Improving Computer Network Defense Analysis Training With Adversary Replication Techniques

Juan J. Güelfo, Ingrid C. Bentzen
Encripto AS

Abstract

This paper proposes two training methods that can be used to improve computer network defense analysis training. The main advantages of these methods are reduced risk and preparation costs, while increasing realism during training sessions. These methods can easily be implemented by both public and private organizations, as well as training institutions such as universities.

1. Introduction

Until the past decade, common threats against computer systems could be stopped by anti-virus software and firewalls. Nowadays, these two countermeasures can be easily bypassed by attackers, and they just offer a basic degree of protection.

Detecting, analyzing and reacting effectively to computer threats is therefore important in order to contain damages, reduce costs and recovery time in the event of a network security breach.

In order to detect, analyze and react, IT personnel are required to have specialized skills within computer network defense analysis and incident response. Currently, the possibilities for training and improving in these disciplines have important constraints mainly related to case realism and its practical implementation, infrastructure costs and the inherent risk of training scenarios.

The information security landscape is not very promising when it comes to finding qualified and experienced professionals. According to ISACA and CSX, the 2015 Global Cybersecurity Status Report [1] shows that 46% of respondents expect their organization to face a cyberattack in 2015. In addition, 83% believe cyberattacks are one of the top three threats facing organizations today. However, 86% say there is a global shortage of skilled cybersecurity professionals and only 38 percent feel prepared to fend off a sophisticated attack.

This paper is an attempt to introduce improvements in current computer network defense analysis training methods. Based on adversary replication techniques, we have developed open source tools that allow the creation of realistic scenarios, while reducing infrastructure costs, implementation time and risk.

First of all, this paper will analyze and classify common methods for computer network defense analysis training, based on four relevant criteria. Next, we will propose alternatives that can solve the challenges and improve training exercises, by using adversary replication techniques and open source tools. Finally, this paper will demonstrate a practical application of these techniques and its comparison to common methods.

2. Terminology

The following terminology will be recurrent in this paper:

Computer Network Defense Analysis [2]: To use defensive measures and information collected from a variety of sources to identify, analyze, and report events

Presented at the Norwegian Information Security Conference 2015 (NISK-2015).

that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Adversary [2]: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Blue Team [2]: A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group.

Red Team [2]: A group authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprises cybersecurity posture.

Indicator [2]: An occurrence or sign that an incident may have occurred or may be in progress.

Targeted attack [3]: A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim's defenses.

Attack scenario [4]: A scenario that enumerates and describes the ways an attacker might make use of a vulnerability. The known attack vectors and steps to perform the attack will be identified.

3. Computer Network Defense Analysis Training Techniques

Computer network defense analysis is a broad topic and skills can be acquired with different methods. This paper is going to focus on common training techniques that are mainly based on studying network traffic that could be either live or previously captured.

In any of these situations, the production and acquisition of network traffic requires an attack scenario with supporting infrastructure. The goal is to successfully monitor the network traffic while the attack is in progress. The result allows a blue team to improve their skills and test the detection tools deployed as part of an organization's IT infrastructure.

Typically, the network traffic produced in such kind of scenario is captured and saved as files in PCAP format. From a training perspective, such files contain a "story" specific to the environment where it was captured, and it can be used again by a blue team, for example when training new members or reviewing a training exercise.

In order to train computer network defense analysts and reach an advanced skill level, it is essential to create realistic attack scenarios that can generate relevant network traffic. In many cases, pieces of malware are used in such scenarios, so computer network defense analysts can train with real indicators. However, this practice comes with an inherent risk. Therefore, a controlled environment ensuring security while keeping a high degree of realism is vital.

We have evaluated common methods for implementing attack scenarios, which can allow monitoring and capturing network traffic. The evaluation is based on four criteria: Difficulty of implementation, costs, risk and realism.

3.1 Evaluation Criteria

The criteria listed below have been chosen based on experience gained by Encripto AS over time. They represent common challenges that arise while planning or conducting computer network defense analysis training sessions.

According to our experience, the challenges usually affect the training sessions in two different ways. On one hand, the challenges could stop a training session already on the planning stage due to the risk and/or cost that the process involves. On the other hand, those organizations that decide to conduct the training tend to do it with limited scope, or less frequently than desired.

3.1.1 Difficulty of Implementation

This criterion describes how difficult it is to create, configure and maintain an environment where the attack scenario is going to be executed. The difficulty of implementation is usually related to the amount of time required for the tasks. The lower the value is, the less work is required in order to successfully setup the environment.

Low: Fully-configured subject machines can be created in a virtualized manner. Network communications can easily be captured and saved in PCAP files.

Medium: Subject machines can be created with virtualization, but these need to be manually configured or customized before the final setup is ready. Network communications can be captured and saved in PCAP files, or in formats which allow simple conversion to PCAP files.

High: Subject machines must be created and configured manually from scratch, either physically or with virtualization technology.

3.1.2 Cost

This criterion defines the amount of resources required for the correct implementation of the attack scenario. The lower the value is, the smaller amount of money an organization will need to invest on its training program.

Low: Standard hardware and network equipment is needed to setup the environment. No commercial software is required for supporting the training sessions.

Medium: A mix of standard and specialized equipment is needed to setup the environment. A mix of commercial and non-commercial software is required for supporting the training sessions.

High: Specialized hardware and network equipment is needed to setup the environment. Commercial software is required for supporting the training sessions.

3.1.3 Risk

This criterion describes the danger that a production network faces when an attack scenario is executed during a training session. Risk can be understood as the combination of likelihood and impact associated to an event. Therefore, the lower the value is, the safer the training environment will be.

Low: The training environment is completely isolated from production networks, or there is no danger for infection or spreading malware in production networks.

Medium: The training environment is a segment within a production network, or there is a limited danger for infection or spreading malware within production networks.

High: The training environment is an integrated part of a production network, or there is unlimited danger for infection or spreading malware within production networks.

3.1.4 Realism

This criterion describes the level of detail that a training environment replicates based on what a real case would be. The higher the value is, the closer to reality the training environment will be.

Low: The training environment does not replicate a production network or an attack scenario.

Medium: The training environment is a partial replica of a production network or an attack scenario.

High: The training environment is a complete replica of a production network and an attack scenario.

3.2 Common Environment Setups

This section covers typical methods used for constructing environments and attack scenarios for computer network defense analysis training.

3.2.1 Closed Lab Environment

A closed lab environment can be anything ranging from a single computer setup, up to a full replica of a production network. In any case, the closed lab environment will be isolated from a production network.

A common approach in this case is to replicate a simple part of a production network, and execute real malware. The results of the case are stored in PCAP files.

Criterion	Evaluation	Reason
Difficulty of Implementation	Low	The common approach can be implemented with fully-configured virtual machines. In more complex setups, the difficulty of implementation is proportional to the size of the production network which is going to be replicated.
Costs	Medium	Standard hardware and network equipment (e.g. PC, router and switch) is required. In more complex setups, the cost is proportional to the size of the production network which is going to be replicated. A mix of commercial and open source tools is usually required for supporting training sessions covering common and targeted attacks.
Risk	Low	Despite executing real malware, a closed lab environment is by definition isolated from production networks. In practice, malware will not be able to reach them.
Realism	Low	The common approach can allow the successful execution of a piece of malware. However, it does not provide a full overview of what the attack scenario would look like, if it were to happen in a production network. Security countermeasures in production cannot be tested during the training session, unless the organization increases the difficulty of implementation and/or its costs. In a more complex setup, the realism is proportional to the level of detail included in the replica.

Table 1: Closed lab environment evaluation

3.2.2 Limited Segment of a Production Network

This approach can be used in cases where an organization wants to train with some understanding what an attack scenario would look like in its infrastructure, but without involving the whole production network. In this case, environment is confined to a segment of a production network.

Criterion	Evaluation	Reason
Difficulty of Implementation	Low	The implementation is very straight forward, since the setup is already implemented. Some work previous to the execution of the attack scenario could be required (e.g. backups).
Costs	Medium	The implementation is using systems in production. Spending on extra hardware resources is not required. A mix of commercial and open source tools is usually required for supporting training sessions covering common and targeted attacks.
Risk	Medium	Training on production environments can have consequences that might be difficult to revert, or which can impact the normal function of the organization. If real malware is used, systems located within the segment will be exposed to attacks or infections.
Realism	Medium	If the chosen segment is representative, the level of realism can be good. In such case, security countermeasures in production can also be tested during the training session. However, given that the exercise is conducted in a segment of a production network, the malware and techniques might need to be customized in order to avoid damages or downtime. Given the risk that a more realistic environment can bring, many organizations face a “Risk versus Realism” dilemma, which usually results in reluctance to use real malware or in incomplete implementation of attack scenarios.

Table 2: Limited segment environment evaluation

3.2.3 Full Production Network

This alternative can be used in cases where an organization wants to train with a full understanding of what an attack scenario would look like in its production network.

Criterion	Evaluation	Reason
Difficulty of Implementation	Low	The implementation is very straight forward, since the setup is already implemented (either physically or virtualized). Some work previous to the execution of the attack scenario could be required (e.g. backups).
Costs	Medium	The implementation is using systems in production. Spending on extra hardware resources is not required. A mix of commercial and open source tools is usually required for supporting training sessions covering common and targeted attacks.

Risk	High	Training on production environments can have consequences that might be difficult to revert, or which can impact the normal function of the organization. If real malware is used, the risk of infection or compromise can escalate to the whole organization.
Realism	Medium	The level of realism in this case can be excellent, and security countermeasures in production can also be tested during the training session. However, given the inherent risk of conducting an exercise in a production network, malware and techniques need to be customized in order to avoid damages or downtime. In practice, many organizations face a “Risk versus Realism” dilemma, which usually results in reluctance to use real malware or in incomplete implementation of attack scenarios.

Table 3: Full production network environment evaluation

4. Challenges

The approaches described in previous sections present different challenges.

Preparation: Implementing an environment and designing an attack scenario requires planning, especially if the training exercise is going to be conducted in a production network. This usually requires extra work or causes administration overhead, which many organizations are reluctant to. As a result, organizations tend to not prioritize the training sessions, or just conduct them a very few number of times during a year.

The actual attack scenario also requires planning, which may require organizations to design a time line, or find the proper piece of malware which applies to the case.

Low product reusability: The traffic generated during an attack scenario is always specific to the environment where it was captured. Customizations to an attack scenario will therefore require the organization to re-conduct the training session with those changes. In cases where two or more cooperating organizations decided to share PCAP data, the network traffic would not be realistic.

Risk versus realism dilemma: Organizations conducting exercises in production networks must find a balance between risk and realism. Those who execute real malware need to ensure that the piece of malware actually does what the organization expects. At the same time, executing malware in production networks could spread and cause a real incident, which could potentially escalate to a disaster. As a result, organizations tend to reduce scope, or choose less realistic methods in order to ensure security. As an illustration, imagine an organization releasing ransomware in its production network during a training session. Accidental spreading of the malware could result in encrypted business data and require an extensive recovery.

Training against advanced adversaries: Organizations, which want to conduct training exercises for defending themselves against advanced adversaries, cannot rely on just executing malware. Advanced adversaries put in practice methods and tradecraft that are not solely related to malware. The need for a qualified red team that can adapt to the training circumstances is therefore imperative. This fact is also affected by the challenges listed above, which requires for example more preparation and resources in order to conduct a successful training exercise.

5. Tackling the Challenges

This paper proposes two methods which tackle the challenges mentioned in the previous section. The first one will be based on adversary replication techniques which support the simulation of advanced adversaries and targeted attacks. The second will be a more general approach which can be applied to training related to common attacks and malware infections. Both methods can complement each other, and both are supported by open source tools.

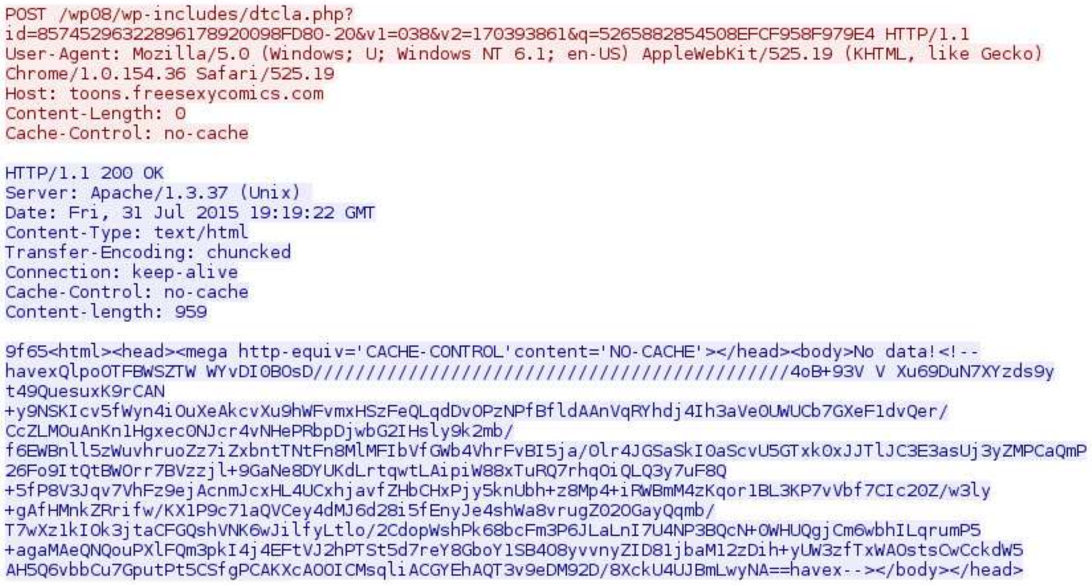
5.1 Targeted Attacks

Targeted attacks tend to use customized malware which presents specific network indicators. Such indicators are usually difficult to reproduce in a safe manner. Targeted attacks could be carried out with different levels of sophistication, and they do not necessarily imply the presence of and Advanced Persistent Threat (APT).

Maligno [5] is an open source tool which allows organizations to simulate malware with specific network indicators and evasion techniques. The result is that blue teams can experience real network behavior and traffic patterns associated to malware used in targeted attacks, without actually executing real malware. The main advantages provided by Maligno focus on reducing risk and preparation costs, while increasing realism during a training exercise.

The following case illustrates how Maligno can be used in order to simulate a targeted attack. A piece of malware known as “Havex” or “Oldrea” has been actively used against western energy companies. Symantec has documented several cases in a report [6] which describes network indicators associated to Havex.

Using the technical information presented in such report, it is possible to build a simple profile in Maligno, which will mimic the malware’s network behavior without risking any infection. As a result, Maligno can help increasing realism and simplifying training exercises on production networks.



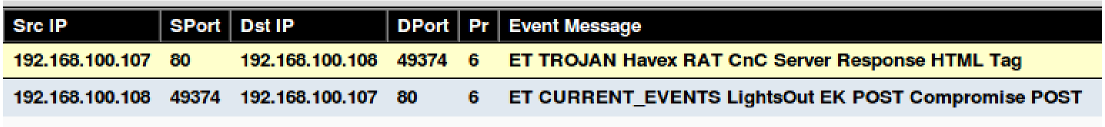
```
POST /wp08/wp-includes/dtcla.php?
id=857452963228961789200098FD80-20&v1=038&v2=170393861&q=5265882854508EFCF958F979E4 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/525.19 (KHTML, like Gecko)
Chrome/1.0.154.36 Safari/525.19
Host: toons.freesexycomics.com
Content-Length: 0
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: Apache/1.3.37 (Unix)
Date: Fri, 31 Jul 2015 19:19:22 GMT
Content-Type: text/html
Transfer-Encoding: chuncked
Connection: keep-alive
Cache-Control: no-cache
Content-length: 959

9f65<html><head><mega http-equiv='CACHE-CONTROL'content='NO-CACHE'></head><body>No data!<!--
havexQlpoOTFBWSZTW WYvDIOBOsD/////////////////////////////////////////////4oB+93V V Xu69DuN7XYzds9y
t49QuesuxK9rCAN
+y9NSKIcv5fWyn4iOuXeAkcvXu9hWFvmxHSzFeQLqdDvOPzNPfBfldAAnVqRYhdj4Ih3aVeOUWUCb7GXeF1dvQer/
CcZLMOuAnKn1HgxecONJcr4vNHePRbpDjwbG2IHsly9k2mb/
f6EWBnll5zWuvhruoZz7iZxbntTNtFn8MlMFIbVfGWb4VhrFvBI5ja/Olr4JGSaSkIOaScvU5GTxkOxJJTlJC3E3asUj3yZMPCaQmP
26Fo9ItQtBWOrr7BVzzjl+9GaNe8DYUKdLrtqwtLAipiW88xTuRQ7rhqOiQLQ3y7uF8Q
+5fP8V3Jqv7VhFz9ejAcnmJcxHL4UCxhjavfZHbCHxPjy5knUbh+z8Mp4+iRWBmM4zKqor1BL3KP7vVbf7CIc2OZ/w3ly
+gAfHMnkZRrifw/KX1P9c71aQVCey4dMJ6d28i5fEnyJe4shWa8vrugZO2OGayQqmb/
T7wXz1kIOk3jtaCFGQshVNK6wJilfyLtlo/2CdopWshPk68bcFm3P6JLaLnI7U4NP3BQcN+OWHUQgjCm6wbhILqrumP5
+agaMAeQNQouPXlFQm3pkI4j4EFtVJ2hPTSt5d7reY8GboY1SB408yvvnyZID81jbaM12zDih+yUW3zfTxWAOstsCwCckdW5
AH5Q6vbbCu7GputPt5CSfgPCAKXcAOOICMsqliACGYEhAQT3v9eDM92D/8XckU4UJBmLwyNA==havex--></body></head>
```

Figure 1Havex network indicators reproduced by Maligno during an HTTP request and response

The screenshot below shows how an Intrusion Detection System (Snort with ET GPL rule set) would react to the network traffic generated by Maligno.



Src IP	SPort	Dst IP	DPort	Pr	Event Message
192.168.100.107	80	192.168.100.108	49374	6	ET TROJAN Havex RAT CnC Server Response HTML Tag
192.168.100.108	49374	192.168.100.107	80	6	ET CURRENT_EVENTS LightsOut EK POST Compromise POST

Figure 2 Alerts generated by Intrusion Detection System (Snort) during the execution of the example

Tools are an essential component in network analysis training, both for attackers and defenders. However, blue teams cannot simply rely on tools when it comes to training against advanced threat actors. From an adversary replication perspective, training exercises should also involve a capable red team. The red team should adapt and put into practice tradecraft and manual techniques related to the threat actor which is going to be replicated during the exercise. We acknowledge that Maligno is an important piece in this puzzle, but it is not the only one. Organizations that want to conduct a complete realistic targeted attack scenario should keep this in mind.

The network traffic produced during the training exercise could also be combined with the next approach proposed in this paper. This would allow organizations to increase the reusability of the generated network traffic, and create a library of training cases. This would again increase the return on investment for each training exercise, and reduce preparation costs in the future.

5.2 Common Attacks and Malware Infections

Common attacks tend to use techniques usually implemented in some form of automatic tool. Typical common attacks include, but are not limited to, credential brute force, Denial of Service, phishing and malware delivered by exploit kits.

In many of these cases, there is a chain of events which is important for a network defense analyst to follow, especially if client computers are involved. The chain of events can provide a context which allows the analyst to understand the whole picture of an attack.

Network traffic stored in PCAP files are usually used for training in these cases. The internet provides a wide range of possibilities to obtain PCAP files with network traffic, which contains common computer attacks, client infections delivered by exploit kits, etc. However, there might be challenges when those resources are used in corporate environments.

The most common challenge is related to the "story" contained in those PCAPs, because it only applies to the environment where the traffic was captured. This means that organizations which attempt to train in-house blue teams with their own infrastructure, tools and configurations, may not be able to leverage those resources.

Pcapteller [5] is an open source tool designed for network traffic manipulation and replay. It allows organizations to re-create a recorded network traffic scenario that occurred in a foreign network, as it really happened in their own infrastructure.

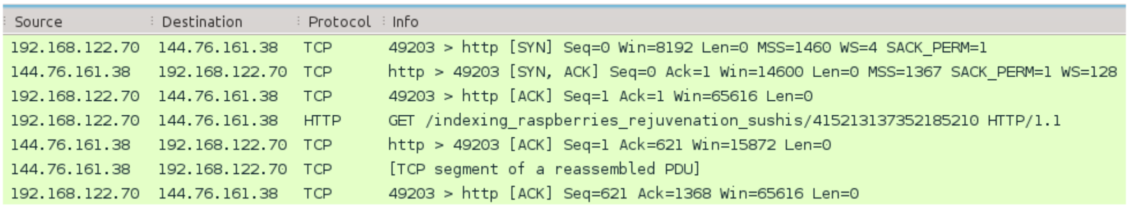
The main advantages of using Pcapteller are summarized below:

Reduced preparation time and costs: PCAP files available on the internet can be easily customized with parameters that are relevant to the organization. This allows blue team to reuse PCAP material and customize it as needed during the training session.

Reduced risk: Given the possibility to manipulate existing PCAP files captured in foreign networks, organizations should not have the need to implement attack scenarios with real malware samples for generating customized network traffic. If organizations desired to train specific situations in which no existing PCAP files were found, it could be possible to put in practice the approach using Maligno, proposed by this paper. In this way, organizations could combine both approaches and obtain wider advantages.

Increased realism: Since existing PCAP files can be manipulated and later replayed back into the network, organizations can train with their existing infrastructure and configurations. This means that organizations can use their production networks, without requiring extra security measures to prevent infections.

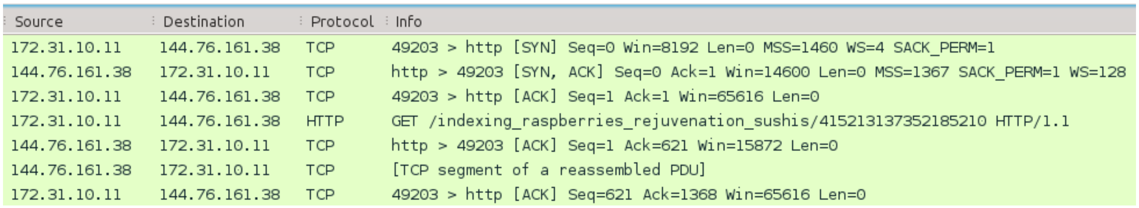
In order to illustrate these advantages, we will use a public PCAP file [7] that contains an attack scenario involving an exploit kit delivering ransomware. This PCAP file describes a chain of events where host 192.168.122.70 is the victim.



Source	Destination	Protocol	Info
192.168.122.70	144.76.161.38	TCP	49203 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
144.76.161.38	192.168.122.70	TCP	http > 49203 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1367 SACK_PERM=1 WS=128
192.168.122.70	144.76.161.38	TCP	49203 > http [ACK] Seq=1 Ack=1 Win=65616 Len=0
192.168.122.70	144.76.161.38	HTTP	GET /indexing_raspberries_rejuvenation_sushis/415213137352185210 HTTP/1.1
144.76.161.38	192.168.122.70	TCP	http > 49203 [ACK] Seq=1 Ack=621 Win=15872 Len=0
144.76.161.38	192.168.122.70	TCP	[TCP segment of a reassembled PDU]
192.168.122.70	144.76.161.38	TCP	49203 > http [ACK] Seq=621 Ack=1368 Win=65616 Len=0

Figure 3 Fragment of the original PCAP file with an attacker IP address and the victim (192.168.122.70)

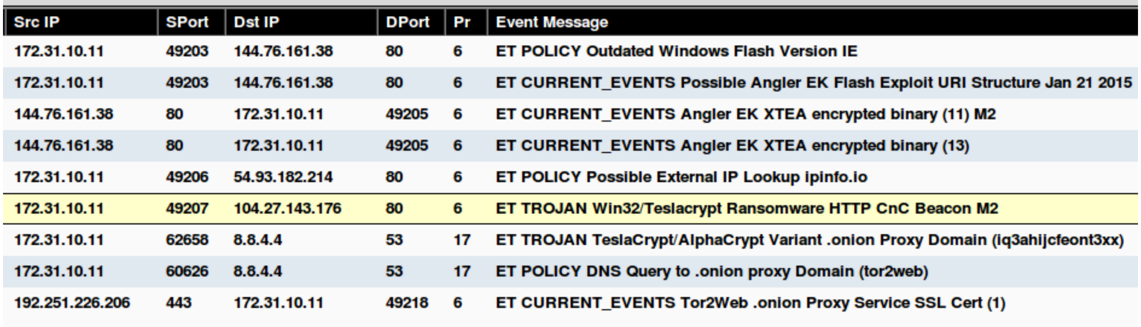
Let us consider a case where an organization would like to use such resource for a training session. The organization is interested in using its current security countermeasures and configurations in production. The production network is using a class B internal IPv4 addressing schema (172.31.0.0/16). For this example, the victim machine will be 172.31.10.11. Using Pcapteller, the result of the customized traffic injected into the network is described in the screenshot below.



Source	Destination	Protocol	Info
172.31.10.11	144.76.161.38	TCP	49203 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
144.76.161.38	172.31.10.11	TCP	http > 49203 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1367 SACK_PERM=1 WS=128
172.31.10.11	144.76.161.38	TCP	49203 > http [ACK] Seq=1 Ack=1 Win=65616 Len=0
172.31.10.11	144.76.161.38	HTTP	GET /indexing_raspberries_rejuvenation_sushis/415213137352185210 HTTP/1.1
144.76.161.38	172.31.10.11	TCP	http > 49203 [ACK] Seq=1 Ack=621 Win=15872 Len=0
144.76.161.38	172.31.10.11	TCP	[TCP segment of a reassembled PDU]
172.31.10.11	144.76.161.38	TCP	49203 > http [ACK] Seq=621 Ack=1368 Win=65616 Len=0

Figure 4 Fragment of the manipulated PCAP file with attacker IP address and the victim (172.31.10.11)

Since Pcapteller injects the manipulated network traffic into the production network, existing security countermeasures can detect and alert about possible threats. This example shows how an Intrusion Detection System (Snort with ET GPL rule set) would react to the manipulated traffic.



Src IP	SPort	Dst IP	DPort	Pr	Event Message
172.31.10.11	49203	144.76.161.38	80	6	ET POLICY Outdated Windows Flash Version IE
172.31.10.11	49203	144.76.161.38	80	6	ET CURRENT_EVENTS Possible Angler EK Flash Exploit URI Structure Jan 21 2015
144.76.161.38	80	172.31.10.11	49205	6	ET CURRENT_EVENTS Angler EK XTEA encrypted binary (11) M2
144.76.161.38	80	172.31.10.11	49205	6	ET CURRENT_EVENTS Angler EK XTEA encrypted binary (13)
172.31.10.11	49206	54.93.182.214	80	6	ET POLICY Possible External IP Lookup ipinfo.io
172.31.10.11	49207	104.27.143.176	80	6	ET TROJAN Win32/Teslacrypt Ransomware HTTP CnC Beacon M2
172.31.10.11	62658	8.8.4.4	53	17	ET TROJAN TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain (iq3ahijcfeont3xx)
172.31.10.11	60626	8.8.4.4	53	17	ET POLICY DNS Query to .onion proxy Domain (tor2web)
192.251.226.206	443	172.31.10.11	49218	6	ET CURRENT_EVENTS Tor2Web .onion Proxy Service SSL Cert (1)

Figure 5 Alerts generated by Intrusion Detection System (Snort) during the execution of the example

Pcapteller is at this point in an early stage of development, but new possibilities will come as soon as new features are implemented.

6. Evaluation of Proposed Training Methods

In this section, we will evaluate the proposed methods based on the evaluation criteria previously described.

6.1 Training Sessions Using Maligno

This approach allows blue teams to experience real network behavior and traffic patterns associated to malware used in targeted attacks, without executing real malware.

Criterion	Evaluation	Reason
Difficulty of Implementation	Low	The implementation is very straight forward and can be done in a fully virtualized manner. The organization can use the attack profiles already included in the tool or make their own profiles based on threat intelligence sources.
Costs	Low	Maligno is a freely available open source tool that allows organizations to use production infrastructure in a safe manner. This means that no spending on extra hardware is required. Inherent costs (e.g. security personnel attending the training session, the need to hire an external red team, etc.) may still apply.
Risk	Low	Maligno does not act as an infecting or spreading piece of malware, which allows a safe conduction of the training session in production infrastructure. The replication of network indicators can therefore be done without risking any infection.
Realism	High	Maligno can support red teams while simulating targeted attacks or attacks coming from specific threat actors. Training sessions can be conducted in full-scaled production environments.

Table 4: Training session evaluation using Maligno

6.2 Training Sessions Using Pcapteller

This approach allows organizations to re-create a recorded network traffic scenario that occurred in a foreign network, as it really happened in their own infrastructure.

Criterion	Evaluation	Reason
Difficulty of Implementation	Low	The implementation is very straight forward and can be done in a fully virtualized manner. PCAP files available on the internet can be easily customized with parameters that are relevant to the organization.
Costs	Low	Pcapteller is a freely available open source tool, which allows a high material reusability. This lowers the overall costs of a training session, and increases its return on investment.

		In addition, organizations can use production infrastructure in a safe manner during the training. This means that no spending on extra hardware is required. Inherent costs (e.g. security personnel attending the training session) may still apply.
Risk	Low	There is no need to implement attack scenarios with real malware samples from scratch, as long as existing PCAP files captured in foreign networks are used. In case of needing specific network indicators, or implementing attack scenarios from scratch, organizations may use Maligno in order to keep a low risk.
Realism	High	Pcapteller can support computer network defense analysts during their training with real attack scenarios contained in PCAP files. Such scenarios can be successfully re-created while using full-scaled production environments.

Table 5: Training session evaluation using Pcapteller

7. Conclusion

This paper has proposed two training methods that can be used to improve computer network defense analysis training. The main advantages of these methods are reduced risk and preparation costs, while increasing realism during training sessions.

This means that organizations will be able to conduct realistic training sessions in a more controlled manner, and obtain results that can be reused over time. In other words, organizations can obtain a higher return on investment and make training more feasible.

The training methods can easily be implemented by both public and private organizations, as well as training institutions such as universities.

We plan to continue developing the training methods and tools described in this paper.

Regarding Maligno, a more flexible version is under development, which will allow the concurrent use of multiple indicator profiles during one single session, and other extended features that can improve the level of replication for cases involving highly complex malware.

When it comes to Pcapteller, the tool is at an early stage. This means that extra functionality for fully customizing and replaying existent traffic in PCAP format will be developed.

We intend to keep these tools in an open source license, and freely available for the security community, since we see training as paramount for improving network defense.

8. References

[1] ISACA and Cybersecurity Nexus (CSX), 2015 Global Cybersecurity Status Report. January 2015. Available at http://www.isaca.org/Pages/Cybersecurity-Global-Status-Report.aspx?cid=pr_1105839&appeal=pr (Accessed October 3, 2015)

[2] National Initiative for Cybersecurity Careers and Studies (NICCS) / U.S. Department of Homeland Security. A Glossary of Common Cybersecurity Terminology. Available at http://niccs.us-cert.gov/glossary (Accessed October 3, 2015)

[3] Trend Micro Incorporated. Glossary. Available at http://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks (Accessed October 3, 2015)

[4] Symantec Corporation. Glossary. Available at http://www.symantec.com/security_response/glossary/define.jsp?letter=a&word=attack-scenario (Accessed October 3, 2015)

[5] Encripto AS. Tools. Available at https://www.encripto.no/tools (Accessed October 3, 2015)

[6] Symantec Corporation, Dragonfly: Cyberespionage Attacks Against Energy Suppliers. June 2014. Available at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf (Accessed October 3, 2015)

[7] Malware-Traffic-Analysis.net, Brad Duncan. Angler EK delivers ransomware. 14th of May, 2015. Available at http://www.malware-traffic-analysis.net/2015/05/14/index.html (Accessed October 3, 2015)