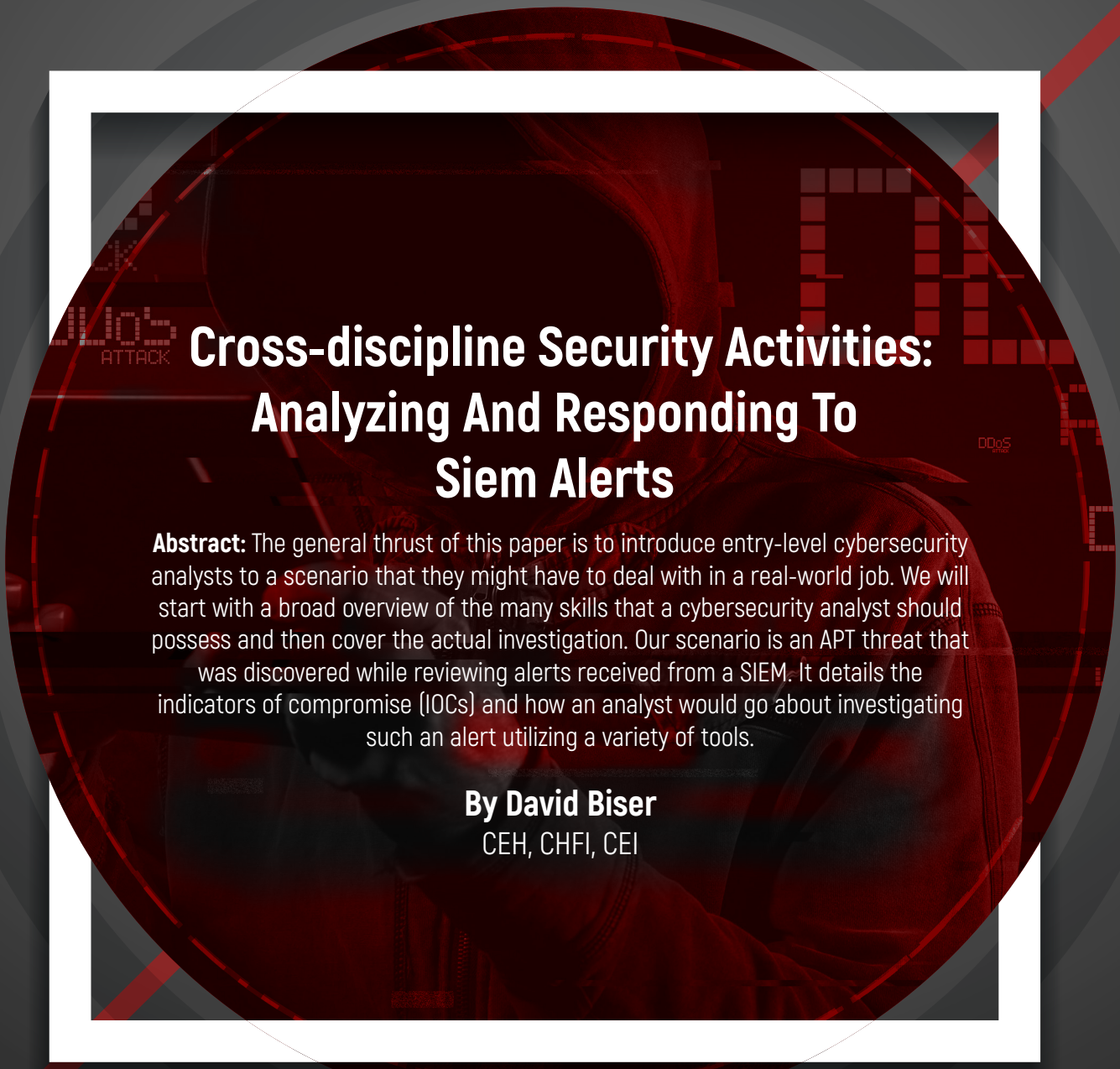
EC-Council



Cross-discipline Security Activities: Analyzing And Responding To Siem Alerts

Abstract: The general thrust of this paper is to introduce entry-level cybersecurity analysts to a scenario that they might have to deal with in a real-world job. We will start with a broad overview of the many skills that a cybersecurity analyst should possess and then cover the actual investigation. Our scenario is an APT threat that was discovered while reviewing alerts received from a SIEM. It details the indicators of compromise (IOCs) and how an analyst would go about investigating such an alert utilizing a variety of tools.

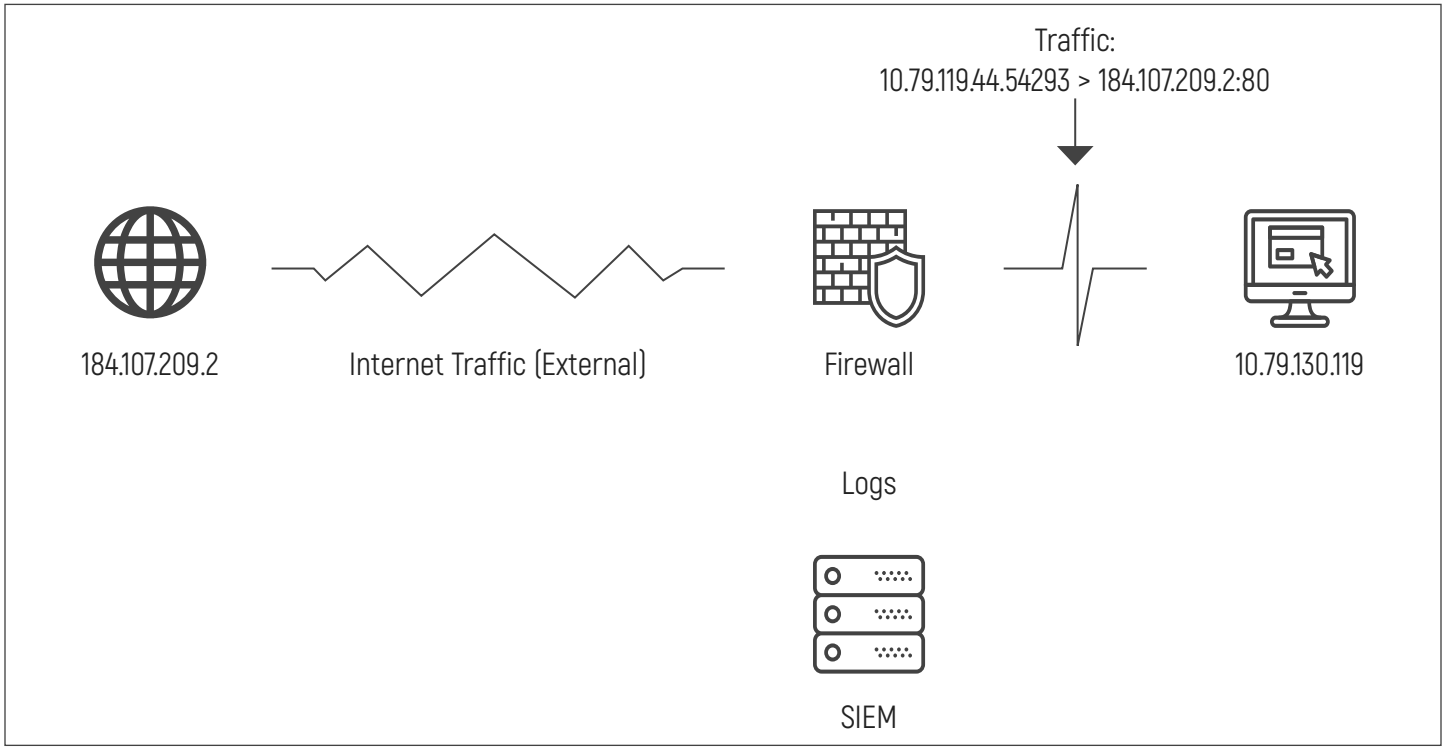
By David Biser
CEH, CHFI, CEI

As cybersecurity professionals, we are called upon many times to exercise what I like to call "cross-discipline" activities. The reason that I call it "cross-discipline" is because the range of activities often required of a cybersecurity professional is vast. Cybersecurity professionals must master many different skillsets, including the following:

- Network fundamentals
- SIEM knowledge
- Knowledge of hacker activities (current and past!)
- Applications
- Programming/Scripting
- In-depth forensic knowledge
- Evidence gathering techniques
- Legal knowledge
- Threat intelligence
- Packet analysis

This list could go on, but I kept it short to enable the reader to stay focused on our primary goal: actively investigating an ongoing threat. This is generally called "threat hunting" and it has become a popular catchphrase in the cybersecurity community. There are a growing number of articles, training programs, and websites that purport to help the analyst become a better threat hunter and as far as I am concerned it is a viable skill set for the cybersecurity professional.

As a cybersecurity analyst, you may find yourself in a variety of circumstances, drawing upon your range of skills and dealing with a wide variety of different people. We need to work to continually educate ourselves and develop the ability to communicate during a crisis. The purpose of this article is to draw your attention to the many skills you will need in order to perform outstanding work as a cybersecurity analyst, no matter what your position. The better we are as professionals, the better we will be able to help secure the networks and data entrusted to our care.



So, on to the main part of the article! The scenario is as follows: You are working as a cybersecurity analyst and while you are reviewing your SIEM alerts you come across the following alert:

Internal Connection to Host Categorized as Malware containing Firewall Permit

The investigation begins, or more accurately, the hunt is on! It is here that I would like you to stop and think about exactly what you are investigating. In the world of law enforcement, when it comes to investigations there are different techniques that can be used depending upon what type of crime you are investigating and the same holds true in the cyber world. In this case, the initial alert is concerning malware that might be communicating outside our network, thus the "firewall permit" wording.

Now, this could be anything or it could be nothing, so we need to do some more work to determine exactly what is occurring. We take a look at the logs themselves.

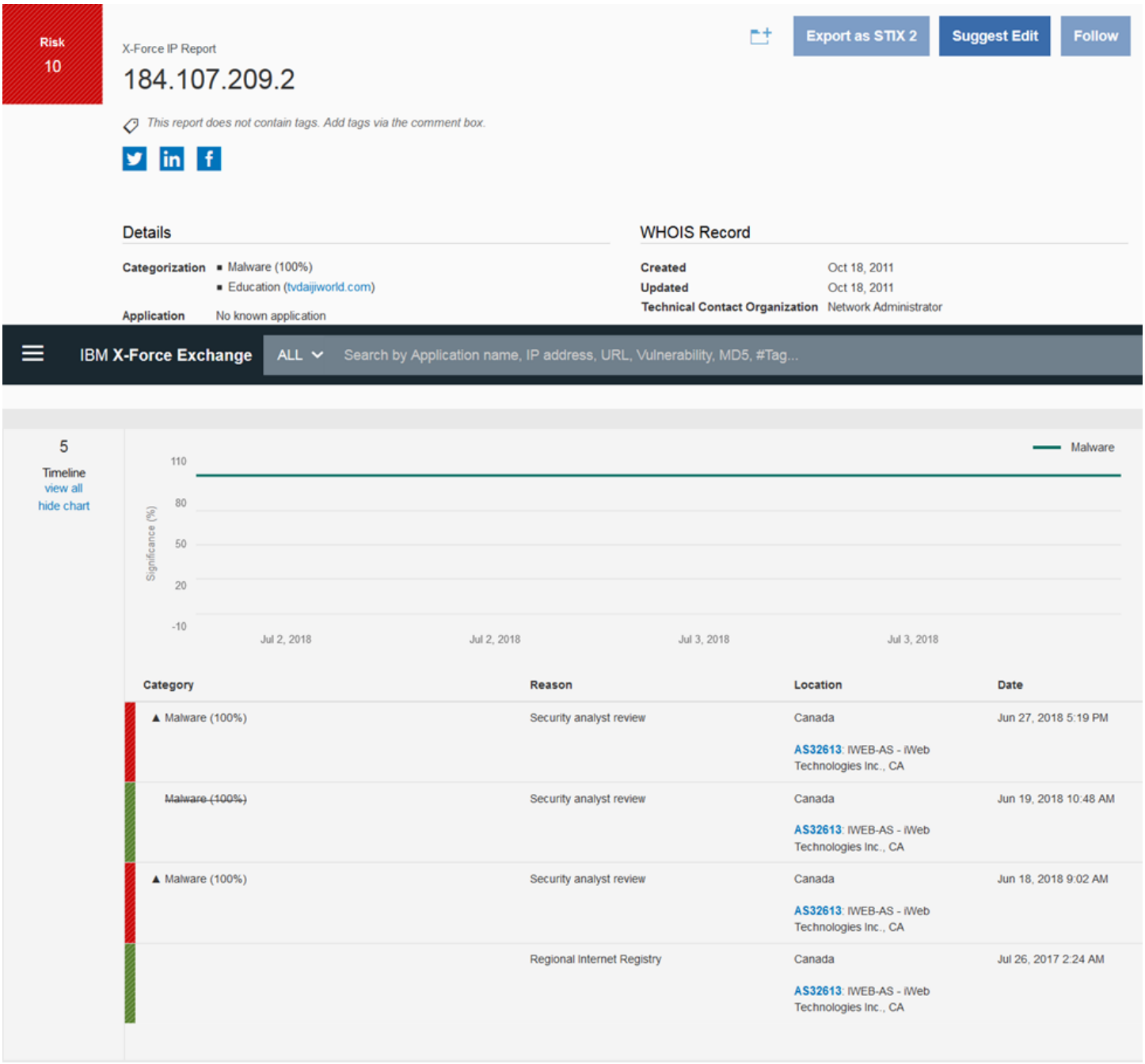
<13>Jul 02 22:01:45 10.130.119.444 02Jul2018 22:01:45 allow 10.130.119.444 product: URL Filtering; src: 10.79.119.444; s_port: 54293; dst: 184.107.209.2; service: 80; proto: tcp; rule: Computers / Internet,URL Filtering;app_risk: 0; app_rule_name: any any allow;appi_name: tvdaijiworld.com;browse_time: 0:00:02;bytes: 20884782;has_accounting: 0;i/f_dir: outbound;i/f_name: eth1-02;matched_category: Computers / Internet; proxy_src_ip: 10.79.240.444; received_bytes: 20548746;resource: http://www.tvdaijiworld.com/img_ad/ ;sent_bytes: 264899;snid: 5d256f09;src_machine_name: testmachine@testnetwork.comsrc_user_name: Test user (tuser)

;user: Test user(tuser) ;web_client_type: Chrome;

This log has been modified some to keep certain information private, but otherwise it is very similar to how an actual log would appear from a SIEM. Now, as we examine the log, we can identify several things which are important to our investigation.

First, the source IP is showing as 10.79.119.444 with port 54293. The second is the destination IP and port, which are 184.107.209.2 and 80. The user and user machine are also identified for us along with the URL visited during the alert. This kind of log provides the analyst with a good amount of information to continue the investigation and also begin to develop a theory as to what is going on. Granted, a single log doesn't provide as much information as the entire series, but for the purpose of this article, we will stick with the information contained in this log. I will note that during an actual incident investigation the analyst will pull all logs sourcing from the infected machine for a period of time and examine those logs for further evidence of infection, data exfiltration, or an adversary traversing the network.

Now, the reason that this alert was set off was actually an external intelligence source feeding IOCs into the SIEM. So, we will turn our attention to these intelligence sources and search for a bit more information to further our investigation.

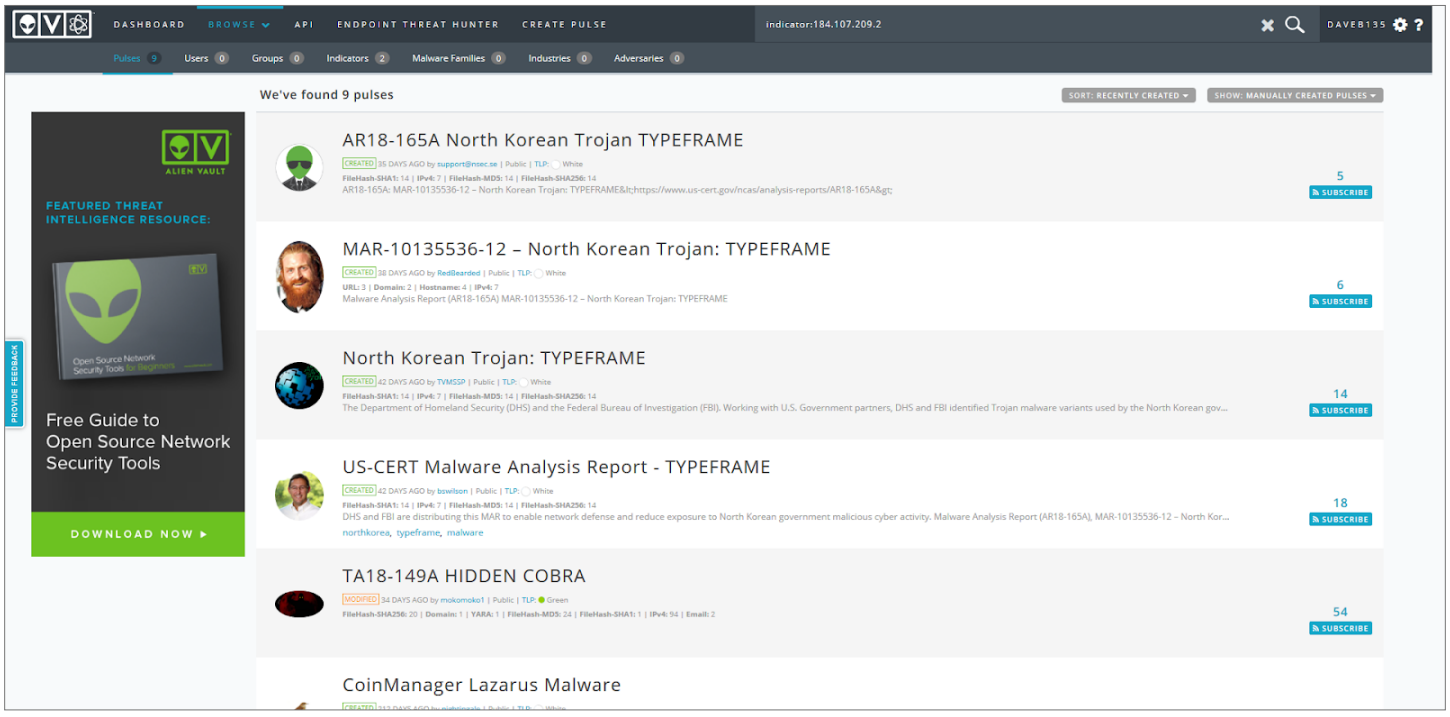


The above picture is taken from IBM's X Force, a program that provides customers with threat intelligence. Utilizing the suspicious IP address, a search was conducted within X Force's Threat Exchange for associated information. As can be seen from the picture, this IP address is listed as malware and stands at 100% certainty. It also has a rating of 10, which is high for an IP address and its associated domain. The domain provided by X Force is tvdaijiworld.com, which is very similar to the one in our generated alert.

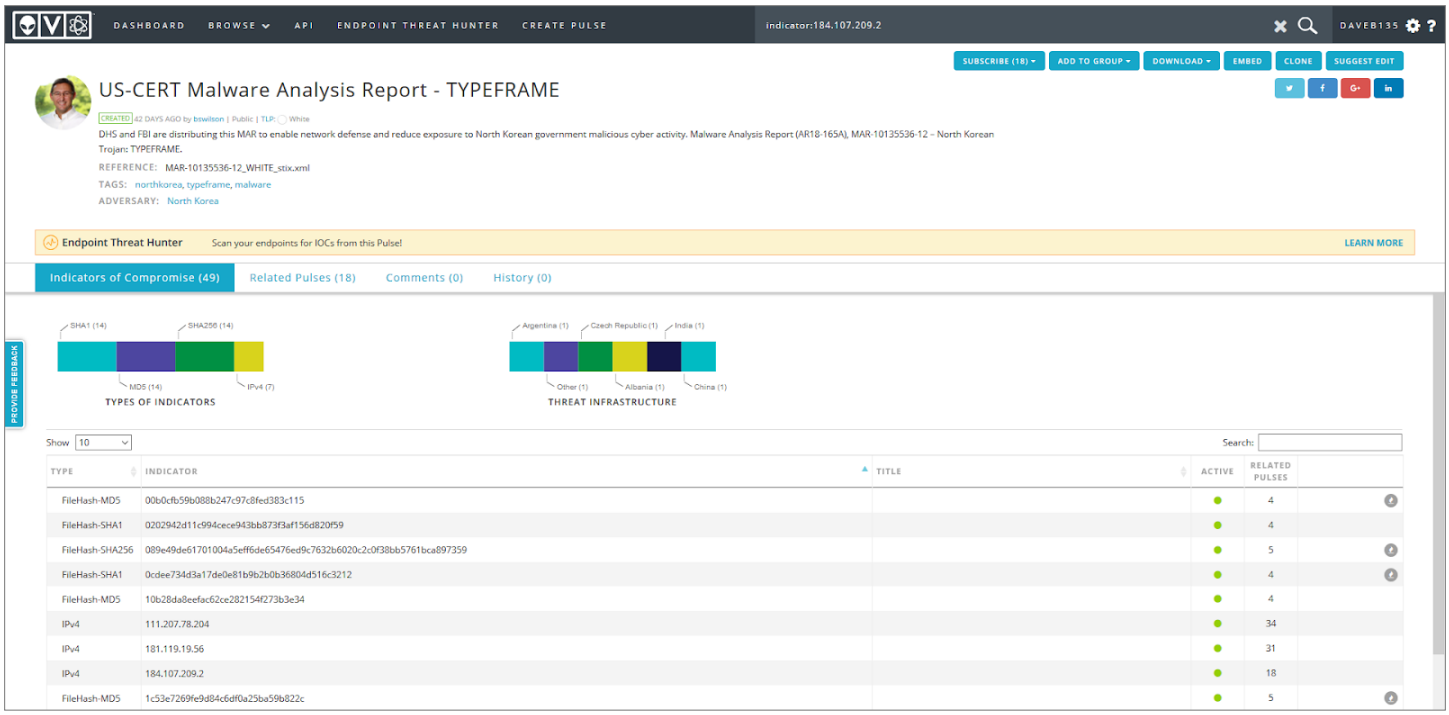
Now that we have some confirmation that this could indeed be a malicious IP address with an associated domain name, we can continue our investigation. We can look further in X Force to gather more information and X Force does indeed provide a link to a U.S. CERT report named "Hidden Cobra – North Korean Malicious Cyber Activity." This link can be found at https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity.

Certainly, by now alarm bells are going off and the security team is stirring, right? Hidden Cobra is a well-known and highly documented threat actor that utilizes malware to infect, infiltrate, and target a variety of different industries. The FBI and DHS released statements along the following lines: "a successful network intrusion attack could result in a temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, a potential harm to an organization's reputation." This is definitely alarming! Now, what should your next steps be as a cybersecurity analyst?

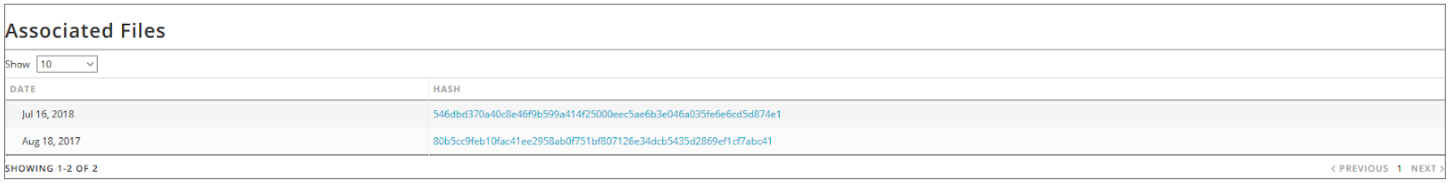
Caution is always a good thing and along with the intelligence you have already discovered, we need to confirm that information. We can turn to a variety of sources and one of my favorites is AlienVault's Open Threat Exchange (https://otx.alienvault.com/). If we use some of the indicators of compromise we already have in our possession, we can learn even more about the alert and the possible threat it introduces into our network.



In the above screen capture, we performed a search for the IP address associated with this investigation and AlienVault OPX gave us a listing of multiple reports that contain the same IP address. We can read all of them or choose from several in order to glean more information.



I choose the above report, which is the U.S. CERT malware analysis report we mentioned earlier. We can use this to confirm the various indicators of compromise and glean some more information with which to search across our network. In many instances, file hashes can be used to search across a network for malicious files and if needed, you can find those right here (see below image).



Once you have conducted your research, you have to make a decision: is this a threat hunt or response to an incident? Does your company have an incident response plan? Do they have an established threat hunting program? Do you have playbooks to direct and guide the process? If not, then these are all areas that you should establish within your security framework. Sadly, most surveys reveal that many companies do not possess these rudiments of security and thus are already in trouble if an event such as the one described above were to occur.

Let us turn our attention back to the matter at hand, the possible malware infection. US-CERT provides the analyst with indicators of compromise, in both a STIK format and also in other formats. These should be compiled by the analyst and utilized to continue the hunt. A series of hashes, IP addresses, and host-based indicators are provided to assist the analyst in determining the extent of the infection or even if the infection is a true positive. Remember, there are such things as false positives and it might be the case that this is a false positive. We need to establish exactly what is occurring.

As precautionary steps, the analyst and team took the following steps as well as conducting ongoing research into the threat. First, they instituted a communication block on the suspect machine. This prevented the machine from any further communication on the network to prevent the spread of infection or theft of data. Second, they ensured that the user's password was changed to ensure that the account was not compromised in any way. I will stop here and ask if your security team has the ability to perform these basic functions in the opening stages of an investigation. Can they quarantine an infected machine? A compromised user? If not, then this is something you should explore and get implemented within your security plan.

As this incident developed, the analyst conducted a search via the SIEM for the malicious domain and eventually learned that all communications were occurring via port 80 and not port 443, which was the actual port listed in the IOCs. This provided an indication that this could be a false positive. A review of the visited URLs did not match the ones provided in the IOCs either, which gave confirmation to the false positive. Analysts further utilized the hashes provided in the IOC report from CERT to determine that absolutely no other indicators of compromise were present on either the host system or network traffic, which gave the analyst the end result that this was in actuality a false positive.

As a sort of quick review, I would like to list out some of the lessons learned from an incident of this type, to help the reader improve their own program and the analyst to develop further skills in investigating cyber intelligence information.

1. Do not take all indicators of compromise as true. There are, in fact, many false positives based upon only one indicator of compromise. Cybersecurity involves a holistic approach and this holds true to information provided by third parties. Threat hunting requires that the analyst sort through a host of information and determine what is true and what is false.
2. Thoroughly investigate all alerts. It is a well-known fact that analysts can become "shell-shocked" and start ignoring alerts. This needs to be combated as much as possible by both the company and the employees. Rather than allowing yourself to start thinking negatively, approach each alert as if it was an actual breach attempt and thoroughly examine the incident. From a company approach, the leaders need to ensure that their employees are not burning out. This can be done in a multitude of ways:
    a. Ensure adequate staffing for analysts.
    b. Ensure that analysts have the proper tools and training to do their jobs correctly.
    c. Ensure that your threat intelligence feeds are updated and providing actionable intelligence and not garbage!
3. Ensure you have the proper tools to monitor, investigate, and protect your network. Do you have a SIEM? Are you performing a log review? Do you have endpoint protection software on each endpoint? Are you monitoring your servers for illicit or unusual activity? The list can go on and on, but the end result is that you need to adequately protect your data and the machines that store and transfer that data.
4. Create a holistic cybersecurity program that provides protection at all levels of the cyber-attack chain. Most attacks are not focused on merely one aspect of the network, but seek to traverse the network, jumping from machine to machine and in order to properly hunt them, you must have the tools and skills to ensure they can be caught.

5. Finally, as was stated above, the security team had to interact with the end user and manager and other members of the IT community. Ensure that there are open and friendly communication lines across these various parties. I worked as a third-party consultant for a time and that was one of the biggest obstacles to performing incident response: a lack of communications. Managers and supervisors need to ensure that these lines are open and available even before an incident begins. This increases the speed and timeliness of response efforts and in the end, helps better protect your network.

Let's also recap our opening claim as briefly as possible. I will list out the skills from the opening section and reference the stage of the investigation when that knowledge came to be used by the analyst.

- Network fundamentals – tracing the network connections across the SIEM from the malware URL and the suspect host system
- SIEM knowledge – tracing the alert and IOCs via the SIEM interface
- Knowledge of hacker activities (current and past!) – identify actual suspicious activity and attack vectors, as well as conduct research
- Applications – determine what applications were running on the host system and if the malware would interfere with or exploit them
- Programming/Scripting – not used in this actual scenario, but scripting could have added speed to the IOC search
- In-depth forensic knowledge – conduct forensic preview on the host system
- Evidence gathering techniques – if the infection had been real, then this area would have been utilized
- Legal knowledge – the analyst had to determine when to notify the supervisor and possibly when to pull in their legal team for guidance and contacting the proper authorities
- Threat intelligence – self-described throughout the scenario
- Packet analysis – this was not used during the scenario because the company did not have access to packet captures. It exposed a weakness in the security program and could have greatly benefited the security team had it been in place.

A great security analyst brings to the table a multitude of different skills. EC-Council can help you prepare for that job via many different course offerings, such as the Certified Threat Intelligence Analyst and the Certified Ethical Hacking course. Take advantage of such training, for yourself and your employees if you are a manager!

References

- https://otx.alienvault.com/
- https://www.us-cert.gov/

EC-Council